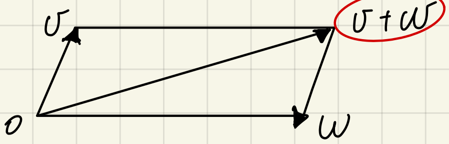
VETTORI NELLO SPAZIO

OPERAZIONI TRA VETTORI

→ SIANO $v = (x_1, x_2, x_3)$ E $w = (y_1, y_2, y_3)$

1. SOMMA E DIFFERENZA → $v \pm w = (x_1 \pm y_1, x_2 \pm y_2, x_3 \pm y_3)$

↳ REGOLA DEL PARALLELOGRAMMA →



2. PRODOTTO → SIA c UN NR QUALSIASI → $cv = (cx_1, cx_2, cx_3)$
↳ MULTIPLO DI v.

3. PRODOTTO SCALARE → $\langle v, w \rangle = x_1 y_1 + x_2 y_2 + x_3 y_3 = z$ → È NR E NON VETTORE

LUNGHEZZE, DISTANZE, ORTOGONALITÀ

1. LUNGHEZZA (NORMA) → $\|v\| = \sqrt{\langle v, v \rangle} \to \sqrt{x_1^2 + x_2^2 + x_3^2}$

2. DISTANZA FRA I PUNTI v E w → $\|v - w\| = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + (x_3 - y_3)^2}$

* LA LUNGHEZZA DI UN VETTORE È DATA DALLA SUA DISTANZA DALL'ORIGINE
↳ $\|v\| = \|v - 0\|$

3. ORTOGONALITÀ → 2 VETTORI SONO ORTOGONALI SE IL LORO PRODOTTO SCALARE ($\langle v, w \rangle$) = 0 (NULLO).

4. PROIEZIONE → SIANO $v, w \in R^3$, $w \neq 0$ → $\underbrace{pr_w(v) = \frac{\langle v, w \rangle}{\|w\|^2} \cdot w}_{\text{PROIEZIONE DI } v \text{ SU } w}$

TEOREMA → SIANO v, w VETTORI DI R^3 → $\|v\|^2 + \|w\|^2 = \|v + w\|^2$ SE E SOLO SE v E w SONO ORTOGONALI

↳ **DIMOSTRAZIONE** → SIANO $v = (x_1, x_2, x_3)$ E $w = (y_1, y_2, y_3)$.

$$v + w = (x_1 + y_1, x_2 + y_2, x_3 + y_3)$$

DUNQUE → $\|v + w\|^2 = (x_1 + y_1)^2 + (x_2 + y_2)^2 + (x_3 + y_3)^2 =$

$$= x_1^2 + x_2^2 + x_3^2 + y_1^2 + y_2^2 + y_3^2 + 2(x_1 y_1, x_2 y_2, x_3 y_3) =$$

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

↳ SE = 0 (ORTOGONALE) → $2 \cdot 0 = 0$

LA DISUGUAGLIANZA DI CAUCHY-SCHWARZ → SIANO v E $w \in \mathbb{R}^3$

$$\boxed{|\langle v,w\rangle| \le \|v\| \cdot \|w\|}$$

DEFINIZIONE DI ANGOLO → SIANO v E $w \in \mathbb{R}$, v E $w \neq 0$.

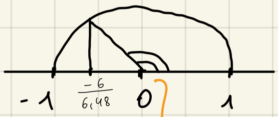
DALLA DISUGUAGLIANZA DI CAUCHY-SCHWARZ SAPPIAMO CHE $\boxed{-1 < \frac{\langle v,w\rangle}{\|v\|\|w\|} < 1}$

QUINDI ESISTE UN UNICO NR θ (THETA) COMPRESO FRA 0 E π ($0 \le \theta \le \pi$) t.c.

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

→ ANGOLO FRA I VETTORI v E w → $\theta = \widehat{vw}$

ESEMPIO → $v = (1,2,3)$, $w = (-1,-1,-1)$ → CALCOLO IL $\cos \widehat{vw} = \frac{-6}{\sqrt{14}\sqrt{3}} \simeq -\frac{6}{6,48}$



→ ANGOLO OTTUSO

PRODOTTO VETTORIALE → SIANO $v = (x_1,x_2,x_3)$, $w = (y_1,y_2,y_3) \in \mathbb{R}$

→ $$\boxed{v \times w = (x_2y_3 - x_3y_2,\ -x_1y_3 + x_3y_1,\ x_1y_2 - x_2y_1)}$$

PROPRIETÀ:

1. SIANO $v,w,u \in \mathbb{R}^3$; $a,b \in \mathbb{R}$ → $(av + bw) \times u = a(v \times u) + b(w + u)$
2. $v \times w = -w \times v$
3. $v \times w = 0 \iff v = kw$ (v È MULTIPLO DI w)
4. $v \times w$ È UN VETTORE ORTOGONALE SIA A v CHE A w → $(v\times w)\cdot v = 0$, $(v \times w)\cdot w = 0$
5. $\|v \times w\| = \|v\| \cdot \|w\| \cdot \sin\theta = b \cdot h$ = AREA DEL PARALLELOGRAMMA
6. $e_1 \times e_2 = e_3$, $e_3 \times e_1 = e_2$, $e_2 \times e_3 = e_1$ } → VERSORI DEGLI ASSI

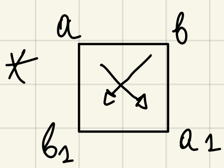
ESEMPIO → $v = (1,2,3)$, $w = (-1,-1,-1)$

$v \times w =$

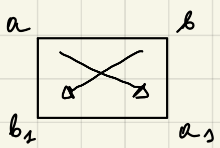
	I	II	III
v	1	2	3
w	-1	-1	-1

→ $(2\cdot(-1)) - (3\cdot(-1)), -(1\cdot(-1)) + (3\cdot(-1)),$

$(1\cdot(-1)) - (2\cdot(-1))$ → $(1, -2, 1)$



$a a_1 - b b_1$



$-(a a_2) + (b b_1)$

RETTE E PIANI

RETTA → LA RETTA NELLO SPAZIO È UNA PARTICOLARE TRAIETTORIA DI UN PUNTO CHE SI MUOVE, SEMPRE SECONDO UNA CERTA DIREZIONE.

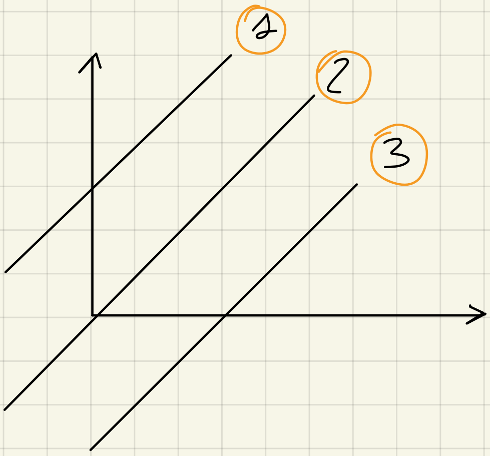
SE PENSIAMO AL PARAMETRO t COME AL TEMPO, I PUNTI X DI UNA RETTA r SONO DESCRITTI DA UNA EQ. PARAMETRICA VETTORIALE

$A \neq 0$ → VETTORE DIREZIONE ← $\boxed{r: X = P + tA}$

t → PARAMETRO TEMPO

P → PUNTO

↳ $\mathbb{R}^3$ → $r = \{ X \in \mathbb{R}^3 \mid X = P + tA, \ t \in \mathbb{R} \}$



→ 1 E 3 SONO TRASLATE DI 2

UNA STESSA RETTA HA MOLTE POSSIBILI EQUAZIONI PARAMETRICHE

↳ ESEMPIO: SCEGLIAMO IL PUNTO P COME QUALSIASI PUNTO DELLA RETTA (CIÒ VUOL DIRE RI-PARAMETRIZZARE LA RETTA, SCEGLIENDO UN PARAMETRO $t' = t + k$), E IL VETTORE PUÒ CAMBIARE DI LUNGHEZZA E DI VERSO

$$s: \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + t \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \equiv s: \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + t' \begin{pmatrix} -2 \\ -2 \\ 0 \end{pmatrix}$$

↓

$$\begin{cases} x = t \\ y = t \\ z = 1 \end{cases}$$

↓

$x = y, \ z = 1$

↓

$$\begin{cases} x = 1 + (-2t) = x = -t \\ y = 1 + (-2t) = y = -t \\ z = 1 \quad = z = 1 \end{cases}$$

↓

$x = y, \ z = 1$

PIANO → INSIEME ORTOGONALE ALLA RETTA

SIA $n = (a, b, c) \neq 0$ → IL PIANO α_0 PASSANTE PER L'ORIGINE E ORTOGONALE ALLA DIREZIONE n.

È L'INSIEME DI TUTTI I VETTORI DELLO SPAZIO CHE SONO PERPENDICOLARI ($\perp$) A n, OVVERO:

PIANO PASSANTE PER L'ORIGINE ← $\alpha_0 = \{x \in \mathbb{R}^3 \mid \langle x, n \rangle = 0\} =$

$= \{x, y, z \in \mathbb{R}^3 \mid ax + by + cz = 0\}$

SIA $n = (a, b, c) \neq 0$ → IL PIANO α PASSANTE PER IL PUNTO P E ORTOGONALE ALLA DIREZIONE n SI SCRIVE:

PIANO PASSANTE PER UN PUNTO QUALSIASI ← $\alpha = \{x \in \mathbb{R}^3 \mid \langle x - P, n \rangle = 0\} =$

$= \{x, y, z \in \mathbb{R}^3 \mid \langle (x, y, z) - (P_x, P_y, P_z), n \rangle = 0\} =$

$= \{x, y, z \in \mathbb{R}^3 \mid a(x - P_x) + b(y - P_y) + c(z - P_z) = 0\}$

EQUAZIONE CARTESIANA DEL PIANO → $ax + by + cz + d = 0$ CON $a, b, c \neq 0$

* SE E SOLO SE $d = 0$ → IL PIANO PASSA PER L'ORIGINE

OSSERVAZIONE → LA RETTA $r: X = P + tA$ È ORTOGONALE AL PIANO $\alpha: ax + by + cz + d = 0$ SE "A" È MULTIPLO DEL VETTORE NORMALE AL PIANO

S ORTOGONALE

S ORTOGONALE → SE S È UN SOTTOINSIEME DI $\mathbb{R}^3$ → $\boxed{S^\perp := \{x \in \mathbb{R}^3 \mid x \cdot s = 0 \ \forall s \in S\}}$

ESEMPIO → $S = \{(1, 0, -1)\}$; $X = (x_1, x_2, x_3)$

CONDIZIONE $S \cdot X = 0$ → $(x_1, x_2, x_3) \cdot (1, 0, -1) = 0$

$x_1 - x_3 = 0$

$x_1 = x_3$

DUNQUE $S^\perp = \{(x_1, x_2, x_3) \mid \underline{x_1 = x_3}\} = \{(x_1, x_2, x_1)\}$

↳ $1x_1 - 1x_3 = 0$ → $\overset{a}{1}x_1 + \overset{b}{0}x_2 + \overset{c}{(-1)}x_3 + \overset{d}{0} = 0$ →

→ $n = (1, 0, -1)$ → IL PIANO PASSA PER L'ORIGINE

$n^\perp$

OSS → UN'EQ. PARAMETRICA VETTORIALE PER LA RETTA PASSANTE PER I PUNTI P E Q (DISTINTI) È $X = P + t(Q - P)$

MUTUE POSIZIONI

MUTUA POSIZIONE $\rightarrow$ VUOL DIRE TROVARE LE INTERSEZIONI (RISOLVENDO IL SISTEMA LINEARE)

PARALLELISMO

1) RETTE $\rightarrow$ LE RETTE $r: X = P + tA$ E $X = P' + t'A'$ SONO PARALLELE ($r \parallel r'$) SE HANNO LA STESSA DIREZIONE, OVVERO $A' = kA$, $k \neq 0$

* $\rightarrow$ SE HANNO UN PUNTO IN COMUNE VUOL DIRE CHE È LA "STESSA" RETTA E QUINDI VENGONO CHIAMATE "COINCIDENTI" (SE NESSUNA DELLE DUE, ALLORA SONO SGHEMBE. SE SI INCONTRANO IN UN PUNTO MA NON SONO COINCIDENTI, ALLORA SONO INCIDENTI

2) PIANO $\rightarrow$ I PIANI $\alpha: ax+by+cz+d=0$ E $\alpha': a'x+b'y+c'z+d'=0$ SONO PARALLELI SE I LORO VETTORI NORMALI SONO UNO MULTIPLO DELL'ALTRO.

* $\rightarrow$ SE ANCHE d È MULTIPLO DI d' $\Rightarrow$ I PIANI SONO "COINCIDENTI" OVVERO LE DUE EQUAZIONI RAPPRESENTANO LO STESSO PIANO.

ESEMPIO: $x+y+z+3=0$

- $2x+2y+2z+5=0$ $\rightarrow$ PARALLELI
- $2x+2y+2z+6=0$ $\rightarrow$ COINCIDENTI

3) RETTA E PIANO $\rightarrow$ LA RETTA $r: X = P + tA$ E IL PIANO $\alpha: ax+by+cz+d=0$ SONO PARALLELI SE $n \perp A$, OVVERO $\langle n, A \rangle = 0$

* $\rightarrow$ SE HANNO, ANCHE, UN PUNTO IN COMUNE SI DICE CHE RETTA r GIACE SUL PIANO α

ESEMPIO: $\alpha: x+y=5 \rightarrow n_\alpha(1,1,0)$
$\beta: z=5 \rightarrow n_\beta(0,0,1)$

NON SONO NÉ PARALLELI NÉ COINCIDENTI
$\downarrow$
ALLORA SONO INCIDENTI

$$\begin{cases} ax+by+cz+d=0 \\ a'x+b'y+c'z+d'=0 \end{cases} \rightarrow \begin{cases} x+y=5 \\ z=5 \end{cases} \rightarrow \begin{cases} x=t \\ t+y=5 \\ z=5 \end{cases} \rightarrow$$

$$\rightarrow \begin{cases} x=t \\ y=5-t \\ z=5 \end{cases} \rightarrow \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 5 \\ 5 \end{pmatrix} + t \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$$

EQUAZIONI CARTESIANE DELLA RETTA

SIA $r: X = P + tA$ (FORMA PARAMETRICA), SE $P = (P_1, P_2, P_3)$ E $A = (A_1, A_2, A_3) \neq 0$

ALLORA I PUNTI $X = (x, y, z)$ DELLA RETTA SODDISFANO, PER t PARAMETRO REALE, LE 3 EQ: →
- $x = P_1 + tA_1$
- $y = P_2 + tA_2$
- $z = P_3 + tA_3$

RICAVANDO t DA UNA EQ. E SOSTITUENDO NELLE ALTRE 2, SI OTTENGONO EQ. CARTESIANE DELLA RETTA: → $\begin{cases} ax+by+cz+d=0 \\ a'x+b'y+c'z+d'=0 \end{cases}$ → QUESTO CORRISPONDE A VEDERE LA RETTA COME INTERSEZIONE DI 2 PIANI.

ESEMPIO: SIA $r: X = P + tA$ CON $P = (0, 1, 2)$ E $A = (1, 0, 1)$ ALLORA I PUNTI DELLA RETTA SONO DEL TIPO $(x, y, z) = (t, 1, 2+t)$.

RISULTA $z = 2+t$ E $x = t$ → $z = 2 + x$ E DUNQUE $r = \alpha \cap \beta$ CON $\alpha = \{x - z + 2 = 0\}$ E $\beta = \{y = 1\}$

NB → UNA STESSA RETTA HA INFINITE POSSIBILI ESPRESSIONI CARTESIANE, POICHÉ CI SONO INFINITE COPPIE DI PIANI CHE, INTERSECANDOSI, INDIVIDUANO LA STESSA RETTA

LO SPAZIO IN R^n

- $P = (x_1, x_2, x_3)$ → TERNA DI NUMERI
- $P = (x_1, x_2, x_3, x_4)$ → QUATERNA DI NUMERI → GEOMETRIA A 4 DIMENSIONI (SPAZIO - TEMPO)
- $P = (x_1, x_2, \dots, x_n)$ → n-UPLA DI NR. REALI → GEOMETRIA A n DIMENSIONI

→ **DEFINIZIONE** → $\forall\, n \geq 1$ CONSIDERIAMO L'INSIEME R^n DELLE n-UPLE ORDINATE DI NR. REALI $R^n = \{v = x_1, \dots, x_n \mid x_i \in R\}$

* → GLI ELEMENTI DELLO SPAZIO n-DIMENSIONALE VENGONO CHIAMATI: PUNTI, VETTORI, n-UPLE (A LORO VOLTA COMPOSTI DA COMPONENTI O COORDINATE)

OPERAZIONI SU VETTORI IN R^n:

1) SOMMA
2) PRODOTTO PER UN NUMERO
3) PRODOTTO SCALARE IN R^n
4) LUNGHEZZA, DISTANZA, ORTOGONALITÀ
5) ANGOLO IN R^n

1) SOMMA → COMPONENTE PER COMPONENTE

$$\left.\begin{array}{l} v = (x_1, \dots, x_n) \\ w = (y_1, \dots, y_n) \end{array}\right\} \to v + w = (x_1 + y_1, \dots, x_n + y_n)$$

PROPRIETÀ:

1. COMMUTATIVA → $v + w = w + v \quad \forall v, w \in \mathbb{R}^n$
2. ASSOCIATIVA → $(v + w) + u = v + (w + u) \quad \forall v, w, u \in \mathbb{R}^n$
3. $v + 0 = v \quad \forall v \in \mathbb{R}^n$
4. $v + (-v) = 0 \quad \forall v \in \mathbb{R}^n$

2) PRODOTTO PER UN NUMERO

$$\left.\begin{array}{l} v = (x_1, \dots, x_n) \\ c \in \mathbb{R}^n \end{array}\right\} \to w = (cx_1, \dots, cx_n)$$

PROPRIETÀ:

1. ASSOCIATIVA → $a(bv) = (ab)v \quad \forall a, b \in \mathbb{R};\ \forall v \in \mathbb{R}^n$
2. DISTRIBUTIVA → $\left.\begin{array}{l} a(v + w) = av + aw \\ (a + b) \cdot v = av + bv \end{array}\right\} \forall a, b \in \mathbb{R};\ \forall v \in \mathbb{R}^n$
3. $1v = v \quad \forall v \in \mathbb{R}^n$

3) PRODOTTO SCALARE IN $\mathbb{R}^n$

$$\left.\begin{array}{l} v = (x_1, \dots, x_n) \\ w = (y_1, \dots, y_n) \end{array}\right\} \langle v, w \rangle = x_1 + y_1 + \dots + x_n + y_n$$

$$\Rightarrow \sum_{i=1}^{n} x_i, y_i \in \mathbb{R}$$

PROPRIETÀ:

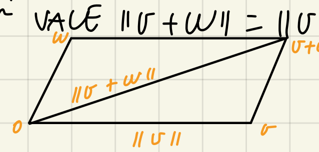
1. COMMUTATIVA → $\langle v, w \rangle = \langle w, v \rangle$
2. DISTRIBUTIVA - SOMMA → $\langle v, w + u \rangle = \langle v, w \rangle + \langle v, u \rangle$
3. DISTRIBUTIVA - PRODOTTO → $\langle cv, w \rangle = \langle v, cw \rangle = c \langle v, w \rangle$
4. POSITIVITÀ → $\langle v, v \rangle \geq 0$ (SE $v = 0 \Rightarrow \langle v, v \rangle = 0$)

4) LUNGHEZZA, DISTANZA, ORTOGONALITÀ

1. LUNGHEZZA (NORMA) → $\| v \| = \sqrt{\langle v, v \rangle}$
2. DISTANZA → $\| w - v \| = \sqrt{w - v}$
3. ORTOGONALITÀ → v E w SONO ORTOGONALI SE $v \cdot w = 0$
4. PROIEZIONE → $pr_w(v) = \dfrac{\langle v, w \rangle}{\| w \|^2} \cdot w$
5. $S^\perp = \{ v \in \mathbb{R}^n \mid \langle v, s \rangle = 0,\ \forall s \in S \}$

5) ANGOLO IN $\mathbb{R}^n$

1. DISUGUAGLIANZA DI CAUCHY - SCHWARZ → SE $v, w \in \mathbb{R}^n \Rightarrow |\langle v, w \rangle| \leq \| v \| \| w \|$
2. DISUGUAGLIANZA TRIANGOLARE IN $\mathbb{R}^n$ → $\forall v, w \in \mathbb{R}^n$ VALE $\| v + w \| = \| v \| + \| w \|$



3. TEOREMA DI PITAGORA → SE $v, w \in \mathbb{R}^n$ SONO ORTOGONALI $\Rightarrow \| v \|^2 + \| w \|^2 = \| v + w \|^2$
4. DISUGUAGLIANZA DI CAUCHY - SCHWARZ → SE v, w SONO NULLI $\Rightarrow -1 \leq \dfrac{\langle v, w \rangle}{\| v \| \| w \|} \leq 1$

MUTUA POSIZIONE 2

MUTUE POSIZIONI DI 2 PIANI

↳ DUE PIANI α E β DI EQ → $\alpha: ax+by+cz+d=0$
$\beta: a'x+b'y+c'z+d'=0$

SONO PARALLELI SE E SOLTANTO SE $rg\begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} = 1$

↓

IL $rg = 2$ SE E SOLTANTO SE $\alpha \cap \beta = r$, CON r UNA RETTA.

SE α E β SONO PARALLELI ⇒ $\alpha = \beta$ OPPURE $\alpha \cap \beta = 0$

SE $rg\begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} = 1$ SE $rg\begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} = 2$

MUTUE POSIZIONI DI 2 RETTE

↳ SIANO r E s DUE RETTE DI EQ. CARTESIANA

$$r: \begin{cases} ax+by+cz+d=0 \\ a'x+b'y+c'z+d'=0 \end{cases} \quad ; \quad s: \begin{cases} ex+fy+gz+h=0 \\ e'x+f'y+g'z+h'=0 \end{cases}$$

$$M_{4\times3} = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ e & f & g \\ e' & f' & g' \end{pmatrix} \quad M'_{4\times4} = \begin{pmatrix} a & b & c & -d \\ a' & b' & c' & -d' \\ e & f & g & -h \\ e' & f' & g' & -h' \end{pmatrix}$$

1) SE $\det M' = 0$ ⇒ LE RETTE SONO COMPLANARI, CIOÈ

- $r = s$ SE $rg\,M' = rg\,M = 2$
- $r \cap s = P$ SE $rg\,M' = rg\,M = 3$
- $r \parallel s$ SE $rg\,M' = 3$ E $rg\,M = 2$

2) LE RETTE SONO SGHEMBE ⇔ $\det M' \neq 0$

MUTUE POSIZIONI DI UNA RETTA E UN PIANO

↳ SIANO UNA RETTA r E UN PIANO α.

LE POSSIBILI MUTUE POSIZIONI SONO:

A) $r \parallel \pi$ (PARALLELE) $\begin{cases} r \subset \pi \text{ (r CONTENUTA IN } \pi) \\ r \cap \pi \neq 0 \text{ (r E } \pi \text{ NON SI INTERSECANO)} \end{cases}$

B) r È INCIDENTE A π (* COME CASO PARTICOLARE SI POTREBBE AVERE r ORTOGONALE A π)

→ CI SONO 3 MODI PER DETERMINARE I VARI CASI

MODO 1 → SIA r FORMA PARAMETRICA E π CARTESIANA:

$$r: P + tA = \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} + t \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$$

$$\pi: ax + by + cz + d = 0 \rightarrow n_\pi = (a, b, c)$$

→ STUDIO IL PRODOTTO SCALARE TRA A E n_π.

A) SE $\langle A, n_\pi \rangle = 0 \Rightarrow r$ E π SONO PARALLELI

↳ SE HANNO, ANCHE, UN PUNTO IN COMUNE ALLORA $r \subset \pi$. ALTRIMENTI SONO PARALLELI E DISGIUNTI.

B) SE $\langle A, n_\pi \rangle \neq 0 \Rightarrow r$ E π SONO INCIDENTI.

↳ SE A È UN MULTIPLO DI n_π, OVVERO $A = k n_\pi \Rightarrow r$ E π SONO ORTOGONALI.

MODO 2 → SIA r E π IN FORMA PARAMETRICA:

$$r: P + tA = \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} + t \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \quad ; \quad \pi: Q + t v_1 + s v_2$$

→ TROVO n_π FACENDO $v_1 \wedge v_2$ $(v_1 \times v_2)$ →

	I	II	III
v_1	·	·	·
v_2	·	·	·

→

→ $(x_2 y_3 - x_3 y_2, -x_1 y_3 + x_3 y_1, x_1 y_2 - x_2 y_1)$. → A QUESTO PUNTO HO TROVATO n_π E POSSO PROCEDE CON IL $\boxed{\text{METODO 1}}$

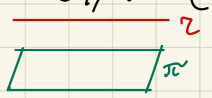
MODO 3 $\rightarrow$ r E π IN FORMA CARTESIANA:

$$r: \begin{cases} ax+by+cz+d=0 \\ a'x+b'y+c'z+d'=0 \end{cases} \quad ; \quad \pi: ex+fy+gz+h=0$$

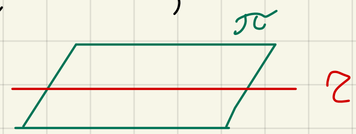
$\rightarrow$ STUDIO LE INTERSEZIONI. $\rightarrow$ (LE INTERSEZIONI SONO I PUNTI $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ CHE SODDISFANO TUTTE E 3 LE EQ, OVVERO IL SISTEMA

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

A) • SE $rgA = 2$ E $rg(A|b) = 3$ $\Rightarrow$ IL SISTEMA NON È COMPATIBILE E QUINDI $r // \pi$ (r NON CONTENUTA IN π)



• SE $rgA = rg(A|b) = 2$ $\Rightarrow$ $\dim Sol = n - rgA = 1$ $\Rightarrow$
$\Rightarrow$ $\pi \cap r$ È UNA RETTA, OVVERO $\pi // r$ E $r \subset \pi$



B) SE $rgA = 3$ $\Rightarrow$ $rg(A|b) = 3$ $\Rightarrow$ IL SISTEMA È COMPATIBILE

$\dim Sol = n - rgA = 3-3 = 0$ $\Rightarrow$ LA SOLUZIONE È UNICA E r, π SONO INCIDENTI

$\boxed{\text{OSS:}}$ NON SI RIESCE A DETERMINARE SE SONO $\perp$ SENZA PASSARE DAI VETTORI DIREZIONE

NUMERI

DIVERSI TIPI DI NUMERI

1. $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ → NUMERI NATURALI
2. $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ → NUMERI INTERI
3. NUMERI PRIMI
4. $\mathbb{Q} = \left\{ \frac{p}{q} \; ; \; p, q \in \mathbb{R} \right\}$ → NUMERI RAZIONALI
5. $\mathbb{C} = \{a + ib \; ; \; a, b \in \mathbb{R}\}$ → NUMERI COMPLESSI

   $* \; i^2 = -1$
6. $\mathbb{R}$ → NUMERI REALI ("SOLITI NUMERI")

1 NUMERI NATURALI → $\mathbb{N}$

PROPRIETÀ:

1) ASSIOMA DEL BUON ORDINAMENTO → OGNI SOTTINSIEME NON VUOTO DI $\mathbb{N}$ HA UN ELEMENTO MINIMO. OVVERO, SE $S \subset \mathbb{N}$, $S \neq 0 \Rightarrow \exists \; m \in S$ t.c. $m \leq n \; \forall \; n \in S$.

2) PRINCIPIO DI INDUZIONE → ASSOCIAMO AD OGNI NR. NATURALE n UNA ASSERZIONE $A(n)$. ALLORA, SE:

   - $A(0)$ È VERA E $\forall n$, $A(n)$ IMPLICA $A(n+1)$

   ALLORA $A(n)$ È VERO $\forall n$.

OPERAZIONI CHE POSSO FARE CON I NATURALI SENZA USCIRE DA $\mathbb{N}$

→ SOMMA: $m + n \in \mathbb{N}$ SE $m, n \in \mathbb{N}$

$* \; 0$ È L'ELEMENTO NEUTRO PERCHÉ $0 + n = n \; \forall n \in \mathbb{N}$

→ MOLTIPLICAZIONE: $m \cdot n \in \mathbb{N}$ SE $m, n \in \mathbb{N}$

$* \; 1$ È L'ELEMENTO NEUTRO PERCHÉ $1 \cdot n = n \; \forall n \in \mathbb{N}$

$* \; 0 \cdot n = 0 \; \forall \; n \in \mathbb{N}$

→ DIVISIONE CON RESTO

OPERAZIONI CHE NON POSSO FARE CON I NATURALI SENZA USCIRE DA $\mathbb{N}$

- SOTTRAZIONE : ESEMPIO $1-5=-4 \notin \mathbb{N}$ $(-4 \in \mathbb{Z})$
- DIVISIONE NORMALE : ESEMPIO $1:2=0,5 \notin \mathbb{N}$ $(\frac{1}{2} \in \mathbb{Q})$
- RADICI : ESEMPIO $\sqrt{2}=1,414\ldots \notin \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ $(\sqrt{2} \in \mathbb{R})$

OSSERVAZIONE → PARTENDO DA $\mathbb{N}$, ATTRAVERSO VARIE OPERAZIONI, POSSIAMO TROVARE GLI ALTRI INSIEMI DI NR.

QUINDI : NUMERI PRIMI $\subseteq \mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$

"È CONTENUTO MA NON UGUALE"

(2) NUMERI INTERI → $\mathbb{Z}$

OPERAZIONI CONCESSE PER RIMANERE IN $\mathbb{Z}$:

- SOMMA
- SOTTRAZIONE
- MOLTIPLICAZIONE (NON C'È L'INVERSO)
- DIVISIONE CON RESTO : ESEMPIO $55:9=6$ RESTO 1

↳ CONVENZIONE SUGLI INTERI : IL RESTO DEVE ESSERE POSITIVO

ESEMPIO : $-55:9=-9\cdot 7+8$ (QUOZIENTE 7, RESTO 8)

OSS: IL DIVISORE È SEMPRE >0, ALTRIMENTI MOLTIPLICO DIVISORE E DIVIDENDO PER -1.

! TEOREMA (DIVISIONE CON RESTO) : SIA $a, b \in \mathbb{Z}$; $b>0$ ALLORA ESISTONO UNICI DUE INTERI q, r t.c. $a=qb+r$, $\boxed{0 \leq r < b}$

↓

IL FATTO CHE IL RESTO SIA ≥ 0 E $<b$ È CRUCIALE E CI DA L'UNICITÀ

MODELLO DI SCRITTURA : $a:b=q$ RESTO r

OPERAZIONI NON CONCESSE PER RIMANERE IN $\mathbb{Z}$:

- DIVISIONI NORMALI
- RADICI

DIVISORE

→ SIANO $a, b \in \mathbb{Z}$. DIREMO CHE b DIVIDE a (b È UN DIVISORE DI a) SE $\exists\, c$ t.c. $a = b \cdot c$.

ESEMPIO:
- I DIVISORI DI 12 SONO $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$.
- I DIVISORI DI 7 SONO $\pm 1, \pm 7$
- I DIVISORI DI 0 SONO TUTTI I NR. INTERI, PERCHÈ $\forall\, b \in \mathbb{Z}$, $0 = 0 \cdot b$

* 0 NON DIVIDE NESSUN NUMERO

OSSERVAZIONI

1) OGNI INTERO a HA ALMENO 4 DIVISORI: ± 1, $\pm a$

2) SE d DIVIDE SIA a CHE b ⇒ DIVIDE ANCHE $a \pm b$

ESEMPIO: 3 DIVIDE SIA 6 CHE 9 ⇒ DIVIDE ANCHE:
$6 + 9 = 15$
$6 - 9 = -3$

3) SE d DIVIDE $a \neq 0$ ⇒ $|d| \leq |a|$

PERCHÈ TUTTI I NR. DIVIDONO $\emptyset$, QUINDI PER $a = 0$ NON È VERO

MODULO/VALORE ASSOLUTO, OVVERO: ESEMPIO → $|10| = 10$ E $|-7| = 7$

MASSIMO COMUN DIVISORE

→ SIANO $a, b \in \mathbb{Z}$ CON $a, b \neq 0$. IL LORO MASSIMO COMUN DIVISORE, $MCD(a, b)$ È IL PIÙ GRANDE INTERO CHE DIVIDE SIA a CHE b.

* $MCD(0,0) = 0$

ESEMPIO:
- $MCD(0, a) = |a| \quad \forall\, a \in \mathbb{Z}$
- $MCD(13, 52) = 13$
- $MCD(12, 6) = 6$

OSSERVAZIONE → IL MCD È SEMPRE POSITIVO PERCHÉ È IL NUMERO PIÙ GRANDE TRA I DIVISORI.

- $MCD(a, a) = MCD(a, -a) = |a|$
- $MCD(1, a) = |a|$

PROPRIETÀ:

1) $MCD(a, b) = MCD(b, a) = MCD(-a, b) = MCD(a, -b)$

2) SE $(a, b) \neq (0, 0)$ ⇒ $MCD(a, b) > 0$

3) SE $a, b \in \mathbb{Z}$; $\forall q \in \mathbb{Z}$ $MCD(a, b+qa) = MCD(a,b)$

OVVERO, SE AGGIUNGO A UN NUMERO IL MULTIPLO DI UN ALTRO, IL SUO MCD CON QUEST'ALTRO NON CAMBIA.

ESEMPIO: • $a=3$, $b=7$, $q=5 \Rightarrow MCD(3, 7+15) =$
$= MCD(3,7) = 1$

• $a=10$, $b=3$, $q=10000 \Rightarrow MCD(10, 3+100000) =$
$= MCD(10, 100003) =$
$= MCD(10, 3) = 1$

DIMOSTRAZIONE 3 $\Rightarrow$ SIA $q \in \mathbb{Z}$. DOBBIAMO DIMOSTRARE:

1) SE d È UN DIVISORE SIA DI a CHE DI b, ALLORA LO È ANCHE DI $b+qa$.

$\hookrightarrow a = n_1 d$, $b = n_2 d \Rightarrow b+qa = n_2 d + q n_1 d =$
$= \underbrace{(n_2 + q n_1) d}_{b+qa}$

QUINDI d DIVIDE $b+qa$

2) SE d È UN DIVISORE SIA DI a CHE DI $b+qa$, ALLORA LO È ANCHE DI b

$\hookrightarrow a = n_1 d$, $b+qa = n_2 d \Rightarrow b = (b+qa) - qa =$
$= n_2 d - q n_1 d =$
$= \underbrace{(n_2 d - q n_1) d}_{b}$

QUINDI d DIVIDE b

TEOREMA $\Rightarrow$ SIANO $a, b \in \mathbb{Z}$ E $(a,b) \neq (0,0) \Rightarrow$

$\Rightarrow MCD(a,b)$ È IL PIÙ PICCOLO ELEMENTO POSITIVO DELL'INSIEME $A = \{ax+by \mid x, y \in \mathbb{Z}\}$

COROLLARIO (CONSEGUENZA DI UN TEOREMA)

$\hookrightarrow$ SIANO $a, b \in \mathbb{Z}$ CON $(a,b) \neq (0,0)$:

1) $\exists\, x, y \in \mathbb{Z}$ t.c. $MCD(a,b) = ax+by$

ESEMPIO: $MCD(25, 10) = 5 = 25 - 10 \cdot 2$

2) SE d DIVIDE SIA a CHE $b \Rightarrow d \mid MCD(a,b)$

ESEMPIO: $MCD(12, 18) = 6$ $\Rightarrow 2, 3$ DIVIDONO $12, 18$ E ALLORA ANCHE 6

3) SE MCD $(a,b)=1$ (OVVERO, PRIMI TRA LORO) E a DIVIDE bc $\Rightarrow$ a DIVIDE c

IN FORMULE $\rightarrow$ $a \mid bc = a \mid c$

ESEMPIO: $a=4$, $b=7$, $c=8$ $\rightarrow$ $MCD(4,7)=1$ $\Rightarrow$

$\Rightarrow$ IL FATTO CHE $a(4)$ DIVIDE $bc(8 \cdot 7)$ IMPLICA CHE a DIVIDE c.

$$\boxed{a \mid b \Leftrightarrow \exists\, m \in \mathbb{Z} \text{ t.c. } b = am}$$

③ NUMERI PRIMI

$p \in \mathbb{N} \setminus \{0\}$ $\rightarrow$ $\mathbb{N}$ ESCLUSO $\emptyset$, OVVERO INTERO POSITIVO

p È UN NUMERO PRIMO SE HA ESATTAMENTE 2 DIVISORI POSITIVI: 1 E p

* A RIGUARDO DEL MCD, $p \mid ab \Rightarrow p \mid a$ e/o $p \mid b$
SE p NON È PRIMO $\rightarrow$ FALSO (INFATTI $6 \mid 9 \cdot 10$ MA $6 \nmid 9$ E $6 \nmid 10$)

TEOREMA FONDAMENTALE DELL'ARITMETICA

↳ (DECOMPOSIZIONE IN FATTORI PRIMI)

$\forall$ NR. NATURALE $n \in \mathbb{N}$, $n \neq 0$ ESISTONO k NUMERI PRIMI (NON NECESSARIAMENTE DISTINTI) t.c. $n = \underbrace{p_1 \cdot p_2 \cdot \ldots \cdot p_k}$

FATTORI PRIMI DI n
E SONO UNICI

! 1 NON È NUMERO PRIMO, QUINDI LA DECOMPOSIZIONE DI 1 È 1. !

* NON È PRIMO PERCHÉ SE LO FOSSE NON AVREMMO PIÙ UNICITÀ NEL TEOREMA FONDAMENTALE (POTREMMO AGGIUNGERE TUTTI I FATTORI 1 CHE VOGLIAMO)

COROLLARIO $\rightarrow$ I NUMERI PRIMI SONO INFINITI!

↳ **DIMOSTRAZIONE**: SUPPONIAMO PER ASSURDO CHE SIANO FINITI, $p_1, \ldots, p_k$.

CONSIDERO IL LORO PRODOTTO $a = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ E $b = a+1$

POICHÉ $1 = \underbrace{b - a}_{(1\cdot b - 1\cdot a)}$ → MCD $(a, b) = 1$

PER IL TEOREMA, MCD È IL PIÙ PICCOLO NUMERO CHE SI SCRIVE COME $ax+by$

ORDINE DI UN INTERO → SIA $a \in \mathbb{N}$, $a \neq 0$ E p PRIMO ⇒

⇒ $ORD_p(a)$ = NUMERO DI VOLTE CHE p COMPARE NEI FATTORI PRIMI DI a

ESEMPIO: $ORD_2(12) = 2$
$ORD_3(12) = 1$
$ORD_7(12) = 0$

* SE $a \in \mathbb{Z}$ NEGATIVO, $ORD_p(a) = ORD_p(-a)$.
* $ORD_p(0)$ NON È DEFINITO

$$\boxed{\text{SEGUE CHE} \quad a = \prod_p p^{ORD_p(a)}}$$

ESEMPIO: $12 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdots = 2^2 \cdot 3$

OSSERVAZIONE → $a, b \in \mathbb{Z}$ CON $(a, b) \neq (0, 0)$

1) $\forall p$ PRIMO, $ORD_p(a \cdot b) = ORD_p(a) \cdot ORD_p(b)$
2) $d \in \mathbb{Z}$, $d \neq 0$ ⇒ $d \mid a$ ⇔ $ORD_p(d) \leq ORD_p(a)$ $\forall$ p PRIMO
3) $MCD(a, b) = \prod_p p^{\min(ORD_p(a),\, ORD_p(b))}$

↳ PRENDO TUTTI I FATTORI PRIMI IN COMUNE, CON L'ESPONENTE PIÙ PICCOLO (METODO DELLE ELEMENTARI)

MINIMO COMUNE MULTIPLO → DATI $a, b \in \mathbb{Z}$ CON $(a, b) \neq (0, 0)$ IL MINIMO COMUNE MULTIPLO $mcm(a, b)$ È IL PIÙ PICCOLO $m > 0$ t.c. $a \mid m$, $b \mid m$

ESEMPIO: $mcm(5, 12) = 60$
$mcm(4, 6) = 12$
$mcm(p_1, p_2) = p_1 \cdot p_2$ ($p_1, p_2 \to$ NUMERI PRIMI)

OSSERVAZIONE

1) $mcm(a, b) = \prod_p p^{\max(ord_p(a), ord_p(b))}$

$\hookrightarrow$ PRODOTTO DI TUTTI I FATTORI, IN COMUNE E NON, CON ESPONENTE MASSIMO

2) $mcm(a, b) \cdot MCD(a, b) = |a, b|$

ALGORITMO DI EUCLIDE (PER CALCOLARE MCD)

$\hookrightarrow$ SIANO $a > b \geq 0$.

1) SE $b = 0 \Rightarrow MCD(a, b) = a$

2) SE $b \neq 0 \Rightarrow$ • $a : b = q$ RESTO r CON $0 \leq r < b$

• SI PONE $a = b$ E $b = r$

• SI RIFÀ FINCHÉ $b = 0$

ESEMPIO: TROVARE $MCD(126, 147)$.

1) POICHÈ $126 < 147$ PONIAMO $a = 147$ E $b = 126$

$147 : 126 = 1$ RESTO 21

2) $a = b$ E $b = r \Rightarrow a = 126$ E $b = 21 \neq 0$

$126 : 21 = 6$ RESTO 0

3) $a = 21$ E $b = 0 \Rightarrow$ FINITO!

$MCD(126, 147) = 21$

④ NUMERI RAZIONALI $\to \mathbb{Q}$

SONO I NUMERI DELLA FORMA $\frac{p}{q}$ CON $p, q \in \mathbb{Z}$ E $q \neq 0$

PROBLEMA: $2/3$, $4/6$, $200/300$ ... SONO "LO STESSO" NR.
p/q, p'/q', p''/q''

QUINDI SI CONSIDERANO LE COPPIE (p, q) CON $p \in \mathbb{Z}, q \in \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$

SI DICE CHE (p, q) È EQUIVALENTE A (p', q') ECC. SE E SOLO SE $pq' = qp'$ (OVVERO $\frac{p}{q} = \frac{p'}{q'}$)

SI DEDUCE, QUINDI, CHE UN NUMERO RAZIONALE È UNA CLASSE DI EQUIVALENZA DI COPPIE IN $\mathbb{Z} \times \mathbb{Z}^*$

↳ PER OGNI CLASSE DI EQUIVALENZA SI SCEGLIE UN RAPPRESENTANTE

↳ • AD ESEMPIO $2/3$ CORRISPONDE A TUTTE LE COPPIE $(2,3), (-2,-3), (4,6) \ldots \in \mathbb{Z} \times \mathbb{Z}^*$

• OPPURE 1 RAPPRESENTA LE COPPIE $(a, a) \in \mathbb{Z} \times \mathbb{Z}^*$ PERCHÉ $a/a = 1$.

* LE CLASSI DI EQUIVALENZA IL CUI RAPPRESENTANTE È $a/1$, OVVERO LE COPPIE $(ba, b) \in \mathbb{Z} \times \mathbb{Z}^*$, SI POSSONO IDENTIFICARE COME INTERI DI a ⇒ $\mathbb{Z} \subset \mathbb{Q}$

OPERAZIONI SU Q

1) SOMMA E SOTTRAZIONE $\quad \frac{p}{q} \pm \frac{p'}{q'} = \frac{pq' \pm qp'}{qq'}$

* ELEMENTO NEUTRO 0
* INVERSO DI $\frac{p}{q} = -\frac{p}{q}$

2) MOLTIPLICAZIONI $\quad \frac{p}{q} \cdot \frac{p'}{q'} = \frac{pp'}{qq'}$

* ELEMENTO NEUTRO 1 (COPPIE (a, a))
* INVERSO DI $\frac{p}{q} = \frac{q}{p}$ (SE $p \neq 0$)

3) DIVISIONE $\quad \frac{p}{q} : \frac{p'}{q'} = \frac{p}{q} \cdot \frac{q'}{p'} = \frac{pq'}{qp'}$ (CON $p \neq 0$)

4) RADICE → NO $\quad$ ESEMPIO $\sqrt{\frac{2}{3}} = \frac{\sqrt{2}}{\sqrt{3}} \notin \mathbb{Q}$ PERCHÉ $\sqrt{2}, \sqrt{3} \notin \mathbb{Z}$

* DAL PUNTO DI VISTA PRATICO SI PUÒ PENSARE AI NR. RAZIONALI COME A FRAZIONI, MA IN REALTÀ SONO CLASSI DI EQUIVALENZA

5 NUMERI COMPLESSI $\to \mathbb{C}$

$\hookrightarrow$ UN NUMERO COMPLESSO È UN OGGETTO DELLA FORMA $a+ib$, CON $a, b \in \mathbb{R}$.

$\mathbb{C} = \{$ NUMERI COMPLESSI $\} = \{ z = a+ib : a, b \in \mathbb{R} \}$

OPERAZIONI SU $\mathbb{C}$

SIANO $\begin{cases} z_1 = a_1 + ib_1 \\ z_2 = a_2 + ib_2 \end{cases}$

1) SOMMA E SOTTRAZIONE $z_1 \pm z_2 = (a_1 \pm a_2) + i(b_1 \pm b_2)$

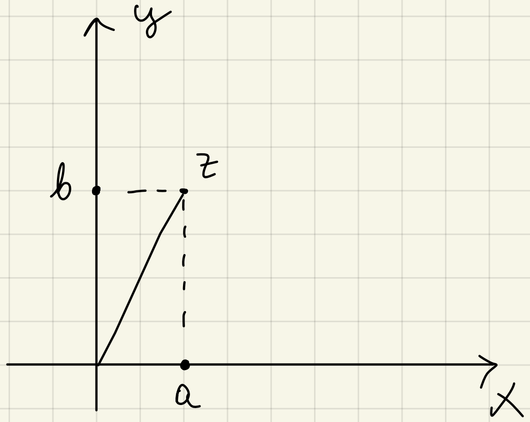
2) MOLTIPLICAZIONE $z_1 \cdot z_2 = a_1 a_2 + i(a_1 b_2 + a_2 b_1) - b_1 b_2$

$\hookrightarrow$ REGOLA STANDARD DEL PRODOTTO DI BINARI CON LA PARTICOLARITÀ CHE $i^2 = -1$

3) $|z_1| := \sqrt{a_1^2 + b_1^2}$ $\to$ MODULO DI UN NR. COMPLESSO

4) CONIUGATO DI z_1 $\to$ $\bar{z}_1 := a_1 - ib_1$

INTERPRETAZIONE GEOMETRICA DEI NR. COMPLESSI



$z = a + ib$

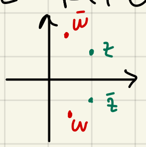
- POSSIAMO VEDERE z COME IL VETTORE $P = (a, b)$

OSSERVAZIONI

1) $|z| = \|P\|$

2) $z = a+ib \Rightarrow |z|^2 = z \cdot \bar{z}$; INFATTI $z \cdot \bar{z} = (a+ib)(a-ib) = a^2 + b^2$

3) $\bar{z}$ È IL RIFLESSO DI z RISPETTO ALL'ASSE DELLE X

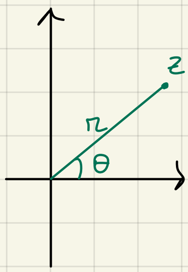


4) $z = a + ib \Rightarrow \frac{1}{z} = \frac{1}{a+ib} = \frac{a-ib}{(a+ib)(a-ib)} = \frac{a-ib}{a^2+b^2} = \frac{\bar{z}}{z^2}$

OSS: $\frac{1}{i} = -i$

5) FORMA TRIGONOMETRICA DEI NUMERI COMPLESSI.

USANDO TAYLOR SI VEDE CHE $\boxed{e^{i\theta} = \cos\theta + i\sin\theta \quad (\theta \in \mathbb{R})}$



$z = a + ib$

$z = r\cos\theta + i\, r\sin\theta \Rightarrow z = re^{i\theta}$

$r = |z|$

$\theta = \arctan \frac{b}{a}$

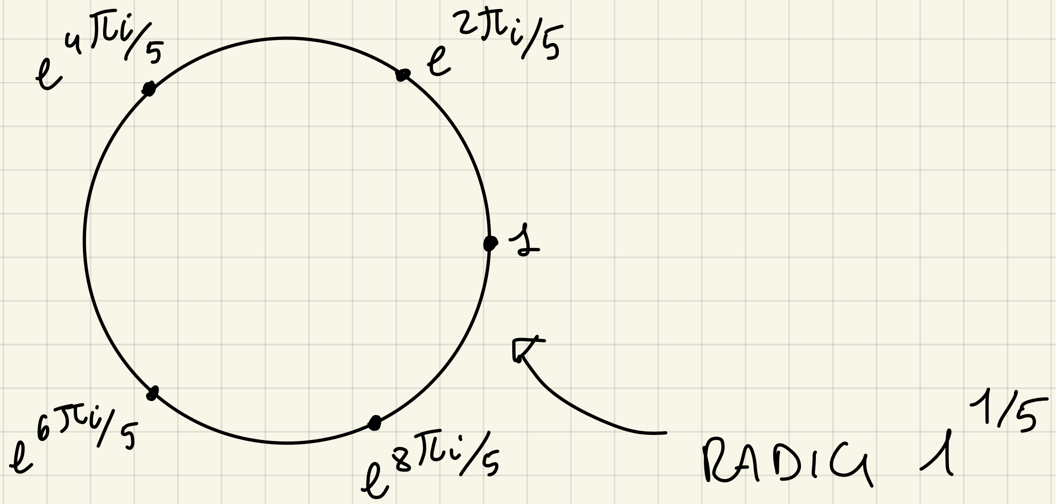
OSS: $r, \theta \in \mathbb{R}$ (COME, ANCHE, a E b)

6) RADICI DEI NUMERI COMPLESSI

$\sqrt[n]{z} = z^{1/n}$ = TUTTI I NUMERI COMPLESSI CHE ELEVATI ALLA n FANNO z.

SE $z = re^{i\theta}$, $z^{1/n} = \{ r^{1/n} \cdot e^{i\theta/n}, r^{1/n} \cdot e^{i(\frac{\theta}{n} + \frac{2\pi}{n})}, r^{1/n} e^{i(\theta/n + \frac{4\pi}{n})}, \ldots, r^{1/n} e^{i(\theta/n + \frac{n-1}{n})} \}$

ESEMPIO: LE RADICI n-ESIME DI 1 SONO I VERTICI DI UN POLIGONO REGOLARE CON n LATI.

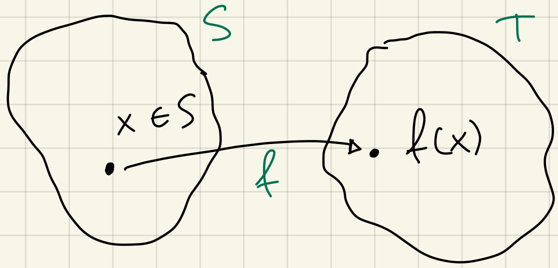


APPLICAZIONI E FUNZIONI

DEF → DATI DUE INSIEMI S, T; UNA <u>FUNZIONE O APPLICAZIONE</u> $f: S \to T$ ASSOCIA AD OGNI ELEMENTO x DI S UNO ED UNO SOLO ELEMENTO $f(x)$ DI T.

<u>S SI DICE DOMINIO DI f.</u>

<u>T SI DICE CODOMINIO DI f</u>



- POSSIAMO SCRIVERE $f(x) = t$ OPPURE $f: x \mapsto t$. E QUINDI DIRE CHE t È L'IMMAGINE DI x, OVVERO CHE t È IL VALORE DI f IN x, OVVERO CHE f MANDA x IN t.

- DUE APPLICAZIONI f E g SI DICONO UGUALI SE HANNO LO STESSO DOMINIO S, LO STESSO CODOMINIO E $\forall x \in S$ $f(x) = g(x)$

- L'APPLICAZIONE IDENTITÀ (Id_X) SU UN INSIEME X È QUELLA CHE AD OGNI x IN X ASSOCIA A SE STESSO, OVVERO $Id_X : X \to X$.

$$Id_X(x) = x \quad \forall x \in X \quad (\text{o } Id_X : x \mapsto x)$$

ESEMPIO: • $f: \mathbb{R} \to \mathbb{R}$, $x \mapsto 2x+5$ OVVERO $f(x) = 2x+5$

$Id_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$, $x \mapsto x$.

* f: INSIEME DEGLI ESSERI UMANI $\to \mathbb{N}$

AD OGNI PERSONA ASSOCIA IL NR. DI ANNI COMPIUTI

DEF → SIA $f: S \to T$ UNA APPLICAZIONE.

- SE $U \subseteq S$, DEFINIAMO $f(U) := \{ t \in T \mid \exists\, x \in U \text{ con } f(x) = t \}$ E LO CHIAMIAMO <u>IMMAGINE DI U SECONDO f</u>.

  IN PARTICOLARE CHIAMIAMO $\mathrm{Im} f := f(x)$ L'IMMAGINE DI f.

- SE $V \subseteq T$, DEFINIAMO $f^{-1}(V) = \{ x \in S \mid f(x) \in V \} \subset S$ E LO CHIAMIAMO <u>CONTROIMMAGINE DI V SECONDO f</u>

  IN PARTICOLARE SI HA $f^{-1}(T) = S$

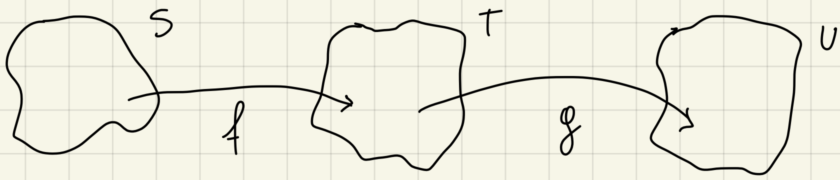
DEF → SIA $f: S \to T$ UNA APPLICAZIONE

1) DIREMO CHE f È SURIETTIVA SE $f(S) = T$, CIOÈ $\forall t \in T, \exists x \in S$ CON $f(x) = t$

2) DIREMO CHE f È INIETTIVA SE $\forall x, u \in S$ CON $x \neq u$, VALE $f(x) \neq f(u)$, CIOÈ $\forall x, u \in S$ CON $f(x) = f(u)$, VALE $x = u$.

3) DIREMO CHE f È BIETTIVA SE È SIA SURIETTIVA CHE INIETTIVA.

COMPOSIZIONE

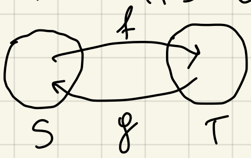


$$\underbrace{g \circ f}_{\downarrow} : S \to U$$
$$S \to g(f(S))$$

OCCHIO ALL'ORDINE

INVERSA

$f: S \to T$ È INVERTIBILE SE $\exists \; g: T \to S$ t.c. $g \circ f = Id_S$ E $f \circ g = Id_T$



. g SI DICE INVERSA DI f, OVVERO $g = f^{-1}$

PROPOSIZIONE → SIA $f: S \to T$.

1) f È INVERTIBILE
2) f È BIETTIVA
3) $\forall t \in T, \exists$ UNICO $x \in S$ CON $f(x) = t$

! OCCHIO A DOMINIO E CODOMINIO ! $f: \mathbb{R} \to \mathbb{R}^+$ $f(x) = x^2$ NON È INVERTIBILE MENTRE $f: \mathbb{R}^+ \to \mathbb{R}^+$ $f(x) = x^2$ LO È.

GRUPPI

OPERAZIONE → UNA OPERAZIONE SU UN INSIEME S È UNA FUNZIONE $f: S \times S \to S$. (PRENDE 2 ELEMENTI DI S E NE RESTITUISCE UN TERZO)

* GENERALMENTE SI INDICA CON $*$, MA ANCHE CON $+, \circ, \cdot, f(a,b)$

PROPRIETÀ:

1) ASSOCIATIVA → $(a * b) * c = a * (b * c)$
2) COMMUTATIVA → $a * b = b * a$
3) s È UN ELEMENTO NEUTRO SE $a * s = a$ E $s * a = a$

↳ SE QUESTO ELEMENTO ESISTE ⇒ È ELEMENTO UNICO E VERRÀ INDICATO CON 0 PER LE OPERAZIONI DI ADDIZIONE E CON 1 PER QUELLE DI MOLTIPLICAZIONE. (O IN ALCUNI CASI CON LA LETTERA e)

ELEMENTO INVERTIBILE → UN ELEMENTO $a \in S$ È DETTO INVERTIBILE SE ESISTE UN ELEMENTO, DETTO a^{-1} O INVERSO DI a t.c.

$$a * a^{-1} = a^{-1} * a = e$$

↳ ELEM. NEUTRO

NOTAZIONE → SE $*$ È UN'OPERAZIONE ASSOCIATIVA SULL'INSIEME S, CON ELEMENTO NEUTRO (INDICATO CON LA TERNA $(S, *, e)$), USEREMO LA NOTAZIONE DELLE POTENZE, OVVERO DEFINIAMO IN MODO RICORSIVO, $\forall a \in S$, $a^0 := e$, $a^1 = a$ E PER $n > 1$, $a^n := a^{n-1} = a * \dots * a$ n VOLTE.

GRUPPO → UN GRUPPO È UNA TERNA $(G, *, e)$ DOVE G È UN INSIEME, $*$ È UN'OPERAZIONE ASSOCIATIVA SU G CON ELEMENTO NEUTRO e, E t.c. OGNI ELEM. DI G HA UN INVERSO IN G.

ESEMPIO: 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 TRANNE CHE PER 0.

2) $(\mathbb{R}^*, \cdot, 1)$, $(\mathbb{C}^*, \cdot, 1)$, $(\mathbb{Q}^*, \cdot, 1)$ SONO GRUPPI, DOVE $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$

$(\mathbb{Z}^*, \cdot, 1) \Rightarrow$ NON È UN GRUPPO PERCHÉ NON CI SONO GLI INVERSI

3) $(\mathbb{R}^n, +, \underset{\text{MATRICE NULLA}}{0})$, $(\mathbb{C}^n, +, 0)$, $(\underset{\text{SIA SU C CHE SU R}}{M_{m\times n}}, +, 0)$

SONO GRUPPI

4) LE MATRICI INVERTIBILI (SIA SU R CHE SU C) SONO UN GRUPPO PER LA MOLTIPLICAZIONE CON LA MATRICE IDENTITÀ COME ELEMENTO NEUTRO.

L'INSIEME DELLE MATRICI INVERTIBILI $n\times n$ (SU $\mathbb{C}$ O $\mathbb{R}$) SI DENOTA CON $\boxed{GL(n,\mathbb{R}) \text{ o } GL(n,\mathbb{C})}$

$\downarrow$

QUINDI, IN FORMULE, $(GL(n,\mathbb{R}), \cdot, I)$ E $(GL(n,\mathbb{C}), \cdot, I)$ SONO GRUPPI PER OGNI n.

$\boxed{\text{OSS:}}$ SE DEFINIAMO M COME L'INSIEME DI TUTTE LE MATRICI SU $\mathbb{R}$ O $\mathbb{C}$, ALLORA $(M, +, 0)$ NON È UN GRUPPO PERCHÉ PER SOMMARE DUE MATRICI È NECESSARIO CHE ABBIANO LA STESSA DIMENSIONE.

SOTTOGRUPPO $\Rightarrow$ SIA $(G, *, e)$ UN GRUPPO; UN SOTTOGRUPPO H DI G È UN INSIEME $H \subset G$ t.c.:
1) $e \in H$
2) $\forall a, b \quad a*b \in H$
3) $\forall a \in H \quad a^{-1} \in H$

SE H È UN SOTTOGRUPPO DI G, SI SCRIVE $H < G \Rightarrow (\mathbb{Z}, +, 0) < (\mathbb{R}, +, 0)$

DEF NON FORMALE $\Rightarrow$ UN SOTTOGRUPPO È UN GRUPPO RISPETTO ALLA OPERAZIONE 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, CHE SIA CHIUSO RISPETTO ALL'OPERAZIONE E CHE CONTENGA GLI INVERSI.

ESEMPIO:
1) $(\mathbb{R}, +, 0)$ È SOTTOGRUPPO DI $(\mathbb{C}, +, 0)$
2) $(\mathbb{R}^*, \cdot, 1)$ È SOTTOGRUPPO DI $(\mathbb{C}^*, \cdot, 1)$
3) $(m\mathbb{Z}, +, 0)$ È SOTTOGRUPPO DI $(\mathbb{Z}, +, 0)$ $\Rightarrow m =$ MULTIPLO
4) MAT. DIAGONALI SONO SOTTOGRUPPO DI $(M_{m\times m}, +, 0)$
5) MAT. INVERTIBILI DIAG. SONO SOTTOGRUPPO DI $(M_{n\times n}, \cdot, I)$

GRUPPO ABELIANO → È UN GRUPPO IN CUI L'OPERAZIONE È ANCHE COMMUTATIVA

OSS → UN GRUPPO NON ABELIANO PUÒ AVERE SOTTOGRUPPI ABELIANI; AD ESEMPIO LE MAT. DIAGONALI INVERTIBILI SONO UN SOTTOGRUPPO ABELIANO DI $(GL(n), \cdot, I)$ CHE NON È ABELIANO.

$\boxed{* \text{ NB}}$ → UN GRUPPO È UNA TERNA $(G, *, e)$ E NON UN INSIEME. LA RAGIONE PER LA QUALE A VOLTE SCRIVIAMO SOLO G O H O $H < G$ È CHE PUÒ CAPITARE CHE $*$ ED e SIANO SOTTINTESI. AD ESEMPIO, $\mathbb{R}$ È SEMPRE $(\mathbb{R}, +, 0)$ E $\mathbb{R}^*$ È SEMPRE $(\mathbb{R}^*, \cdot, 1)$ / $(\mathbb{R}^*, +, 1)$.

GRUPPO FINITO → UN GRUPPO È FINITO SE HA UN NUMERO FINITO DI ELEMENTI.

LEGGE DI CANCELLAZIONE → $\forall\, a, b, c \in G$, SE $a * b = a * c \Rightarrow b = c$
SE $b * a = c * a \Rightarrow b = c$

DIMOSTRAZIONE → ! SIANO $a, b, c \in G$; SE $a * b = a * c \Rightarrow$
$\Rightarrow a^{-1} * (a * b) = a^{-1} * (a * c) \Rightarrow (a^{-1} * a) * b =$
$= (a^{-1} * a) * c \Rightarrow$ PER LA PROPRIETÀ DELL'INVERSO $\Rightarrow$
$\Rightarrow e * b = e * c \Rightarrow$ PER LA PROPR. DELL'ELEM. NEUTRO
$\Rightarrow b = c$.

(*) PER LE MATRICI VALE SOLO SE UNA DELLE MATRICI È INVERTIBILE.

↳ $AB = AC$ → NON POSSO SEMPLIFICARE A.

↳ MA SE A È INVERTIBILE ⇒ POSSO FARE $BA = AC$ E PER LE PROPRIETÀ DELLE MATRICI POSSO SEMPLIFICARE A.

GRUPPO DELLE PERMUTAZIONI (O SIMMETRICO)

↳ È UN ESEMPIO DI GRUPPO FINITO E CI SERVE ANCHE PER PARLARE DI TAVOLA DI MOLTIPLICAZIONE

S_n → GRUPPO DELLE PERMUTAZIONI SU n ELEMENTI. $S_n = \{Aut(T)\}$ DOVE T È UN INSIEME CON n ELEMENTI, CHE INDICHIAMO CON LE CIFRE DA 1 A n E $Aut(T)$ = AUTOMORFISMI DI T.

ESEMPIO: 1) $T = \{1, 2\}$ → $S_2 = \{\overset{Id}{(1, 2)}; (2, 1)\}$ $\left.\begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 1 \end{array}\right\}$ IN BASE ALL'Id

2) $T = \{1, 2, 3\}$ → $S_3 = \{\overset{Id}{(1, 2, 3)}; (1, 3, 2); (2, 1, 3); (2, 3, 1); (3, 1, 2); (3, 2, 1)\}$

$\boxed{S_n}$ È UN GRUPPO CON L'OPERAZIONE DI COMPOSIZIONE ED ELEM. NEUTRO (Id), OVVERO LA PERMUTAZIONE CHE MANDA OGNI ELEMENTO IN SÈ

TAVOLE DI MOLTIPLICAZIONE

→ PER I GRUPPI FINITI POSSIAMO SINTETIZZARE TUTTE LE OPERAZIONI IN UNA TABELLA.

	Id	p
Id	Id	p
p	p	Id

← ESEMPIO ←

	(1,2)	(2,1)
(1,2)	(1,2)	(2,1)
(2,1)	(2,1)	(1,2)

CHE INFO MI DA LA TAVOLA DI MOLTIPLICAZIONE?

1) MI DICE SE IL GRUPPO È ABELIANO O SE CONTIENE SOTTOGRUPPI ABELIANI → INFATTI È ABELIANO ⟺ LA TAVOLA DI MOLTIPLICAZIONI È UNA MATRICE SIMMETRICA. PER I SOTTOGRUPPI CERCO SOTTOMATRICI SIMMETRICHE, MA STANDO ATTENTO AGLI INVERSI

2) MI FA TROVARE SUBITO L'INVERSO DI UN NUMERO → BASTA ANDARE A VEDERE CON QUALE ELEMENTO DEVO COMPORRE PER OTTENERE Id

3) POSSO DEFINIRE UN GRUPPO TRAMITE UNA TAVOLA DI MOLTIPLICAZIONE

$\boxed{\text{ES:}}$ 4 ELEMENTI (e, b, c, d)

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

→ OSS: • È ABELIANO PERCHÉ È SIMM.

• COME FACCIO A CAPIRE SE È UN GRUPPO?

① DEVE ESSERCI UN ELEM. NEUTRO, OVVERO UNA RIGA E UNA COLONNA IDENTICA AGLI ELEMENTI

② IN OGNI RIGA E IN OGNI COLONNA DEVE APPARIRE L'ELEMENTO NEUTRO

GRUPPI DI MATRICI

→ SOLO 2 OPERAZIONI POSSIBILI:
1) + CON ELEM. NEUTRO 0
2) · CON ELEM. NEUTRO Id (SOLO X MAT $n \times n$)

CAMPO

→ UN CAMPO È UN GRUPPO ABELIANO CON UN'OP. AGGIUNTIVA • CHE SODDISFA DETERMINATE PROPRIETÀ.

$(F, +, \cdot, 0, 1)$ È UN CAMPO SE:

1. $(F, +, 0)$ È UN GRUPPO ABELIANO
2. $(F^*, \cdot, 1)$ È UN GRUPPO ABELIANO ← $F^* = F \setminus \{0\}$
3. $\forall a, b, c \in F$ $\underbrace{(a+b)c = ac+bc}_{\text{PROPRIETÀ DISTRIBUTIVA}}$

CAMPI CON UN NR ∞ DI ELEMENTI:

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. ($GL(n, \mathbb{R})$ NON È CAMPO MA SOLO "ANELLO")

I GRUPPI DI MATRICI NON HANNO MAI LA STRUTTURA DI CAMPO PERCHÉ IL PRODOTTO TRA MATRICI NON È COMMUTATIVO

CAMPI CON UN NR FINITO DI ELEMENTI: $\mathbb{Z}_p$

(*) NON CONFONDERE CON $p\mathbb{Z}$ (CIOÈ p COME MULTIPLO DI $\mathbb{Z}$)

I CAMPI CON NR FINITO DI ELEMENTI LO DEFINIAMO MEDIANTE LE CONGRUENZE

↳ SIA $n \in \mathbb{N}$, $n \neq 0$ FISSATO, E SIANO $a, b \in \mathbb{Z}$. DIREMO CHE a È CONGRUO A b MODULO n, E SCRIVIAMO:

$$a \equiv b \mod n$$

SE $b-a$ È MULTIPLO DI n, CIOÈ SE $b = a+nk$, $k \in \mathbb{Z}$.

LA CLASSE DI CONGRUENZA DI $a \in \mathbb{Z}$ $(\bar{a})$ È L'INSIEME DI TUTTI GLI INTERI CONGRUENTI AD a:

$$\bar{a} = \{\dots, a-2n, a-n, a, a+n, a+2n, \dots\}$$

OSSERVIAMO, QUINDI, CHE ESISTONO n CLASSI DI CONGRUENZA MODULO n: $\underbrace{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}}$.

↳ QUESTO INSIEME SI DENOTA COME $\frac{\mathbb{Z}}{n\mathbb{Z}}$, OVVERO $\mathbb{Z}_n$.

(*) DIRE CHE DUE ELEMENTI a, b SONO UGUALI IN $\mathbb{Z}_n$ SIGNIFICA CHE $a \equiv b \mod n$

OSS → IN $\mathbb{Z}_n$ LE OP. DI SOMMA E PRODOTTO.

- $\bar{a} + \bar{b} = \overline{a+b}$ → OGNI ELEMENTO DI $\mathbb{Z}_n$ HA INVERSO, COME ACCADE ANCHE IN $\mathbb{Z}$
- $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$ → NON TUTTI GLI ELEMENTI HANNO UN INVERSO, A DIFFERENZA DI $\mathbb{Z}$.

TEOREMA → SE p È UN NUMERO PRIMO ⇒ OGNI ELEMENTO NON NULLO ($\neq \bar{0}$) HA INVERSO IN $\mathbb{Z}_p$, PERCIÒ $(\mathbb{Z}_p, +, \bar{0}, \bar{1})$ È UN CAMPO FORMATO DA p ELEMENTI.

OMOMORFISMO (DEF) → SIANO $(G, *, e)$ E $(G', *', e')$ DUE GRUPPI. UN OMOMORFISMO $\varphi : G \to G'$ È UNA APPLICAZIONE CHE RISPETTA LA STRUTTURA DI GRUPPO, OVVERO $\forall\, a, b \in G \quad \varphi(a) *' \varphi(b) = \varphi(a * b)$

ISOMORFISMO (DEF) → UN OMOMORFISMO $\varphi : G \to G'$ È UN ISOMORFISMO SE È INVERTIBILE, OVVERO INIETTIVO E SURIETTIVO

! * SE $\varphi : G \to G'$ È INIETTIVO MA NON SURIETTIVO ⇒ φ È UN ISOMORFISMO TRA G E $\varphi(G) < G'$

AUTOMORFISMO (DEF) → UN ISOMORFISMO DA UN GRUPPO G IN SÈ STESSO SI CHIAMA AUTOMORFISMO

ESEMPIO: $\varphi : \mathbb{Z} \to \mathbb{Z}$ $\quad k \to 7k$ È UN OMOMORFISMO LA CUI IMMAGINE È $7\mathbb{Z}$.

QUINDI $\varphi : \mathbb{Z} \to 7\mathbb{Z} \quad k \to 7k$ È UN ISOMORFISMO.

NUCLEO E IMMAGINE DI UN OMOMORFISMO

↳ SE $\varphi : G \to G'$ È UN OMOMORFISMO, IN PARTICOLARE È UNA APPLICAZIONE (FUNZIONE) QUINDI LA SUA IMMAGINE È LA SOLITA: ↳ $\boxed{\mathrm{Im}\,\varphi = \{ g' \in G' : \exists g,\ \varphi(g) = g' \}}$

IL CONCETTO DI NUCLEO (O KERNEL) DA CUI LA NOTAZIONE $\ker \varphi$ È PIÙ SOTTILE, MA LA DEF È PIÙ SEMPLICE: ↳ SE $\varphi : G \to G'$

$$\boxed{\ker \varphi = \{ g \in G \mid \varphi(g) = e' \}}$$

ELEMENTO NEUTRO

OSSERVAZIONI:

1) POICHÉ φ È UN OMOMORFISMO, $\varphi(e) = e'$ E ALLORA STA SEMPRE NEL KERNEL

2) SE φ È UN OMOMORFISMO, $\ker(\varphi) = \{e\}$, ALTRIMENTI AVREMMO $\exists\, g \in \ker(\varphi)$, $g \neq e$ MA $\varphi(g) = \varphi(e) = e'$ E QUINDI φ NON È INIETTIVA.

3) $\varphi : M_{n \times m}(\mathbb{R}) \to \mathbb{R}$

$A \mapsto \operatorname{tr} A$; $\operatorname{Im}\varphi = \mathbb{R}$; $\ker\varphi$ = MATRICI A $\operatorname{tr} = 0$

4) $\varphi : (GL_n(\mathbb{R}), \cdot, 1) \to (\mathbb{R}^*, \cdot, 1)$

$A \mapsto \det A$

$\ker\varphi$ = MATRICI CON $\det 1$

PROPOSIZIONE → SIANO $(G, *, e)$ E $(G', *', e')$ DUE GRUPPI, $\varphi : G \to G'$ OMOMORFISMO. ⇒

⇒ a) $\operatorname{Im}\varphi < G'$ b) $\ker\varphi < G$

DIMOSTRAZIONE (IMPORTANTE)

a) φ OMOM. ⇒ $\varphi(e) = e'$ ⇒ $e' \in \operatorname{Im} G$

SE $a', b' \in \varphi(G)$ DOBBIAMO MOSTRARE CHE $a' *' b' \in \varphi(G)$

MA $a' \in \varphi(G) \Leftrightarrow \exists\, a \in G,\ \varphi(a) = a'$
$b' \in \varphi(G) \Leftrightarrow \exists\, b \in G,\ \varphi(b) = b'$

POICHÉ φ È UN OMOM., $\varphi(a * b) = \varphi(a) *' \varphi(b) = a' * b'$ ⇒

⇒ $a' * b' \in \varphi(G)$ PERCHÉ $\varphi(a * b) = a' * b'$

b) $e \in \ker\varphi$ PERCHÉ φ OMOM. ⇒ $\varphi(e) = e'$.

SE $a, b \in \ker\varphi$, DOBBIAMO CONTROLLARE $a * b \in \ker\varphi$

MA $\underbrace{\varphi(a * b) = \varphi(a) *' \varphi(b)}_{\text{PROPR. OMOM.}} \underbrace{= e' * e'}_{a,b \in \ker\varphi} = e'$ ⇒ $a * b \in \ker\varphi$

(DIFFERENZA TRA OPERAZIONI E APPLICAZIONI):
- OPERAZIONI → OP. NELLO STESSO INSIEME
- APPLICAZIONI → OP. TRA DUE INSIEMI DIVERSI

APPLICAZIONI LINEARI

DEFINIZIONE → UNA APPLICAZIONE $\mathcal{L}: \mathbb{R}^n \to \mathbb{R}^m$ SI DICE APPLICAZIONE LINEARE (O OPERATORE SE $n=m$) SE VALGONO LE SEGUENTI PROPRIETÀ:

- $\mathcal{L}(u+v) = \mathcal{L}(u) + \mathcal{L}(v) \quad \forall u, v \in \mathbb{R}^n$
- $\mathcal{L}(kv) = k\mathcal{L}(v) \quad \forall v \in \mathbb{R}^n, \forall k \in \mathbb{R}$

* SE $\mathcal{L}$ È UNA APPLICAZIONE LINEARE, $\mathcal{L}(0) = 0$ E
$\mathcal{L}(a_1 v_1 + \ldots + a_p v_p) = a_1 \mathcal{L}(v_1) + \ldots + a_p \mathcal{L}(v_p)$.

OSSERVAZIONE (IMPORTANTE)

↳ UNA APPLICAZIONE LINEARE $\mathcal{L}: \mathbb{R}^n \to \mathbb{R}^m$ È COMPLETAMENTE DETERMINATA DAI VALORI CHE ASSUME SU UNA BASE DEL DOMINIO:

↳ QUESTO SIGNIFICA CHE PER CONOSCERE L'IMMAGINE DI UN QUALSIASI VETTORE DI $\mathbb{R}^n$, MI BASTA CONOSCERE LE IMMAGINI DEGLI n VETTORI DI UNA BASE, E POI USARE LE DUE PROPRIETÀ CHE DEFINISCONO LA APPLICAZIONE LINEARE.

ESEMPIO → SIA $f: \mathbb{R}^2 \to \mathbb{R}^2$ UNA APPLICAZIONE LINEARE t.c. $f(1,0) = (2,0)$, $f(0,1) = (3,2)$. ALLORA $f(x,y)$ È DETERMINATO IN QUESTO MODO: $(x,y) = x(1,0) + y(0,1)$, DUNQUE:

$$f(x,y) = f(x(1,0) + y(0,1)) = f(x(1,0)) + f(y(0,1)) =$$
$$= xf(1,0) + yf(0,1) = x(2,0) + y(3,2) =$$
$$= \underline{(2x+3y, 2y)}$$

PROPOSIZIONE →
- LA SOMMA (E ANCHE LA COMBINAZIONE LINEARE) DI APPLICAZIONI LINEARI È UNA APPLICAZIONE LINEARE
- LA COMPOSTA DI APPLICAZIONI LINEARI È UNA APPLICAZIONE LINEARE
- L'INVERSA (QUANDO ESISTE) DI UNA APPLICAZIONE LINEARE È UNA APPLICAZIONE LINEARE.

SIANO $\mathcal{L}$ E $\mathcal{T}$, $\mathcal{H}$ E $\mathcal{G}$ APPLICAZIONI LINEARI E $k \in \mathbb{R}$. ALLORA:

1) $(\mathcal{G}+\mathcal{H}) \circ \mathcal{L} = \mathcal{G} \circ \mathcal{L} + \mathcal{H} \circ \mathcal{L}$

2) $\mathcal{H} \circ (\mathcal{L}+\mathcal{T}) = \mathcal{H} \circ \mathcal{L} + \mathcal{H} \circ \mathcal{T}$

3) $(k\mathcal{H}) \circ \mathcal{L} = k(\mathcal{H} \circ \mathcal{L}) = \mathcal{H} \circ (k\mathcal{L})$

OSS → SI POTREBBERO VEDERE LE APPLICAZIONI LINEARI COME SPAZIO VETTORIALE (SIA CON + CHE CON $\circ$) E LE APPLICAZIONI LINEARI INVERTIBILI COME GRUPPO RISPETTO ALLA COMPOSIZIONE.

APPLICAZIONE LINEARE → MATRICE → APPLICAZIONE LINEARE

↳ ① UNA MATRICE DEFINISCE UNA APPLICAZIONE LINEARE IN QUESTO MODO: ↳ SE $x = (x_1, \dots, x_n)^T \in \mathbb{R}^n \Rightarrow \mathcal{L}_A(x) := Ax$.

$\mathcal{L}_A$ È UNA APPLICAZIONE LINEARE A MOTIVO DELLE PROPRIETÀ DELLE MATRICI: INFATTI $\forall x, y \in \mathbb{R}^n$ E $\forall t \in \mathbb{R}$,

- $\mathcal{L}_A(x+y) = A(x+y) = Ax + Ay = \mathcal{L}_A(x) + \mathcal{L}_A(y)$
- $\mathcal{L}_A(tx) = A(tx) = tAx = t\mathcal{L}_A(x)$

→ OGNI APPLICAZIONE LINEARE $\mathcal{L} : \mathbb{R}^n \to \mathbb{R}^m$ INDIVIDUA UNA MATRICE $M_\mathcal{L}$ $m \times n$, DEFINITA DA ↳ $M_\mathcal{L} = (\mathcal{L}(e_1), \dots, \mathcal{L}(e_n))$

LE COLONNE DI $M_\mathcal{L}$ SONO FORMATE DALLE IMMAGINI TRAMITE $\mathcal{L}$ DEI VETTORI DELLA BASE CANONICA DI $\mathbb{R}^n$

NB → LE DUE COSTRUZIONI SONO COMPATIBILI, NEL SENSO CHE LA MATRICE ASSOCIATA A $\mathcal{L}_A$ È PROPRIO A, E L'APPLICAZIONE LINEARE ASSOCIATA A $M_\mathcal{L}$ È PROPRIO $\mathcal{L}$. INOLTRE, LA MATRICE ASSOCIATA A $\mathcal{L} \circ \mathcal{L}$ È PROPRIO $(M_\mathcal{L})^2$

ESEMPIO → SE $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$, $\mathcal{L}_A : \mathbb{R}^3 \to \mathbb{R}^2$ È DATTA DA

$$\mathcal{L}_A(x_1, x_2, x_3) = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 + 2x_2 + 3x_3 \\ 4x_1 + 5x_2 + 6x_3 \end{pmatrix}$$

SE $\mathcal{L}(x, y) = (2x, 2y, x-y)$, LA MATRICE ASSOCIATA È $M_\mathcal{L} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \\ 1 & -1 \end{pmatrix}$

NUCLEO E IMMAGINE DI UNA APPLICAZIONE

NUCLEO → SIA $\mathcal{L}: \mathbb{R}^n \to \mathbb{R}^m$ UNA APPLICAZIONE LINEARE, IL NUCLEO DI $\mathcal{L}$ È $\ker \mathcal{L} := \{ v \in \mathbb{R}^n \mid \mathcal{L}(v) = 0 \} = \mathcal{L}^{-1}(0)$

IL NUCLEO SONO I VETTORI IN $\mathbb{R}^n$ CHE VENGONO MAPPATI IN 0 ⇒

⇒ $\boxed{\ker \mathcal{L} \subset \mathbb{R}^n}$

IMMAGINE → SIA $\mathcal{L}: \mathbb{R}^n \to \mathbb{R}^m$ UNA APPLICAZIONE LINEARE, L'IMMAGINE DI $\mathcal{L}$ È $\operatorname{Im} \mathcal{L} = \{ v \in \mathbb{R}^m \mid \exists w \in \mathbb{R}^n, \ \mathcal{L}(w) = v \}$

L'IMMAGINE SONO I VETTORI CHE TROVO IN $\mathbb{R}^m$ APPLICANDO $\mathcal{L}$ A $\mathbb{R}^n$ ⇒ $\boxed{\operatorname{Im} \mathcal{L} \subset \mathbb{R}^m}$

PROPOSIZIONE → SIA $\mathcal{L}: \mathbb{R}^n \to \mathbb{R}^m$ L'APPLICAZIONE LINEARE ASSOCIATA ALLA MATRICE $A \in M_{m \times n}$. ALLORA:

1) $\operatorname{Sol}(A|0) = \ker \mathcal{L}$

2) $\operatorname{Im} \mathcal{L} = \mathcal{L}(\mathcal{L}(e_1), \dots, \mathcal{L}(e_n))$

3) IL NR. MASSIMO DI VETTORI LINEARMENTE INDIPENDENTI DI $\operatorname{Im} \mathcal{L}$ È UGUALE AL RANGO DI A, CIOÈ $\dim(\operatorname{Im} \mathcal{L}) = \operatorname{rg} A$

DIMOSTRAZIONI

1) $\operatorname{SOL}(A|0) = \{ x \in \mathbb{R}^n \mid Ax = 0 \} = \{ x \in \mathbb{R}^n \mid \mathcal{L}(x) = 0 \} = \ker \mathcal{L}$

2) SE $w \in \operatorname{Im} \mathcal{L} \Rightarrow \exists \, v \in \mathbb{R}^n$ CON $w = \mathcal{L}(v)$; MA $v = x_1 e_1 + \dots + x_n e_n$ E PERTANTO, $w = \mathcal{L}(x_1 e_1 + \dots + x_n e_n) = x_1 \mathcal{L}(e_1) + \dots + x_n \mathcal{L}(e_n)$, CIOÈ $w \in \mathcal{L}(\mathcal{L}(e_1), \dots, \mathcal{L}(e_n))$.

3) SE r È IL NUMERO MASSIMO DI VETTORI INDIPENDENTI FRA I VETTORI $\mathcal{L}(e_1), \dots, \mathcal{L}(e_n)$, OGNI VETTORE $\mathcal{L}(e_i)$ È COMBINAZIONE LINEARE DEGLI r VETTORI CHE COMPONGONO UN SOTTOINSIEME MASSIMALE DI VETTORI INDIPENDENTI.

POICHÉ OGNI VETTORE DELL'IMMAGINE È COMBINAZIONE LINEARE DI $\mathcal{L}(e_1), \dots, \mathcal{L}(e_n)$, ESSO È ANCHE COMBINAZIONE DEGLI r VETTORI DI UN INSIEME MASSIMALE.

ORA, IL NUMERO (MAX.) DI VETTORI LI FRA I VETTORI $\mathcal{L}(e_1), \dots, \mathcal{L}(e_n)$ COINCIDE CON IL NUMERO (MAX.) DI COLONNE LI DELLA MATRICE A. MA QUEST'ULTIMO NON È ALTRO CHE IL RANGO DI A.

PROPOSIZIONE → SIA $\mathcal{L}: \mathbb{R}^n \to \mathbb{R}^m$ UNA APPLICAZIONE LINEARE. LE SEGUENTI AFFERMAZIONI SONO EQUIVALENTI:

1) $\mathcal{L}$ È INIETTIVA
2) $\ker \mathcal{L} = \{ 0_{\mathbb{R}^n} \}$
3) $rg\, M_{\mathcal{L}} = n$

DIMOSTRAZIONE → SE $\mathcal{L}$ È INIETTIVA, SOLO IL VETTORE $0_{\mathbb{R}^n}$ VA IN $0_{\mathbb{R}^m}$, PERTANTO $\ker \mathcal{L} = \{0_{\mathbb{R}^n}\}$.

VICEVERSA, SUPPONIAMO CHE $\ker \mathcal{L} = \{ 0_{\mathbb{R}^n} \} \Rightarrow$
$\Rightarrow \mathcal{L}(v) = \mathcal{L}(w)$ IMPLICA $\mathcal{L}(v-w) = 0_{\mathbb{R}^m} \Leftrightarrow$
$\Leftrightarrow v - w \in \ker \mathcal{L} \Leftrightarrow v - w = 0_{\mathbb{R}^n} \Leftrightarrow v = w$.

NB. → UNA APPLICAZIONE LINEARE È SURIETTIVA SE E SOLO SE $rg\, M_{\mathcal{L}} = m$

DEFINIZIONE → UNA APPLICAZIONE LINEARE INVERTIBILE È DETTA ISOMORFISMO (INIETTIVA + SURIETTIVA) $\Leftrightarrow m = n = rg A_{\mathcal{L}}$

ESEMPIO:

1) $A_{\mathcal{L}} = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$ $\quad rg A = 3$

- INIETTIVA PER ROUCHÉ-CAPELLI
- SURIETTIVA PERCHÉ $\dim \operatorname{Im} A = rg A = \dim \mathbb{R}^3 = 3$

2) $A_{\mathcal{L}} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & 0 & 0 \end{pmatrix}$

- SURIETTIVA
- NON INIETTIVA → $\dim \ker = \dim Sol\, A|0 = 4 - rg A = 2$
  $\dim \operatorname{Im} = rg A = \dim \mathbb{R}^2 = 2$

3) $A_{\mathcal{L}} = \begin{pmatrix} 1 & -1 \\ 2 & 0 \\ 0 & 0 \end{pmatrix}$

- INIETTIVA
- NON SURIETTIVA → $\ker = Sol\,(A_{\mathcal{L}} | 0) \Rightarrow \dim \ker A_{\mathcal{L}} = 2 - rg A = 0$
  $\operatorname{Im} A_{\mathcal{L}} = \mathcal{L}\left\{ \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix} \right\}$ CHE SONO LI $\Rightarrow$
  $\Rightarrow \dim \operatorname{Im} A_{\mathcal{L}} = 2$

PROPOSIZIONE → SIA $\mathcal{L}: \mathbb{R}^n \to \mathbb{R}^n$ UN OPERATORE. ALLORA $\mathcal{L}$ È UN ISOMORFISMO $\Leftrightarrow \det M_{\mathcal{L}} \neq 0$

DIAGONALIZZAZIONE

CAMBIAMENTO DI BASE

$\hookrightarrow$ SIANO $B = (v_1, \dots, v_2)$ E $B' = (w_1, \dots, w_n)$ BASI IN $\mathbb{R}^n$. CHIAMEREMO MATRICE DEL CAMBIAMENTO DI BASE DA B A B' LA MATRICE $P = M(B, B') = (p_{ij})$ CHE HA COME j-ESIMA COLONNA LE COORDINATE DI w_j RISPETTO ALLA BASE B, E CIOÈ t.c. $w_j - \sum_{i=1}^{n} p_{ij} v_i$, $1 \leq j \leq n$. IN ALTRI TERMINI: $\hookrightarrow p^j = [w_j]_B$

ESEMPIO: SIANO $B = \left(v_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, v_2 = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right)$

$B' = \left(w_1 = \begin{pmatrix} -2 \\ 0 \end{pmatrix}, w_2 = \begin{pmatrix} 0 \\ 3 \end{pmatrix} \right)$ BASI DI $\mathbb{R}^2$.

ALLORA $\rightarrow$ • $w_1 = 2\begin{pmatrix} 0 \\ 1 \end{pmatrix} - 1\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ DA CUI $p_{11} = 2$, $p_{21} = -1$.

• $w_2 = 3\begin{pmatrix} 0 \\ 1 \end{pmatrix} + 0\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ DA CUI $p_{12} = 3$, $p_{22} = 0$

PERCIÒ $\rightarrow M(B, B') = \begin{pmatrix} 2 & 3 \\ -1 & 0 \end{pmatrix}$

* $\rightarrow$ ANALOGAMENTE SI CALCOLA $M(B', B) = \begin{pmatrix} 0 & -1 \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}$. SI OSSERVI CHE $\underline{M(B,B') \cdot M(B',B) = I_2}$.

$\hookrightarrow$ FATTO GENERALE

PROPOSIZIONE $\rightarrow$ SIANO $B = (v_1, \dots, v_n)$ E $B' = (w_1, \dots, w_n)$ BASI DI $\mathbb{R}^n$, ALLORA:

1) $M(B, B) = I_n$

2) $M(B, B')$ È UNA MATRICE INVERTIBILE, E LA SUA INVERSA È $M(B', B)$

3) SIANO $[v]_B$ E $[v]_{B'}$ I VETTORI DELLE COORDINATE DI v RISPETTO ALLA BASE B E B', RISPETTIVAMENTE, ALLORA: $\hookrightarrow$ $[v]_{B'} = M(B', B)\,[v]_B$

$[v]_B = M(B, B')\,[v]_{B'}$

AUTOVETTORE

$\rightarrow$ SIA T UN OPERATORE SU $\mathbb{R}^n$. UN VETTORE NON NULLO v DI $\mathbb{R}^n$ È DETTO AUTOVETTORE DI T SE ESISTE UN NUMERO REALE λ t.c. $T(v) = \lambda v$, CIOÈ SE T MANDA v IN UN SUO MULTIPLO

AUTOVALORE → UN NUMERO REALE λ È DETTO UN AUTOVALORE DI T SE ESISTE UN VETTORE $v \neq 0$ t.c. $T(v) = \lambda v$

AUTOSPAZIO → SE λ È UN AUTOVALORE DI T, CHIAMEREMO $\ker(T - \lambda id_{\mathbb{R}^n})$ L'AUTOSPAZIO DI λ E LO INDICHEREMO CON V_λ

PROPOSIZIONE → L'AUTOSPAZIO DI λ È FORMATO DAL VETTORE NULLO E DA TUTTI I VETTORI CHE HANNO λ COME AUTOVALORE

DIMOSTRAZIONE: L'AUTOSPAZIO DI λ È $\ker(T - \lambda id)$, A CUI APPARTIENE SICURAMENTE IL VETTORE NULLO. INOLTRE, → $\ker(T - \lambda id) = \{v \in \mathbb{R}^n \mid (T - \lambda id) \cdot (v) = 0\} = \{v \in \mathbb{R}^n \mid T(v) = \lambda id(v)\}$

E QUINDI CONTIENE COME VETTORI NON NULLI TUTTI E SOLO GLI AUTOVETTORI

POLINOMIO CARATTERISTICO → IL POLINOMIO CARATTERISTICO DI UNA MATRICE QUADRATA A È $p(t) := \det(A - tI)$.

CHIAMEREMO POLINOMIO CARATTERISTICO DELL'OPERATORE T QUELLO DELLA SUA MATRICE ASSOCIATA M_T

TEOREMA → SIA A LA MATRICE ASSOCIATA ALL'OPERATORE T, E SIA λ UN NUMERO REALE. ALLORA λ È UN AUTOVALORE DI T SE E SOLO SE È RADICE DEL POLINOMIO CARATTERISTICO DI A, CIOÈ $\det(A - \lambda I) = 0$

DIMOSTRAZIONE: UN NUMERO REALE λ È UN AUTOVALORE DI T SE E SOLO SE ESISTE UN VETTORE $v \neq 0$ t.c. $T(v) - \lambda v = 0$, OVVERO SE E SOLO SE C'È UN VETTORE NON NULLO IN $\ker(T - \lambda id)$.
SAPPIAMO (DAL CAP. 11) CHE QUESTO SUCCEDE SE E SOLO SE $\det(A - \lambda I) = 0$

DIAGONALIZZAZIONE → * SE A È SIMMETRICA ⇒ È DIAGONALIZZABILE

SIA T UN OPERATORE SU $\mathbb{R}^n$. T SI DICE DIAGONALIZZABILE SE $\mathbb{R}^n$ HA UNA BASE FORMATA DA AUTOVETTORI DI T. DUNQUE, SE $B = (v_1, \dots, v_n)$ È QUESTA BASE, ESISTONO DEI NUMERI $\lambda_1, \dots, \lambda_n$ PER CUI $T(v_1) = \lambda_1 v_1, \dots, T(v_n) = \lambda_n v_n$

Nota. Se $T = L_A$ è diagonalizzabile e $\mathcal{B} = (v_1, \dots, v_n)$ è una base di autovettori di T, consideriamo la matrice

$$P = \begin{pmatrix} \uparrow & & \uparrow \\ v_1 & & v_n \\ \downarrow & & \downarrow \end{pmatrix},$$

che è la matrice di passaggio dalla base canonica di $\mathbb{R}^n$ alle base di autovettori $\mathcal{B}$. Allora

$$\begin{aligned} AP &= \begin{pmatrix} \uparrow & & \uparrow \\ Av_1 & \dots & Av_n \\ \downarrow & & \downarrow \end{pmatrix} = \begin{pmatrix} \uparrow & & \uparrow \\ \lambda_1 v_1 & \dots & \lambda_n v_n \\ \downarrow & & \downarrow \end{pmatrix} \\ &= \begin{pmatrix} \uparrow & & \uparrow \\ v_1 & \dots & v_n \\ \downarrow & & \downarrow \end{pmatrix} \begin{pmatrix} \lambda_1 & & 0 \\ 0 & \ddots & 0 \\ 0 & & \lambda_n \end{pmatrix} = P \begin{pmatrix} \lambda_1 & & 0 \\ 0 & \ddots & 0 \\ 0 & & \lambda_n \end{pmatrix}. \end{aligned}$$

Quindi, se L_A è diagonalizzabile, esiste una matrice P invertibile tale che $P^{-1}AP$ sia diagonale; ricordando 13.2, $P^{-1}AP$ è la matrice diagonale degli autovalori $D = M(\mathcal{B}, \mathcal{C}) \cdot A \cdot M(\mathcal{C}, \mathcal{B})$. Diremo che la matrice D *rappresenta l'operatore L_A nella base $\mathcal{B}$*.

Vale anche il viceversa: se P è invertibile e $P^{-1}AP$ è diagonale, allora L_A è diagonalizzabile.

TEOREMA → SIA T UN OPERATORE SU $\mathbb{R}^n$ ⇒ ESISTE UNA BASE ORTONORMALE DI $\mathbb{R}^n$ COSTITUITA DA AUTOVETTORI DI T (E QUINDI T PUÒ ESSERE DIAGONALIZZATO IN BASE ORTONORMALE) SE E SOLO SE LA MATRICE M_T È SIMMETRICA

NOTA → DUE VETTORI NON NULLI DI V_0 E V_4 NON POSSONO ESSERE ORTOGONALI: $? \quad \langle \begin{pmatrix} -3k \\ k \end{pmatrix}, \begin{pmatrix} h \\ h \end{pmatrix} \rangle = -2kh$.