



## **RIASSUNTO II PARTE**

## • NUMERI NATURALI IN

### ■ 2 PROPRIETÀ FONDAMENTALI:

1) ASSIOMA DEL BUON ORDINAMENTO, ogni sottoinsieme non vuoto di  $\mathbb{N}$  ha un elemento minimo

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

S. insieme dei numeri interi pari, maggiori o uguali a 0. S. è infinito (non ha un elemento massimale), non c'è elemento minimo.

2) PRINCIPIO DI INDUZIONE, associamo ad ogni  $n$  una asserzione  $A(n)$ . allora, se

- $A(0)$  è vera

- $\forall n, A(n) \Rightarrow A(n+1) \Rightarrow A(n) \text{ è vero } \forall n$

### ■ op. sui numeri naturali

- SOMMA  $m+n \in \mathbb{N}$  con  $m, n \in \mathbb{N}$

- o è l'elemento neutro

- MOLTIPLICAZIONE  $m \cdot n \in \mathbb{N}$  con  $m, n \in \mathbb{N}$

- 1 è l'elemento neutro

- DIVISIONE CON RESTO

**NON** possiamo:

- SOTTRAZIONE  $m \geq n$

- DIVISIONE  $m \mid 0$

- RADICI / RISOLVERE EQ  $\rightsquigarrow \mathbb{R}$

- $\rightsquigarrow \mathbb{C}$

volgono le seguenti inclusioni:

numeri primi  $\subseteq \mathbb{N} \not\subseteq \mathbb{Z} \not\subseteq \mathbb{Q} \not\subseteq \mathbb{R} \not\subseteq \mathbb{C}$

$\not\subseteq$  contenuto ma non uguale

## • NUMERI INTERI $\mathbb{Z}$

### ■ op. COMMESSE: SOMMA, MOLTIPLICAZIONE, DIVISIONE CON RESTO

op. mon. CONMESSE: DIVISIONE, RADICI

### • DIVISIONE CON RESTO

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

Sorvianno  $a:b = q$  resto  $r$

**DEF: DIVISORE**, Siano  $a, b \in \mathbb{Z}$  diciamo che  $b$  divide  $a$  se

$$\exists c \text{ t.c. } a = b \cdot c$$

OSS. 1) ogni intero  $a$  ha almeno quattro divisori:  $\pm 1, \pm a$

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

$$d \mid a \Rightarrow \exists c_1 \text{ t.c. } a = d \cdot c_1 \quad \Rightarrow \quad a+b = d \cdot c_1 + d \cdot c_2 = d(c_1 + c_2) \quad \boxed{c}$$

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

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

$$d \mid a, \exists c \text{ t.c. } a = d \cdot c \rightarrow |a| = |d| \cdot |c| \quad \text{se } a \neq 0, c \neq 0$$

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

## • MASSIMO COMUN DIVISORE (MCD)

**DEF:** Sono  $a, b \in \mathbb{Z}$ ,  $a$  e  $b$  non entrambi 0. Il loro massimo comun divisore (MCD) è il più grande intero che divide sia  $a$  che  $b$ .

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

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

**PROPRIETÀ:**

- è sempre positivo
- $\text{MCD}(a, a) = \text{MCD}(a, -a) = |a|$
- $\text{MCD}(1, a) = 1$
- $\text{MCD}(a, b) = \text{MCD}(b, a) = \text{MCD}(-b, a) = \text{MCD}(b, -a)$
- Se  $(a, b) \neq (0, 0) \Rightarrow \text{MCD}(a, b) > 0$

**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  $p$ .

**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 aggiungo a uno dei due numeri un multiplo dell'altro.

**DIMOSTRAZIONE:**

Sia  $q \in \mathbb{Z}$  ( $a, b$  fissati) dimostriamo:

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

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

1)  $d \mid b$  e  $d \mid a \Rightarrow a = m_1d \Rightarrow b = m_2d \Rightarrow b+qa = m_2d + qm_1d = (m_2 + qm_1)d \Rightarrow d \mid (b+qa)$

2)  $d \mid a$  e  $d \mid b+qa$

$$\begin{aligned} a = m_1d &\Rightarrow b = (b+qa) - qa = \\ b+qa = m_2d &= m_2d - qm_1d = (m_2 - qm_1)d \Rightarrow d \mid b \end{aligned}$$

**LEMMA DI BEZOUT:**

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

$\text{MCD}(a, b)$  è il più piccolo elemento positivo dell'insieme  $S = \{ax + by \mid x, y \in \mathbb{Z}\}$

**COROLLARIO:** Sono  $a, b \in \mathbb{Z}$ ,  $(a, b) \neq (0, 0)$

1) Esistono  $x, y \in \mathbb{Z}$  tali che  $\text{MCD}(a, b) = ax + by$

2) Se  $d$  divide sia  $a$  che  $b \Rightarrow d \mid \text{MCD}(a, b)$

3) Se  $\text{MCD}(a, b) = 1$  (SONO PRIMI TRA LORO)

e  $a$  divide  $bc \Rightarrow a$  divide  $c$

$$a \mid bc \Rightarrow a \mid c$$

(3) D.M.

$$1 = \text{MCD}(a, b) = ax + by \quad \text{per qualche } x, y \in \mathbb{Z} \Rightarrow$$

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

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

$$\Rightarrow c = cax + cbm = cax + amy = a(cx + my) \Rightarrow a | c$$

bzout

**PROPRIETÀ** Siano  $a, b \in \mathbb{Z}$   $p$  primo

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

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

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

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

Poiché  $p \nmid a \Rightarrow \text{MCD}(a, p) = 1$ .

**TEOREMA FONDAMENTALE DELL'ARITMETICA**

(decomposizione in fattori primi)

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

$$m \neq 1$$

tali che  $m = p_1 p_2 \cdots p_k$

$p_1 \cdots p_k$  si chiamano **FATTORI PRIMI** di  $m$  e sono unici a meno dell'ordine.

**COROLLARIO:** i numeri primi sono infiniti.

**Def.** ORDINE DI UN INTERO Sia  $a \in \mathbb{N}$ ,  $a \neq 0, 1$ . Sia  $p$  primo

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

$$\text{ord}_2(12) = 2 \quad 12 = 2^2 \cdot 3$$

$\Rightarrow$  Si può scrivere la decomposizione in fattori primi come  $a \in \mathbb{N}$ ,  $a \neq 0, 1$

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

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

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

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

$$\textcircled{2} \quad d \in \mathbb{Z}, d \neq 0 \Rightarrow d | a \Leftrightarrow \text{ord}_p(a) \geq \text{ord}_p(d) \quad \forall p \text{ primo}$$

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

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

(prendo tutti i fattori primi in comune com'è esponeente più piccolo)

**MINIMO COMUNE MULTIPLO**

**Def.** Dati  $a, b \in \mathbb{Z}$ ,  $(a, b) \neq (0, 0)$ .  $\text{mcm}(a, b)$  è il più piccolo  $m > 0$  t.c.  $a | m$ ,  $b | m$ .

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

(multiplo di entrambi)

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

## • NUMERI RAZIONALI $\rightsquigarrow \mathbb{Q}$

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

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

■ op. su  $\mathbb{Q}$ : • somma e sottrazione  $\frac{p}{q} \pm \frac{p'}{q'} = \frac{pq' \pm p'q}{qq'}$ , elemento neutro: 0

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

• moltiplicazione/divisione

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

elemento neutro: 1

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

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

• NO RADICI E EQUAZIONI

## • NUMERI COMPLESSI $\rightsquigarrow \mathbb{C}$

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

$$\mathbb{C} = \{\text{numeri complessi}\}$$

$$i^2 = -1 \vee$$

$$= \{z = a + ib \quad a, b \in \mathbb{R}, i^2 = -1\}$$

$\operatorname{Re} z = a = \text{PARTE REALE}$ ,  $\operatorname{Im} z = b = \text{PARTE IMMAGINARIA}$

### ■ op. sui complessi

$$z_1 = a_1 + ib_1 \quad z_2 = a_2 + ib_2$$

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

$$\cdot z_1 \cdot z_2 = (a_1 + ib_1)(a_2 + ib_2) = a_1a_2 - b_1b_2 + ia_1b_2 + ia_2b_1$$

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

$$\cdot \overline{z_1} = a_1 - ib_1 \quad (\text{coniugio})$$

### ■ Interpretazione geometrica

$$z = a + ib \quad z \text{ vettore } (a, b) = \sqrt{a^2 + b^2}$$

$$\cdot |z| = \|v\| = \sqrt{a^2 + b^2}$$

•  $\overline{z}$  è il riflesso di  $z$  rispetto all'asse  $x$

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

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

$$\operatorname{Re}(z) = \frac{z + \overline{z}}{2}$$

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

### ■ FORMA TRIGONOMETRICA

$$e^{i\theta} = \cos \theta + i \sin \theta$$

$$z = a + ib = r \cos \theta + i \sin \theta \Rightarrow z = r e^{i\theta}$$

$$= r(\cos \theta + i \sin \theta)$$

$$r = \sqrt{a^2 + b^2}$$

$$z =$$

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

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

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

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

$$a = r \cos \theta \quad b = r \sin \theta$$

FORME TRIGONOMETRICHE UTILI:

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

$$z^m = (a+ib)^m = r^m e^{im\theta}$$

$$+ se w = s e^{i\varphi} \rightarrow z \cdot w = r \cdot s \cdot e^{i(\theta+\varphi)}$$

## TEORIA DEI GRUPPI

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

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

Proprietà: • ASSOCIAZIONE  $(a * b) * c = a * (b * c) \rightarrow$  SEMPRE

• COMMUTATIVITÀ  $a * b = b * a \rightarrow$  NON SEMPRE

**def.** Un elemento  $e \in S$  e' detto ELEMENTO NEUTRO per un operazione  $*$  se

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

**def.** Un elemento  $a \in S$  e' detto INVERTIBILE (rispetto a  $*$ ) se esiste un altro elemento  $a^{-1}$  detto inverso di  $a$  t.c.  $a * a^{-1} = a^{-1} * a = e$  (elemento neutro)

**Notazione** Se  $*$  e' associativa, denotiamo  $\underbrace{a * a * \dots * a}_{m \text{ volte}}$  come  $a^m$

**def. GRUPPO:** Un gruppo e' una Terna  $(G, *, e)$  dove  $G$  e' un INSIEME,  $*$  e' una OPERAZIONE ASSOCIAZIONE SU  $G$  con ELEMENTO NEUTRO  $e$ , e tale che ogni elemento di  $G$  ha un INVERSO IN  $G$ .

**def. SOTOGRUPO:** Sia  $(G, *, e)$  un gruppo. Un Sottogruppo  $H$  di  $G$  e' un insieme  $H \subset G$  tale che:

- ①  $e \in H$
- ②  $\forall a, b, a * b \in H$
- ③  $\forall a \in H, a^{-1} \in H$

Si indica con  $H < G$ .

**Notazione:** Se  $H$  e' un sottogruppo di  $G$ , si scrive  $H < G \Rightarrow (\mathbb{Z}, +, 0) < (\mathbb{R}, +, 0)$

Come controllo se  $G$  e' un gruppo? ① Dobbiamo dimostrare che l'operazione e' ASSOCIAZIONE

- ② ELEMENTO NEUTRO E' G?
- ③ INVERSO E' G?

**ESEMPIO:**  $SL(m, \mathbb{R}) = \{ A \in M_{m \times m} \mid \det A = 1 \} \quad (SL(m, \mathbb{R}), \cdot, I)$

① OP. ASSOCIAZIONE?

$$SL(m, \mathbb{R}) \times SL(m, \mathbb{R}) \longrightarrow SL(m, \mathbb{R})$$

$$\Rightarrow \text{Se } A, B \in SL(m, \mathbb{R}) \rightarrow AB \in (SL(m, \mathbb{R}))$$

$$\det(A) = 1 \quad \det(B) = 1$$

$$\Rightarrow \det(AB) = \det(A) \cdot \det(B) = 1 \cdot 1 = 1$$

$$\Rightarrow AB \in SL(m, \mathbb{R})$$

Il prodotto tra matrici e' ASSOCIAZIONE.

③ INVERSO?

$A \in SL(m, \mathbb{R})$  cioè  $\det A = 1 \neq 0 \Rightarrow \exists A^{-1}$ , devo controllare se  $A^{-1} \in SL(m, \mathbb{R})$

$$\det A^{-1} = \frac{1}{\det A} = \frac{1}{1} = 1$$

$$\Rightarrow A^{-1} \in \text{SL}(m, \mathbb{R})$$

$\Rightarrow (\text{SL}(m, \mathbb{R}), \cdot, I)$  e' un gruppo

### TIPI PARTICOLARI DI GRUPPI

def. GRUPPO ABELIANO: e' un gruppo in cui l'operazione e' 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.

Notazione Il numero di elementi di  $G$  si indica: 1)  $\#G$  (cardinalità)

$$2) |G| \text{ (modulo)}$$

oss. Un gruppo non abeliano può avere sottogruppi ABELIANI.

### LEGGI DI CANCELLAZIONE

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

$$(\mathbb{R}, +, 0) \Rightarrow x + y = z + y \Rightarrow x = z \quad b * a = c * a \Leftrightarrow c = b$$

$$\begin{array}{c} \hookrightarrow x + y - y = z + y - y \\ \overbrace{e} \qquad \qquad \overbrace{e} \end{array} \quad \exists a^{-1}$$

dim.  $(G, *, e)$   $a, b, c \in G$ . Se  $a * b = a * c \stackrel{\downarrow}{\Rightarrow} a^{-1} * (a * b) = a^{-1} * (a * c)$

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

$$\text{prop. invertibilità} \Rightarrow e * b = e * c$$

$$\text{prop. elem. neutro} \Rightarrow b = c$$

### TEOREMA SOTTOGRUPPI DI $\mathbb{Z}$

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

$$b\mathbb{Z} = \{a \in \mathbb{Z}, a = kb \text{ con } k \in \mathbb{Z}\}$$

$$= \{ \text{multipli di } b \}$$

oss.  $\mathbb{Z}$  non ha sottogruppi FINITI, tranne il sottogruppo banale  $\{0\}$

### GRUPPO DELLE PERMUTAZIONI

$S_m$  = gruppo delle permutazioni di  $m$  elementi.

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

$$= \{ \text{Aut}(T) \}$$

$$= \{ \text{automorfismi di } T \}$$

= Tutti i modi in cui posso scambiare tra loro gli elementi di  $T$

• un elemento di  $S_m$  si scrive come:  $q = (b_1, \dots, b_m)$

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

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

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

$$\begin{array}{ccccc} & q & & p & \\ & \downarrow & \rightarrow & \downarrow & \\ 1 & \rightarrow & b_1 & \rightarrow & a_{b_1} \\ & & P & & \\ & & \downarrow & & \\ & & a_1 & \rightarrow & b_{a_1} \end{array}$$

$$\begin{array}{ccccc} & q & & p & \\ & \downarrow & \rightarrow & \downarrow & \\ 1 & \rightarrow & b_1 & \rightarrow & a_{b_1} \\ & & P & & \\ & & \downarrow & & \\ & & a_1 & \rightarrow & b_{a_1} \end{array}$$

• e' elemento neutro e' l'identità che mantiene inalterato l'ordine degli elementi.  
 $(1, 2, \dots, m)$

• Usiamo la composizione per scrivere l'inverso:

p Cerchiamo  $q = p^{-1} + c$ .  $q \circ p = (1, 2, \dots, m)$

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

- $Id \in S_m : Id = (1, 2, \dots, m)$
- $p \circ q \in S_m \quad \forall p, q$ . (La composizione di funzioni biiettive è biiettiva.)
- $p^{-1} \in S_m$  (l'inversa di una funzione biiettiva è ed è biiettiva)

## TAVOLE DI MOLTIPLICAZIONE

modo di sintetizzare le proprietà di un gruppo, in modo che possiamo ricavare:

- il gruppo è abeliano  $\Leftrightarrow$  è simmetrico rispetto alla diagonale principale
- vedo subito qual'è l'inverso, guardo in quale posizione della sua riga / colonna compare l'elemento neutro.  
+ in ogni riga / colonna compare l'elemento neutro.
- si vedono bene i sottogruppi (e se sono abeliani)
- un gruppo si può ottenere attraverso una tavola di moltiplicazione

## CAMPIONI

Un campo è un gruppo (abeliano) con una operazione aggiuntiva · con le proprietà.

**def.** Un campo è un insieme F con due operazioni +, · t.c.:

- $(F, +, 0)$  gruppo abeliano
- $(F^*, \cdot, 1)$  gruppo abeliano
- $\forall a, b, c \in F, (a+b)c = ac + bc$  (PROPRIETÀ DISTRIBUTIVA)

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

· campi con infiniti elementi  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

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

## CONGRUENZA MODULO m

Sia  $p, q \in \mathbb{Z}$  e sia  $m \in \mathbb{N}$

$$* \Rightarrow k_1m + z_1 = k_2m + z_2 + k_1m$$

Divisione con resto:  $p = k_1m + z_1 \quad 0 \leq z_1, z_2 < m$

OK, se  $z_1 = z_2$

$$* \quad q = k_2m + z_2 \quad k_1, k_2 \in \mathbb{Z}$$

$$p = q \pmod m$$

se hanno lo stesso resto, ovvero  $p = q + km$  per qualche  $k \in \mathbb{Z}$

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

• hanno lo stesso resto quando diviso per m  $p = k_1 m + r_1$  con  $r_1 = r_2$

$$q = k_2 m + r_2$$

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

- la loro differenza è multiplo di m  $p - q = km \text{ con } k \in \mathbb{Z}$
- uno è uguale all'altro a meno di sommare un multiplo di m

$$(es \ m = 7 \quad \mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{6}\})$$

$$\bar{3} + \bar{5} = \bar{8} = \bar{1} \quad [8 = 7 + 1]$$

$$\bar{3} \cdot \bar{6} = \bar{18} = \bar{4} \quad [18 = 14 + 4]$$

### MATRICI A COEFFICIENTI MODULO P PRIMO

Possono uscire come coefficienti delle matrici le classi di congruenza mod p e ottengo gruppi FINITI NON ABELIANI.

**TEOREMA:** Se p primo,  $\mathbb{Z}_p$  è un campo (se p non è primo potrebbero non esistere gli inversi moltiplicativi)

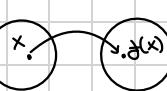
### DOMINIO e CODOMINIO

**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 un solo elemento  $f(x) \in T$ .

S si dice dominio

S

T si dice codominio



NOTAZIONE:  $f(x) = t$   
 $\underset{S}{\overset{T}{f}} \quad x \in S \quad t \in T$

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

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

• applicazione Id su un insieme X associa ad ogni elemento di X se stesso:

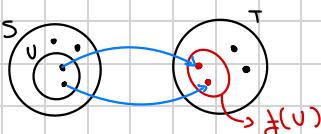
$$Id: x \rightarrow x \quad Id(x) = x \quad \forall x \in X \quad Id: x \rightarrow x$$

### IMMAGINE e CONTROIMMAGINE

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

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

e' l'immagine sta nel codominio



**def.** Se  $V \subseteq T$  fa **controimmagine / preimmagine** di V secondo f è l'insieme

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

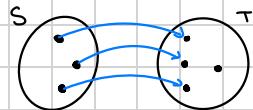


**INIEKTIVITÀ e SURIEKTIVITÀ**  $f: S \rightarrow T$

def.  $f: S \rightarrow T$  è **INIEKTIVA** se  $\forall s, u \in S, s \neq u \Rightarrow f(s) \neq f(u)$ , ovvero:

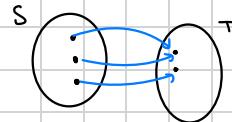
$$\cdot f(u) = f(s) \Leftrightarrow s = u$$

• elementi distinti di  $S$  vengono mappati in elementi distinti di  $T$



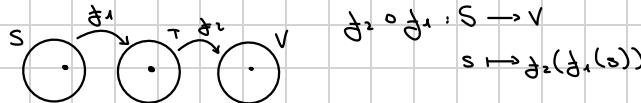
def.  $f: S \rightarrow T$  è **SURIEKTIVA** se  $f(S) = T$ , ovvero:

- Ogni elemento di  $T$  ha una prima immagine in  $S$
- $\forall t \in T \exists s \in S$  t.c.  $f(s) = t$



def. Se  $f$  è sia INIEKTIVA che SURIEKTIVA, si dice **BIETTIVA**

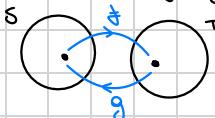
### COMPOSIZIONE



### INVERSA

$f: S \rightarrow T$  è invertibile se  $\exists g: T \rightarrow S$  tale che  $g \circ f = \text{Id}_S$  e  $f \circ g = \text{Id}_T$

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



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

! Dipende dalle sette di dominio e codominio

-  $f$  è invertibile

-  $f$  è biettiva

-  $\forall t \in T \exists s$  t.c.  $f(s) = t$

### OMOMORFISMI e ISOMORFISMI

def **OMOMORFISMO**: Siano  $(G, *, e)$ ,  $(G', *,', e')$  due gruppi. Un omomorfismo  $\varphi: G \rightarrow G'$  è una applicazione che rispetta la struttura di gruppo, ovvero

$$\forall g_1, g_2 \in G \quad \varphi(g_1 * g_2) = \varphi(g_1) *' \varphi(g_2)$$

def **ISOMORFISMO**: Un omomorfismo che è INVERTIBILE (ovvero imiettivo e suriettivo) si dice **ISOMORFISMO**.

OSS. Se  $\varphi: G \rightarrow G'$  è imiettivo ma non suriettivo  $\Rightarrow \varphi$  è un **ISOMORFISMO**

tra  $G$  e  $\varphi(G) \subseteq G'$

def. **AUTOMORFISMO**: È un ISOMORFISMO da un gruppo a sé stesso.

## NUCLEO e IMMAGINE

**def.** Sia  $\varphi: G \rightarrow G'$  omomorfismo.

$$\text{d'IMMAGINE } \varphi(G) = \{ g' \in G' : \exists g \in G, \varphi(g) = g' \}$$

$\varphi$  suriettiva  $\Leftrightarrow \text{Im } \varphi = G'$

**def.** Il nucleo o KERNEL di un omomorfismo  $\varphi: G \rightarrow G'$  è

$$\text{Ker } \varphi = \{ g \in G : \varphi(g) = e' \} = \varphi^{-1}(e')$$

↑ elem. neutro di  $G'$

**PROPOSIZIONE** Siano  $(G, *, e)$  e  $(G', *, e')$  due gruppi. Allora:

- $\text{Im } \varphi \leq G'$
- $\text{Ker } \varphi \leq G$

**dim.** a)  $\text{Im } \varphi \leq G'$

- $\varphi$  omomorfismo  $\Rightarrow \varphi(e) = e' \Rightarrow e' \in \text{Im } \varphi$
  - Se  $a', b' \in \varphi(G)$ , vogliamo provare a vedere  $a' *' b' \in \varphi(G)$   
 Ma  $a' \in \varphi(G) \Leftrightarrow \exists a \in G, \varphi(a) = a'$   
 $b' \in \varphi(G) \Leftrightarrow \exists b \in G, \varphi(b) = b'$   
 $\Rightarrow a' *' b' = \varphi(a) *' \varphi(b) = \varphi(a * b)$
- ↑  
omomorfismo

- Inverso: Se  $a' \in \varphi(G)$ , come prima  $a' = \varphi(a)$  per qualche  $a$

Sia  $a'^{-1}$  l'inverso di  $a$  omomorfismo

$$\begin{aligned} &\Rightarrow a' *' \varphi(a'^{-1}) = \varphi(a) *' \varphi(a'^{-1}) \downarrow = \varphi(a * a'^{-1}) = \varphi(e) = e' \\ &\Rightarrow \varphi(a'^{-1}) = (a'^{-1})^{-1} \end{aligned}$$

b)  $\text{Ker } \varphi \leq G$

- $e \in \text{Ker } \varphi$  perché  $\varphi(e) = e'$
- Se  $a, b \in \text{Ker } \varphi$   $\varphi(a * b) = \varphi(a) *' \varphi(b) = e' *' e' = e'$
- Se  $a \in \text{Ker } \varphi$  devo dire che  $a'^{-1} \in \text{Ker } \varphi$  ovvero  $\varphi(a'^{-1}) = e'$   
 $e' = \varphi(e) = \varphi(a'^{-1} * a) = \varphi(a'^{-1}) * \varphi(a) = \varphi(a'^{-1}) * e' = \varphi(a'^{-1})$   
 $\Rightarrow \varphi(a'^{-1}) = e'$

## SPAZI VETTORIALI

**def.** Uno spazio vettoriale (SV) su un campo  $\mathbb{K}$  ( $\mathbb{R}, \mathbb{C}$ )

è un insieme  $V$  su cui sono definite:

- SOMMA  $v, w \mapsto v + w \in V$
- MOLTIPLICAZIONE  $v \in V, c \in \mathbb{K} \mapsto cv$

PER SCALARE

■ ELEMENTO NEUTRO RISPETTO ALLA SOMMA  $0$ ,

$$\forall v, 0 \cdot v = 0_v \quad (\text{vettore nullo})$$

$$0_v + v = v + 0_v = v \quad \forall v \in V$$

- Una OPERAZIONE prende due elementi di  $G$  e sostituisce un elemento di  $G$
- Una APPLICAZIONE prende un elemento di  $G$  e sostituisce un elemento di  $G'$ .

## SOTTO SPAZI VETTORIALI

V spazio vettoriale su  $\mathbb{K}$ , un sottoinsieme  $W \subset V$  e' un ssv se:

- $0_V \in W$
- $\forall w_1, w_2 \in W, w_1 + w_2 \in W$
- $\forall w \in W, c \in \mathbb{K} cw \in W$

I sottospazi bonoli sono  $\{0_V\}$  e  $V$

- In generale, lo spazio delle soluzioni di un sistema lineare omogeneo e' un ssv ovvero:  $\text{Sol}(AX=0)$ ,  $A \in \mathbb{M}_{m \times n}$ , e' un ssv di  $\mathbb{R}^n$
- le rette o i piani che passano per l'origine sono ssv di  $\mathbb{R}^3$

PROPRIETÀ Sia  $AX=b$  un sistema lineare con m equazioni e n incognite

$$\Rightarrow \text{Sol}(AX=b) \text{ sono um ssv di } \mathbb{R}^n \Leftrightarrow b=0$$

• Mostriamo che  $W = \text{Sol}(AX=0)$  sono ssv

- $0 \in W$  perche'  $A \cdot 0 = 0 \checkmark$
- Se  $w_1, w_2 \in W \Rightarrow A(w_1 + w_2) = Aw_1 + Aw_2 = 0 \Rightarrow w_1 + w_2 \in \text{Sol}(AX=0)$  ✓
- Se  $w \in W$ , c scalare
- $A(cw) = c(Aw) = c \cdot 0 = 0 \Rightarrow cw \in \text{Sol}(AX=0) \checkmark$
- Mostriamo che  $W = \text{Sol}(AX=b)$  NON e' ssv di  $\mathbb{R}^n$  se  $b \neq 0$

Imposs  $0 \in W$  perche'  $A \cdot 0 \neq b \neq 0 \checkmark$

(oppure: Se  $v_1, v_2 \in W$ ,  $A(v_1 + v_2) = Av_1 + Av_2 = b + b \neq b \Rightarrow v_1 + v_2 \notin W$ )

## COMBINAZIONI LINEARI (CL)

def Un vettore  $v \in \mathbb{R}^n$  e' COMBINAZIONE LINEARE di  $v_1, \dots, v_k$  se  $\exists a_1, \dots, a_k \in \mathbb{R}$  t.c.

$$v = a_1v_1 + \dots + a_kv_k = \sum_i a_i v_i$$

OSS. Dato qualunque insieme di vettori  $v_1, \dots, v_k$ , posso sempre scrivere:

$$0 = 0v_1 + \dots + 0v_k$$

OSS. Vedrai se  $v$  e' CL di  $v_1, \dots, v_k$  e' la stessa cosa che chiedere se il SL  $AX=v$  ha soluzione,

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

Dove:  $a_1, \dots, a_k$  sono le incognite

$\bullet A = \begin{pmatrix} | & | \\ v_1 & \dots & v_k \\ | & | \end{pmatrix}$  e' la matr. dei coefficienti

$\bullet$  termine noto  $\rightarrow$  se  $v=0 \Rightarrow$  compatibile per  $a_1, \dots, a_k$

$$\bullet \begin{pmatrix} 1 \\ 2 \end{pmatrix} \text{ e' CL di } \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} ? \iff \exists a_1, a_2 \text{ t.c. } \begin{pmatrix} 1 \\ 2 \end{pmatrix} = a_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} + a_2 \begin{pmatrix} 1 \\ 1 \end{pmatrix} ?$$

$$\Rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \text{ e' compatibile}$$

$$\iff \text{rg} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \text{rg} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 2 \end{pmatrix}$$

## SPAZIO GENERATO

**def.** Dati  $v_1, \dots, v_k \in \mathbb{R}^m$ , lo spazio generato da  $v_1, \dots, v_k$  è

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

= spazio delle combinazioni lineari di  $v_1, \dots, v_k$

### ESEMPIO

1. z retta in  $\mathbb{R}^3$  passante per 0

$$z: X = tA$$

$$z: \mathcal{L}(A)$$



2. M piano in  $\mathbb{R}^3$  passante per 0

$$M: X = sA_1 + tA_2$$



**oss.** lo spazio generato è semplicemente un SSV di  $\mathbb{R}^m$

**def.** Insieme di generatori. Sia  $w$  SSV di  $\mathbb{R}^m$ , un insieme di generatori per  $w$  è un insieme di vettori  $v_1, \dots, v_k$  t.c.  $w = \mathcal{L}(v_1, \dots, v_k)$

**CASO PARTICOLARE:**  $v_1, \dots, v_k$  generano  $\mathbb{R}^m$ ?

$$A = \begin{array}{c|ccccc} \top & & & & & \bottom \\ \hline m & & & & & \\ & \longleftarrow K \longrightarrow & & & & \end{array} \quad \Rightarrow \boxed{\text{K vettori in } \mathbb{R}^m \text{ generano } \mathbb{R}^m \Leftrightarrow \text{rg } A = m}$$

richiedono almeno  $m$  vettori per generare  $\mathbb{R}^m$

## VETTORI LINEARMENTE DIPENDENTI

**def.**  $v_1, \dots, v_k \in \mathbb{R}^m$  sono LINEARMENTE DIPENDENTI se  $\exists a_1, \dots, a_k$  non tutti nulli

t.c.  $a_1 v_1 + \dots + a_k v_k = 0$  Ie sis. LINEARE  $Ax=0$  non ha soluzione unica

$$\Leftrightarrow \# \text{ variabili} > \text{rg } A$$

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

+ sono L.D. se esistono keri a<sub>i</sub> che danno 0, ma in cui almeno uno dei coefficienti è non nullo

## VETTORI LINEARMENTE INDEPENDENTI

**def.**  $v_1, \dots, v_k \in \mathbb{R}^m$  sono LINEARMENTE INDEPENDENTI se

$$a_1 v_1 + \dots + a_k v_k = 0 \Rightarrow a_i = 0 \quad \forall i \Leftrightarrow \text{Ie sis. LINEARE } Ax=0 \text{ ha soluzione unica}$$

+ sono L.I. Se c'è unica c.l. che

$$\Leftrightarrow \# \text{ variabili} = \text{rg } A$$

dai 0 è quella con tutti i coeff.

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

nulli

**oss.** se ho  $k$  vettori in  $\mathbb{R}^m$  e  $k > m \Rightarrow$  non

possono essere L.I.

$$\text{rg } A \leq \min(k, m) \leq m < k$$

### ESEMPIO

3 vettori in  $\mathbb{R}^2$ , non possono essere L.I.

$\text{rg } A \leq 2$  perché i vettori sono in  $\mathbb{R}^2$  ma per essere L.I.  $\text{rg } A = \# \text{ vct} = 3$  ( $\because$   $\# \text{ vct} = 3$ )

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

• generano  $\mathbb{R}^m$

• sono L.I.

**CRITERI per generare  $\mathbb{R}^m$ :**

$$\bullet \text{ rg } A = m \Rightarrow K \geq m$$

$$\bullet \text{ sono L.I.} \Leftrightarrow \text{rg } A = K \Rightarrow K \leq m$$

Per avere entrambe servono:

- esattamente  $m$  vettori

- $\text{rg } A = m$

$\Rightarrow v_1 - v_k$  sono una base per  $\mathbb{R}^m \Leftrightarrow k = m$

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

OSS.  $k$  vettori in  $\mathbb{R}^m$  generano  $\Leftrightarrow \text{rg } A = \text{dimensione dello spazio} = m$   
sono lin. indipendenti  $\Leftrightarrow \text{rg } A = \# \text{ vettori}$

OSS. Se ho  $m$  vettori in  $\mathbb{R}^m$ , generare e essere l.i. sono equivalenti, perché entrambi valgono  $\Leftrightarrow \text{rg } A = m$

OSS. Se ho  $k < m$  i vettori possono essere l.i., ma non possono generare  
Se ho  $k > m$  i vettori possono generare, ma non possono essere l.i.

### TIPI SPECIALI DI BASI

•  $v_1 - v_m$  sono base di  $\mathbb{R}^m \Leftrightarrow A$  ha rango  $m$ , ovvero è INVERTIBILE  
( $A$  è invertibile  $\Leftrightarrow$  le sue colonne formano una base)

• se  $A$  è ortogonale ( $\Rightarrow$  invertibile)

le sue colonne sono mutualmente ortogonali e di norma 1: formano una base ortogonale.

In questo caso i coefficienti delle c.l. si trovano semplicemente con il prodotto scalare.

### APPPLICAZIONI LINEARI

un vettore  $b$  appartiene a  $L(v_1 - v_k) \Leftrightarrow Ax = b$  comp.

def.  $F: \mathbb{R}^m \rightarrow \mathbb{R}^m$  è una applicazione lineare 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  $F(v_1) = w_1 \in \mathbb{R}^m$   
:

$$F(v_m) = w_m \in \mathbb{R}^m$$

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

$v = a_1 v_1 + \dots + a_m v_m$  ai univocamente determinati perché la base

$$\begin{aligned} F(v) &= F(a_1 v_1 + \dots + a_m v_m) = a_1 F(v_1) + \dots + a_m F(v_m) = \\ &= a_1 w_1 + \dots + a_m w_m \end{aligned}$$

IMMAGINE DI  $v$

### A.L. e MATRICI

Ad ogni matrice  $m \times m$  corrisponde una A.L. da  $\mathbb{R}^m \rightarrow \mathbb{R}^m$ , ad ogni A.L. da  $\mathbb{R}^m \rightarrow \mathbb{R}^m$  corrisponde una mat.  $m \times m$  (per ogni scelta di base)

■ Per vedere se una A.L.  $\mathbb{R}^m \rightarrow \mathbb{R}^m$  è invertibile il determinante della matrice deve essere  $\neq 0$ .

+ per essere invertibile deve essere BIETIVA.

■ Per essere **INIETTIVA** serve  $m \leq n$

**SURGETTIVA** serve  $m > n$

⇒ Per essere **INVERTIBILE** serve  $m = n$  e  $\det(A) \neq 0$ .

**def.** Data  $B, B'$  di  $\mathbb{R}^m$ , la matrice cambio base  $M(B', B)$  è la matrice che trasforma le coordinate di un vettore rispetto a  $B$  nelle sue coordinate rispetto a  $B'$ , avendo  $M(B', B)[v]_B = [v]_{B'}$

$v \in \mathbb{R}^m \rightsquigarrow [v]_B$  coefficienti di  $v$  come c.l. dei vettori di  $B$

$[v]_{B'}$  coefficienti di  $v$  come c.l. dei vettori di  $B'$

**def.** Una A.L.  $T: \mathbb{R}^m \rightarrow (\text{da uno spazio a se stesso})$  si dice **OPERATORE**.

**oss.** Due matrici  $A, B$  che rappresentano un operatore  $T$  rispetto a basi diverse sono simili, ovvero  $\exists P$  invertibile tale che  $B = P^{-1}AP$

### NUCLEO e IMMAGINE NELLE APPLICAZIONI LINEARI

**def.**  $L: \mathbb{R}^m \rightarrow \mathbb{R}^m$  A.L., 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  $A_L$

**def.**  $L: \mathbb{R}^m \rightarrow \mathbb{R}^m$  A.L., il nucleo di  $L$  è

$$\text{Ker } L = \{v \in \mathbb{R}^m \mid L(v) = 0\} = \text{Sol}(A_L = 0) - \text{Sol}\{A_L = 0\}$$

**def.**  $L: \mathbb{R}^m \rightarrow \mathbb{R}^m$  suriettiva se  $\forall w \in \mathbb{R}^m \exists v \text{ t.c. } L(v) = w$  ovvero  $\text{Im } L = \mathbb{R}^m$   
 $\text{Im } L = \{\text{spazio generato dalle colonne di } A_L\} \Rightarrow L \text{ suriettiva}$   
 $\Leftrightarrow \dim \text{Im } L = m$  ovvero  $A_L$  ha  $m$  colonne L.I.  
 $\Rightarrow L$  è suriettiva  $\Leftrightarrow \text{rg } A_L = m = \dim \mathbb{R}^m$   
codominio

**def.**  $L: \mathbb{R}^m \rightarrow \mathbb{R}^m$  è iniettiva  $\Leftrightarrow \forall v \neq w \Rightarrow L(v) \neq L(w)$

$$\Leftrightarrow \text{Ker } L = \{\emptyset\}$$

$$\Leftrightarrow \dim \text{Ker } L = \# \text{ voci} - \text{rg } A = 0$$

"m (dim. dominio)"

### AUTOVALORI e AUTOVETTORI

**def.**  $T$  operatore su  $\mathbb{R}^n$ ,  $\lambda \in \mathbb{R}$  è **AUTOVALORE** per  $T$  se  $\exists v \neq 0$  tale che  $T(v) = \lambda v$   
dove  $v \rightarrow$  **AUTOVETTORE**

$\Rightarrow \lambda$  AUTOVALORE  $\Leftrightarrow$  il sistema  $(A - \lambda I)v = 0$  ha soluzione non banale

$$\# \text{ parametri} = \# \text{ variabili} - \text{rg}(A - \lambda I) = m - \text{rg}(A - \lambda I) > 0$$

$$\Leftrightarrow \text{rg}(A - \lambda I) < m \Leftrightarrow \det(A - \lambda I) = 0$$

$\Rightarrow$  gli autovalori di  $A$  sono le radici del polinomio  $\det(A - \lambda I)$   
(per trovarli cerco i  $\lambda$  tali che  $\det(A - \lambda I) = 0$ )

Calcolo gli AUTOVETTORI, dopo aver trovato gli autovalori,  $v$  è autovettore relativo a un autovalore  $\lambda \Leftrightarrow v \neq 0$  e  $(A - \lambda I)v = 0$

Si definisce l'autospazio relativo all'autovettore  $\lambda$  come:

$$V_\lambda = \text{Sol}\{(A - \lambda I)v = 0\}$$

■ Ad ogni autovettore  $\lambda$  associamo due numeri:

- $M_a(\lambda)$ , MOLTEPLICITÀ ALGEBRICA ovvero il numero di volte che compare come radice di  $\det(A - \lambda I)$  (grado di  $\lambda$ )
- $M_g(\lambda)$ , MOLTEPLICITÀ GEOMETRICA  
 $= \dim V_\lambda = M - \text{rg}(A - \lambda I)$

### DIAZONALIZZAZIONE

def. Una matrice  $A \in M_{m \times m}$  è diagonalizzabile  $\Leftrightarrow \exists D$  diagonale,  $P$  invertibile, tali che  $D = P^{-1}AP$

def. equivalente (in termini di operatori)

$T: \mathbb{R}^m \rightarrow \mathbb{R}^m$  è diagonalizzabile  $\Leftrightarrow \exists$  base  $B$  di autovettori, ovvero  $A_T(B, B)$  è diagonale

E' diagonalizzabile se

- l'autovettore trovato  $M_a = M_g$
- $\exists$  tutte le radici  $p_A(t)$  in  $\mathbb{R}$

## ESEMPI II PARTE

MARIA ANDREA ZOCCOLI

MAT: 364943

ES. 1

- $(5+2i)(1-2i) = 5+4i - 10i + i^2 = 9-8i$

- $\operatorname{Re}(2e^{i\pi}) = 2(\cos \pi + i \sin \pi) = 2(-1+0i) = -2$

- $\operatorname{Im}(e^{i\pi}) = (\cos \pi + i \sin \pi) = -1+0i = 0$

- $\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right)^3 = \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2}\right)^3$

$$\left(\frac{\sqrt{2}}{2}\right)^3 + 3\left(\frac{\sqrt{2}}{2}\right)^2 \left(\frac{\sqrt{2}i}{2}\right) + 3\left(\frac{\sqrt{2}}{2}\right) \left(\frac{\sqrt{2}i}{2}\right)^2 + \left(\frac{\sqrt{2}i}{2}\right)^3$$

$$\frac{2\sqrt{2}}{8} + \frac{6}{4} \left(\frac{\sqrt{2}i}{2}\right) + 3\left(\frac{\sqrt{2}}{2}\right) \left(\frac{2i^2}{4}\right) + \frac{2\sqrt{2}i^3}{8} =$$

$$= \frac{2\sqrt{2}}{8} + \frac{6\sqrt{2}i}{8} + \frac{3\sqrt{2} \cdot 2i^2}{8} + \frac{2\sqrt{2}i^3}{8} =$$

$$= \frac{2\sqrt{2}}{8} + \frac{6\sqrt{2}i}{8} + \frac{3}{8} \frac{6\sqrt{2}(-1)}{4} + \frac{1}{8} \frac{2\sqrt{2}(-i)}{4} =$$

$$= \frac{\sqrt{2}}{4} + \frac{3\sqrt{2}i}{4} - \frac{3\sqrt{2}}{4} - \frac{\sqrt{2}i}{4} =$$

$$= \frac{\cancel{\sqrt{2}}}{\cancel{4}} + \frac{\cancel{\sqrt{2}}i}{\cancel{4}} = \boxed{-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2}}$$

ES. 2

- PRINCIPIO 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.  $m \leq m \forall m \in S$

- TEOREMA DELLA DIVISIONE CON RESTO.**

Sia  $a, b \in \mathbb{Z}$ ,  $b > 0$ . Allora esistono unici due intiari  $q, r$  (quoziente e resto)

tali che,  $a = qb + r$ ,  $0 \leq r < b$

- $\text{MCD}(7560, 651) = 651 \cdot 11 + 399$

$$\text{MCD}(651, 399) = 399 \cdot 1 + 252$$

$$\text{MCD}(399, 252) = 252 \cdot 1 + 147$$

$$\text{MCD}(7560, 651) = 21$$

$$\text{MCD}(252, 147) = 147 \cdot 1 + 105$$

$$\text{MCD}(147, 105) = 105 \cdot 1 + 42$$

$$\text{MCD}(105, 42) = 42 \cdot 2 + 21$$

$$\text{MCD}(42, 21) = 21 \cdot 2 + 0$$

## ES.3

- gruppo finito abeliano:  $(\mathbb{Z}_m, +, 0) \rightarrow$  gruppo degli interi modulo m
  - gruppo finito non abeliano:  $(S_3, \circ, e) \rightarrow$  gruppo delle permutazioni su due elementi
  - gruppo infinito abeliano:  $(\mathbb{Z}, +, 0)$
  - gruppo infinito non abeliano:  $(GL(m), \cdot, I) \rightarrow$  gruppo delle matrici quadrate invertibili.
  - ISOMORFISMO tra due gruppi:  $(\mathbb{Z}, +, 0) \rightarrow (\mathbb{Z}, +, 0)$
- $$M \rightarrow 3M$$
- $$\text{OMOMORFISMO NON ISO.}: (\mathbb{Z}, +, 0) \rightarrow (\mathbb{Z}_7, +, 0)$$
- $$x \rightarrow \bar{x}$$

## ES.4

Def. Classe di congruenza mod q.

Due numeri m, n ∈ ℤ appartengono alla stessa classe di congruenza mod q se:

- hanno lo stesso resto quando diviso per q  $m = k_1q + r_1 \quad n = k_2q + r_2$
  - la loro differenza è multiplo di q  $m - n = kq$  con  $k \in \mathbb{Z}$   $r_1 = r_2$
  - uno è uguale all'altro al meno di sommare un multiplo di q
- $$m = m + qk \text{ con } k \in \mathbb{Z}$$

Def.  $\mathbb{Z}_q = \{\text{classi di congruenza modulo } q\}$

$$\mathbb{Z}_q = \{\bar{0}, \dots, \bar{q-1}\}$$

Per ogni intero  $a \in \mathbb{Z}_q$ , la classe di congruenza di a modulo q è l'insieme di tutti gli interi che danno lo stesso resto quando divisi per q.

$\mathbb{Z}_q$  è un campo  $\iff q$  è un numero primo

ESEMPIO:  $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} \quad (\mathbb{Z}_5^*, \cdot, 1) \quad \begin{array}{c|ccc} \cdot & 1 & 2 & 3 \\ \hline 1 & 1 & 2 & 3 \\ 2 & 2 & 0 & 2 \\ 3 & 3 & 2 & 1 \end{array} \quad 0 \notin (\mathbb{Z}_5^*, \cdot, 1)$

2	0	2
3	3	2

Se q non è primo, allora

ha divisori non banali  $\Rightarrow$

ci sono elementi in  $\mathbb{Z}_q$  che non sono invertibili rispetto al prodotto.

## ES.5

$A = \begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix} \quad a, b \in \mathbb{R} \text{ e } a \neq 0. \quad (A, \cdot, I) \text{ è un gruppo?}$

$$1) (A, \cdot, I) \times (A, \cdot, I) \rightarrow (A, \cdot, I)$$

$$A, B \in A \quad A = \begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix} \quad B = \begin{pmatrix} c & d \\ 0 & 1/c \end{pmatrix} \quad a, b, c, d \in \mathbb{R} \quad a \neq 0, c \neq 0$$

$$AB \in G? \quad AB = \begin{pmatrix} ac & ad + alc \\ 0 & 1/a \end{pmatrix} \in G$$

//

$$2) I \in G \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$$

//

3)  $A \in G$ . Dobbiamo trovare  $A^{-1}$  t.c.  $AA^{-1}=I$  e  $A^{-1} \in G$

$$A = \begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix} \quad \det A = a \cdot \frac{1}{a} - 0 = 1$$

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} 1/a & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1/a & -b \\ 0 & a \end{pmatrix} \in G$$

$$AA^{-1} = \begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix} \begin{pmatrix} 1/a & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1+0 & -ab+ab \\ 0+0 & 0+1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

$\Rightarrow (G, \cdot, I)$  è un gruppo

SOTTOGRUPPI di  $(G, \cdot, I)$ :

$$1) H = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} \mid a \in \mathbb{R}, a \neq 0 \right\} \quad 2) L = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}$$

$$3) M = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} = \{Id\}$$

• Tutte le matrici di questa forma sono invertibili perché il loro determinante è sempre diverso da zero ed è importante perché se non avessero l'inverso allora non sarebbero un gruppo.

ES. 6

$H$  sottoinsieme  $(M_{3 \times 3}, +, \Omega)$  formato dalle matrici antisimmetriche ( $A^T = -A$ )

1)  $A, B \in H \quad A+B \in H?$

$$A = \begin{pmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & d & e \\ -d & 0 & f \\ -e & -f & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{pmatrix} + \begin{pmatrix} 0 & d & e \\ -d & 0 & f \\ -e & -f & 0 \end{pmatrix} = \begin{pmatrix} 0 & a+d & b+e \\ -a-d & 0 & c+f \\ -b-e & -c-f & 0 \end{pmatrix}$$

2)  $\Omega \in H?$

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in H$$

3) INVERSO

$$-A \in H? \quad -A = \begin{pmatrix} 0 & -a & -b \\ a & 0 & -c \\ b & c & 0 \end{pmatrix} \in H$$

$\Rightarrow H$  è un sottogruppo.

$$\bullet F: H \rightarrow (\mathbb{R}, +, 0)$$

$$A \mapsto \det A$$

$$A, B \in H$$

$$\varphi(A+B) = \varphi(A) + \varphi(B)$$

↓

$$\det(A+B) = \det(A) + \det(B)$$

$$0 = 0 + 0$$

(il determinante di una matrice antisimmetrica è sempre zero)

$\Rightarrow$  F è un OMOMORFISMO

$$\bullet F: H \rightarrow (\mathbb{R}, +, 0)$$

$$A, B \in H$$

$$A \mapsto \operatorname{tr} A$$

$$\varphi(A+B) = \varphi(A) + \varphi(B)$$

$\Rightarrow$  F è un OMOMORFISMO

$$\operatorname{tr}(A+B) = \operatorname{tr}(A) + \operatorname{tr}(B)$$

$$0 = 0 + 0 \checkmark$$

• F è un ISOMORFISMO? No, perché:

• non è INIEZIONE, elementi distinti di H vengono mappati in elementi distinti di  $\mathbb{R}$ .  
 (tutte le matrici hanno  $\operatorname{tr} = 0$ )

• non è SURIETTIVA perché l'insieme H non ordina in tutti gli elementi di  $\mathbb{R}$ .

ES. 8

• SSV di  $\mathbb{R}^3$  con  $\dim=0$   $H = \{\emptyset\}$   $B = \{\emptyset\}$

• SSV di  $\mathbb{R}^2$  con  $\dim=1$   $H = \mathcal{L}\left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}\right)$   $B = \left\{\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}\right\}$

• SSV di  $\mathbb{R}^3$  con  $\dim=2$   $H = \mathcal{L}\left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}\right)$   $B = \left\{\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}\right\}$

• SSV di  $\mathbb{R}^3$  con  $\dim=3$   $H = \mathcal{L}\left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right)$   $B = \left\{\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right\}$

ES. 9

1. A.L. invertibile

$$F(x_1, x_2, x_3) = \begin{pmatrix} x_1 + x_2 + x_3 \\ x_2 + x_3 \\ x_3 \end{pmatrix} \quad F: \mathbb{R}^3 \rightarrow \mathbb{R}^3$$

La matrice associata ha  $\operatorname{rg} F = 3$

$$\rightarrow \dim \operatorname{Im} F = \operatorname{rg} A$$

$\Rightarrow$  F è suriettiva

$$\rightarrow \dim \operatorname{Ker} F = \# \text{var} - \operatorname{rg} A = 3 - 3 = 0$$

$\Rightarrow$  F è iniettiva

$$2. F(x_1, x_2, x_3) = \begin{pmatrix} x_1 + x_3 \\ x_2 \\ x_3 \\ x_2 \end{pmatrix} \quad F: \mathbb{R}^3 \rightarrow \mathbb{R}^4$$

La matrice associata ha  $\operatorname{rg} F = 3$

$$\rightarrow \dim \operatorname{Im} F = \operatorname{rg} A \text{ ma } 3 < 4$$

$\Rightarrow$  F non è suriettiva

$$\rightarrow \dim \operatorname{Ker} F = \# \text{var} - \operatorname{rg} A = 3 - 3 = 0$$

$\Rightarrow$  F è iniettiva

$$3 \cdot F(x_1, x_2, x_3) = \begin{pmatrix} x_1 + 2x_2 + 3x_3 \\ 2x_2 + x_3 \end{pmatrix} \quad F: \mathbb{R}^3 \rightarrow \mathbb{R}^2$$

La matrice associata ha  $\text{rg } F = 2$   
 $\rightarrow \dim \text{Im } F = \text{rg } A$   
 $\Rightarrow F$  è suriettiva  
 $\rightarrow \dim \text{Ker } F = \# \text{var} - \text{rg } A = 3 - 2 = 1$   
 $\Rightarrow F$  non è iniettiva

Esercizio

$$\bullet F: \mathbb{R}^2 \rightarrow \mathbb{R}^4 \quad F(x, u) = \begin{pmatrix} x+3u \\ x-u \\ 0 \\ x+u \end{pmatrix}$$

$\text{rg } A = 2$

$\dim \text{Im } F = \text{rg } A = 2 > 2$

$\Rightarrow F$  non è suriettiva

$\dim \text{Ker } F = \# \text{var} - \text{rg } A = 2 - 2 = 0$

$\Rightarrow F$  è iniettiva

$$\bullet \text{Im } F = \mathcal{L} \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ -1 \\ 0 \\ 1 \end{pmatrix} \right\} = \left\{ X \in \mathbb{R}^4 \mid X = s \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} + t \begin{pmatrix} 3 \\ -1 \\ 0 \\ 1 \end{pmatrix} \right\}$$

$$B_{\text{Im } F} = \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ -1 \\ 0 \\ 1 \end{pmatrix} \right\}$$

$$\bullet \text{Ker } F = \text{Sol}(AX=0), \text{ ma } \dim \text{Ker } F = 0 \Rightarrow \text{Ker } F = \{\emptyset\}$$

$$B_{\text{Ker } F} = \{\emptyset\}$$

$$\bullet T: \mathbb{R}^3 \rightarrow \mathbb{R}^2 \quad T(e_1) = \begin{pmatrix} 5 \\ 1 \end{pmatrix} \quad T(e_2) = \begin{pmatrix} 0 \\ 2 \end{pmatrix} \quad T(e_3) = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$A = \begin{pmatrix} 5 & 0 & 1 \\ 1 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 1 \\ 5 & 0 & 1 \end{pmatrix} =$$

$\dim \text{Im } T = \text{rg } A = \dim \mathbb{R}^2$   
 $\Rightarrow T$  è suriettiva

$\dim \text{Ker } T = \# \text{var} - \text{rg } A = 3 - 2 = 1$   
 $\Rightarrow T$  non è iniettiva

$$\bullet \text{Im } T = \mathcal{L} \left\{ \begin{pmatrix} 5 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\} = \left\{ X \in \mathbb{R}^2 \mid X = s \begin{pmatrix} 5 \\ 1 \end{pmatrix} + t \begin{pmatrix} 0 \\ 2 \end{pmatrix} + u \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$$

$$B_{\text{Im } T} = \left\{ \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$$

$$\bullet \text{Ker } T = \text{Sol}(AX=0) \quad \left( \begin{array}{ccc} 1 & 2 & 1 \\ 0 & -10 & -6 \end{array} \right) = \left( \begin{array}{ccc} 1 & 2 & 1 \\ 0 & 1 & 2/5 \end{array} \right)$$

$$\begin{cases} x+2y+2=0 \\ 4+\frac{2}{5}y=0 \end{cases} \quad \begin{cases} x+2(-\frac{2}{5}z)+2=0 \\ y=-\frac{2}{5}z \end{cases} \quad \rightarrow z=t \quad \begin{cases} x=-\frac{1}{5}t \\ y=-\frac{2}{5}t \end{cases}$$

(1 param.  
libero)  
 $\rightarrow \dim \text{Ker } T = 1$

$$\text{Ker } T = \left\{ x \in \mathbb{R}^3 \mid x = \begin{pmatrix} -1/5t \\ -2/5t \\ t \end{pmatrix} \right\} = \left\{ x \in \mathbb{R}^3 \mid x = t \begin{pmatrix} -1/5 \\ -2/5 \\ 1 \end{pmatrix} \right\}$$

$$B_{\text{Ker } T} = \left\{ \begin{pmatrix} -1/5 \\ -2/5 \\ 1 \end{pmatrix} \right\}$$

$$\bullet G: \mathbb{R}^4 \rightarrow \mathbb{R}^3, \quad G(e_1) = \begin{pmatrix} 2 \\ 0 \\ -2 \end{pmatrix}, \quad G(e_2) = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \quad G(e_3) = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \quad G(e_4) = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$$

$$A = \begin{pmatrix} 2 & 0 & -1 & 1 \\ 0 & 1 & 0 & 0 \\ -2 & 1 & 1 & -1 \end{pmatrix} \quad R_1 + R_3 \quad \begin{pmatrix} 2 & 0 & -1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad \text{rg } A = 2 \quad \begin{array}{l} \dim \text{Im } G = \text{rg } A \neq \dim \mathbb{R}^3 \\ \Rightarrow G \text{ non surjektiv} \\ \dim \text{Ker } G = \# \text{Var} - \text{rg } A = \\ \Rightarrow 4 - 2 = 2 \end{array}$$

$$\text{Im } G = \text{L} \left\{ \begin{pmatrix} 2 \\ 0 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \right\}$$

$$B_{\text{Im } G} = \left\{ \begin{pmatrix} 2 \\ 0 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\}$$

$$\text{Ker } G = \text{Sol}(Ax=0) \quad \begin{cases} 2a-c+d=0 \\ b=0 \end{cases} \quad \begin{cases} 2a-c-d \\ b=0 \end{cases} \quad \begin{cases} c=t, d=3 \\ a=t \frac{1}{2} - s \frac{1}{2} \\ b=0 \end{cases}$$

$$\text{Ker } G = \left\{ x \in \mathbb{R}^4 \mid x = \begin{pmatrix} s^{1/2}-t^{1/2} \\ 0 \\ s \\ t \end{pmatrix} \right\} = \left\{ x \in \mathbb{R}^4 \mid x = s \begin{pmatrix} 1/2 \\ 0 \\ 1 \\ 0 \end{pmatrix} + t \begin{pmatrix} 1/2 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

$$B_{\text{Ker } G} = \left\{ \begin{pmatrix} 1/2 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1/2 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

## ES. 11

### POLINOMIO CARATTERISTICO:

Il polinomio caratteristico di una matrice  $A \in M_{n \times n}$  è un polinomio ottenuto dal determinante della matrice  $A - \lambda I$ , dove  $\lambda$  è un parametro scalare e  $I$  è la matrice identità. È definito come  $p_A(\lambda) = \det(A - \lambda I)$

### AUTONAVORE:

$T$  operatore su  $\mathbb{R}^n$ ,  $\lambda \in \mathbb{R}$  è **AUTONAVORE** per  $T$  se  $\exists v \neq 0$  tale che  $T(v) = \lambda v$  dove  $v \rightarrow$  AUTOVETTORE

$\Rightarrow \lambda$  AUTONAVORE  $\Leftrightarrow$  il sistema  $(A - \lambda I)v = 0$  ha soluzione non banale

$$\# \text{ parametri} = \# \text{ variabili} - \text{rg}(A - \lambda I) = n - \text{rg}(A - \lambda I) > 0$$

$$\Leftrightarrow \text{rg}(A - \lambda I) < n \Leftrightarrow \det(A - \lambda I) = 0$$

$\Rightarrow$  gli autonavori di  $A$  sono le radici del polinomio  $\det(A - \lambda I)$

(per trovarli cerco i  $\lambda$  tali che  $\det(A - \lambda I) = 0$ )

### AUTOVETTORE:

Un AUTOVETTORE di una matrice  $A \in M_{n \times n}$ , associato a un autonavore  $\lambda$  è un vettore non nullo  $v \in \mathbb{R}^n$  che soddisfa l'equazione  $Av = \lambda v$

$$\bullet \quad A = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \quad \det(A - \lambda I) = \det \begin{pmatrix} 1 - \lambda & 2 \\ 3 & -\lambda \end{pmatrix} = 1 - \lambda(-\lambda) - 3 \cdot 2 = -\lambda + \lambda^2 - 6 = \lambda^2 - \lambda - 6$$

Gli autonavori sono  $\lambda_1 = 3$     $\lambda_2 = -2$

$$m_a(\lambda_1) = 1 \quad m_a(\lambda_2) = 1$$

$$V_1 = \text{Sd}(A - \lambda_1 I | \Omega)$$

$$A = \left( \begin{array}{cc|c} -2 & 2 & 0 \\ 3 & -3 & 0 \end{array} \right) \quad \begin{cases} -2x + 2y = 0 \\ 3x - 3y = 0 \end{cases} \quad \begin{cases} -2x + 2x = 0 \\ \frac{2x}{3} = \frac{2y}{3} \end{cases} \quad \begin{cases} 0 = 0 \\ x = y \end{cases}$$

$$V_1 = \left\{ \begin{pmatrix} 4 \\ 4 \end{pmatrix} \in \mathbb{R}^2 \right\} \quad L = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\} \quad \dim(V_{\lambda_1}) = 1 = M_g(\lambda_1) = 1 \\ M_g(3) = M_a(3) = 1$$

$$V_2 = \text{Sd}(A - \lambda_2 I | \Omega)$$

$$A + 2I = \begin{pmatrix} 3 & 2 \\ 3 & 2 \end{pmatrix} \quad \begin{cases} 3x + 2y = 0 \\ \frac{3x}{3} = -\frac{2y}{3} \end{cases} \quad \begin{cases} 3x + 2y = 0 \\ x = -\frac{2}{3}y \end{cases}$$

$$V_2 = \left\{ \begin{pmatrix} -2 & 3 & 4 \\ & 4 \end{pmatrix} \in \mathbb{R}^2 \right\} \quad \mathcal{L} = \left\{ \begin{pmatrix} -2 & 3 \\ & 1 \end{pmatrix} \right\}$$

$$\dim(V_{\lambda_2}) = 1 = M_g(\lambda_2) = 1$$

$$N_g(-2) = N_a(-2) = 1$$

$\Rightarrow A$  è diagonalizzabile  $m_a = m_g$

$$D = \begin{pmatrix} 3 & 0 \\ 0 & -2 \end{pmatrix} \quad P = \begin{pmatrix} 1 & -2 & 3 \\ 1 & 1 \end{pmatrix}$$

- $B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad \det(B - \lambda I) = (1-\lambda)(-1) - 1 \cdot 1$   
 $= -\lambda + \lambda^2 - 1$   
 $= \lambda^2 - \lambda - 1 \quad \lambda_1 = \frac{1+\sqrt{5}}{2} \quad \lambda_2 = \frac{1-\sqrt{5}}{2}$

$$m_a(\lambda_1) = 1 \quad m_a(\lambda_2) = 1$$

$$V_1 = \text{Sol}(A - \frac{1+\sqrt{5}}{2} I | \underline{0})$$

$$\begin{pmatrix} 1 - \frac{1+\sqrt{5}}{2} & 1 \\ 1 & -\frac{1+\sqrt{5}}{2} \end{pmatrix} = \begin{pmatrix} (1-\sqrt{5})/2 & 1 \\ 1 & -(1+\sqrt{5})/2 \end{pmatrix} = \begin{pmatrix} 1 & -(1+\sqrt{5})/2 \\ (1-\sqrt{5})/2 & 1 \end{pmatrix}$$

$$R_2 - ((1-\sqrt{5})/2 \cdot R_1) \quad \begin{pmatrix} 1 & -(1+\sqrt{5})/2 \\ 0 & 0 \end{pmatrix} \quad x - \frac{1+\sqrt{5}}{2} \cdot 1 = 0$$

$$x = \frac{1+\sqrt{5}}{2} \cdot 1$$

$$V_1 = \left\{ \begin{pmatrix} \frac{1+\sqrt{5}}{2} & 1 \\ 1 & 1 \end{pmatrix} \in \mathbb{R}^2 \right\} = \mathcal{L} \left\{ \begin{pmatrix} \frac{1+\sqrt{5}}{2} \\ 1 \end{pmatrix} \right\}$$

$$m_a(\lambda_1) = m_g(\lambda_1) = 1$$

$$V_2 = \text{Sol}(A - \frac{1-\sqrt{5}}{2} I | \underline{0})$$

$$\begin{pmatrix} 1 - \frac{1-\sqrt{5}}{2} & 1 \\ 1 & -\frac{1-\sqrt{5}}{2} \end{pmatrix} = \begin{pmatrix} \frac{1+\sqrt{5}}{2} & 1 \\ 1 & -\frac{1-\sqrt{5}}{2} \end{pmatrix} = \begin{pmatrix} 1 & -\frac{1-\sqrt{5}}{2} \\ \frac{1+\sqrt{5}}{2} & 1 \end{pmatrix}$$

$$R_2 - \left(\frac{1+\sqrt{5}}{2}\right) R_1$$

$$\begin{pmatrix} 1 & -\frac{1-\sqrt{5}}{2} \\ 0 & 0 \end{pmatrix} \times -\frac{1-\sqrt{5}}{2} q = 0$$

$$x = \frac{1-\sqrt{5}}{2} q$$

$$V_2 = \left\{ \begin{pmatrix} \frac{1-\sqrt{5}}{2} q \\ q \end{pmatrix} \in \mathbb{R}^2 \right\} = \mathbb{L} \left\{ \begin{pmatrix} \frac{1-\sqrt{5}}{2} \\ 1 \end{pmatrix} \right\} \quad M_{\alpha}(\lambda_2) = M_g(\lambda_2) = 1$$

$$D = \begin{pmatrix} \frac{1+\sqrt{5}}{2} & 0 \\ 0 & \frac{1-\sqrt{5}}{2} \end{pmatrix} \quad P = \begin{pmatrix} \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \\ 1 & 1 \end{pmatrix}$$

$$\bullet C = \begin{pmatrix} -1 & 0 & 5 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} \quad \det(C - \lambda I) = (-1-\lambda) \cdot \det \begin{pmatrix} 2-\lambda & 1 \\ 0 & 2-\lambda \end{pmatrix}$$

$$= (-1-\lambda) \cdot (2-\lambda)^2$$

$$\lambda_1 = -1 \quad \lambda_2 = 2$$

$$M_{\alpha}(\lambda_1) = 1$$

$$M_{\alpha}(\lambda_2) = 2$$

$$V_{\lambda_1} = \text{Sol}(A + \lambda_1 I | \Omega)$$

$$\lambda_1 = -1$$

$$\begin{pmatrix} -1+1 & 0 & 5 \\ 0 & 2+1 & 1 \\ 0 & 0 & 2+1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 5 & | & 0 \\ 0 & 3 & 1 & | & 0 \\ 0 & 0 & 3 & | & 0 \end{pmatrix} \quad \begin{cases} 5z = 0 \\ 3y+z = 0 \\ 3z = 0 \end{cases} \quad \begin{cases} z = 0 \\ 3y = 0 \\ y = 0 \end{cases}$$

$$V_{\lambda_1} = \left\{ \begin{pmatrix} x \\ 0 \\ 0 \end{pmatrix} \in \mathbb{R}^3 \right\} = \mathbb{L} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\} \quad M_{\alpha}(\lambda_1) = M_g(\lambda_1) = 1$$

$$V_{\lambda_2} = \text{Sol}(A - \lambda_2 I | \Omega)$$

$$\lambda_2 = 2$$

$$\begin{pmatrix} -1-2 & 0 & 5 \\ 0 & 2-2 & 1 \\ 0 & 0 & 2-2 \end{pmatrix} = \begin{pmatrix} -3 & 0 & 5 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \begin{cases} -3x + 5z = 0 \\ z = 0 \end{cases} \quad \begin{cases} x = 0 \\ z = 0 \end{cases}$$

$$V_{\lambda_2} = \left\{ \begin{pmatrix} 0 \\ 4 \\ 0 \end{pmatrix} \in \mathbb{R}^3 \right\} = \mathcal{L} \left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\} \quad M_\alpha(\lambda_2) \neq M_g(\lambda_2)$$

La matrice non è diagonalizzabile.

•  $D = \begin{pmatrix} 2 & 0 & 2 \\ 0 & 1 & 0 \\ 2 & 0 & 2 \end{pmatrix}$  La matrice è diagonalizzabile perché simmetrica

$$\begin{aligned} \det(D - \lambda I) &= \det \begin{pmatrix} 2-\lambda & 0 & 2 \\ 0 & 1-\lambda & 0 \\ 2 & 0 & 2-\lambda \end{pmatrix} = (2-\lambda) \cdot \det \begin{pmatrix} 1-\lambda & 0 \\ 0 & 2-\lambda \end{pmatrix} + 2 \cdot \det \begin{pmatrix} 0 & 2 \\ 1-\lambda & 0 \end{pmatrix} \\ &= (2-\lambda) \cdot (1-\lambda) \cdot (2-\lambda) + 2 \cdot (-(\lambda-1) \cdot 2) \\ &= (2-\lambda)^2(1-\lambda) + 2((\lambda-1) \cdot 2) = \\ &= (2-\lambda)^2(1-\lambda) + 2(z\lambda - z) = \\ &= (2-\lambda)^2(1-\lambda) + (4\lambda - 4) \end{aligned}$$

$$(2-\lambda)^2(1-\lambda) + (4\lambda - 4) = 0$$

$$(4 - 4\lambda + \lambda^2)(1 - \lambda) + 4\lambda - 4 = 0$$

$$4 - 4\lambda + \lambda^2 + \lambda^2 - 4\lambda + \lambda^3 - \lambda^3 + 4\lambda - 4 = 0$$

$$-\lambda^3 + 5\lambda^2 - 4\lambda = 0$$

$$-\lambda(\lambda^2 - 5\lambda + 4) = 0$$

$$-\lambda(\lambda^2 - \lambda - 4\lambda + 4) = 0$$

$$-\lambda(\lambda(\lambda-1) - 4(\lambda-1)) = 0$$

$$-\lambda((\lambda-1)(\lambda-4)) = 0$$

$$\lambda(\lambda-1)(\lambda-4) = 0$$

$$\lambda_1 = 0 \quad M_\alpha(\lambda_i) = 1 \quad \forall i = 1, 2, 3$$

$$\lambda_2 = 1$$

$$\lambda_3 = 4$$

$$V_{\lambda_1} = \text{Sol}(A - 0I | \Omega)$$

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

$$\begin{cases} x+z=0 \\ y=0 \end{cases} \quad \begin{cases} x=-z \\ y=0 \end{cases} \quad V_{\lambda_1} = \left\{ \begin{pmatrix} -z \\ 0 \\ z \end{pmatrix} \in \mathbb{R}^3 \right\} = \mathcal{L} \left\{ \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} \right\}$$

$$V_{\lambda_2} = \text{Sol}(A - \lambda_2 I | \underline{0})$$

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 0 \\ 2 & 0 & 1 \end{pmatrix} \quad \begin{cases} x + 2z = 0 \\ 2x + z = 0 \end{cases} \quad \begin{cases} x = 0 \\ z = 0 \end{cases}$$

$$V_{\lambda_2} = \left\{ \begin{pmatrix} 0 \\ 4 \\ 0 \end{pmatrix} \in \mathbb{R}^3 \right\} = \mathcal{L} \left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$$

$$V_{\lambda_3} = \text{Sol}(A - \lambda_3 I | \underline{0})$$

$$\begin{pmatrix} 2-a & 0 & 2 \\ 0 & 1-a & 0 \\ 2 & 0 & 2-a \end{pmatrix} \xrightarrow{R_3 + R_2} \begin{pmatrix} -2 & 0 & 2 \\ 0 & -3 & 0 \\ 2 & 0 & -2 \end{pmatrix} \xrightarrow{-\frac{1}{2}R_1} \begin{pmatrix} -2 & 0 & 2 \\ 0 & -3 & 0 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{-\frac{1}{3}R_2} \begin{pmatrix} 1 & 0 & -1 \\ 0 & -3 & 0 \\ 0 & 0 & 0 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \begin{cases} x - z = 0 \\ y = 0 \end{cases} \quad \begin{cases} x = z \\ y = 0 \end{cases} \quad V_{\lambda_3} = \left\{ \begin{pmatrix} z \\ 0 \\ z \end{pmatrix} \in \mathbb{R}^3 \right\} = \mathcal{L} \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\}$$

$$M_\alpha(\lambda_i) = M_g(\lambda_i) \quad \forall i = 1, 2, 3$$

$$D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a \end{pmatrix} \quad P = \begin{pmatrix} -1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

$$\bullet E = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \det(E - \lambda I) = \det \begin{pmatrix} 1-\lambda & 1 \\ 0 & 1-\lambda \end{pmatrix} = (1-\lambda)^2$$

$$\lambda = 1 \quad M_\alpha = 2$$

$$V_\lambda = \text{Sol}(A - \lambda I | \underline{0})$$

$$\begin{pmatrix} 1-\lambda & 1 \\ 0 & 1-\lambda \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad y=0 \quad V_\lambda = \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix} \in \mathbb{R}^2 \right\} = \mathcal{L} \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$$

La matrice non e' diagonalizzabile

$$\bullet F = \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix} \quad (\text{la matrice e' simmetrica} \Rightarrow \text{e' diagonalizzabile})$$

$$\det(F - \lambda I) = \det \begin{pmatrix} 1-\lambda & 3 \\ 3 & 1-\lambda \end{pmatrix} = (1-\lambda)^2 - 9 \quad \lambda_1 = 4 \quad \lambda_2 = -2$$

$$M_\alpha(\lambda_1) = 1 \quad M_\alpha(\lambda_2) = 1$$

$$V_{\lambda_1} = \text{Sol}(A - \lambda_1 I | \underline{0}) \quad \begin{pmatrix} 1-\lambda & 3 \\ 3 & 1-\lambda \end{pmatrix} = \begin{pmatrix} -3 & 3 \\ 3 & -3 \end{pmatrix} = \begin{pmatrix} -3 & 3 \\ 0 & 0 \end{pmatrix} \quad \begin{array}{l} R_2 + R_1 \\ -3x + 3y = 0 \\ 3x = 3y \end{array}$$

$$x = y$$

$$V_{\lambda_1} = \left\{ \begin{pmatrix} 4 \\ 4 \end{pmatrix} \in \mathbb{R}^2 \right\} = \text{I} \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$$

$$V_{\lambda_2} = \text{Sol}(A + 2I | \underline{0})$$

$$\begin{pmatrix} 1+2 & 3 \\ 3 & 1+2 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 0 & 0 \end{pmatrix} \quad \begin{array}{l} R_2 - R_1 \\ 3x + 3y = 0 \\ 3x = -3y \\ x = -y \end{array}$$

$$V_{\lambda_2} = \left\{ \begin{pmatrix} -4 \\ 4 \end{pmatrix} \in \mathbb{R}^2 \right\} = \text{L} \left\{ \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right\}$$

$$D = \begin{pmatrix} 4 & 0 \\ 0 & -2 \end{pmatrix} \quad P = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$