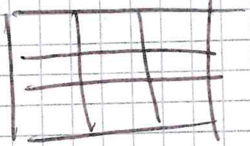
$\#(A \cup B) = \#A + \#B - \#(A \cap B)$

$$\binom{50}{3} + 50 \cdot \binom{50}{2}$$

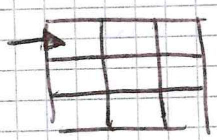
es: Coloro le caselle di bianco o nero



griglia 3·3

• Quante possibilità? 2^9 ⇒ ho 2 scelte per le 9 caselle.

• se ogni riga è colorata in modo diverso?



1ª riga 2^3 modi

2ª riga 2^3-1 modi

3ª riga 2^3-2 modi

$$2^3 \cdot (2^3-1)(2^3-2)$$

• Ciascuna (almeno) riga monocolore?

algebra lineare 9/05/2017.

il rango per riga = rango per colonna.

Rango: $L: V \to W$ lineare

Rango di L = dim (Imm L)

matrici:

A matrice $n \times k$ (in $\mathbb{R}$)

possiamo associargli un'applicazione lineare $L_A : \mathbb{R}^k \to \mathbb{R}^n$

$$L_A\begin{pmatrix}x_1\\ \vdots \\ x_k\end{pmatrix} = A\begin{pmatrix}x_1\\ \vdots \\ x_k\end{pmatrix}$$

moltiplicazione

applicazione della funzione al suo argomento.

Rango di L_A = dimensione dell'immagine di L_A

span delle colonne di A

$$L_A\begin{pmatrix}x_1\\ \vdots \\ x_k\end{pmatrix} = A\begin{pmatrix}x_1\\ \vdots \\ x_k\end{pmatrix} = x_1 \left|c_1\right| + \dots + x_k \left|c\right|$$

rango L_A = dim (span (colonne di A)) = rango della matrice

massimo numero di colonne indipendenti

per colonna.

Rango per riga di A = massimo numero di righe indipendenti

$\Vert$

dim (span (righe))

$\Downarrow$

Teorema: rango per riga = rango per colonna.

- mosse di colonna $\Rightarrow$ non cambia il rango di colonna
- mosse di riga $\Rightarrow$ non cambia il rango di riga

$\Downarrow$ $\Downarrow$

il rango non cambia per mosse di riga e colonna $\rightarrow$ cambiano sia Ker che Im ma non le loro dimensioni.

es:

$$A = \begin{pmatrix} 2 & 1 & 3 & 5 \\ 1 & -1 & 0 & 1 \\ 0 & -1 & -1 & -1 \end{pmatrix}$$ rango di A ?

- con matrice a scalini il rango = # di pivot.

$$\xrightarrow[R_1-2R_2]{} \begin{pmatrix} 0 & 3 & 3 & 3 \\ 1 & -1 & 0 & 1 \\ 0 & -1 & -1 & -1 \end{pmatrix} \xrightarrow[R_1+3R_3]{} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 1 \\ 0 & -1 & -1 & -1 \end{pmatrix}$$

con queste mosse non ho cambiato il Ker.

$$\xrightarrow{C_2+C_1} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & -1 & -1 & -1 \end{pmatrix} \xrightarrow[C_4-C_2]{C_3-C_2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

- Il rango è calcolabile anche con il determinante.

Se A $n \times n$ (quadrata) $\Rightarrow \det \neq 0$

$\Updownarrow$

$\mathrm{Ker} = \bar{0}$.

Per matrici quadrate

L_A è iniettiva $\Leftrightarrow$ L_A è surgettiva

$\Updownarrow$ $\Updownarrow$

$\mathrm{Ker}(A) = 0$ rango $A = n$

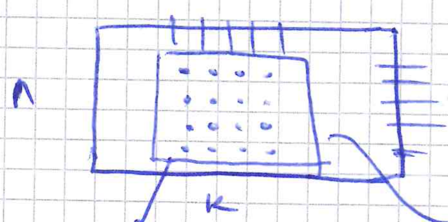
$\Rightarrow \mathrm{Ker}\, A = 0 \Leftrightarrow L_A$ biunivoca
$\Leftrightarrow L_A$ invertibile
$\Leftrightarrow A$ è invertibile

$\Bigg\} \Leftrightarrow \det(A) \neq 0$.

Per A $n \times n$

$\det A \neq 0 \Leftrightarrow$ Rango $= n$

• Matrici $n \times k$



det = ?

matrice quadrata ottenuta togliendo delle righe e delle colonne.

minore $m \times m$

$\downarrow$

trovo un $\det \neq 0$.

teorema*: Rango di A = massimo m tale che esiste un minore $m \times m$ con $\det \neq 0$.

$\boxed{\text{un minore può essere ottenuto prendendo numeri non contigui.}}$

es:

$$A = \begin{vmatrix} \lambda & 1 & 2 \\ 1 & -1 & 2\lambda \\ 1 & 0 & 1 \end{vmatrix}$$

considero il sistema

$$A\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 \\ 2\lambda \\ 1 \end{pmatrix}$$

• per quali λ il sistema ha soluzione?

- non è omogeneo $\Rightarrow$ sottospazio traslato.

2 metodi:

"classico" $\left(\begin{array}{ccc|c} \lambda & 1 & 2 & 2 \\ 1 & -1 & 2\lambda & 2\lambda \\ 1 & 0 & 1 & 1 \end{array}\right) \longrightarrow$ riduco a scalini

$\hookrightarrow$ e calcolo le soluzioni.

"imposto con i determinanti"

- ha soluzione se e solo se

$$\text{Rango } A = \text{rango}\left[A \middle| \begin{matrix} 2 \\ 2\lambda \\ 1 \end{matrix}\right]$$

teorema di Rouché - Capelli

il rango lo possiamo calcolare con i determinanti (mai riduco quindi a scalini).

Det(A) =

sviluppo rispetto della seconda colonna

$$\det\begin{vmatrix} \lambda & 1 & 2 \\ 1 & -1 & 2\lambda \\ \lambda & 0 & 1 \end{vmatrix} = 0 \qquad (-1)\det\begin{bmatrix} \lambda & 2 \\ 1 & 1 \end{bmatrix} - (1)\det\begin{vmatrix} 1 & 2\lambda \\ 1 & 1 \end{vmatrix}$$

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

$$= -\lambda + 2 + 2\lambda - 1 = \underline{\lambda + 1}$$

$$\text{Det}(A) = 0 \Rightarrow \lambda + 1 = 0$$

$\lambda = -1$ Se $\lambda \neq -1 \Rightarrow \text{Det} \neq 0$ quindi Rango$A = 3$ e il sistema ha soluzione

Se $\lambda \neq -1 \Rightarrow \det \neq 0$

allora c'è soluzione
- rango$A = 3$
- $\dim(A) = 3$ ← dim.
- matrice è invertibile → $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = A^{-1}\begin{vmatrix} 2 \\ 2\lambda \\ 1 \end{vmatrix}$
- $\text{rango}\left[A \middle| \begin{matrix} 2 \\ 2\lambda \\ 1 \end{matrix}\right] = 3$

caso in cui $\lambda = -1$.

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

matrice completa $\left(\begin{array}{ccc|c} -1 & 1 & 2 & 2 \\ 1 & -1 & -2 & -2 \\ 1 & 0 & 1 & 1 \end{array}\right)$

colonne identiche

rango A = Rango $\left(A \,\middle|\, \begin{matrix} 2 \\ -2 \\ 1 \end{matrix}\right)$

ha infinite soluzioni.

Rango $A \neq 3 \Rightarrow$ il $\det A = 0$

- considero un <u>minore</u> $\det = 1$ ← $1 \cdot 0 - (-1) \cdot 1$

rango $A = 2 = \dim(\text{Imm } A)$.

↳ $2 \times 2 \rightarrow$ minore

sono partita da una matrice 3×3 con $\det = 0$

⇓

"scalo" a minori 2×2 e cerco $\det \neq 0$.

- <u>le righe e le colonne che passano per il minore sono indipendenti.</u>

dimostrazione del Teorema*

① Sia B un minore $m \times m$ di A $(n \times k)$ con $\det B \neq 0$

$$\begin{array}{c} \quad m \\ n \quad \boxed{\quad \boxed{B} \; m \quad} \\ k \end{array}$$

⇓ da dimostrare.

rango $A \geq m$

visto che $\det(B) \neq 0 \Rightarrow$ le righe di B sono indipendenti. (anche le colonne)

$\Rightarrow$ le righe di A che passano per B sono indipendenti a loro volta.

⇓

rango per riga $A \geq m$.

es:
$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \text{ righe lunghe}$$

righe corte

Se le lunghe sono dipendenti $\Rightarrow \exists\, x, y, z \neq 0$

t.c. $x(a_{11}, a_{12}, a_{13}) +$
$y(a_{21}, a_{22}, a_{23}) +$
$z(a_{31}, a_{32}\ a_{33}) = (0,0,0)$

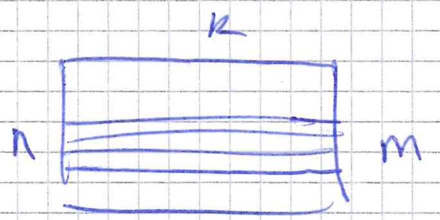
② Se il rango di $A \geq m \Rightarrow$ trovo un minore B $m \times m$ con $\det(B) \neq 0$.

- suppongo rango $A \geq m$

$\Downarrow$

ci sono m righe di A indipendenti

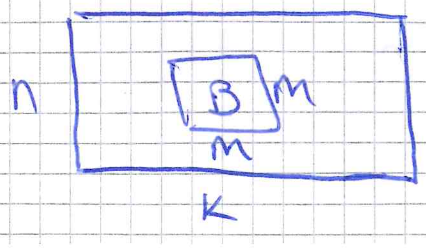
- estraggo la matrice con le righe m indipendenti $\Rightarrow$ $m \times k$



- la matrice estratta ha rango $= m$.
quindi ha anche m colonne indipendenti (per un Teorema)

ho ottenuto un minore $m \times m$ con m righe e m colonne ind. $\Rightarrow \det \neq 0$

Teorema degli orlati!



trovato un minore $m \times m$ con $\det(B) \neq 0$.

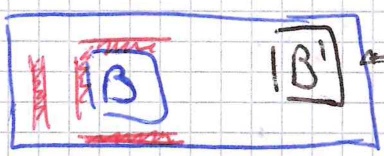
$\Rightarrow$ Rango $(A) \geq m$.

per sapere se è esattamente m
devo controllare tutti gli altri minori
$(m+1)\times(m+1)$ - $(m+2)\times(m+2)$...
hanno det $= 0$.
↑ approccio lungo.

il teorema mi dice che posso controllare
solo i minori che orlano B.

↓ tutte le volte aumento di 1 colonna
e di 1 riga a volta.

non importa andare a prendere un
minore $m \times m$ distribuito da un'altra
parte rispetto a B.



non imp.

AUTOVALORI E AUTOVETTORI e autospazi

$f: V \to W$ lineare , K = scalari

$\lambda \in K$ è un autovalore di f se

$\exists v \in V$ $v \neq 0$ t.c. $f(v) = \lambda v$ → cioè v non cambia direzione.
↓
v è un autovettore corrispondente / associato a λ.

$V_\lambda \subseteq V$ autospazio
sono tutti i vettori che vengono
allungati di un valore λ

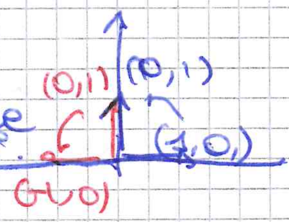
$$V_\lambda = \{ v \mid f(v) = \lambda v \}$$
↓
contiene anche lo $\{\bar{0}\}$ che non è
un autovettore.

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

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

$$f(x,y) = A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -y \\ x \end{pmatrix}$$

caso della matrice di rotazione di 90°.



non ci sono autovettori $\Rightarrow$ vengono tutti ruotati e nessuno viene allungato.

noi cerchiamo qualcosa del tipo:

$$f(x,y) = \lambda(x,y) = (\lambda x, \lambda y)$$

$\Downarrow$

$(-y, x)$ $\quad \begin{cases} -y = \lambda x \\ x = \lambda y \end{cases}$ $\quad -y = \lambda(\lambda y) = \lambda^2 y$

$\Downarrow$

$y = 0$

$\Downarrow$

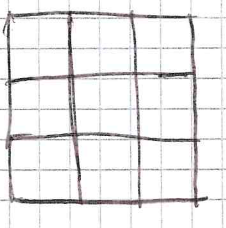
$x = \lambda y = 0$

l'unico $V_\lambda = \{\bar{0}\}$

quindi non ci sono autovettori.

matematica discreta 10/05/2017

es: almeno una riga monocolore?



↳ con complemento

$=$ tutte $-$ quelle che non hanno nessuna riga monocolore

tutte $= 2^9$

scelgo la 1ª riga $\#$modi $= 2^3 - 2$

2ª riga $\#$modi $= 2^3 - 2$

3ª riga $\#$modi $= 2^3 - 2$

moltiplico

$(2^3 - 2)^3$

risposta: $2^9 - (2^3 - 2)^3 = 296$

$= 216$

Da non fare:
- scelgo la riga monocolore — 3 modi
- coloro la riga — 2 "
- coloro le altre 2 righe — 2^6 modi

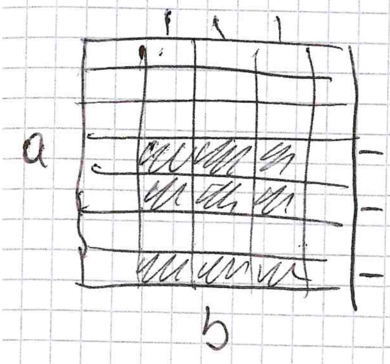
$$\Downarrow$$

$$3 \cdot 2 \cdot 2^6 \neq 296$$

conto 2 volte

o	o	o
x	x	x
x	o	x

es: In una matrice $a \times b$ quanti minori $k \times k$ esistono?



- $\emptyset$ se $k > a$, $k > b$
- se $k < a$ e $k < b$
  - devo scegliere k righe: # modi $\binom{a}{k} = \frac{a!}{k!(a-k)!}$
  - devo scegliere k colonne: # modi $\binom{b}{k} = \frac{b!}{k!(b-k)!}$

totale: $\binom{a}{k}\binom{b}{k}$

es: Se fisso un minore $(k-1) \times (k-1)$, quanti sono i minori $k \times k$ che orlano il precedente?

totale: $(a-(k-1)) \cdot (b-(k-1))$

es: Quante sono le funzioni da

$$f : [10] \longrightarrow [20]$$ che contengono

almeno un numero $n > 10$ nell'immagine?

$\Downarrow$

complemento: considero quelle che non contengono $n > 10$ nell'immagine?

$f(1) = ?$ 10
$f(2) = ?$ 10
⋮
$f(10) = ?$ 10 $= 10^{10}$

tutte sono: 20^{10}

$\Rightarrow 20^{10} - 10^{10}$

Quante sono quelle con esattamente un $n > 10$ nell'immagine.

soluzione errata: • scelgo quale numero >10 sta nell'immagine.
10 scelte.
• poi scelgo la x t.c. $f(x) = y$
ERRORE → 10 modi
non è detto che ci vada solo un elemento del dominio.
es: $f(x_1) = y$
$f(x_2) = y$ è possibile

soluzione:
• scelgo $y > 10$ ⟹ # modi 10
• riduco il codominio (cambio la funzione)

$f : [10] \to [10] \cup \{y\}$ con y nell'imm.

quante sono? risolvo con complemento
cerco quelle che non hanno y nell'immagine

tutte 11^{10}

$f(1) = ?$ 11 scelte
$f(2) = ?$ " "
⋮
$f(10) = ?$ " "

10^{10}

$f(1) = ?$ 10 scelte
$f(2) = ?$ " "
⋮
$f(10) = ?$ " "

soluzione $10(11^{10} - 10^{10})$.

es: ho 7 borse indistinguibili da dare a 7 persone.
Quanti modi?

quante ne posso dare alla prima?
• scelgo quante ne do alla 1ª 7 scelte.
alla 2ª BOH

viene fuori un albero molto irregolare:
ricordo che c'è un vincolo:

$a_1 = \#$ borse che do alla 1ª persona
$a_2 = \#$ " " " " 2ª "
$a_3 =$
$\vdots$
$a_7 = \#$ borse che do alla 7ª persona.

$0 \le a_1 \le 7$
$\vdots$
$0 \le a_7 \le 7$

$a_1 + a_2 + \dots + a_7 = 7$
Quante sono le settuple
$\langle a_1, a_2, \dots, a_7 \rangle$. $a_1 + \dots + a_7 = 7$
con $a_i \ge 0$

- associo a $\langle a_1, a_2, \dots, a_7 \rangle$
una stringa binaria fatta:

$$\underbrace{11..1}_{a_1}\ \overset{\text{sono le virgole}}{0}\ \underbrace{11..1}_{a_2}\ 0 \dots 0\ \underbrace{11..1}_{a_7}$$

$\langle 0, 1, 0, 5, 0, 1, 0 \rangle \leftrightarrow 0\,1\,0\,0\,1\,1\,1\,1\,1\,0\,0\,1\,0$ stringa binaria associata.

metto 0 1 nella stringa — metto un 1 nella stringa — metto 5 1 nella stringa

corrispondenza biunivoca

sono stringhe di lunghezza max 13 (7 uni e 6 virgole)
⇓
quante: $\binom{13}{7}$ → coefficiente usato qui anche se non parliamo di sottoinsiemi
↓
i decido dove mettere gli "1"
⇓
insieme di posizioni

Polinomi (sono nelle dispense Di Martino-Gaiffi capitolo 7).

<u>divisione con resto</u> (come in $\mathbb{Z}$)

$$\begin{array}{c|c} p(x) & b(x) \\ \hline r(x) & q(x) \end{array}$$

$\mathbb{Z}$
$$\begin{array}{c|c} a & b \\ \hline r & q \end{array}$$
→ il resto aveva una restrizione
$0 \le r < b$

$\mathbb{Z}[x]$ insieme di polinomi con scalari $\mathbb{Z}$

in $\mathbb{Z}[x]$ $r(x)$ ha sempre una restrizione:

$$\underbrace{deg}\,(r(x)) < \underbrace{deg}\,(b(x))$$

grado

es:

$$\begin{array}{r|l} x^4 - 4x^3 + 3x^2 + 14x + 26 & \overbrace{x^2 - 6x + 13}^{\text{moltiplico}} \quad \text{moltiplico} \\ \hline - \quad x^4 - 6x^3 + 13x^2 & x^2 + 2x + 2 \\ \hline / \quad 2x^3 - 10x^2 + 14x + 26 & \\ 2x^3 - 12x^2 + 26x & \\ \hline / \quad 2x^2 - 12x + 26 & \\ 2x^2 - 16x + 26 & \\ \hline / \quad / \quad / & \end{array}$$

sottraggo

sottraggo

grado di questo è maggiore di quello del divisore ⇓ continuo a dividere.

$\Rightarrow r(x) = 0$

$$\underbrace{x^4 - 4x^3 + 3x^2 + 14x + 26}_{\text{polinomio quindi riducibile}} = (x^2 - 6x + 13)(x^2 + 2x + 2) + 0$$

polinomio quindi, riducibile

es:

$$\begin{array}{r|l} x^2 + 1 & x \\ \hline x^2 & x \\ \hline 1 & \end{array} \Rightarrow x^2 + 1 = x \cdot x + 1$$

$r(x) =$ costante $\Rightarrow$ divido per un polinomio di grado 1.

Differenza tra stare nel campo e stare negli anelli

$b(x)$ è monico se il coefficiente di grado massimo è 1

$= x^3 + 3$ ✓ $\qquad = 3x^2 + 1$ ✗

- se il divisore è monico non c'è differenza se sto nel campo e nell'anello.

• se il divisore non è monico devo lavorare su un campo di coefficienti

es: $x^2+2x+3 \,|\, 3x+1$

$\frac{1}{3}x$

negli interi non è "permesso"

serve un campo per fare le divisioni.

$$
\begin{array}{l|l}
x^2+2x+3 & 3x+1 \\
\hline
x^2+\frac{1}{3}x & \frac{1}{3}x+\frac{5}{9} \\
\hline
/ \quad \frac{5}{3}x+3 & \\
\quad \frac{5}{3}x+\frac{5}{9} & \\
\hline
\qquad \frac{22}{9} &
\end{array}
$$

• se il divisore è monico non vengono fuori le frazioni.

teorema: per ogni $p(x), b(x) \in K[x]$ (K è un campo)

esiste $q(x), r(x)$ tale che

$$p(x) = b(x)q(x) + r(x)$$

con $\deg(r(x)) < \deg(b(x))$.

dimostrazione:

se $\deg(b(x)) > \deg(p(x))$,

$$
\begin{array}{l|l}
p(x) & b(x) \\
\hline
p(x) & 0
\end{array}
$$

$\Downarrow$

$$p(x) = b(x) \cdot \underset{q(x)}{0} + \underset{r(x)}{p(x)}$$

altrimenti:

$\deg(b(x)) \leq \deg(p(x))$

• $\exists\, k, r \in K$ tale che

$$r_1(x) = \underbrace{p(x) - r x^k b(x)}_{\deg < p(x)}$$

$k = \deg(p(x)) - \deg(b(x))$

$\deg[a(x) \cdot b(x)] =$
$= \deg(a(x)) + \deg(b(x))$

$$
\begin{array}{l|l}
p(x) & b(x) \\
\hline
r_1(x) & r x^k
\end{array}
$$

ora procedo per induzione sul grado del divisore.

Quindi posso supporre di saper fare

$$\begin{array}{r|l} r_1(x) & b(x) \\ \hline r(x) & q_1(x) \end{array} \Rightarrow \begin{array}{r|l} q(x) & b(x) \\ \hline r(x) & rx^k + q_1(x) \end{array}.$$

teorema $\quad a \in K \quad p(a)=0 \Rightarrow$ cioè a è una radice

$$(x-a) \mid p(x)$$

dimostrazione:

$$\begin{array}{r|l} p(x) & (x-a) \\ \hline r & q(x) \end{array}$$

costante

$$p(x) = (x-a)q(x) + r$$

sostituisco $x=a$

$$\underset{\underset{\text{per ipotesi}}{0}}{p(a)} = \underbrace{(a-a)\,q(a)}_{0} + r$$

$\Rightarrow 0 = r$

algebra lineare 10/05/2017

Autovettori e autovalori

$f: V \to V$ lineare

$\lambda \in K$ scalare $\quad V_\lambda = \{ v \in V \mid f(v) = \lambda v \}$

autospazio

Se $V_\lambda \neq \{\bar{0}\}$ (quindi contiene vettori diversi da $\emptyset$)

$\Rightarrow \lambda$ è un autovalore di f.

Gli elementi di $V_\lambda \neq \{\bar{0}\}$ sono autovettori

$$V_\lambda = \{\text{autovettori}\} \cup \{\bar{0}\}.$$

es: $\quad f: V \to V \qquad f(x,y) = (x+2y, -x+4y) \qquad V = \mathbb{R}^2$

- Cerco $\lambda \in \mathbb{R}$ e $v \neq \bar{0} \in V$

t.c.

$$\boxed{f(v) = \lambda v} \Rightarrow f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+2y \\ -x+4y \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \end{pmatrix}$$

$v = \begin{pmatrix} x \\ y \end{pmatrix}$

se $\begin{pmatrix} x \\ y \end{pmatrix} \in V_\lambda$

- prima trovo l'autospazio poi λ:

$$\begin{cases} x + 2y = \lambda x \\ -x + 4y = \lambda y \end{cases}$$ sistema ottenuto da $f(v) = \lambda v$.

$$\begin{cases} x(1-\lambda) + 2y = 0 \\ -x + y(4-\lambda) = 0 \end{cases}$$

· quale è la matrice di f rispetto alla base standard?

$V = \mathbb{R}^2$ $\quad \mathcal{E} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$

es: $v = \begin{pmatrix} 3 \\ 5 \end{pmatrix} \in V$ $\quad (v)_\mathcal{E} = \begin{pmatrix} 3 \\ 5 \end{pmatrix} \in \mathbb{R}^2$

$A = [f]^\mathcal{E}_\mathcal{E}$?

1ª colonna di $A = A\begin{pmatrix} 1 \\ 0 \end{pmatrix} = [f]^\mathcal{E}_\mathcal{E}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

2ª colonna di $A = A\begin{pmatrix} 0 \\ 1 \end{pmatrix} = [f]^\mathcal{E}_\mathcal{E}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$A = \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix}$

la matrice del sistema è:

abbiamo sottratto λ sulle diagonale =

$$\begin{pmatrix} 1-\lambda & 2 \\ -1 & 4-\lambda \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix} - \lambda \overbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}^{I}$$

matrice identità.

l'autospazio sono le x, y che risolvono il sistema

$\begin{pmatrix} x \\ y \end{pmatrix} \in V_\lambda \iff \begin{pmatrix} x \\ y \end{pmatrix}$ risolve il sistema

$\iff (A - \lambda I)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

$\iff \begin{pmatrix} x \\ y \end{pmatrix} \in \mathrm{Ker}(A - \lambda I)$

$V_\lambda = \mathrm{Ker}(A - \lambda I)$

$\hookrightarrow \neq 0$ quando il $\det(A - \lambda I) = 0$ (funzione non invertibile)

$$p(\lambda) = \det\begin{pmatrix} 1-\lambda & 2 \\ -1 & 4-\lambda \end{pmatrix} = (1-\lambda)(4-\lambda) + 2 = \lambda^2 - \lambda - 4\lambda + 2 + 4 =$$

$= \lambda^2 - 5\lambda + 6$

è sempre lo stesso anche con un'altra base. ← polinomio caratteristico della matrice A. → è il determinante

teorema

autovalore = radice di $p(\lambda)$

λ = autovalore $\iff p(\lambda) = 0$ (già dim.)

Polinomio caratteristico di A $= p(\lambda) = \det(A - \lambda I)$ ~~(per questo es)~~

$$\lambda = \frac{5 \pm \sqrt{25-24}}{2} = \frac{5 \pm 1}{2} \begin{cases} 3 = \lambda_1 \\ 2 = \lambda_2 \end{cases}$$ sono gli autovalori

$(x-3) \mid p(\ )$

$p(x) = (x-3)(x-2)$
$p(\lambda) = (\lambda-3)(\lambda-2)$

- cerco gli autospazi

$V_3 = \{ v \mid f(v) = 3v \} \Rightarrow (f - 3I)v = 0$
$V_2 = \{ v \mid f(v) = 2v \}$

$= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \middle| f\begin{pmatrix} x \\ y \end{pmatrix} = 3\begin{pmatrix} x \\ y \end{pmatrix} \right\}$

a livello di matrice:

$= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \middle| A\begin{pmatrix} x \\ y \end{pmatrix} = 3\begin{pmatrix} x \\ y \end{pmatrix} \right\} = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \middle| (A-3I)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}$

$\Rightarrow V_3 = \mathrm{Ker}(A - 3I)$

calcolo questo Ker:

$A - 3I = \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix} - \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} -2 & 2 \\ -1 & 1 \end{pmatrix}$

mosse di riga $\begin{pmatrix} -2 & 2 \\ 0 & 0 \end{pmatrix}$ $V_3 = \begin{pmatrix} y \\ y \end{pmatrix} = \mathrm{span}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$

y è libera

$v_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \rightarrow$ autovettore

$V_2 = \mathrm{Ker}(A - 2I)$ calcolo il Ker:

$A - 2I = \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix} - \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ -1 & 2 \end{pmatrix}$

mosse di riga $\begin{pmatrix} -1 & 2 \\ 0 & 0 \end{pmatrix}$ $V_2 = \begin{pmatrix} 2y \\ y \end{pmatrix} = \mathrm{span}\begin{pmatrix} 2 \\ 1 \end{pmatrix}$

$v_2 = \begin{pmatrix} 2 \\ 1 \end{pmatrix} \rightarrow$ autovettore.

essendo det = 0 avranno sempre righe dipendenti (se non lo fossero ci sarebbe un errore).

- ho trovato 2 autovalori diversi tra loro λ_1, λ_2

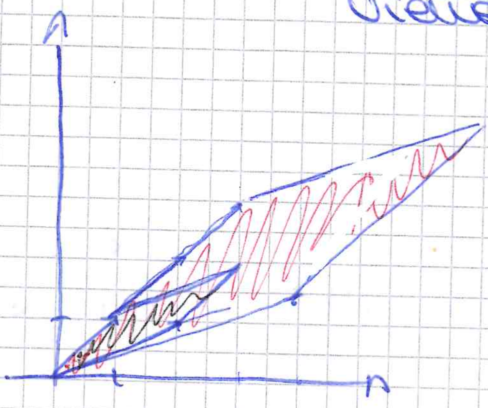
$$f\begin{pmatrix}2\\1\end{pmatrix} = \lambda_2\begin{pmatrix}2\\1\end{pmatrix} = \begin{pmatrix}4\\2\end{pmatrix} \text{ torna}$$

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

e 2 autovettori $\begin{pmatrix}1\\1\end{pmatrix}$ e $\begin{pmatrix}2\\1\end{pmatrix}$

vettore che viene triplicato

vettore che viene



$$f: V \to V \qquad \begin{pmatrix}x\\y\end{pmatrix} \mapsto \begin{pmatrix}x+2y\\-x+4y\end{pmatrix}$$

$$[f]^{\mathcal{E}}_{\mathcal{E}} = \begin{bmatrix}1 & 2\\-1 & 4\end{bmatrix}$$

ora cerco

matrice rispetto agli autovettori $\leftarrow [f]^{\{v_1, v_2\}}_{\{v_1, v_2\}} = D$ $\qquad \mathcal{B}$ = base di autovettori

↓ sono una base.

↓ la forma che rimetterà alla fine sarà molto semplice.

$$D = \left[D_1 \,\middle|\, D_2 \right]$$

$$D_1 = D\begin{pmatrix}1\\0\end{pmatrix} \qquad D = [f]^{\mathcal{B}}_{\mathcal{B}}(v_1)_{\mathcal{B}} \qquad v_1 = 1v_1 + 0v_2$$

$$(v_1)_{\mathcal{B}} = \begin{pmatrix}1\\0\end{pmatrix}$$

$$= (f v_1)_{\mathcal{B}}$$

⇓

esattamente $3v_1$

$$(f(v_1))_{\mathcal{B}} = \begin{pmatrix}3\\0\end{pmatrix} = D_1$$

$D_2 = \begin{pmatrix}0\\2\end{pmatrix} \to$ seconda colonna $[f]^{\mathcal{B}}_{\mathcal{B}}(v_2)_{\mathcal{B}} = (f v_2)_{\mathcal{B}} =$

$$= (2v_2)_{\mathcal{B}} = \begin{pmatrix}0\\2\end{pmatrix}$$

$$D = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

matrice diagonale con gli autovalori nella diagonale. (sempre per ogni matrice).

vantaggi: *

con matrici diagonali i conti sono più facili.

teorema:

$f: V \to V$ lineare $\qquad v$ autovettore $f(v) = \lambda v$

$\mathcal{B}$ base contenente v

$\mathcal{B} = \{v_1, v_2, \dots v_i, \dots, v_n\}$

$$[f]^{\mathcal{B}}_{\mathcal{B}} (v)_{\mathcal{B}} = [f]^{\mathcal{B}}_{\mathcal{B}} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \to \text{i-esima posizione} = \text{ottengo la i-esima colonna di } [f]^{\mathcal{B}}_{\mathcal{B}}$$

$$= (fv)_{\mathcal{B}} = (\lambda v)_{\mathcal{B}} = \begin{pmatrix} 0 \\ \vdots \\ \lambda \\ \vdots \\ 0 \end{pmatrix} \to \text{i-esima posizione}$$

$$[f]^{\mathcal{B}}_{\mathcal{B}} = \begin{bmatrix} \ddots & 0 & \\ & \lambda & \\ & 0 & \ddots \end{bmatrix} \leftarrow \text{quando abbiamo } \underline{\text{un}} \text{ solo autovettore}$$

↑ i-esima colonna

Se tutti gli v_i sono autovettori $f(v_i) = \lambda_i v_i$

$$\Rightarrow [f]^{\mathcal{B}}_{\mathcal{B}} = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & \lambda_n \end{bmatrix} \text{ matrice diagonale.}$$

* vantaggi:

$$\begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}^n = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \cdots \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} =$$

$$\to = \begin{pmatrix} 3^n & 0 \\ 0 & 2^n \end{pmatrix} \text{ senza troppi conti.}$$

in generale:

$$\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_k \end{pmatrix}^n = \begin{pmatrix} \lambda_1^n & & \\ & \ddots & \\ & & \lambda_k^n \end{pmatrix}$$

$[f]_{\mathcal{B}}^{\mathcal{B}} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \longrightarrow$ se ho una matrice di questo genere allora $\lambda_1, \dots, \lambda_n$ sono autovalori? **Sì**

$\mathcal{B} = \{v_1, \dots, v_n\}$

e $\{v_1, \dots, v_n\}$ sono autovettori? **Sì**

$f(v_1) = \lambda_1 v_1$

$\vdots$ per forza

$f(v_n) = \lambda_n v_n$

la matrice $\begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \lambda_1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

$[f]_{\mathcal{B}}^{\mathcal{B}} (v_1)_{\mathcal{B}} = (f v_1)_{\mathcal{B}}$

unica possibilità: $f(v_1) = \lambda_1 v_1$

• prendo $\mathcal{B} = \{v_1, v_2, v_3\}$ base di autovettori

$f: V \longrightarrow V$ $\quad f(v_i) = \lambda_i v_i \quad [f]_{\mathcal{B}}^{\mathcal{B}} = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}$

chi è $V_{\lambda_1} = ?$ $\quad$ es: $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{bmatrix}$

$= \{v \mid f(v) = 2v\} \ni v_1$

è tutto lo span(v_1)

es:

$[f]_{\mathcal{B}}^{\mathcal{B}} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix} \quad \mathcal{B} = \{v_1, v_2, v_3\}$

$V_2 = \{v \mid f(v) = 2v\} = \text{span}\{v_1, v_2\}$

$w = 5v_1 + 7v_2 \quad f(w) = f(5v_1 + 7v_2) =$

$= 5 f(v_1) + 7 f(v_2) =$

$= 5 \cdot 2v_1 + 7 \cdot 2v_2$

$= 2(5v_1 + 7v_2) = 2w$ ✓

combinazione lineare $\in V_\lambda$

es: $V=\mathbb{R}^2$ $\quad f: V \to V$

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

$\mathcal{E}$ = base standard $\left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right\}$

$$[f]^{\mathcal{E}}_{\mathcal{E}} = \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}$$

$$f\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}x+y\\x\end{pmatrix} = x\begin{pmatrix}1\\1\end{pmatrix} + y\begin{pmatrix}1\\0\end{pmatrix}$$

prendo $\begin{pmatrix}1\\0\end{pmatrix} \xrightarrow{f} \begin{pmatrix}1\\1\end{pmatrix} \xrightarrow{f} \begin{pmatrix}2\\1\end{pmatrix} \xrightarrow{f} \begin{pmatrix}3\\2\end{pmatrix}$

$\xrightarrow{f} \begin{pmatrix}5\\3\end{pmatrix} \xrightarrow{f} \begin{pmatrix}8\\5\end{pmatrix} \xrightarrow{f} \begin{pmatrix}13\\8\end{pmatrix} \xrightarrow{f}$ fibonacci

$$f^n\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}F_{n+1}\\F_n\end{pmatrix}$$

cerco gli autovettori

$\Uparrow$

cerco una base rispetto alla quale la matrice diventa diagonale

$$f\begin{pmatrix}F_{n+1}\\F_n\end{pmatrix} = \begin{pmatrix}F_{n+2}\\F_{n+1}\end{pmatrix}$$

$$\begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}^n \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}F_{n+1}\\F_n\end{pmatrix}$$

$\Downarrow$ si potesse diagonalizzare = tutto + facile.

$f: V \to V \quad V=\mathbb{R}^2 \quad f\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}x+y\\x\end{pmatrix}$

1) Polinomio caratteristico.

$$p_f(\lambda) = \det\underbrace{(A-\lambda I)} \Rightarrow \underbrace{\begin{pmatrix}1-\lambda & 1\\1 & -\lambda\end{pmatrix}}$$

$$\det\begin{pmatrix}1-\lambda & 1\\1 & -\lambda\end{pmatrix} = (1-\lambda)(-\lambda) - 1 = +\lambda^2 - \lambda - 1$$

$\lambda_1 = \frac{1+\sqrt5}{2} \qquad \lambda_2 = \frac{1-\sqrt5}{2} \qquad$ (zeri del $p_f(\lambda)$)

autovalori

calcolo dei autospazi

$$V_{\lambda_1} = \ker(A - \lambda_1 I) = \ker\begin{pmatrix} +1-\lambda_1 & 1 \\ 1 & -\lambda \end{pmatrix}$$

mosse di riga: $\cdot R_2 \cdot (1-\lambda_1) \rightarrow R_2 - R_1$

$$\begin{pmatrix} 1-\lambda_1 & 1 \\ 1-\lambda_1 & \underbrace{(-\lambda)(1-\lambda_1)}_{=1} \end{pmatrix} \Rightarrow R_1 = R_2$$

$$\rightarrow \begin{pmatrix} 1-\lambda_1 & 1 \\ 0 & 0 \end{pmatrix} \quad V_{\lambda_1} = \ker\begin{pmatrix} 1-\lambda_1 & 1 \\ 0 & 0 \end{pmatrix}$$

$$V_{\lambda_1} = \left\{ \begin{pmatrix} -\frac{y}{1-\lambda_1} \\ y \end{pmatrix} \middle| \, y \right\} = \mathrm{span}\begin{pmatrix} -\frac{1}{1-\lambda_1} \\ 1 \end{pmatrix} =$$

abbiamo che
$(-\lambda)(1-\lambda) - 1 = 0$
$1 - \lambda = \frac{1}{-\lambda}$
$(-\lambda)(1-\lambda) = 1$

$$= \mathrm{span}\begin{pmatrix} \lambda_1 \\ 1 \end{pmatrix}$$

$$V_{\lambda_2} = \mathrm{span}\begin{pmatrix} \lambda_2 \\ 1 \end{pmatrix}$$

autovettori:

$$v_1 = \begin{pmatrix} \lambda_1 \\ 1 \end{pmatrix} \qquad v_2 = \begin{pmatrix} \lambda_2 \\ 1 \end{pmatrix}$$

$\{v_1, v_2\} = \mathcal{B} \rightarrow$ base di autovettori

sono indipendenti $\qquad [f]_{\mathcal{B}}^{\mathcal{B}} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$

eravamo partiti da:

$f^n\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} \qquad [f]_{\varepsilon}^{\varepsilon} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = A$

$$[f]_{\mathcal{B}}^{\mathcal{B}} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} = D$$

$D = M^{-1} A M \qquad D^2 = \begin{pmatrix} \lambda_1^2 & 0 \\ 0 & \lambda_2^2 \end{pmatrix}$

$$D^2 = (M^{-1} A \cancel{M})(\cancel{M^{-1}} A M) = M^{-1} A^2 M$$

in generale $\quad D^n = M^{-1} A^n M.$

Matematica discreta 11/05/2017 (Teoria del corso appunti su discreta)

Polinomi:

$\mathbb{R}[x]$ $\mathbb{Z}/(p)[x]$ dato un polinomio

$$\begin{array}{r|l} p(x) & b(x) \\ \hline r(x) & q(x) \end{array}$$

dove $p(x) = b(x)q(x) + r(x)$
con $\deg(r(x)) < \deg(b(x))$

Quando lavoriamo negli anelli:
tutto funziona se $b(x)$ è monico.

Per sicurezza lavoriamo nei "campi"

K campo $a \in K$ $p(a) = 0 \Rightarrow (x-a) \mid p(x)$

dimostrazione:

prendo $p(x)$ lo divido

$$\begin{array}{r|l} p(x) & (x-a) \\ \hline r & q(x) \end{array}$$

coefficiente perché il suo grado deve essere minore di quello $x-a \Rightarrow$ è un numero.

$p(x) = (x-a)q(x) + r$
$\Downarrow$
$\underset{\overset{\shortparallel}{0}}{p(a)} = 0\,q(x) + r \Rightarrow r = 0$

Se ho una radice del polinomio $\Rightarrow p(x)$ è riducibile

il viceversa non è detto.

es: in $\mathbb{R}[x]$ $5x^2 + 5 = 5(x^2+1)$

non conta come riduzione $\rightarrow$ 5 è un'unità

in $\mathbb{Z}[x]$ lo considero riducibile

non conta perché esiste il suo inverso.

$p(x)$ è riducibile $\Leftrightarrow$ esistono a, b t.c.

$p(x) = a(x) b(x)$ con $a(x), b(x)$ non invertibili.

- Un oggetto a è invertibile se $\exists b$ t.c. $a \cdot b = 1$.
- In $\mathbb{R}[x]$ gli invertibili sono solo le costanti (diverse da $\emptyset$).

→ es. 5 è invertibile $5 \cdot \frac{1}{5} = 1$

A anello K campo

per entrambi:

un polinomio $p(x) \in A[x]$ di grado ≥ 1 non è mai invertibile.

↓

perché $p(x) q(x) = 1$

quindi

$\deg(p(x)) + \deg(q(x)) = 0 \Rightarrow p(x), q(x)$ sono costanti.

⇓

Gli unici invertibili possono essere le costanti $(\neq 0)$

↳ dipende, non sempre tutte.

L'esclusione degli invertibili è dovuta al fatto che sennò anche x^2+1 potrebbe essere ridotto come $\frac{1}{5}(5x^2+5)$

$p(x)$ è riducibile non è detto che ci sia una radice.

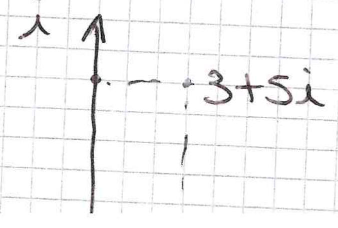
es: $\underbrace{(x^2+1)}_{\text{in } \mathbb{R} \text{ non ha radici}}(x^2+1) = \underbrace{x^4+2x^2+1}_{\text{riducibile ma non ha radici reali}}$

↓

in $\mathbb{C}$ sì perché $i = \sqrt{-1}$ $i^2 + = 0$

Numeri complessi:

possono disegnare in un piano (e non su una retta)



in generale

$a+bi$

somma tra numeri complessi

$$(a+bi)+(a'+b'i)=(a+a')+(b+b')i$$

moltiplicazione

$$(a+bi)(a'+b'i)=aa'+ab'i+a'bi-bb'=$$

$$i=\sqrt{-1} \Rightarrow i\cdot i=\sqrt{-1}\cdot\sqrt{-1}=-1$$

$$=\underbrace{(aa'-bb')}_{\text{parte reale}}+i\underbrace{(a'b+ab')}_{\text{parte immaginaria}}$$

Ogni polinomio ha una radice complessa $\Rightarrow$ motivo per cui sono stati inventati $\mathbb{C}$.

Proprio per il polinomio

$x^2+1 \Rightarrow$ così ha una radice pure lui

$x^2=-1$

$x=i$

l'inverso di i?

$(-i)\cdot i=1$

$\boxed{\mathbb{C} \Rightarrow \text{è un campo.}}$

$\Downarrow$

$\exists$ gli inversi (escluso lo $\emptyset$).

l'inverso di $a+bi$?

$$(a+bi)\underbrace{(c+di)}_{\text{quando lo trovo è } \frac{1}{a+bi}}=1$$

$$ac+adi+bci-db=1$$

$$ac-db+i(ad+bc)=1 \Rightarrow \begin{cases} ac-db=1 \\ ad+bc=0 \end{cases}$$

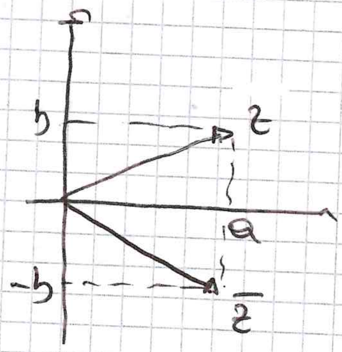
le incognite sono c, d

al punto del sistema possiamo adoperare un altro metodo per trovare l'inverso:

se $z = a+ib$

$\bar{z} = a-ib$ è detto coniugato

ribaltato rispetto all'asse x.



$z\cdot\bar{z} = (a+ib)(a-ib) = a^2+b^2$ lunghezza di z al quadrato.

$a^2+b^2 = |z|^2$ modulo del numero complesso. (al quadrato).

⇓ norma al quadrato.

quindi

$$z\left(\frac{\bar{z}}{|z|^2}\right) = 1$$

⇓

$$\cancel{(a+ib)}\left(\frac{a-ib}{\cancel{(a+ib)}(a-ib)}\right)$$

$$\frac{1}{z} = \frac{a-ib}{a^2+b^2}$$

$$\frac{1}{z} = \frac{a}{a^2+b^2} + i\left(\frac{b}{a^2+b^2}\right)$$

torniamo ai polinomi:

$p(x) = x^2+1$ $\quad p(i)=0$

⇓

$(x-i) \mid x^2+1 \Rightarrow x^2+1 = (x-i)(\quad)$

anche $-i$ è una radice

$(x+i)$

abbiamo usato "somma per differenza"

$$x^2+1 = x^2-(+i^2) = (x-i)(x+i).$$

Teorema fondamentale dell'algebra:

ogni $p(x) \in \mathbb{C}[x]$ non costante ha una radice. (no dim).

se $z \in \mathbb{C}$ $\quad z = \bar{z} \iff z \in \mathbb{R}$

in pratica non ha la parte immaginaria.

$\overline{z_1 z_2} = \bar{z}_1 \cdot \bar{z}_2$ e $\overline{z_1+z_2} = \bar{z}_1 + \bar{z}_2$

verifica per la moltiplicazione:

$$\overline{(a+ib)(c+di)} = \overline{(ac-bd)+i(ad+cb)} =$$

$$= (ac-bd)-i(ad+cb)$$

$=$

$$\overline{(a+ib)}\cdot\overline{(c+id)} = (a-ib)(c-id) =$$

$$= (ac-db)+i(-cb-ad)$$

i polinomi irriducibili sono gli equivalenti dei numeri primi.

Chi sono gli irriducibili in $\mathbb{C}[x]$?

Quelli di grado $=1$.

perché $\deg(p(x)) \geq 2 \Rightarrow \exists \alpha \in \mathbb{C}.\ p(\alpha)=0$

$$p(x) = (x-\alpha)\cdot g(x)$$

così compenso $\deg(p(x))$ con $g(x)$.

Chi sono gli irriducibili in $\mathbb{Z}$?

Sicuramente quelli di grado $=1$

poi x^2+1, x^3+4, $\vdots$ e i numeri primi $(1,2,3,5\ldots)$

Quali sono gli irriducibili in $\mathbb{R}[x]$?

ogni polinomio di grado ≥ 3 è riducibile.

dimostrazione:

in $\mathbb{C}[x]$ ogni $p(x)$ (grado n.) si scrive come prodotto del tipo $\alpha(x-\lambda_1)(x-\lambda_2)\ldots(x-\lambda_n)$

dove λ_i sono radici.

se $n=0 \Rightarrow$ c'è solo $\alpha\in\mathbb{C}$ caso base dell'induzione.

$p(x)=\alpha$

se $n>0 \Rightarrow \exists \lambda_1.\ p(\lambda_1)=0 \Rightarrow (x-\lambda_1) | p(x)$

trovato il primo fattore trovo anche gli altri.

$p(x) = (x-\lambda_1) \cdot g(x)$ dove $\deg(g(x)) < \deg(p(x))$

g per ipotesi induttiva (ho fatto induzione nel grado di p)

$g(x) = \alpha (x-\lambda_2) \cdots (x-\lambda_n) \to n-1$ fattori.

$\Downarrow$

$$p(x) = \alpha \underbrace{(x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_n)}_{\text{fattori primi irriducibili}}$$

in $\mathbb{R}[x]$

$p(x) \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$

se scomponiamo $p(x)$ in $\mathbb{C}[x]$ avremmo una certa scomposizione con $\alpha, \lambda_i \in \mathbb{C}$

$\lambda_1, \dots, \lambda_n$ sono radici complesse di $p(x)$

Se $\lambda \in \mathbb{C}$ con $p(\lambda) = 0$ una $p(x) \in \mathbb{R}[x]$

$\Downarrow$

$p(\bar{\lambda}) = 0$ coniugato di λ.

es:

x^2+1: i, $-i$ $\to$ esattamente coniugato di i.

quindi $p(\lambda) = 0 \Rightarrow \overline{p(\lambda)} = \bar{0} = 0$

$\overline{p(\lambda)} = p(\bar{\lambda}) = 0$

quindi tra $\lambda_1, \dots, \lambda_n$ ci sono radici coniugate due a due oppure ci può essere la radice reale che è la sua stessa coniugata.

$\Downarrow$

presa λ_i $\to$ o è reale
$\to$ o c'è tra le altre λ_i la sua coniugata.

$p(x) \in \mathbb{R}[x]$ può essere scritto come

$$p(x) = \alpha \underbrace{(x-r_1)\dots(x-r_k)(x-\lambda_1)(x-\bar{\lambda}_1)\dots}_{n \text{ termini}}$$

$\alpha \in \mathbb{R}$ (due a due)

i gruppi di λ_i complessi se moltiplicati risultano un polinomio reale di grado 2.

$$(x-\lambda)(x-\bar\lambda) = x^2 - x(\lambda+\bar\lambda) + \boxed{\lambda\bar\lambda} = |\lambda|^2$$

viene cancellata la parte immaginaria

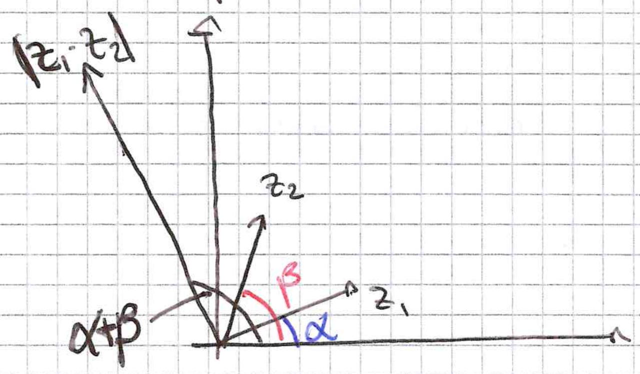
sarà $\mathbb{R}$.

$\lambda + \bar\lambda = 2a$

$p(x) \in \mathbb{R}[x]$ si possono fattorizzare con polinomi di grado 1 o 2 $\square$.

Interpretazione geometrica dei numeri complessi.

- moltiplicazione

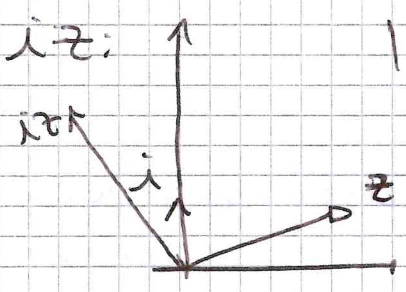


$z_1 \cdot z_2$

↳ si moltiplicano le lunghezze e si sommano gli angoli.

- addizione ⇒ funziona come vettori ⇒ regola del parallelogramma.

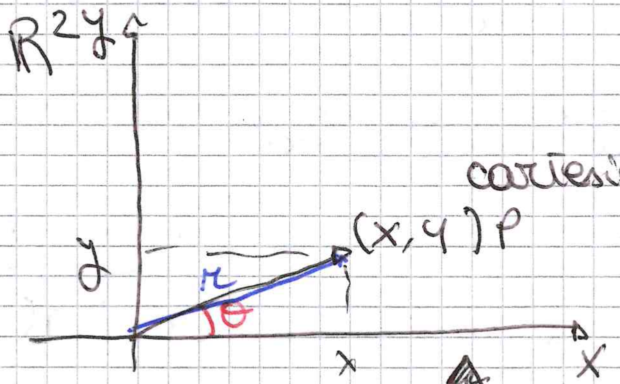
iz:



$|i| = 1$ $i \Rightarrow 90°$

fa ruotare z di $90°$ ⇒ gli angoli vengono sommati.

con le coordinate polari:



cartesiane

coordinate cartesiane.

(r, θ) coordinate polari corrispondenti ⇒ $(r\cos\theta, r\sin\theta)$

$r = \sqrt{x^2+y^2}$

$\theta = \tan^{-1}\left(\frac{y}{x}\right)$

P in C viene scritto come
$$P = r(\underbrace{\cos\theta + i\,\text{sen}\,\theta}_{e^{i\theta}})$$
$$= x + iy$$
$$e^{i\theta} = \cos\theta + i\,\text{sen}\,\theta$$
$$|e^{i\theta}| = 1$$
$$|re^{i\theta}| = r.$$
risulta facile la moltiplicazione:
$$(re^{i\theta})(r'e^{i\theta'}) = rr'e^{i(\theta+\theta')}$$

ALGEBRA lineare 16/05/2017

autovalori, autovettori.

$f: V \to V$ lineare $n = \dim(V)$ $\mathcal{B} = \{v_1, \dots, v_n\}$

f è diagonalizzabile se e solo se V ha una basi di autovettori di f.

$f(v_i) = \lambda_i v_i$

↑ autovalori

$$D = [f]^{\mathcal{B}}_{\mathcal{B}} = \begin{bmatrix} \lambda_1 & & 0 \\ & \lambda_2 & \\ & & \ddots \\ 0 & & & \lambda_n \end{bmatrix} \to \text{diagonale}$$

se scelgo un'altra base C ottengo un'altra matrice $A = [f]^{C}_{C}$

A e D si dicono matrici simili (cioè descrivono la stessa funzione ma con basi diverse).

↓ devono essere le stesse in partenza e in arrivo.

eorema: A, B matrici

A, B sono simili se e solo se $\exists M$ invertibile tale che $A = M^{-1}BM$

$\downarrow \times M$ a sinistra

$$MA = \cancel{MM^{-1}}BM \xrightarrow{\times M^{-1}\text{ destra}} MAM^{-1} = B$$

con $f: V \to V$ e

$$D = [f]^{B}_{B}$$

$$A = [f]^{standard}_{standard}$$

$\exists M$

$D = M^{-1}AM$

Per trovare M:

teorema:

Sia $f: V \to V$ endomorfismo (f lineare da V a V)

$n = \dim(V)$.

$B \Rightarrow$ base di autovettori $\{v_1, \dots, v_n\}$

con autovalori $\lambda_i \in K$

$$D = [f]^{B}_{B} = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix} \qquad A = [f]^{stand.}_{stand.}$$

$\exists M$ (invertibile) $n \times n$ t.c. $M^{-1}AM = D$

$A = MDM^{-1}$

matrice del cambio di base

$$M = \begin{pmatrix} | & | & | & \cdots & | \end{pmatrix}$$

coordinate di v_1 rispetto alla base canonica

coordinate di v_n rispetto alla base canonica

$M \to$ matrice che ha sulle colonne le coordinate degli autovettori rispetto alla base canonica.

dimostrazione:

$$\begin{tikzcd}
 & w \arrow[rr, bend left] & & w \\
V \arrow[r, "f"] \arrow[d, "E"] & V \arrow[rr, "id"] \arrow[d, "E"] & & V \arrow[d, "B"] \\
K^n \arrow[r, "{[f]^{E}_{E}}"] & K^n & &
\end{tikzcd}$$

associo ai vettori una ennupla di scalari

coordinate rispetto a E

$(v)_E$

$(w)_E$

$$\begin{tikzcd}
v \arrow[r, mapsto] & v \arrow[r, mapsto] & w \arrow[r, mapsto] & w \\
V \arrow[r, "id"] \arrow[d, "B"] & V \arrow[r, "f"] \arrow[d, "\mathcal{E}"] & V \arrow[r, "id"] \arrow[d, "\mathcal{E}"] & V \arrow[d, "B"] \\
K^n \arrow[r, "{M = [id]^B_{\mathcal{E}}}"] & K^n \arrow[r, "{A = [f]^{\mathcal{E}}_{\mathcal{E}}}"] & K^n \arrow[r, "{M^{-1} = [id]^{\mathcal{E}}_B}"] & K^n \\
(v)_B \arrow[rrr, bend right] & (v)_{\mathcal{E}} & (w)_{\mathcal{E}} & (w)_B
\end{tikzcd}$$

$$[f]^B_B = D$$

$$D = [f]^B_B = \underbrace{[id]^{\mathcal{E}}_B \, [f]^{\mathcal{E}}_{\mathcal{E}} \, [id]^B_{\mathcal{E}}} = M^{-1} A M$$

scritte al contrario perché
quando applico il vettore lo faccio a
destra ⇒ la prima matrice applicata
è quella più a destra

Es:

fibonacci $\quad f: \mathbb{R}^2 \to \mathbb{R}^2 \quad f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ x \end{pmatrix}$

$$[f]^{\mathcal{E}}_{\mathcal{E}} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = A$$

f è diagonalizzabile?

$$p_f(x) = p_A(x) = \det(A - \lambda I) =$$

polinomio caratteristico

$$= \det\left(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) =$$

$$= \det\begin{pmatrix} 1-\lambda & 1 \\ 1 & -\lambda \end{pmatrix} = (1-\lambda)(-\lambda) - 1 =$$

$$= \lambda^2 - \lambda - 1$$

autovalori = radici del polinomio caratteristico

$$\lambda_1 = \frac{1+\sqrt{5}}{2}, \quad \lambda_2 = \frac{1-\sqrt{5}}{2}$$

$$\Downarrow$$

$$D = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} = \begin{bmatrix} \frac{1+\sqrt{5}}{2} & 0 \\ 0 & \frac{1-\sqrt{5}}{2} \end{bmatrix}$$

D e A sono simili $\Rightarrow \exists M \ . \ M^{-1} A M = D$

Trovare M. 1) trovare gli autospazi

$$V_{\lambda_1} = \{ v \mid f(v) = \lambda_1 v \}$$

$$(V_{\lambda_1})_{\mathcal{E}} = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid \underbrace{A \begin{pmatrix} x \\ y \end{pmatrix} = \lambda_1 \begin{pmatrix} x \\ y \end{pmatrix}} \right\} =$$

$$A \begin{pmatrix} x \\ y \end{pmatrix} - \lambda_1 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\Updownarrow$$

$$(A - \lambda_1 I)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$= \operatorname{Ker}(A - \lambda_1 I) \Leftarrow$$

$$= \operatorname{span} \begin{pmatrix} \lambda_1 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} \lambda_1 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1+\sqrt{5}}{2} \\ 1 \end{pmatrix} \in V_{\lambda_1} \text{ e } \neq 0. \Rightarrow$$ coordinate del primo autovettore.

prima colonna di M.

$$V_{\lambda_2} = \{ v \mid f(v) = \lambda_2 v \} = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid A \begin{pmatrix} x \\ y \end{pmatrix} = \lambda_2 \begin{pmatrix} x \\ y \end{pmatrix} \right\}$$

$$= \operatorname{Ker}(A - \lambda_2 I) = \operatorname{span} \begin{pmatrix} \lambda_2 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} \lambda_2 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1-\sqrt{5}}{2} \\ 1 \end{pmatrix} \Rightarrow$$ coordinate del secondo autovettore.

secondo colonna di M

$$M = \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix} \qquad D = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = M^{-1} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} M$$

$M^{-1} = ?$ l'inversa di $M \Rightarrow 2$ modi

$$\left(\begin{array}{cc|cc} \lambda_1 & \lambda_2 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array} \right) \xrightarrow[\text{di riga}]{\text{mosse}} \left(\begin{array}{cc|c} 1 & 0 & \\ 0 & 1 & M^{-1} \end{array} \right)$$

essendo una matrice 2×2 abbiamo la formula:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{\det\begin{pmatrix} a & b \\ c & d \end{pmatrix}} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$\begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix}^{-1} = \frac{1}{\lambda_1 - \lambda_2} \begin{pmatrix} 1 & -\lambda_2 \\ -1 & \lambda_1 \end{pmatrix} = M^{-1}$$

$P_A(x) = x^2 - x - 1$ polinomio caratteristico

$$= (x-\lambda_1)(x-\lambda_2) = x^2 - (\underbrace{\lambda_1+\lambda_2}_{})x + \lambda_1\lambda_2$$

traccia (somma degli elementi sulla diagonale).

ie prodotto delle radici = det.

Perché $[id]_{\mathcal{E}}^{\mathcal{B}} = \left((v_1)_{\mathcal{E}} \mid (v_2)_{\mathcal{E}} \right)$

cioè $M \Rightarrow$ ha sulle colonne le coordinate dei vettori?

$\mathcal{B} \Rightarrow$ base autovettori $\quad \mathcal{E} \Rightarrow$ base canonica.

$[id]_{\mathcal{E}}^{\mathcal{B}} (v)_{\mathcal{B}} = (v)_{\mathcal{E}}$ $\quad v$ generico.

per $v = v_1$ (primo autovettore)

$[id]_{\mathcal{E}}^{\mathcal{B}} (v_1)_{\mathcal{B}} = [id]_{\mathcal{E}}^{\mathcal{B}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} =$ 1° colonna di $[id]_{\mathcal{E}}^{\mathcal{B}}$

ma deve essere uguale a $(v_1)_{\mathcal{E}}$

$f(V) \to W$

$$\boxed{[f]_{\mathcal{C}}^{\mathcal{B}} \left((v)_{\mathcal{B}} \right) = (w)_{\mathcal{C}}}$$

es:

$$A = \begin{pmatrix} 1 & 3 \\ -3 & 1 \end{pmatrix} \qquad A = [f]_{\mathcal{E}}^{\mathcal{E}} \qquad \mathcal{E} = \text{base canonica}$$

provo a diagonalizzarla:

$$P_A(\lambda) = \det\begin{pmatrix} 1-\lambda & 3 \\ -3 & 1-\lambda \end{pmatrix} =$$

$$= (1-\lambda)^2 + 9$$ mai può essere $\emptyset$.

$$\lambda^2 - 2\lambda + 1 + 9 = 0$$

$$\lambda^2 - 2\lambda + 10 = 0$$

radici: $\lambda = 1 \pm \sqrt{1-10} = 1 \pm \sqrt{-9}$

$\Delta < 0$ però se ragiono con $f: \mathbb{C}^2 \to \mathbb{C}^2$ (numeri complessi) allora trovo le radici.

in $\mathbb{R}$ non è diagonalizzabile

in $\mathbb{C}$

$$\lambda = 1 \pm 3i$$

$$\lambda_1 = 1+3i \qquad \lambda_2 = 1-3i \qquad D = \begin{bmatrix} 1+3i & 0 \\ 0 & 1-3i \end{bmatrix}$$

teorema:
Se ~~una~~ matrice $n \times n$ ha n autovalori diversi $\Rightarrow$ è diagonalizzabile.

e $D = \begin{bmatrix} \lambda_1 & \cdots & 0 \\ 0 & \cdots & \lambda_n \end{bmatrix}$

(*) invece di usare la formula per risolvere un polinomio di 2° grado posso anche vedere un'altra cosa:

$$(1-\lambda)^2 + 9 = P(\lambda)$$

$$(A^2 - B^2) = (A+B)(A-B)$$

noi abbiamo somma di quadrati ma $9 = -(i3)^2$

$$(1-\lambda)^2 - (i3)^2 \Rightarrow (1-\lambda+i3)(1-\lambda-i3)$$

radici: $\lambda_1 = 1+3i \qquad \lambda_2 = 1-3i$.

Trovata U ⇒ cerco M:

1) autovettori e autospazi

$$M = (v_1 | v_2) \qquad v_1 = ?$$

$$V_{\lambda_1} = \mathrm{Ker}(A - \lambda_1 I) = \mathrm{Ker}\begin{pmatrix} 1-\lambda_1 & 3 \\ -3 & 1-\lambda_1 \end{pmatrix} =$$

$$= \mathrm{span}\begin{pmatrix} 1 \\ i \end{pmatrix}$$

$$V_{\lambda_2} = \mathrm{Ker}(A - \lambda_2 I) = \mathrm{Ker}\begin{pmatrix} 1-\lambda_2 & 3 \\ -3 & 1-\lambda_2 \end{pmatrix} =$$

$$= \mathrm{span}\begin{pmatrix} 1 \\ -i \end{pmatrix}$$

$$M = \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$$

controllo i conti: $\begin{pmatrix} 1 \\ i \end{pmatrix}$ è un autovettore con autovalore $1+3i$

$$\begin{pmatrix} 1 & 3 \\ -3 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ i \end{pmatrix} = \begin{pmatrix} 1+3i \\ -3+i \end{pmatrix} = \lambda_1 \begin{pmatrix} 1 \\ i \end{pmatrix} \checkmark$$

es:

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

polinomio caratteristico:

$$P_A(\lambda) = \det\begin{pmatrix} 2-\lambda & 1 \\ 0 & 2-\lambda \end{pmatrix}$$

$$= (2-\lambda)(2-\lambda)$$

abbiamo 1 sola radice di molteplicità 2.

$\lambda_1 = 2 \quad \lambda_2 = 2$

È diagonalizzabile? Solo se $\dim(V_{\lambda_2}) = 2$

matematica discreta 17/05/2017

es: RSA $\quad p, q$ primi $\quad ed \equiv 1 \ (p-1)(q-1)$

$$\Rightarrow (m^e)^d \equiv m \ (pq)$$

Bob $\underbrace{p = 11 \quad q = 19}_{\text{segreti}}$, pubblica $pq = 209$ e $e = 13$

Alice vuole inviare a Bob un messaggio m, lo cripta e gli manda $m^e = m^{13} = 152$ (criptato)

Bob decripta 152 cercando $\underline{d}$ (inverso di e (...))

attuale di decriptazione

$$13d \equiv 1 \ (180) \longrightarrow (p-1)(q-1)$$ lo conosce solo Bob.

metodo di Bezout per risolvere la congruenza

$$(180, 13) \xrightarrow{180-13\cdot 13} (13, 11) \xrightarrow{13-11} (11, 2) \xrightarrow{11-5\cdot 2}$$

$$(2, 1) \Rightarrow 1$$

$$1 = 180x + 13y$$

$$180 = \boxed{1}\,180 + \boxed{0}\,13$$

$$13 = \boxed{0}\,180 + \boxed{1}\,13$$

$$11 = \boxed{1}\,180 + \boxed{-13}\,13$$

$$2 = \boxed{-1}\,180 + \boxed{14}\,13$$

$$1 = \boxed{6}\,180 + \boxed{-83}\,13 \qquad 1 = 6\cdot 180 - 83\cdot 13$$

$$13\cdot \underbrace{(-83)}_{d} \equiv 1 \ (180)$$

$$= 97$$

$m^e = 152 \rightarrow$ elevo alla d

$$m = (152)^d \equiv \underbrace{(152)^{97}}_{\text{calcolo.}} \ (209)$$

$$\begin{cases} x \equiv 152^{97} \ (11) \\ x \equiv 152^{97} \ (19) \end{cases} \Rightarrow \begin{cases} x \equiv 9^{97} \ (11) \\ x \equiv 0 \ (19) \end{cases}$$

per Fermat: $9^{10} \equiv 1 \ (11)$

$$9^{97} \equiv 9^7 \ (11)$$

$$\begin{cases} x \equiv 9^7 \ (11) \Rightarrow x \equiv -2^7 \ (11) \\ x \equiv 0 \ (19) \end{cases}$$

$$-2^7 = -128 \Rightarrow x \equiv -7 \ (11)$$

$$\begin{cases} x \equiv 4 \, (11) \\ x \equiv 0 \, (19) \end{cases}$$

$x = 19k$

$19k \equiv 4 \, (11)$

$8k \equiv 4 \, (11)$

$2k \equiv 1 \, (11)$

$5 \, (\quad -k \equiv 5 \, (11)$

$k \equiv -5 \, (11)$

$k \equiv 6 \, (11) \Rightarrow k = 6 + 11\ell$

$x = 19(6 + 11\ell) = 114 + 209\ell$

$x \equiv 114 \, (209)$

114 è il messaggio.

es: $\mathbb{C}$, polinomi.

$p(x) = x^4 - 4x^3 + 4x^2 + 14x + 26$ fattorizzarlo in $\mathbb{C}[x]$

Suggerimento $3 - 2i$ è una radice.

se è una radice allora sicuramente ci sarà anche il suo coniugato

$\lambda = 3 - 2i \Rightarrow \bar{\lambda} = 3 + 2i$

possibile perché $p(x)$ ha coefficienti reali.

$p(\lambda) = 0 \to \overline{p(\lambda)} = 0$

|| sempre vero

$\bar{p}(\bar{\lambda}) = 0 \Rightarrow p(\bar{\lambda}) = 0$

$(x - \lambda), (x - \bar{\lambda})$ sono fattori

e anche il loro prodotto è una radice

$(x - \lambda)(x - \bar{\lambda}) = x^2 - x\underbrace{(\lambda + \bar{\lambda})}_{6} + \underbrace{\lambda\bar{\lambda}}_{(3-2i)^2 = 13}$

quadrato della lunghezza di λ.

$$(x-\lambda)(x-\bar{\lambda}) = x^2-6x+13$$

$$(a+ib)(a-ib) = a^2+b^2$$

ora divido $p(x)$ per il fattore trovato

$$\begin{array}{l|l}
x^4-4x^3+3x^2+14x+26 & x^2-6x+13 \\
\hline
-\;x^4-6x^3+13x^2 & x^2+2x+2 \\
\quad / \quad 2x^3-10x^2+14x+26 & \\
-\quad 2x^3-12x^2+26x & \\
\qquad / \qquad 2x^2-12x+26 & \\
\qquad\qquad 2x^2-12x+26 & \\
\qquad\qquad / \quad / \quad / &
\end{array}$$

la scomposizione deve essere di fattori di primo grado

$$p(x) = (x^2-6x+13)(x^2+2x+2)$$

non vanno bene così:

$$= (x-\lambda)(x-\bar{\lambda})\cdot(\quad)(\quad)$$

cerco le sue radici

$$x^2+2x+2=0$$

$$x = -1 \pm \sqrt{1-2} = -1 \pm \sqrt{-1} = \begin{cases} -1+i = \lambda_1 \\ -1-i = \bar{\lambda}_1 \end{cases}$$

$$p(x) = (x-\lambda)(x-\bar{\lambda})(x-\lambda_1)(x-\bar{\lambda}_1)$$

es: fattorizzare

$$p(x) = x^4 - 2x^2 - 3 \quad \text{in } \mathbb{R}[x]$$

$y = x^2$

$$y^2 - 2y - 3 = p(y)$$

$$y = 1 \pm \sqrt{1+3} = 1 \pm 2 \begin{cases} 1+2 = 3 \\ 1-2 = -1 \end{cases}$$

$$\begin{cases} x^2 = 3 \\ x^2 = -1 \end{cases}$$

$$y^2 - 2y - 3 = (y-3)(y+1)$$

$$x^4 - 2x^2 - 3 = (x^2-3)(x^2+1)$$

$x = \pm\sqrt{3}$

$\Rightarrow (x-\sqrt{3})(x+\sqrt{3})(x^2+1)$

$x^2 = -1$ irriducibile nei $\mathbb{R}$

se vado in $\mathbb{C}[x]$

$x^2 = -1 \Rightarrow x = \pm i \quad p(x) = (x-\sqrt{3})(x+\sqrt{3})(x-i)(x+i)$.

es:

$x^2 = 1 \Rightarrow x = \pm 1$

$x^2 = -1 \Rightarrow x = \pm i$

| equazioni di secondo grado

$\Downarrow$

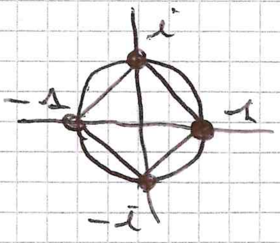
2 radici

$x^4 = 1 \Rightarrow x = \pm 1$

in $\mathbb{C}[x]$ le radici di un polinomio di grado n ha esattamente n radici.

$x^4 = 1$ in $\mathbb{C}[x] \Rightarrow x = 1, \; x = -1$

$x = i, \; x = -i$

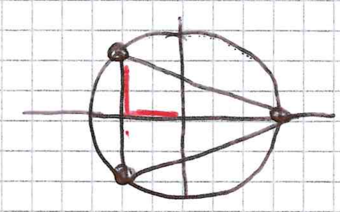


"i" ruota di 90° le radici

"i" è una soluzione PRIMITIVA → radice primitiva di $x^n = 1$ è la radice le cui potenze generano tutte le altre

Quante radici ci sono in $x^n + 1 = 0$?
Esattamente $\phi(n)$.

es: $x^3 - 1 = 0$ radici $x = 1$



ha 3 radici $\mathbb{C}$

$(x-1)$ è un fattore

$$
\begin{array}{r|l}
x^3 - 1 & x-1 \\
x^3 - x^2 & x^2 + x + 1 \\
\hline
/ \; + x^2 - 1 & \\
x^2 - x & \\
\hline
/ \; x - 1 & \\
\hline
x - 1 & \\
\hline
/ &
\end{array}
$$

$(x^3 - 1) = (x-1)(x^2+x+1)$

trovo le radici di

$x^2 + x + 1 = 0$

$$x = \frac{-1 \pm \sqrt{1-4}}{2} = \begin{cases} \boxed{-\frac{1}{2} + i\frac{\sqrt{3}}{2}} \\ \boxed{-\frac{1}{2} - i\frac{\sqrt{3}}{2}} \end{cases}$$

es: $x^5 - 1 = 0$ come trovo le radici di questo polinomio?

$x = a + ib$ lo porto in coordinate polari $e^{i\theta} = \cos\theta + i\sin\theta$

$x = re^{i\theta}$

$\Rightarrow x^5 = (a+ib)^5$ complicato perché c'è bisogno di Newton

ma $x^5 = (re^{i\theta})^5$ è più semplice

$\Downarrow$

$x^5 = r^5 e^{i5\theta}$ si moltiplicano le lunghezze e si sommano gli angoli.

radici z di $z^5 - 1 = 0$

scrivo z in $re^{i\theta}$

$$z^5 = r^5 e^{i5\theta} = 1 \quad \text{quindi} \quad r^5 e^{i5\theta} = 1$$

oss: $e^{i2\pi k} = 1$ (faccio giri di 2π)

oss:

$$e^{i\gamma} = e^{i\theta} \Rightarrow \gamma = \theta + 2\pi k$$

$$r^5 e^{i5\theta} = 1 = 1 \cdot e^{i\emptyset} \qquad r = 1$$

$$e^{i5\theta} = e^{i\emptyset} \qquad 5\theta = 2\pi k i$$

$$\theta = \frac{2\pi}{5} k i \quad \forall k.$$

$z = e^{\frac{2\pi k i}{5}}$ è radice di $z^5 - 1 = 0$.

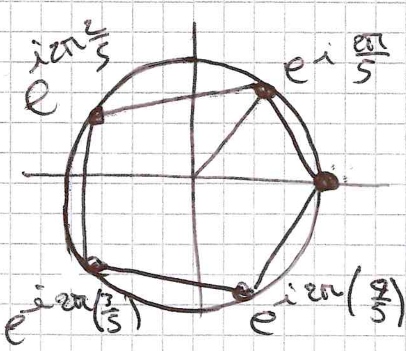
$\Downarrow$

sono infinite radici ma si ripetono:

$$z_0 = 1$$
$$z_1 = e^{i\frac{2\pi}{5}}$$
$$z_2 = e^{i\frac{2\pi 2}{5}}$$
$$z_3 = e^{i\frac{2\pi 3}{5}}$$
$$z_4 = e^{i\frac{2\pi 4}{5}}$$
$$z_5 =$$

quindi $0 \leq k < 5$

disposizione a pentagono:



Posso fattorizzare

$z^5 - 1 = 0$ come

$$z^5 - 1 = (z-1)(z - e^{i2\pi(\frac{1}{5})}) \cdot$$
$$\cdot (z - e^{i2\pi\frac{2}{5}}) \dots$$

posso passare di linea alle coordinate cartesiane

$$\Rightarrow e^{i2\pi\frac{1}{5}} = \cos\left(2\pi\frac{1}{5}\right) + i\sin\left(2\pi\frac{1}{5}\right).$$

es: Quali sono le radici di

$z = \sqrt[3]{9} = ?$ $\Rightarrow z^3 = 9$ $z = re^{i\theta}$

$z^3 = r^3 e^{i\theta} = 9$

$r = \sqrt[3]{9} \in \mathbb{R}$

nei $\mathbb{C}$ z ha 3 radici.

$z_1 = \sqrt[3]{8} \Rightarrow z^3 = 8 \Rightarrow z = re^{i\theta}$

$z^3 = r^3 e^{i\theta 3} = 2$

$\underline{r = 2}$ $z^3 = 2(e^{i\theta})^3$