GRUPPI

Sia G un insieme, $e \in G$ e $\oplus$ un operazione t.c.:

1) per ogni $a \in G$, $a + e = a$ (e è neutro)
2) $\forall$ $a, b, c \in G$ $a + (b + c) = (a + b) + c$ (associativa)
3) $\forall$ $a \in G$, $a \neq e$, esiste $b \in G$ t.c.

$a + b = b + a = e$ b si dice inverso addittivo e si indica con $-a$.

Allora $(G, \oplus)$ si dice gruppo.

CAMPI E ANELLI

Sia A un insieme, $0, 1 \in A$ e $\oplus, \odot$ operazioni t.c.

1) $(A, +)$ sia un gruppo addittivo, con neutro addittivo 0.

2) $\forall$ $a \in A$, $0 \cdot a = a \cdot 0 = 0$
3) $\forall$ $a \in A$, $a \cdot 1 = a$ (1 neutro moltiplicativo)
4) $\forall$ $a, b, c \in A$ $a \cdot (b \oplus c) = a \cdot b + a \cdot c$ (distributività del prodotto sulla somma)
5) $\forall$ $a \in A$ $\exists$ inverso moltiplicativo

$\forall a \in A - \{0\}$ $\exists$ $b \in A$ t.c $a \cdot b = b \cdot a = 1$

Se la 5, viene soddisfatta si definisce campo, se no è un anello.

POLINOMI A COEFFICENTI IN R

$$f(x) \in \mathbb{R}[x], \quad f(x) = \sum_{i=0}^{n} a_i x^n = a_n x^n + \dots + a_1 x + a_0$$

con $a_n \neq 0$

1) Il grado di $f(x)$ è n, e si scrive $\partial f(x)$
2) I reali $a_n, \dots, a_0$ sono i coefficenti
3) I termini del polinomio sono gli x^i
4) Il termine di testa di $f(x)$ è x^n
5) Il coefficente di testa è a_n.
6) Il termine noto è a_0.

PRINCIPIO DI IDENTITÀ DEI POLINOMI

Due polinomi ridotti in forma normale sono identici se e solo se hanno lo stesso grado ed i coefficenti dei termini dello stesso grado sono uguali

$$f(x) \underset{\mathbb{R}[x]}{\equiv} g(x) \iff \partial f(x) = \partial g(x)$$

$$a_n = b_n \dots a_0 = b_0$$

$$f(x) = a_n x^n + \dots + a_1 x + a_0$$
$$g(x) = b_m x^m + \dots + b_1 x + b_0$$

TEOREMA DEL BINOMIO

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-1} \qquad a,b \in \mathbb{R} \qquad n \in \mathbb{N}$$

dove $\binom{n}{i}$ è l'elemento della n-esima riga, i-esima colonna del triangolo di Tartaglia.

$$\binom{n}{i} = \frac{n!}{i!(n-i)!} \qquad \text{dove } n! = (n)(n-1)(n-2)\dots 3 \cdot 2 \cdot 1$$

DIVISIONE FATTORIZZAZIONE ED IRRIDUCIBILI

Siano $f(x), g(x) \in K[x]$, allora
Diciamo che $g(x)$ divide $f(x)$ se esiste $q(x) \in K[x]$ t.c.

$$f(x) = g(x)\, q(x)$$

Sia $p \in K[x]$ un polinomio non identicamente nullo. Allora una radice di p è un elemento $\alpha \in K$

$$p(\alpha) = 0$$

<u>Definizione</u>: Un polinomio $f(x) \in K[x]$ di grado ≥ 1 che non ha divisori propri (diversi da 1 e se stesso) si dice irriducibile. Se ce li ha è riducibile

TEOREMA DELLA FATTORIZZAZIONE UNICA

Sia $f(x) \in K[x]$, allora esistono unici $f_1(x), \dots, f_m(x) \in K[x]$ irriducibili distinti e $\alpha_1, \dots, \alpha_m \in \mathbb{N}$ t.c.

$$f(x) = \prod_{i=1}^{m} f_i(x)^{\alpha_i} = f_1(x)^{\alpha_1} \cdots\cdots f_m(x)^{\alpha_m}$$

I polinomi $f_i(x)$ si dicono fattori irriducibili di $f(x)$ e i naturali α_i sono le loro molteplicità.

ES. $f(x) = x^4 - 1 \longrightarrow (x-1)(x+1)(x+1)^2$

- Tutti i polinomi di grado 1 sono irriducibili
- Un polinomio di 2° grado è irriducibile se ha discriminante negativo (Δ).

<u>Definizione</u> : Dati due polinomi in $K[x]$ privi di fattori irriducibili comuni, sono detti coprimi.

Oss: In $\mathbb{K}[x]$ un polinomio irriducibile è coprimo con ogni altro polinomio di grado minore del suo.

TEOREMA DELLE RADICI $\exists \mathbb{Q}$ ma $\nexists \mathbb{R}$

Sia $f(x) = a_n x^n + \dots + a_1 x + a_0$

Allora abbiamo che tutte le radici razionali sono date da un divisore del termine noto diviso un divisore del termine di testa

$f(a) = 0 \Rightarrow a = \pm \frac{c_i}{b_j}$ divisori di a_0 $i: 1 \dots k$

divisori di a_n $j: 1 \dots p$

ES: $2x^3 - x^2 - 6x + 3$.

Le possibili radici razionali sono:

$$\pm \frac{1}{1}, \pm \frac{1}{2}, \pm 3, \pm \frac{3}{2}$$

Si sostituisce dentro $f(x)$.

Se uno fa 0, il polinomio è diviso da $(x - a)$.

TEOREMA DI RUFFINI

Sia $f(x)$ un polinomio in $\mathbb{K}[x]$ e $a \in \mathbb{K}$. Allora

$$f(a) = 0 \iff (x-a) \mid f(x)$$

Ovvero a è una radice di $f(x) \iff x-a$ è un fattore di $f(x)$

Vuol dire che abbiamo trovato una radice a del polinomio $f(x)$ ed esso sarà divisibile per $(x-a)$

Oss: un polinomio non nullo ha al più n radici quanto il suo grado.

CRITERIO DI EISENSTEIN

Sia $f(x)$ un polinomio in $\mathbb{K}[x]$, di grado n Allora se esiste $p \in \mathbb{N}$ primo t.c.

$$p \nmid a_n \quad p \mid a_{n-1} \ldots\ldots p \mid a_0 \quad e \quad p^2 \nmid a_0$$

Il polinomio $f(x)$ è irriducibile su $\mathbb{Q}[x]$.
Si dice che $f(x)$ è irriducibile per Eisenstein, con primo p.

Oss: I polinomi della forma $x^n - p$, con p intero primo, sono irriducibili.

Oss: Un polinomio è irriducibile o meno a seconda del campo che consideriamo

DIVISIONE CON RESTO

Sia $f(x) \in K[x]$,

Allora esistono unici $q(x), r(x) \in \mathbb{K}[x]$ t.c.

$$f(x) = g(x)\, q(x) + r(x)$$

con:

- $r(x) = 0$ oppure
- $\deg(r(x)) < \deg(g(x))$

ES:

$$\begin{array}{rrrr|l}
x^3 & +2x^2 & +2x & -1 & x^2-1 \\
\cline{5-5}
-x^3 & & +x & & \underbrace{x+2}_{\text{quoto}} \\
\cline{1-4}
 & 2x^2 & +3x & -1 & \\
 & -2x^2 & & +2 & \\
\cline{2-4}
 & & \underbrace{3x+1}_{\text{resto}} & &
\end{array}$$

<u>Definizione</u>: Sia $f(x) \in \mathbb{K}[x]$ con $LC\, f(x) = 1$

Con coefficente del termine di testa $= 1$

Allora $f(x)$ si dice monico

ES $x^2 + 6x - 27$ è monico

$2x - 7$ non lo è

MASSIMO COMUNE DIVISORE E MINIMO COMUNE MULTIPLO

Dati $f(x), g(x) \in \mathbb{K}[x]$

GCD di $f(x), g(x)$ è il polinomio monico di grado minore tra quelli che dividono $f(x), g(x)$.
Tale polinomio esiste sempre, al limite è 1.

lcm di $f(x), g(x)$ sono i fattori comuni e non comuni presi una volta con massimo esponente.

ES: $h(x) = (x+1)^4(x-1)(x^2+1)^3 \qquad p(x) = (x+1)^2(x-1)^2(x^2+2)^3$

$$GCD(h(x), p(x)) = (x+1)^2(x-1)$$
$$lcm(h(x), p(x)) = (x+1)^4(x-1)^2(x^2+1)^3(x^2+2)^3$$

ALGORITMO EUCLIDEO

Dati $f_0(x), f_1(x) \in \mathbb{K}[x]$
con $\deg f_0(x) \geq f_1(x)$. Sia

$$f_i(x) = q_i(x) f_{i+1}(x) + f_{i+2}(x)$$

la divisione con resto di $f_i(x)$ rispetto a $f_{i+1}(x)$ per opportuni $q_i(x)$. La sequenza di coppie

$$(f_i(x), f_{i+1}) \longrightarrow (f_{i+1}, f_{i+2})$$

termina con una coppia $(g(x), 0)$
e il GCD tra $(f_0(x), f_1(x))$ è $g(x)$.

SQUAREFREE Un polinomio che abbia fattorizzazione in irriducibili su $\mathbb{K}[x]$

$$f(x) = \prod_{i=1}^{n} f_i(x)^{\alpha_i} \quad \text{con } \alpha_1 = \dots = \alpha_n = 1$$

si dice squarefree.

TEOREMA: CRITERIO DELLA MOLTEPLICITÁ O DEL GCD.

Sia $f(x) \in \mathbb{K}[x]$ e una sua fattorizzazione in irriducibili su $\mathbb{K}[x]$

$$f(x) = \prod_{i=1}^{n} f_i(x)^{\alpha_i}$$

1) $\gcd(f(x), f'(x)) = \prod_{i=1}^{n} f_i(x)^{\alpha_i - 1}$

2) $\gcd(f(x), f'(x)) \mid f(x)$

3) $f(x)$ è squarefree $\iff \gcd(f(x), f'(x)) = 1$

4) il polinomio $\dfrac{f(x)}{\gcd(f(x), f'(x))}$ è squarefree

ES: Fattorizzare $p(x) = x^6 + x^5 - 5x^4 - 6x^3 + 3x^2 + 9x + 9$

$$p'(x) = 6x^5 + 5x^4 - 20x^3 - 18x^2 + 9x + 9$$

$(p(x), p'(x))$

$(p'(x), p_2(x))$

$(p_2(x), p_3(x))$

$(p_3(x), -x^2+3)$ $\qquad GCD = -x^2+3 = x^2-3$

$(-x^2+3, 0)$

$$\frac{p(x)}{(x^2-3)^2} = x^2 + x + 1$$

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

PRODOTTO CARTESIANO

Siano A, B insiemi. Allora l'insieme delle coppie ordinate composte da un elemento di A ed uno di B si dice prodotto cartesiano di A e B e si indica con $A \times B$.

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

Due elementi $A \times B$ sono uguali se sono uguali elemento per elemento

OSS. Se A e B sono anelli allora possiamo considerare $A \times B$ anello con le operazioni ovvie:

- $(0_A, 0_B)$ neutro additivo
- $(1_A, 1_B)$ neutro moltiplicativo

<u>Definizione</u> Dato un anello A, un suo elemento $a \neq 0$ è zero divisore se esiste $b \in A$, $b \neq 0$ t.c. $a \cdot b = 0$

ES: $(2, 0)(0, 7) = (0, 0)$

OSS: Sia A un campo $\Rightarrow \nexists$ 0-divisori

Se $\exists$ 0-divisori $\Rightarrow$ A non è un campo

IL CAMPO DEI COMPLESSI

L'equazione $x^2+1=0$ non ha soluzione sui reali
Per questo introduciamo l'oggetto $\{i\} \notin \mathbb{R}$ con la proprietà $i=\sqrt{-1}$

$\mathbb{R}[i] = \{a+ib \mid a,b \in \mathbb{R}\}$ è un campo?

$(\mathbb{R}[i],+,\cdot)$ è un anello commutativo verificando le sue proprietà. Verifichiamo la commutività:

$$(a+ib)(c+id) \overset{?}{=} (c+id)(a+ib)$$

$(a+ib)(c+id) = ac-bd+i(ad+bc)$ $\qquad i^2=-1$

$(c+id)(a+id) = ac-bd+i(ad+bc)$

Rimane da verificare che $\mathbb{R}[i]$ sia un campo.

Dato $a+ib \in \mathbb{R}[i]$, non nullo esiste $(x+iy) \in \mathbb{R}[i]$ t.

$$(a+ib)(x+iy)=1$$

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

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

E quindi $a+ib$ ha l'inverso che si può indicare con $(a+ib)^{-1}$.

Quindi è un campo

DEFINIZIONI

1. Il campo $\mathbb{R}[i]$ si dice campo dei complessi e si indica con $\mathbb{C}$.
2. Un complesso scritto $(a+ib)$ è in forma cartesiana $z = a + ib$
3. La parte reale di z è a e si indica con $Re(z)$
4. La parte immaginaria di z è b e si indica $Im(z)$
5. $\{i\}$ è l'unità immaginaria
6. Se $b=0$ allora z è detto immaginario puro
7. Il modulo di z è $\sqrt{a^2+b^2} \in \mathbb{R}$ e si indica $|z|$.
8. Il coniugato di z è $(a-ib)$ e si indica $\bar{z}$.

FORMA TRIGONOMETRICA

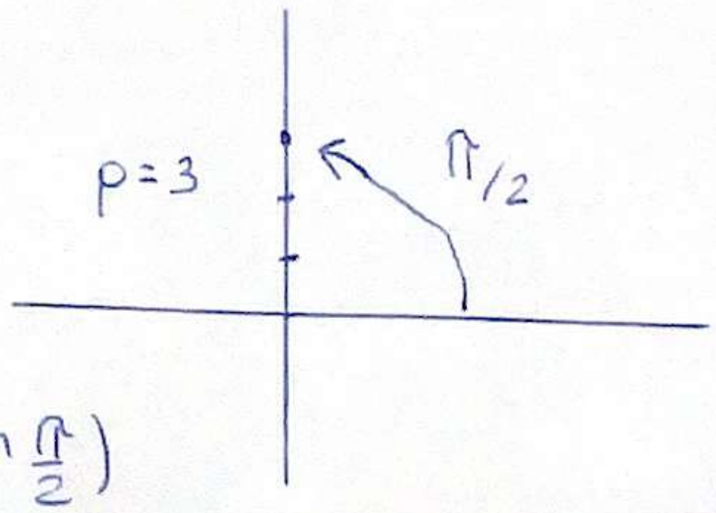
Un numero complesso $a+ib$, può essere identificato con l'elemento (a,b) sul piano $\mathbb{R}^2$, riportando sulle ascisse la parte reale e sulle ordinate quella immaginaria (Piano di Argand-Gauss).
In questo caso il modulo $|z|$, indicato con ρ, è la lunghezza del vettore e possiamo definire l'argomento $\arg(z) = \theta$

$$a = Re(z) = \rho \cos\theta \qquad b = Im(z) = \rho \sin\theta$$

quindi

$$z = \rho(\cos\theta + i \sin\theta)$$

ES $z = 3i$



$$z = 3\left(\cos\frac{\pi}{2} + i \sin\frac{\pi}{2}\right)$$

Principio di identità dei complessi in forma trigonometrica

$$\rho_1(\cos\theta_1 + i\sin\theta_1) = \rho_2(\cos\theta_2 + i\sin\theta_2)$$

$$\Updownarrow$$

$$\begin{cases} \rho_1 = \rho_2 \\ \theta_1 = \theta_2 + 2k\pi \text{ per qualche } k \in \mathbb{Z} \end{cases}$$

PROPRIETÀ $\quad z, z_1 \in \mathbb{C}$

$$\overline{\overline{a+ib}} = \overline{a-ib} = a+ib$$

1) $\bar{\bar{z}} = z$

2) $\overline{z+z_1} = \bar{z} + \bar{z}_1$

3) $\overline{1/z} = 1/\bar{z}$

Siano $z, z_1, z_2 \in \mathbb{C}$

1) $|z| = 0 \iff z = 0$

2) $|\bar{z}| = |z|$

3) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$

4) $|z_1 + z_2| \leq |z_1| + |z_2|$ Disuguaglianza triangolare

OSS: $\forall a, b \in \mathbb{C}$

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

Definizione

Si usa scrivere il complesso $z = \rho(\cos\theta + i\sin\theta)$ come $z = \rho e^{i\theta}$. Questa è la forma esponenziale del complesso.

PROPRIETÀ

1. Principio di identità dei complessi in forma esponenziale

$$\rho_1 e^{i\theta_1} = \rho_2 e^{i\theta_2} \iff \exists\, k \in \mathbb{Z} \text{ tale che } \begin{cases} \rho_1 = \rho_2 \\ \theta_1 = \theta_2 + 2k\pi \end{cases}$$

2. $\rho_1 e^{i\theta_1} \cdot \rho_2 e^{i\theta_2} = \rho_1 \rho_2 e^{i(\theta_1+\theta_2)}$

3. $\left(\rho_1 e^{i\theta_1}\right)^{-1} = \frac{1}{\rho_1} e^{-i\theta_1}$

4. $\frac{\rho_1 e^{i\theta_1}}{\rho_2 e^{i\theta_2}} = \frac{\rho_1}{\rho_2} e^{i(\theta_1-\theta_2)}$

5. $|(\rho_1 e^{i\theta_1})| = \rho_1$

6. $\arg(\rho_1 e^{i\theta_1}) = \theta_1$

7. $\overline{\rho_1 e^{i\theta_1}} = \rho_1 e^{-i\theta_1}$

8. $e^{i\pi} = -1$

9. $e^{i0} = 1$

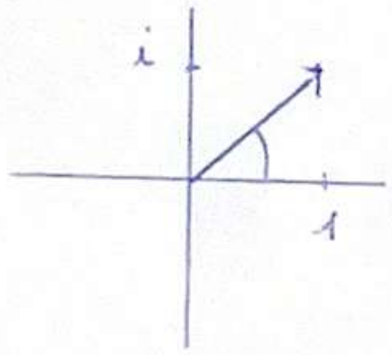
10. Se $a, b \in \mathbb{R}$ allora $e^z = e^{a+ib} = e^a e^{ib}$

FORMULA DELLE RADICI IN FORMA ESPONENZIALE

Se $z = \rho e^{i\theta} \in \mathbb{C}$

$$\sqrt[n]{z} = \left\{ \sqrt[n]{\rho}\, e^{i\frac{\theta+2k\pi}{n}} \right\} \qquad k: 0, \dots, n-1$$

ESEMPIO: Calcolare le radici seste di $1+i$



$$1+i = \sqrt{2}\, e^{i\frac{\pi}{4}}$$

$$\rho = \sqrt{1+1} = \sqrt{2}$$

$$\theta = \frac{\pi}{4}$$

$$\sqrt[6]{\sqrt{2}\, e^{i\pi/4}} = \sqrt[12]{2}\; e^{i\frac{\frac{\pi}{4}+2k\pi}{6}} \qquad k: 0, \dots, 5$$

$k=0$ $\quad \sqrt[12]{2}\; e^{i\frac{\pi}{24}}$

$k=1$ $\quad \sqrt[12]{2} \cdot e^{i\frac{9\pi}{24}}$

$k=2$ $\quad \sqrt[12]{2} \cdot e^{i\frac{17}{24}\pi}$

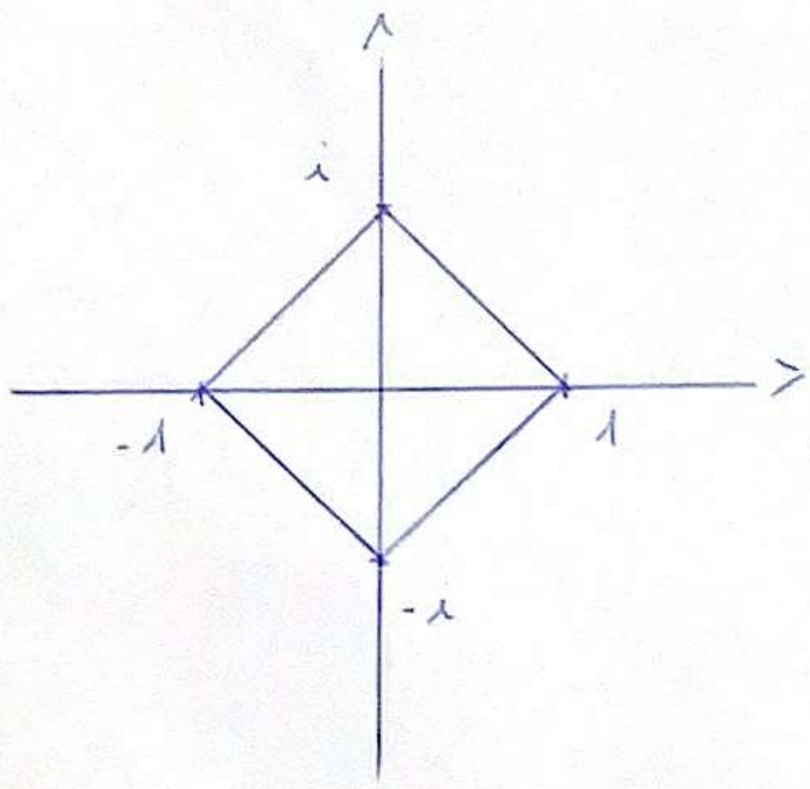
$k=3$ $\quad \sqrt[12]{2}\; e^{i\frac{25}{24}\pi}$

$k=4$ $\quad \sqrt[12]{2}\; e^{i\frac{33}{24}\pi}$

$k=5$ $\quad \sqrt[12]{2}\; e^{i\frac{41}{24}\pi}$

Le radici n-esime di un complesso z sono i vertici di un poligono regolare con n lati nel piano di Argand-Gauss

Radici di $z^4 = 1$



POTENZE E RADICI DI UN COMPLESSO

$i^0 = 1 \quad i^1 = i \quad i^2 = -1 \quad i^3 = i\,i^2 = -i \quad i^4 = 1$

Le potenze di i ciclano di ordine 4 e $i^n = i^r$ dove r è la divisione di n per 4.

<u>Proposizione</u>: Dati due complessi in forma trigonometrica

$$z_1 = \rho_1(\cos\theta_1 + i\sin\theta_1 \qquad z_2 = \rho_2(\cos\theta_2 + i\sin\theta_2)$$

1) $z_1 \cdot z_2 = \rho_1\rho_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2))$

2) $\dfrac{z_1}{z_2} = \dfrac{\rho_1}{\rho_2}(\cos(\theta_1-\theta_2) + i\sin(\theta_1-\theta_2))$

3) $z^n = \rho^n(\cos n\theta_1 + i\sin n\theta_2)$ Formula di De Moivre

<u>Definizione</u>

Sia $w \in \mathbb{C}$ e $n \geq 1$. Una radice n-esima di w è un complesso z tale che $z^n = w$

L'insieme delle radici n-esime di w si indica $\sqrt[n]{w}$

ES $\sqrt[2]{-1} = \{\pm i\}$

Sia w un complesso non nullo e $n \geq 1$.
Allora esistono esattamente n-radici distinte di w.

Se $w = \rho(\cos\theta + i\sin\theta)$ allora:

$$z_k = \sqrt[n]{\rho}\left[\cos\left(\frac{\theta + 2k\pi}{n}\right) + i\sin\left(\frac{\theta + 2k\pi}{n}\right)\right] \quad \text{con } k: 0, \dots, n-1$$

e quindi abbiamo $\sqrt[n]{w} = \{z_0, \dots, z_{n-1}\}$

Dimostrazione:

Grazie alla formula di DeMoivre si ha:

$$z_k^n = \rho(\cos\theta + i\sin\theta) = w$$

Quindi gli z_k sono radici di w.

Bisogna vedere che siano le uniche e distinte:

Per l'unicità se $z = r(\cos\alpha + i\sin\alpha)$ è una radice dato che $z^n = \rho(\cos\theta + i\sin\theta) = w$

Si ha per il principio di identità dei complessi

$$r = \sqrt[n]{\rho} \quad \text{e} \quad n\alpha = \theta + 2k\pi \quad \text{per qualche } k \in \mathbb{Z}$$

Rimane da dimostrare che $\{z_0, \dots, z_{n-1}\}$ sono tutti distinti

Supponiamo che esistano interi h, k tra 0 e $n-1$ tali che $z_h = z_k$

$$\cos\left(\frac{\theta + 2h\pi}{n}\right) = \cos\left(\frac{\theta + 2k\pi}{n}\right), \quad \sin\left(\frac{\theta + 2h\pi}{n}\right) = \sin\left(\frac{\theta + 2k\pi}{n}\right)$$

Quindi $\frac{\theta + 2h\pi}{n}$ e $\frac{\theta + 2k\pi}{n}$ differiscono di multipli di 2π

E quindi esiste $l \in \mathbb{Z}$ tale che:

$$\frac{\theta + 2h\pi}{n} = \frac{\theta + 2k\pi}{n} + 2l\pi \implies \begin{array}{l} h - k = nl \\ h = k \end{array}$$

FATTORIZZAZIONI IN $\mathbb{R}, \mathbb{C}$

Teorema: Un polinomio $f(x) \in \mathbb{C}[x]$ ha esattamente n radici complesse, non necessariamente distinte.

OSS: Per ogni $f(x) \in \mathbb{C}[x]$ esistono $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ non necessariamente distinte tali che:

$$f(x) = (x-\alpha_1) \cdots\cdots (x-\alpha_n) = \prod_{i=1}^{n} (x-\alpha_i)$$

OSS: Notiamo che dato $z_0 \in \mathbb{C}$, il prodotto dei due fattori lineari $(x-z_0)(x-\bar{z}_0)$, che stanno in $\mathbb{C}[x]$ è un polinomio in $\mathbb{R}[x]$:

$$(x-z_0)(x-\bar{z}_0) = x^2 - 2(\mathrm{Re}\, z_0)x + |z_0|^2$$

Infatti:

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

Quindi fattorizzando un polinomio di 2° e $\Delta < 0$ si ha due fattori complessi coniugati, e il prodotto di questi mi dà un polinomio reale.

Le radici complesse sono sempre a due a due coniugate, infatti ogni polinomio a coefficienti reali di grado dispari ha almeno una radice reale.

ES $p(x)$ $\partial 5$:
- 5 radici reali
- 2 nei complessi, 3 nei reali
- 4 nei complessi, 1 nei reali.

TEOREMA FONDAMENTALE DELL'ALGEBRA

Proposizione

Sia $f(x) \in \mathbb{R}[x]$ e $z_0 \in \mathbb{C}$. Allora se z_0 è radice, anche il suo coniugato lo è, con la stessa molteplicità

Se indichiamo con μ la molteplicità

$$f(z_0) = 0 \Rightarrow f(\bar{z}_0) = 0 \quad e \quad \mu(z_0) = \mu(\bar{z}_0)$$

Dimostrazione:

Sia $f(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_0$

$$f(\bar{z}) = a_n \bar{z}^n + \dots + a_0 = \overline{a_n z^n + \dots + a_0} = \overline{p(z)}$$

in quanto $a_i = \bar{a}_i$ per $i: 0, \dots, n$ per cui

$$z_0 \text{ è radice} \Longleftrightarrow \bar{z}_0 \text{ è radice}$$

Se z_0 è radice, allora possiamo scrivere

$$f(x) = (x - z_0)(x - \bar{z}_0)\, q(x) \rightarrow \text{perché } (x-z_0)(x-\bar{z}_0) \text{ dividono } p(x)$$

Siccome $(x - z_0)(x - \bar{z}_0) = x^2 - 2\mathrm{Re}(z_0)x + |z_0|^2$ è un polinomio a coefficienti reali, anche $q(x)$ lo è.

Quindi un polinomio in $\mathbb{R}[x]$ si fattorizza:

$$f(x) = \prod_{i=1}^{k} (x - \alpha_i) \cdot \prod_{j=0}^{m} P_j(x)$$

Quindi ad ogni fattore $x - z_0$ corrisponde uno ed un solo fattore del tipo $x - \bar{z}_0$ e questo ci porta a dire che $\mu(z_0) = \mu(\bar{z}_0)$

SISTEMI DI EQUAZIONI LINEARI

$$S = \begin{cases} 2x + 3y + z = 1 \\ x - y + 2z = 1 \\ 3x + y - 5z = 2 \end{cases}$$

Come possiamo scrivere questo sistema in maniera più compatta?

Attraverso una matrice: $S = \left(\begin{array}{ccc|c} 2 & 3 & 1 & 1 \\ 1 & -1 & 2 & 1 \\ 3 & 1 & -5 & 2 \end{array}\right)$

<u>Definizione</u>: Sia $A \in \mathbb{K}^{nm}$. Se scriviamo A come

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

Diciamo che A è una matrice con m righe e n colonne. L'insieme di queste matrici su $\mathbb{K}$ si indica come $Mat_{m \times n}(\mathbb{K})$. Se $m = n$ la matrice è quadrata.

OSS: Le righe di A si indicano come $A_1, \dots, A_m$
le colonne di A come $A^1, \dots, A^n$

ESEMPIO: Data la matrice

$$A = \begin{pmatrix} 3 & 7 & 5 & -3 \\ 2 & 1 & 2 & 6 \end{pmatrix} \qquad A \in Mat_{2 \times 4}$$

$$A_1 = (3, 7, 5, -3)$$

$$A^3 = \begin{pmatrix} 5 \\ 2 \end{pmatrix}$$

Definizione: Sia $A \in Mat_{n \times n}(\mathbb{K})$ una matrice quadrata:

1) La diagonale di A è data dagli elementi $a_{11}, \dots, a_{nn}$

2) A si dice diagonale, se tutti gli elementi di A fuori dalla diagonale sono nulli.

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & a_{nn} \end{pmatrix}$$

3) A si dice triangolare superiore se tutti gli elementi di A sotto la diagonale sono nulli

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & & \\ \vdots & & \ddots & \\ 0 & \cdots & & a_{nn} \end{pmatrix}$$

4) A si dice triangolare inferiore se tutti gli elementi di A sopra la diagonale sono nulli.

Definizione Sia:

$$S = \begin{cases} a_{11}x_1 + a_{12}x_2 + \dots a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots a_{mn}x_n = b_m \end{cases}$$

Un sistema lineare con m equazioni ed n incognite, diciamo che la matrice completa associata al sistema è

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right)$$

mentre la matrice incompleta è:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

e la colonna dei termini noti è: $\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$

Il sistema S viene anche scritto: $A\underline{x} = \underline{b}$

PRODOTTO SCALARE

Viene comodo per descrivere in modo compatto i sistemi lineari introdurre il prodotto scalare.

<u>Definizione</u> Sia $\mathbb{K}$ un campo e $\underline{v} = (v_1, \dots, v_n)$ e $\underline{w} = (w_1, \dots, w_n)$. L'operazione:

$$\mathbb{K}^n \times \mathbb{K}^n \longrightarrow K$$

$$(v_1, \dots, v_n)(w_1, \dots, w_n) \longrightarrow (v_1 w_1, \dots, v_n w_n) = \sum_{i=1}^{n} v_i w_i$$

è detta prodotto scalare

ES: $(1, 2, 3) \cdot (5, 0, 2) = 1 \cdot 5 + 2 \cdot 0 + 3 \cdot 2 = 11$

ES: $(-1, 1) \cdot (1, 1) = -1 \cdot 1 + 1 \cdot 1 = 0$

OSS: se $\underline{v} \perp \underline{w} \iff \underline{v} \cdot \underline{w} = 0$

PROPRIETÀ DEL PRODOTTO SCALARE

Sia $\mathbb{K}$ campo, $\underline{u}, \underline{v}, \underline{w} \in \mathbb{K}^n$ e $\lambda \in \mathbb{K}$. Allora:

1) $\underline{u} \cdot \underline{v} = \underline{v} \cdot \underline{u}$ è commutativo
2) $(\underline{u} + \underline{v}) \cdot \underline{w} = \underline{u} \cdot \underline{w} + \underline{v} \cdot \underline{w}$ distributività sulla somma
3) $\lambda (\underline{u} \cdot \underline{v}) = (\lambda \underline{u}) \cdot \underline{v}$

Dimostrazione punto 3.

$$\lambda ((u_1, \dots u_n)(v_1, \dots v_n) = \lambda (u_1, \dots, u_n) \cdot w_1 \dots w_n$$

$$\lambda \left(\sum_{i=1}^{n} u_i w_i \right)$$

$$\sum_{i=1}^{n} \lambda u_i w_i = \sum_{i=1}^{n} (\lambda u_i) w_i$$

Osservazione: Sia $\mathbb{K}$ campo e $Ax=b$ un sistema di equazioni lineari. Usando il prodotto scalare possiamo indicare la prima equazione del sistema

$$A_1 \cdot \underline{x} = b_1$$

o una generica $A_i \cdot \underline{x} = b_i \quad i: 1, \dots, n$

Definizione

$$\begin{aligned} K \times K^n &\longrightarrow K^n \\ \lambda, \underline{v} &\longrightarrow \lambda(v_1, \dots, v_n) = (\lambda v_1, \dots, \lambda v_n) \end{aligned}$$

si dice prodotto esterno di K^n.

Proprietà: Se $\lambda, \mu \in K$ e $\underline{v}, \underline{w} \in \mathbb{K}^n$

1. $(\lambda + \mu)\underline{v} = \lambda \underline{v} + \mu \underline{v}$
2. $\lambda(\underline{v} + \underline{w}) = \lambda \underline{v} + \lambda \underline{w}$
3. $\lambda \mu \underline{v} = \lambda(\mu \underline{v})$
4. $0\underline{v} = 0 \qquad \lambda \underline{0} = \underline{0} \qquad 1\underline{v} = \underline{v}$

OPERAZIONI SU MATRICI

(scambio di righe) Sia $\mathbb{K}$ campo, $A\underline{x}=\underline{b}$ un sistema con m equazioni ed n incognite. Seguendo la notazione per le righe si ha:

$$A=[A_1,\dots\dots,A_i,\dots\dots,A_j,\dots\dots,A_m] \quad \text{con } i<j$$

Se $A'=[A_1,\dots\dots,A_j,\dots\dots,A_i,\dots\dots,A_m]$

$$b'=[b_1,\dots\dots,b_j,\dots\dots,b_i,\dots\dots,b_m]$$

Allora $Sol(A\underline{x}=b)=Sol(A'\underline{x}=b')$

(combinazione lineare di righe)

Sia $\mathbb{K}$ campo, $A\underline{x}=b$ un sistema con m equazioni ed n incognite. Seguendo la notazione per righe

$$A=[A_1,\dots\dots,A_i,\dots\dots,A_j,\dots\dots A_m] \quad \text{con } i<j$$

Se $\alpha,\beta\in\mathbb{K}$ con $\beta\neq 0$

$$A'=[A_1,\dots\dots,A_i,\dots\dots,\alpha A_i+\beta A_j,\dots\dots,A_m]$$

$$b'=[b_1,\dots\dots,b_i,\dots\dots,\alpha b_i+\beta b_j,\dots\dots,b_m]$$

Allora $Sol(A\underline{x}=b)=Sol(A'\underline{x}=b')$

Dimostrazione

1) Proviamo prima che ogni soluzione di $A\underline{x}=\underline{b}$ è anche di $A'\underline{x}=\underline{b}'$, e poi il viceversa

- Sia $\underline{v}=(v_1,\dots,v_m) \in Sol(A\underline{x}=\underline{b})$. Allora

$$\forall i: 1,\dots,m \quad \text{abbiamo} \quad (A_i \cdot \underline{v} = b_i)$$

Dobbiamo dimostrare che $\underline{v} \in Sol(A'\underline{x}=\underline{b}')$, ovvero che

$$\forall i: 1,\dots,m,\ i \neq j \quad A_i \cdot \underline{v} = b_i \quad e \quad (\alpha A_i + \beta A_j)\cdot \underline{v} = \alpha b_i + \beta b_j$$

Ma questo è evidente per ogni riga diversa dalla j-esima, ma grazie alla proprietà di prodotto esterno, si ha:

$$(\alpha A_i + \beta A_j)\cdot \underline{v} = \alpha A_i \cdot \underline{v} + \beta A_j \cdot \underline{v} = \alpha b_i + \beta b_j$$

2) Sia $\underline{v}=(v_1,\dots,v_m) \in Sol(A'x=\underline{b}')$. Allora

$$\forall i: 1,\dots,m \quad i \neq j \quad A'_i \cdot \underline{v} = b'_i \quad e \quad (\alpha A'_i + \beta' A_j)\cdot \underline{v} = \alpha b'_i + \beta' b_j$$

Vogliamo dimostrare che $\underline{v} \in Sol(A\underline{x}=\underline{b})$ ovvero che

$$\forall i: 1,\dots m \quad \text{abbiamo} \quad A_i \cdot \underline{v} = b_i$$

Ma questo è vero per ogni riga tranne la j-esima.
Perché $\underline{v}$ sia soluzione di $A\underline{x}=\underline{b}$ rimane da dimostrare

$$A_j \cdot \underline{v} = b_j$$

$$(\alpha A_i + \beta A_j)\cdot \underline{v} = \alpha b_i + \beta b_j$$

$$\alpha A_i \cdot \underline{v} + \beta A_j \cdot \underline{v} = \alpha b_i + \beta b_j$$

Dato che $A_i \cdot \underline{v} = b_i \Rightarrow \alpha A_i \cdot \underline{v} = \alpha b_i$

$$\beta A_j \cdot \underline{v} = \beta b_j$$

$$\beta (A_j \cdot \underline{v} - b_j) = 0 \quad \text{ma } \beta \neq 0 \quad \text{quindi}$$

$$A_j \cdot \underline{v} = b_j$$

Definizione Sia $\underline{v}, \underline{w} \in \mathbb{K}^n$ $\alpha, \beta \in \mathbb{K}$

$\alpha \underline{v} + \beta \underline{w}$ è detta combinazione lineare di $\underline{v}, \underline{w}$

a coefficenti α, β

OPERAZIONI DI GAUSS

Sia $A \in Mat_{m \times n}(\mathbb{K})$ chiamo operazioni di Gauss:

1. Lo scambio di righe $A_i \longleftrightarrow A_j$
2. Lo scambio di colonne $A^i \longleftrightarrow A^j$
3. La sostituzione $A_i \longrightarrow A_i - \lambda A_j$

ES:
$$\begin{cases} x + y + z + 3t + s = 0 \\ x + y + z - 2t - s = 2 \\ x + y + z + t + 3s = 3 \end{cases}$$

$$\begin{pmatrix} 1 & 1 & 1 & 3 & 1 & 0 \\ 1 & 1 & 1 & -2 & -1 & 2 \\ 1 & 1 & 1 & 1 & 3 & 3 \end{pmatrix} \begin{matrix} \\ II^1 - I^1 \\ III^1 - I^1 \end{matrix} \begin{pmatrix} 1 & 1 & 1 & 3 & 1 & 0 \\ 0 & 0 & 0 & -5 & -2 & 2 \\ 0 & 0 & 0 & -2 & 2 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 & 3 & 1 & 0 \\ 0 & 0 & 0 & 5 & 2 & -2 \\ 0 & 0 & 0 & 0 & \frac{14}{5} & \frac{11}{5} \end{pmatrix} \qquad \begin{pmatrix} \underline{1} & 1 & 1 & 0 & 0 & -\frac{1}{14} \\ 0 & 0 & 0 & \underline{1} & 0 & -\frac{5}{7} \\ 0 & 0 & 0 & 0 & \underline{1} & \frac{11}{14} \end{pmatrix}$$

OSS: Gli elementi sopra indicati vengono chiamati pivot.

INDIPENDENZA LINEARE

Risolvendo in $\mathbb{K}$ il sistema

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 2 \end{pmatrix}$$

Si vede che nessuna riga è superflua. Ciò non si può dire per $\begin{array}{c} \begin{pmatrix} 2 & 3 & 4 \\ 1 & 5 & 2 \\ 3 & 8 & 6 \end{pmatrix} \end{array} \begin{array}{l} \underline{v}_1 \\ \underline{v}_2 \\ \underline{v}_3 \end{array}$ Dato che $\underline{v}_3 = \underline{v}_1 + \underline{v}_2$

Quindi il terzo vettore è combinazione dei primi due.

<u>Definizione</u>: i vettori $\underline{v}_1, \dots, \underline{v}_n \in \mathbb{K}^s$ sono linearmente dipendenti se e solo se:

$$\exists\, \underline{\lambda} \in \mathbb{K}^n,\ \underline{\lambda} \neq \underline{0} \text{ tale che } \underline{\lambda} \cdot \underline{v} = \underline{0}$$

oppure: $\exists\, \lambda_1, \dots \lambda_n \in \mathbb{K}^n,\ (\lambda_1, \dots, \lambda_n) \neq 0$ tali che

$$(\lambda_1 \cdot \underline{v}_1 + \dots + \lambda_n \underline{v}_n) = 0$$

<u>Definizione</u> Siano $\underline{v}_1, \dots, \underline{v}_n \in \mathbb{K}^n$. Diciamo che i vettori sono linearmente indipendente se una loro combinazione lineare nulla ha forzatamente tutti i coefficenti nulli.

$$\forall\, \underline{\lambda} \in \mathbb{K}^n,\quad \underline{\lambda} \cdot \underline{v} = \underline{0} \Rightarrow \underline{\lambda} = 0 (\lambda_1, \dots \lambda_n) = \underline{0}$$

oppure $\forall\, \lambda_1, \dots, \lambda_n \in \mathbb{K}^n$

$$\lambda_1 v_1 + \dots + \lambda_n v_n = 0 \Rightarrow (\lambda_1 \dots \lambda_n) = \underline{0}$$

Proposizione: Sia $\mathbb{K}$ campo, $A\underline{x} = \underline{b}$ $\quad A \in Mat_{n \times n}(\mathbb{K})$

Allora $\exists!$ Sol di $(A\underline{x} = \underline{b}) \iff \exists\, D \in Mat_{n \times n}(\mathbb{K})$

con gli elementi sulla diagonale non nulli, e posso trasformare $[A|\underline{b}]$ in $[D|\underline{c}]$ con operazioni di Gauss.

DIMOSTRAZIONE PER INDUZIONE

- Base $n=1$

  Il sistema è $(a_{11}x = b_1)$ ha soluzione unica se e solo se $a_{11} \neq 0$

- Passo induttivo: Supponiamo vera la tesi per $n-1$, dimostriamo che è vera per n.

  (Ipotesi induttiva) $A''\underline{x} = \underline{b}''$ con $A'' \in Mat_{n-1 \times n-1}(\mathbb{K})$

  ammette unica soluzione $\iff \exists\, D''\underline{x} = \underline{c}''$ con D'' diagonale.

  $\Leftarrow$ Se la matrice D è diagonale e $d_{11}, \dots, d_{nn}$ sono non nulli, il sistema ha la forma

$$\begin{cases} d_{11}x_1 = c_1 \\ \vdots \\ d_{nn}x_n = c_n \end{cases} \qquad \begin{cases} x_1 = \dfrac{c_1}{d_{11}} \\ \vdots \\ x_n = \dfrac{c_n}{d_{nn}} \end{cases} \qquad d_{ii} \neq 0$$

Quindi ammette un unica soluzione, dato che è equivalente a $A\underline{x} = \underline{b}$

$\Rightarrow$ Il sistema $A\underline{x} = \underline{b}$ ammette un unica soluzione, quindi voglio trovare D diagonale.

Suppongo $a_{11} \neq 0$

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{nn} & \cdots & a_{nn} & b_n \end{pmatrix} \xrightarrow[\text{con Gauss}]{\text{Opero}} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ 0 & a'_{22} & \cdots & a'_{2n} & b'_2 \\ \vdots & \vdots & & & \\ 0 & a'_{n2} & \cdots & a'_{nn} & b'_n \end{pmatrix}$$

La matrice tra parentesi soddisfa la tesi ed ha ordine $n-1$.

Siccome per ipotesi ho $d_{ii} \neq 0$, posso arrivare con trasformazioni di Gauss a $D''\underline{x} = \underline{c}''$. Quindi la tesi è vera.

COROLLARI

1. Sia $\mathbb{K}$ campo, $A \in Mat_{m \times n}$, posso sempre utilizzando operazioni di Gauss, ridurre la matrice in forma: a scala, standard o normale.

2. Sia $\mathbb{K}$ campo, $A \in Mat_{n \times n}$, operando con Gauss posso mettere la matrice in forma triangolare superiore.

<u>Definizione</u>: Una matrice diagonale di ordine n con gli elementi sulla diagonale tutti uguali a 1 si denota come matrice identità di ordine n. $[I_n]$

PRODOTTO DI MATRICI

Siano $A, B \in Mat_{n \times n}(\mathbb{K})$

$$A \cdot B = (A_i \cdot B^j) \qquad i, j : 1, \dots, n$$

riga i-esima colonna j-esima

è il prodotto di matrici quadrate

<u>Definizione</u>: la matrice identità I_n, con le righe i-esima e j-esima scambiate si indica con S_n^{ij}.

Data una matrice $B \in Mat_{n \times n}(K)$,

la matrice $S_n^{ij} \cdot B$ è uguale alla matrice B ma con le righe i-esima e j-esima scambiate.

ES: $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 7 & 8 & 9 \\ 4 & 5 & 6 \\ 1 & 2 & 3 \end{pmatrix}$

PROPRIETÀ DEL PRODOTTO DI MATRICI

L'insieme delle matrici $(Mat_{n \times n}(K), +)$

è un gruppo commutativo perché $A+B = B+A$

con neutro additivo 0, la matrice con elementi tutti nulli

<u>Proposizione</u>: l'insieme delle matrice $(Mat_{n \times n}(K), +, \cdot)$

è un anello non commutativo, con:

- neutro moltiplicativo $= I_n$
- neutro additivo $= \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} = O_n$

Valgono le seguenti proprietà:

$$(A+B) \cdot C = AC + BC$$

$$C(A+B) = CA + CB$$

$$\lambda(A \cdot B) = (\lambda \cdot A) \cdot B = A \cdot (\lambda B)$$

Per vedere che il prodotto di matrici non è commutativo, basta far vedere che: $A \cdot B \neq B \cdot A$

$$\begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 11 & 6 \end{pmatrix} \neq \begin{pmatrix} 5 & 6 \\ 11 & 12 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}$$

Quindi $(A+B)^2 = A^2 + B^2 + AB + BA$

OSSERVAZIONE: Nell'anello delle matrici esistono zero-divisori. Quindi esistono:

$$A, B \in Mat_{n \times n}(\mathbb{K}) \qquad \text{con } A, B \neq O_n$$

$$A \cdot B = O$$

Definizione: Una matrice $A \in Mat_{n \times n}(K)$ è detta NIPOTENTE se esiste $k > 0$ tale che:

$$A^k = O \qquad \text{con } A \neq O$$

ES:

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

Proposizione: non vale la legge di cancellazione del prodotto ovvero, per $A, B, C \in Mat_{n \times n}$ non vale necessariamente:

$$A \cdot B + A \cdot C = O \implies B + C = O \qquad \text{con } A \neq O$$

$$\begin{pmatrix} -2 & 1 \\ -2 & 1 \end{pmatrix}\left[\begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 2 \\ 0 & 4 \end{pmatrix}\right] = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

PRODOTTO PER MATRICI NON QUADRATE

Sia $A \in Mat_{m \times n}(\mathbb{K})$ e $B \in Mat_{n \times k}(\mathbb{K})$

Allora la matrice $A \cdot B \in Mat_{m \times k}$ è definita:

$$A \cdot B = (A_i \cdot B^j) \quad \text{con } i: 1, \dots, m \quad \text{e } j: 1, \dots, k$$

Si dice prodotto matriciale di A, B

OSS: il numero delle colonne di A coincide con il numero delle righe di B.

Queste matrici non formano un anello, dato che hanno l'identità destra e quella sinistra

ESEMPIO

$$\underset{2 \times 3}{\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}} \underset{3 \times 2}{\begin{pmatrix} 1 & 2 \\ 4 & 5 \\ 1 & 1 \end{pmatrix}} = \underset{2 \times 2}{\begin{pmatrix} 12 & 15 \\ 30 & 39 \end{pmatrix}}$$

MATRICI INVERTIBILI

Sia $A \in Mat_{n \times n}(\mathbb{K})$. Una matrice $X \in Mat_{n \times n}$ si dice inversa moltiplicativa destra di A, se $A \cdot X = I_n$.
Una matrice Y si dice inversa moltiplicativa sinistra di A, se $Y \cdot A = I_n$.

PROBLEMA

1. L'inversa dx è sempre uguale a quella sx?
2. È unica?
3. Determinare se una matrice è invertibile senza calcolare tale inversa.

Voglio determinare tutte le matrici 2×2 tali che:

$$A \cdot X = I_2 \quad e \quad Y \cdot A = I_2$$

Iniziamo da quella destra:

$$\left(\begin{array}{cc|cc} a & b & 1 & 0 \\ c & d & 0 & 1 \end{array}\right)$$

$a \neq 0$

$$\begin{array}{c} \\ II^{\wedge} - \frac{c}{a} I^{\wedge} \end{array} \left(\begin{array}{cc|cc} a & b & 1 & 0 \\ 0 & \frac{(ad-bc)}{a} & -\frac{c}{a} & 1 \end{array}\right)$$

$(ad-bc) \neq 0$

$$\left(\begin{array}{cc|cc} 1 & 0 & \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ 0 & 1 & \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{array}\right) \qquad X = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Se $ad-bc = 0$ il sistema è impossibile

Se $ad-bc \neq 0$ tale inversa è unica

A questo punto vogliamo vedere se esiste unica l'inversa sinistra (Y), sapendo che l'inversa destra (X) esiste ovvero che $A \cdot X = I_2$. Vogliamo risolvere $Y \cdot A = I_2$, quindi:

$$Y \cdot A \cdot X = I_2 X$$
$$Y I_2 = X$$
$$Y = X$$

quindi esiste unica l'inversa sinistra ed è uguale a quella destra

<u>Definizione</u>: Sia $A \in Mat_{n \times n}(\mathbb{K})$. Se esiste unica l'inversa destra, allora esiste unica l'inversa sinistra e viceversa. Chiamiamo questa matrice inversa di A e la scriviamo con A^{-1}. Diremo che A è invertibile.

$$A \cdot A^{-1} = A^{-1} \cdot A = I_n$$

COROLLARIO

$$\left(\{ A \in Mat_{n \times n}(\mathbb{K}) \mid A \text{ è invertibile} \}, \cdot \right)$$

è un gruppo, con neutro moltiplicativo I_n.

<u>OSSERVAZIONE</u> Sia $A \in Mat_{m \times n}(K)$ con $m \neq n$ non hanno inversa

Proposizione: Sia $A \in Mat_{n \times n}(\mathbb{K})$, allora le seguenti condizioni sono equivalenti.

1. A ha inversa destra
2. A ha inversa sinistra
3. Il sistema $A\underline{x} = \underline{0}$ ha unica soluzione $\underline{x} = \underline{0}$
4. Il sistema $A\underline{x} = \underline{b}$ ha unica soluzione
5. A è invertibile.

Definizione: Sia $A \in Mat_{n \times n}(\mathbb{K})$ che soddisfi le condizioni della preposizione precedente. Diremo che la matrice A è non singolare, altrimenti, la diremo singolare. La non singolarità e l'invertibilità sono sinonimi.

ESEMPI:

Calcolare l'inversa:

$\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$ $\quad ad - bc = 1 - 2 = -1 \quad$ $\begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix}$

$\begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}$ $\quad ad - bc = 2 - 2 = 0 \quad$ non invertibile

MATRICE TRASPOSTA

Sia $A \in Mat_{m \times n}(\mathbb{K})$

$A = (a_{ij})$ $i: 1, \dots m$ e $j: 1 \dots n$

la matrice (a_{ji}) $j: 1, \dots, n$ e $i: 1, \dots, m$

è detta matrice trasposta di A e si scrive A^T.

Trasporre una matrice ne scambia le righe con le colonne

ESEMPIO $A = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{pmatrix}$ $A^T = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

Proprietà

Sia $A \in Mat_{m \times n}(\mathbb{K})$

1. $(A^T)^T = A$
2. $\forall t \in K$ $(tA)^T = tA^T$
3. $B \in Mat_{m \times n}(\mathbb{K})$ $(A+B)^T = A^T + B^T$
4. $B \in Mat_{n \times m}(\mathbb{K})$ $(A \cdot B)^T = B^T \cdot A^T$

   Poiche $B^T \cdot A^T \in Mat_{n \times m}(\mathbb{K})$ e $A \cdot B \in Mat_{n \times m}(\mathbb{K})$
5. Se A invertibile $(A^{-1})^T = (A^T)^{-1}$

Basta dimostrare che $(A^T)^{-1}$ è inversa sinistra di A^T.

e grazie al punto 4:

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

Definizione: Sia $A(a_{ij})$ quadrata, e detta simmetrica se $A = A^T$, ovvero se $(a_{ij}) = (a_{ji})$

ES: $\begin{pmatrix} 1 & 0 & 3 \\ 0 & \pi & 2 \\ 3 & 2 & e \end{pmatrix}$

Definizione: A quadrata è antisimmetrica se $A^T = -A$, ovvero $(a_{ij}) = (-a_{ji})$. Gli elementi sopra la diagonale sono uguali all'opposto dei corrispondenti elementi sotto la diagonale, e gli elementi sulla diagonale sono zeri.

ES $\begin{pmatrix} 0 & 1 & 2 \\ -1 & 0 & 3 \\ -2 & -3 & 0 \end{pmatrix}$

Proposizione Una matrice $A \in Mat_{m \times m}(K)$ è somma di una matrice simmetrica $B = A + A^T$ e una antissimmetrica $C = A - A^T$

$$A = \frac{1}{2}(A + A^T) + \frac{1}{2}(A - A^T)$$

Basta dimostrare che $A + A^T$ è simmetrica e $A - A^T$ è antisim.

- Verifichiamo che $(A + A^T)_{ij} = (A + A^T)_{ji}$. Infatti

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

- Per il secondo caso dobbiamo verificare:

$$(A - A^T)_{ij} = -(A + A^T)_{ji} \quad \text{Infatti}$$

$$(A - A^T)_{ij} = a_{ij} - a_{ji} = -a_{ji} + a_{ij} = -(a_{ji} - a_{ij}) = (A - A^T)_{ji}$$

Definizione: Data una matrice quadrata $A \in Mat_{n \times n}(\mathbb{K})$ e due interi i, j tali che $1 \leq i, j \leq n$, definiamo minore (i,j) di A, e scriviamo $A_{i,j}$, la matrice ottenuta dalla cancellazione della i-esima riga e j-esima colonna

ES: $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ $\quad A_{1,1} = \begin{pmatrix} 5 & 6 \\ 8 & 9 \end{pmatrix}$

TEOREMA DEL DETERMINANTE LAPLACE

Esiste un unica applicazione

$$\det : Mat_{n \times n}(\mathbb{R}) \longrightarrow \mathbb{R}$$

Che soddisfa le seguenti applicazioni:

1. Se $A = (a_{11}) \in Mat_{1 \times 1}(\mathbb{K})$, $\det(A) = a_{11}$
2. Sviluppo di Laplace sulla riga i-esima, $i: 1, \dots, n$

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{i,j} \cdot \det(A_{i,j}) \qquad \text{N.B. } i \text{ è fissato}$$

3. Sviluppo di Laplace sulla colonna j-esima, $j: 1, \dots, n$

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{i,j} \cdot \det(A_{i,j}) \qquad \text{N.B. } j \text{ è fissato}$$

4. $\det(AB) = \det(A) \cdot \det(B)$ <u>Teorema di Binet</u>

OSS: Sappiamo che una matrice

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

è invertibile se e solo se $ad - bc \neq 0$. Questo vuol dire anche che le righe, o le colonne di A sono linearmente indipendenti, e quindi hanno $\det \neq 0$

COROLLARI

1. $\det(I_n) = 1$ $\qquad$ $\det(O_n) = 0$

2. Il determinante di una matrice diagonale D è il prodotto degli elementi sulla diagonale, ovvero:

$$\det D = \prod_{i=1}^{n} d_{ii}$$

3. $\det(A^T) = \det(A)$

La dimostrazione viene dal fatto che posso calcolare il det. sviluppando sia per riga che per colonna

4. $\det(A^{-1}) = \dfrac{1}{\det(A)}$

Dato che $\det(A^{-1}) \cdot \det(A) = 1$

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

Definizione Scambiare una riga o una colonna mi cambia il segno del determinante.

DIMOSTRAZIONE

$$A = I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \longrightarrow \det = 1$$

Prendiamo $Sm_4^{1,4}$, la matrice elementare che scambia le righe 1,4

$$Sm_4^{1,4} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \leftarrow \quad : 1 \cdot \det \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \leftarrow$$

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

OSSERVAZIONE

Un operazione di Gauss del tipo

$$R_j \longrightarrow R_j + \lambda R_i$$

non cambia il determinante della matrice.

COROLLARIO Una matrice e una sua riduzione a scala hanno lo stesso determinante.

Dato che S si ottiene mediante operazioni di Gauss dobbiamo solo ricordarsi gli scambi di riga o di colonna, dato che mi fanno cambiare il segno del det.

A questo punto il det. di S è dato dagli elementi sulla diagonale (i pivot).

REGOLA DI SARRUS

Sia $A \in Mat_{3\times 3}(\mathbb{K})$

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \qquad S = \begin{pmatrix} a & b & c & a & b \\ d & e & f & d & e \\ g & h & i & g & h \end{pmatrix}$$

Allora il suo determinante si può calcolare:

$$\det : A = aei + bfg + cdh - gec - hfa - idb$$

Ovvero è la somma del prodotto degli elementi su ogni diagonale meno la somma del prodotto degli elementi su ogni antidiagonale

Proposizione (Combinazioni lineari)

Una matrice $A \in Mat_{n \times n}(\mathbb{K})$ ha:

$\det(A) \neq 0 \iff A_1, \dots, A_n$ sono linearmente indipendenti

$\Updownarrow$

$A \xrightarrow{GAUSS} S$ $\det(S) \neq 0 \iff$ ho n pivot e quindi $S_1, \dots, S_n$ sono linearmente indipendenti

ridurre una matrice a scala non cambia il det.

Quindi:

$\det(A) \neq 0$ righe / colonne linearmente indipendenti

$\det(A) = 0$ righe / colonne linearmente dipendenti.

RANGO DI UNA MATRICE

Il rango mi dice il numero di righe o di colonne dentro una matrice che sono linearmente indipendenti.

Definizione: Sia $A \in Mat_{m \times n}(\mathbb{K})$ tale che:

1. Esiste una sottomatrice quadrata di ordine r non singolare. ($\det \neq 0$)
2. Tutte le sue sottomatrici quadrate di ordine $> r$ sono singolari.

Allora diciamo che la matrice A ha rango r.

$rk(A) = r$

Proposizione Sia $A \in Mat_{m \times n}(\mathbb{K})$

ed $A_{(i_1, \dots, i_s)(j_1, \dots, j_s)}$ una sua sottomatrice

non singolare. Allora le sue righe $(i_1 \dots i_s)$ sono

linearmente indipendenti.

DIMOSTRAZIONE

Supponiamo per assurdo che non lo siano.

Allora esistono $\alpha_1, \dots, \alpha_s \in \mathbb{K}$, $\underline{\alpha} \neq \underline{0}$ tali che:

$$\alpha_1 A_{i_1} + \dots + \alpha_s A_{i_s} = \underline{0}$$

Ogni riga A_i, può essere scritta come:

$A_i = A_i' + A_i''$ dove: A_i' sono le colonne "impigliate"

A_i'' sono le colonne non "impigliate"

(Per capire) $A = (1, \overset{A_i'}{\boxed{2, 3, 4}}, 5) = \overset{A'}{(0, 2, 3, 4, 0)} + \overset{A''}{(1, 0, 0, 0, 5)}$

Possiamo scrivere

$$\alpha_1 (A_{i_1}' + A_{i_1}'') + \dots + \alpha_s (A_{i_s}' + A_{i_s}'') = \underline{0}$$

$$\begin{cases} \alpha_1 (A_{i_1}') + \dots + \alpha_s (A_{i_s}') = \underline{0} \\ \alpha_1 (A_{i_1}'') + \dots + \alpha_s (A_{i_s}'') = \underline{0} \end{cases}$$

ma la prima equazione ci dice che le righe $i_1, \dots, i_s$

sono linearmente dipendenti. ASSURDO

TEOREMA DEGLI ORLATI

Sia $A \in Mat_{m \times n}(\mathbb{K})$ e $B_{(i_1, \dots, i_R)(j_1, \dots, j_R)}$ una sua sottomatrice non singolare di ordine r.

Allora $\forall\, i, j$ $\quad i \notin \{i_1 \dots i_R\}$ $\quad j \notin \{j_1, \dots, j_R\}$

il $\det(B')_{(i_1, \dots, i_R, i)(j_1, \dots, j_R, j)} = 0$

$\Rightarrow rk(A) = r$

Stiamo 'orlando' B, con una riga e una colonna di A

COROLLARIO

1. $rk(A) = r$
2. $A \xrightarrow{GAUSS} S$ $\quad$ S ha r righe non nulle
3. $A \xrightarrow{GAUSS} S$ $\quad$ S ha r pivot
4. Il numero massimo di righe o colonne linearmente indipendenti è r.

Definizione Il vettore di $\mathbb{K}^n$ che ha tutte le componenti nulle tranne la i-esima si indica come $\underline{e}_i$ e si chiama vettore canonico

$$\mathbb{K}^5 \ni \underline{e}_3 = (0, 0, 1, 0, 0)$$

FORMULA DI CRAMER

Sia $A \in Mat_{n \times n}(\mathbb{K})$ non singolare, con il sistema $A\underline{x} = \underline{b}$ con:

- $A = (A^1, \dots, A^n)$ data per colonne
- $B_i = (A^1, \dots, A^{i-1}, \underline{b}, A^{i+1}, \dots, A^n)$ la i-esima colonna è sostituita da $\underline{b}$.

Allora: $x_i = \dfrac{\det(B_i)}{\det(A)}$

Vorremmo usare il teorema di Binet su $A \cdot X_i = B_i$

Costruiamo X_i per colonne:

$$X_i = (\underline{e}_1, \dots, \underline{e}_{i-1}, x_i, \underline{e}_{i+1}, \dots, \underline{e}_n) \quad \det(X_i) = x_i$$

Quindi:

$$A \cdot X_i = (A^1, \dots, A^{i-1}, A \cdot x, A^{i+1}, \dots, A_n)$$

$$A \cdot X_i = (A^1, \dots, A^{i-1}, b, A^{i+1}, \dots, A_n) = B_i$$

$$A \cdot X_i = B_i$$

Applicando il teorema di Binet:

$$\det(A \cdot X_i) = \det(B_i)$$

$$\det(A) \cdot x_i = \det(B_i)$$

$$x_i = \frac{\det(B_i)}{\det(A)}$$

<u>Definizione</u> Sia $A \in Mat_{n \times n}(\mathbb{K})$. La matrice

$$(A^*)_{ij} = (-1)^{i+j} \det A_{ji}$$

si dice matrice complemento di A

TEOREMA DELL' INVERSA

Sia $A \in Mat_{n \times n}(\mathbb{K})$ invertibile e A^* la sua matrice complemento. Allora $A^{-1} = \frac{1}{\det A} \cdot A^*$

DIMOSTRAZIONE

L'inversa X di A, che esiste unica, è la soluzione dell'equazione $AX = I_n$ e scritto per colonna

$$AX^1 = \underline{e}_1 \quad \dots\dots\dots \quad AX^n = \underline{e}_n$$

$$A \cdot (x_{i1}) = \underline{e}_1 \quad \dots\dots \quad A(x_{in}) = \underline{e}_n \qquad i: 1, \dots, n$$

Usando la formula di Cramer:

$$x_{ij} = \frac{\det(A^1, \dots, A^{i-1}, \underline{e}_j, A^{i+1}, \dots A^n)}{\det(A)}$$

Sviluppando con Laplace secondo la i-esima riga:

$$x_{ij} = \frac{1}{\det(A} \cdot (-1)^{i+j} \cdot \det A_{ji}$$

Quindi $x_{ij} = X$ che è l'inversa A^{-1}

ESEMPIO

Calcolare l'inversa : $A = \begin{pmatrix} 2 & 1 & 2 \\ 3 & 0 & 1 \\ 1 & 1 & 2 \end{pmatrix}$

Calcoliamo il det : $\begin{pmatrix} 2 & 1 & 2 & 2 & 1 \\ 3 & 0 & 1 & 3 & 0 \\ 1 & 1 & 2 & 1 & 1 \end{pmatrix} = 1+6-2-6 = -1$

$x_{11} = (-1)^{1+1} \cdot \det A_{11} = + \det \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} = -1$

$x_{1,2} = -1 \cdot \det \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = 0$

$x_{1,3} = +1 \cdot \det \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = 1$

$x_{21} = -1 \cdot \det \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix} = -5$

$x_{22} = +1 \cdot \det \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix} = 2$

$x_{23} = -1 \cdot \det \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix} = 4$

$x_{31} = 1 \cdot \det \begin{pmatrix} 3 & 0 \\ 1 & 1 \end{pmatrix} = 3$

$x_{32} = -1 \cdot \det \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = -1$

$x_{33} = 1 \cdot \det \begin{pmatrix} 2 & 1 \\ 3 & 0 \end{pmatrix} = -3$

$A^* = \begin{pmatrix} -1 & 0 & 1 \\ -5 & 2 & 4 \\ 3 & -1 & -3 \end{pmatrix}$

$A^{-1} = \begin{pmatrix} 1 & 0 & -1 \\ 5 & -2 & -4 \\ -3 & 1 & 3 \end{pmatrix}$

$$\begin{pmatrix} 2 & 1 & 2 \\ 3 & 0 & 1 \\ 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 5 & -2 & -4 \\ -3 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

SPAZI VETTORIALI

Uno spazio vettoriale su $\mathbb{R}$ è un insieme V su cui sono definite due operazioni:

- una somma (che a due elementi di V associa un elemento di V)
- un prodotto per scalari (che a un elemento di $\mathbb{R}$ e a uno di V ne associa uno di V)

In particolare $(V, +)$ è un gruppo commutativo.

OSSERVAZIONE: Sia A un insieme qualunque, e V l'insieme di tutte le funzioni da A in $\mathbb{R}$. Definiamo una somma e un prodotto per scalari su V nel seguente modo: se $f, g \in V$ e $\lambda \in \mathbb{R}$

allora $f+g, \lambda f : A \to \mathbb{R}$ sono definite da

$\forall a \in A \quad (f+g)a = f(a)+g(a)$ e $(\lambda f)(a) = \lambda f(a)$

ESEMPIO:

- $\mathbb{C}$ è un $\mathbb{C}$-spazio
- $\mathbb{Q}[\sqrt{2}]$ è $\mathbb{Q}$-spazio
- $\mathbb{Q}[\sqrt{2}]$ non è $\mathbb{R}$-spazio

ESEMPIO

$(W, \circ, \cdot)$ non è un $\mathbb{K}$-spazio perché sebbene $(W, \circ)$ sia un gruppo non è commutativo.

<u>Definizione</u> Sia $\mathbb{K}$-spazio $(V, +, \cdot)$ e $W \subseteq V$, diciamo che W è un SOTTOSPAZIO di V come $\mathbb{K}$-spazio se e solo se V è chiuso rispetto alle operazioni di somma e moltiplicazione (esterna) per elementi di $\mathbb{K}$.
Quindi il risultato di tali operazioni su W appartiene ancora a W.

Ovvero:
- $\forall\, \underline{w}_1, \underline{w}_2 \in W \quad \underline{w}_1 + \underline{w}_2 \in W$
- $\forall\, \lambda \in \mathbb{K}, \underline{w}_1 \in W \quad \lambda \underline{w}_1 \in W$

Scriveremo $W \underset{SSP}{\subseteq} V$

OSS:

Dato V $\mathbb{K}$-spazio, ci sono almeno due sottospazi banali $V \underset{SSP}{\subseteq} V$ e $\{0\} \underset{SSP}{\subseteq} V$

Esempi: I polinomi in $\mathbb{K}[x]$ di grado minore od uguale a d formano un sottospazio vettoriale.

$$\mathbb{K}[x]_{\leq d} = \{ p(x) \in K[x] \mid \deg(p(x) \leq d) \} \underset{SSP}{\subseteq} \mathbb{K}[x]$$

Ogni retta passante per l'origine è un sottospazio di $\mathbb{R}^2$

GENERATORI

Sia V un $\mathbb{K}$-spazio e $\underline{v}_1, \dots, \underline{v}_m \in V$, abbiamo che

$$\text{span}(\underline{v}_1, \dots, \underline{v}_m) = \{\lambda_1 \underline{v}_1 + \dots \lambda_m \underline{v}_m \mid \lambda_1, \dots \lambda_m \in \mathbb{K}\} \underset{SSP}{\subseteq} V$$

I vettori $\underline{v}_1 \dots \underline{v}_m$ si dicono generatori di $\text{span}_{\mathbb{K}}(\underline{v}_1, \dots, \underline{v}_m)$

Dati $\alpha, \beta \in \mathbb{K}$ e $\underline{w}_1, \underline{w}_2 \in \text{span}(\underline{v}_1 \dots \underline{v}_m)$ abbiamo che

$$\alpha \underline{w}_1 + \beta \underline{w}_2 \in \text{span}(\underline{v}_1, \dots, \underline{v}_m)$$

<u>Definizione</u>: I vettori $\underline{e}_i$ si dicono generatori canonici di $\mathbb{K}^n$

Da qui potrebbe sorgere un dubbio, ovvero: quanti generatori sono necessari per generare tutto uno spazio o un sottospazio vettoriale?

BASI

Sia V un $\mathbb{K}$-spazio e $\underline{v}_1, \dots, \underline{v}_m \in V$. Se:

1. $\underline{v}_1, \dots, \underline{v}_m$ generano V

   equivalentemente: $\text{span}(\underline{v}_1, \dots \underline{v}_m) = V$

2. $\underline{v}_1, \dots, \underline{v}_m$ sono linearmente indipendenti

Diciamo che $\underline{v}_1, \dots, \underline{v}_m$ formano una base di V come $\mathbb{K}$-spazio.

ESEMPI

1. $\underline{e}_1, \dots, \underline{e}_n$ formano una base di $\mathbb{K}^n$
2. $1, x, \dots, x^n$ formano una base di $\mathbb{K}[x]_{\leq n}$

COROLLARIO

Le basi non sono uniche.

Proposizione Sia V $\mathbb{K}$-spazio e $B = \underline{v}_1, \dots, \underline{v}_n$ una sua base

Allora per ogni vettore $\underline{w} \in V$ esiste un unica n-upla di elementi di $\mathbb{K}$ tale che.

$$\lambda_1 \underline{v}_1 + \dots + \lambda_n \underline{v}_n = \underline{\lambda}\, \underline{\underline{v}} = \underline{w}$$

DIMOSTRAZIONE

Dato che i vettori $\underline{\underline{v}}$ generano V, per ogni vettore $\underline{w} \in V$ esistono scalari $\underline{\lambda}$ tali che $\underline{\lambda} \cdot \underline{\underline{v}} = \underline{w}$. Voglio dimostrare che sono unici:

$$\underline{\lambda} = \lambda_1, \dots, \lambda_n \quad \text{t.c.} \quad \underline{\lambda} \cdot \underline{\underline{v}} = \underline{w}$$

$$\underline{\beta} = \beta_1, \dots, \beta_n \quad \text{t.c.} \quad \underline{\beta} \cdot \underline{\underline{v}} = \underline{\underline{w}}$$

Supponiamo per assurdo che $\underline{\lambda} \neq \underline{\beta}$ e $\underline{\lambda} \cdot \underline{\underline{v}} = \underline{\beta} \cdot \underline{\underline{v}} = \underline{w}$

Avremmo $(\underline{\lambda} - \underline{\beta}) \cdot \underline{\underline{v}} = \underline{0}$

ma dato che $\underline{v}_1, \dots \underline{v}_n$ sono linearmente indipendenti

$$\underline{\lambda} - \underline{\beta} = 0 \implies \underline{\lambda} = \underline{\beta}$$

ASSURDO!

Definizione: Sia V un $\mathbb{K}$-spazio. I vettori $\underline{v}_1, \dots \underline{v}_m \in V$ si dicono sistema minimale di generatori di V se generano V, e se togliendone uno non lo generano più.

PROPOSIZIONE Sia V un $\mathbb{K}$-spazio e $B = \underline{v}_1, \dots, \underline{v}_m \in V$. Allora

B è base $\iff$ B è un sistema minimale di generatori di V

"$\Leftarrow$" Voglio dimostrare che $\underline{v}_1, \dots, \underline{v}_m$ sono linearmente indipendenti

Suppongo per assurdo che non lo siano

Questo vuol dire che esiste v_i inutile nella generazione di V.

ASSURDO

"$\Rightarrow$" basta far vedere che $\underline{v}_1, \dots, \underline{v}_{i-1}, \underline{v}_{i+1}, \underline{v}_m$ non generano V

Infatti, per assurdo:

$$\mathrm{Span}(\underline{v}_1, \dots, \underline{v}_m) = V \quad - \{v_i\}$$

Avremmo che $\underline{v}_i$ è combinazione lineare di

$\underline{v}_1, \dots \underline{v}_{i-1}, \underline{v}_{i+1}, \dots \underline{v}_m$ e questo è assurdo perché per ipotesi $\underline{v}_1, \dots, \underline{v}_m$ sono linearmente indipendenti

OSS: Possiamo eliminare da un sistema di generatori $\underline{v}_1, \dots, \underline{v}_m$ di V i vettori dipendenti e quando raggiungiamo un sistema minimale di V abbiamo trovato una base.

Definizione: Sia V un $\mathbb{K}$-spazio. I vettori $\underline{v}_1, \dots, \underline{v}_m$ di V, linearmente indipendenti, si dicono un sistema massimale di vettori linearmente indipendenti per V se non esiste $\underline{w} \in V$ tale che $\underline{w}, \underline{v}_1, \dots, \underline{v}_m$ sono linearmente indipendenti.

Ovvero

- $\underline{v}_1, \dots, \underline{v}_m$ sono indipendenti tra loro
- $\forall \underline{v} \in V$ $\underline{v}_1, \dots, \underline{v}_m, \underline{v}$ sono dipendenti

PROPOSIZIONE

B è base $\Leftrightarrow$ B è un sistema massimale di vettori linearmente indipendenti di V

OSSERVAZIONE

Se continuo ad aggiungere al vettore di V $\underline{v}_1$, dei vettori $\underline{v}_i$, in modo tale che $\underline{v}_1, \dots, \underline{v}_m$ sono linearmente indipendenti, SE ad un certo punto non riesco più a procedere trovo una base.

TEOREMA DEL COMPLETAMENTO

Sia V un $\mathbb{K}$-spazio e $\underline{w}_1, \dots, \underline{w}_p \in V$ linearmente indipendenti

Sia $B = \underline{v}_1, \dots, \underline{v}_m$ una base di V con $m > p$.

Allora esistono $m-p$ vettori di B che insieme a $\underline{w}_1, \dots, \underline{w}_p$ formano una base di V.

Quindi $\underline{w}_1, \dots, \underline{w}_p, \underline{v}_{i_1}, \dots \underline{v}_{i_{m-p}}$ sono una base di V.

DIMOSTRAZIONE

$$\underline{v}_i = \underline{e}_{i_B}$$

$$\begin{bmatrix} \underline{w}_1 \\ \vdots \\ \underline{w}_p \\ \underline{e}_1 \\ \vdots \\ \underline{e}_m \end{bmatrix}$$

Senza scambi di riga riduco i primi p vettori con Gauss, mettendo la matrice in forma normale

$$\left[\begin{array}{c|c} I_p & A \\ \hline \multicolumn{2}{c}{\underline{e}_{k_1}} \\ \multicolumn{2}{c}{\vdots} \\ \multicolumn{2}{c}{\underline{e}_{k_m}} \end{array}\right]$$

← perché potrei aver scambiato delle colonne

Adesso operiamo sulla seconda parte.

Dividiamo le righe $\underline{e}_{k_1}, \dots \underline{e}_{k_m}$ in due insiemi:

B': che contiene le righe che hanno le seconde coordinate p nulle

B'': che contiene le righe che hanno le prime coordinate p nulle.

Ottenendo riordinando le righe la matrice a blocchi

$$\begin{array}{c} \underline{w} \\ B' \\ B'' \end{array} \left(\begin{array}{c|c} I_p & A \\ \hline I_p & O_p \\ \hline O_{m-p} & I_{m-p} \end{array}\right)$$

Riducendo con Gauss (sostituzione all'indietro)

$$\begin{array}{c} \underline{w} \\ B' \\ B'' \end{array} \left(\begin{array}{c|c} I_p & O_p \\ \hline O_p & O_p \\ \hline O_{m-p} & I_{m-p} \end{array}\right)$$

Posso affermare che i vettori $\underline{w}_1, \dots, \underline{w}_p, \underline{v}_{i_1}, \dots, \underline{v}_{m-p}$ sono una base di V, dato che sono linearmente indipendenti

OSS: avrei potuto ridurre $\underline{w}$ a scala e poi aggiungere i vettori $\underline{e}_i$ corrispondenti alle righe che non si riducano a zero.

COROLLARIO

Siano B_1, B_2 base di V $\mathbb{K}$-spazio.

allora $\# B_1 = \# B_2$

DIMENSIONI

Sia V un $\mathbb{K}$-spazio con base $B = v_1, \dots, v_n$.

Diciamo che V ha dimensione B e scriviamo

$$\dim B = n$$

ESEMPI

- $\dim \mathbb{K}^n = n$
- $\dim \mathbb{K}[x]_d = d+1$
- $\dim \mathrm{Mat}_{m \times n}(\mathbb{K}) = m \times n$

SOMMA E INTERSEZIONE DI SOTTOSPAZI

Sia V un $\mathbb{K}$-spazio, e $U, W \underset{SSP}{\subseteq} V$. Allora

1. L'insieme

$$U + W = \{ \underline{u}_1 + \underline{w}_2 \mid \underline{u}_1 \in U \text{ e } \underline{w}_2 \in W \}$$

$$= \{ \lambda \underline{u}_1 + \mu \underline{w}_2 \mid \underline{u}_1 \in U \text{ e } \underline{w}_2 W \text{ e } \lambda, \mu \in \mathbb{K} \}$$

si dice lo spazio somma $U + W \underset{SSP}{\subseteq} V$.

2. L'insieme

$$U \cap W = \{ \underline{t} \mid \underline{t} \in U \text{ e } \underline{t} \in W \} \underset{SSP}{\subseteq} V$$

si dice lo spazio di intersezione $U \cap W$.

DIMOSTRAZIONE

Siano $\underline{t}_1 \in U \cap W$ e $\underline{t}_2 \in U \cap W$ e $\lambda, \mu \in \mathbb{K}$. Quindi

$$\lambda \underline{t}_1 + \mu \underline{t}_2 \in U \cap W$$

$\underline{t}_1 \in U \cap W \Rightarrow \underline{t}_1 \in U$ e $\underline{t}_1 \in W$

$\underline{t}_2 \in U \cap W \Rightarrow \underline{t}_2 \in U$ e $\underline{t}_2 \in W$

dato che $W, U \underset{SSP}{\subseteq} V$ abbiamo

$$\lambda \underline{t}_1 + \mu \underline{t}_2 \in U \quad \text{e} \quad \lambda \underline{t}_1 + \mu \underline{t}_2 \in W,$$

quindi $\lambda \underline{t}_1 + \mu \underline{t}_2 \in U \cap W$

OSS: l'unione insiemista $U \cup W$, non è un sottospazio.

LEMMA

Sia V un $\mathbb{K}$- spazio $W_1, W_2 \underset{SSP}{\subseteq} V$. Siano B, C sistemi di generatori di W_1, W_2. Allora $B \cap C$ è un sistema di generatori di $W_1 + W_2$

Ex: $W_1 = \text{span}(1,1,1,1)(2,1,3,3)$

$W_2 = \text{span}(3,2,4,4)(1,1,2,2)$

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 1 & 3 & 3 \\ 3 & 2 & 4 & 4 \\ 1 & 1 & 2 & 2 \end{pmatrix} \xrightarrow[\text{senza scambi di riga}]{\text{GAUSS}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & -1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Ho trovato una base di $W_1 + W_2$

$\text{span}(1,1,1,1)(0,-1,1,1)(0,0,1,1)$

Base $W_1 \cap W_2 \rightarrow \text{span}(3\ 2\ 4\ 4)$

↳ Perché l'ho ridotto a $\underline{0}$ con solo elementi di W_1, quindi $\in W_1$ e $\in W_2 \Rightarrow \in W_1 \cap W_2$

FORMULA DI GRASSMAN

Sia V $\mathbb{K}$-spazio di dimensione finita n,

e $U, W \underset{SSP}{\subseteq} V$, allora:

$$\dim(U+W) = \dim U + \dim W - \dim U \cap W$$

DIMOSTRAZIONE

Esiste una base di $U \cap W$ $v_1, \dots, v_p$.

Dato che U e W hanno dimensione finita e dato che contengono $U \cap W$, li completo a base:

$\underline{v}_1, \dots, v_p, \underline{u}_1, \dots \underline{u}_t$ base di U

$\underline{v}_1, \dots, v_p, \underline{w}_1, \dots, \underline{w}_s$ base di W

Esprimiamo queste basi in forma matriciale:

$$\begin{bmatrix} \underline{v} \\ \hline \underline{u} \end{bmatrix} \xrightarrow{\text{sono lin ind.}} \begin{bmatrix} I_p & V_1 \\ O & U_1 \end{bmatrix} \text{ forma normale}$$

$$\begin{bmatrix} \underline{v} \\ \hline \underline{w} \end{bmatrix} \longrightarrow \begin{bmatrix} I_p & V_1 \\ O & W_1 \end{bmatrix}$$

Mettiamo tutto nella stessa matrice

$$\begin{bmatrix} I_p & V_1 \\ O & U_1 \\ I_p & V_1 \\ O & W_1 \end{bmatrix} \longrightarrow \begin{bmatrix} I_p & V_1 \\ O & \boxed{\begin{matrix} U_1 \\ W_1 \end{matrix}} \\ O & \end{bmatrix} \longrightarrow \begin{bmatrix} I_p & V_1' & V_1'' \\ O & \begin{bmatrix} I_t & U_1' \\ I_s & W_1' \end{bmatrix} \end{bmatrix} \text{ FORMA NORMALE}$$

SONO L'IND.

Voglio dimostrare che le righe della matrice sono linearmente indipendenti.

Per trovare se esistono relazioni di dipendenza lineare, riduciamo completamente con Gauss questa matrice. Supponiamo per assurdo che una riga del 3° blocco si riduca a $\underline{0}$. Sarebbe quindi combinazione lineare dei primi due blocchi, quindi apparterrebbe a U. Dato che già appartiene a W, apparterrebbe a $U \cap W$. Ma allora questo vettore non sarebbe potuto far parte di una base di W ed essere linearmente indipendente da $U \cap W$ per costruzione. ASSURDO

Quindi:

$$\underset{p+t+s}{\dim(U+W)} = \underset{p+t}{\dim U} + \underset{p+s}{\dim W} - \underset{p}{\dim U \cap W}$$

SOMME DIRETTE

Se U e W sono sottospazi di V $\mathbb{K}$-spazio e che $U \cap W = \{0\}$, il Teorema di Grassman ci dice che:

$$\dim(U+W) = \dim U + \dim W$$

In questo caso scriveremo $U \oplus W$ e diremo che $U \oplus W$ è la somma diretta di U e W.

In generale $W_1, \dots, W_n$ sono in somma diretta se:

$$\mathrm{Span}(W_1, \dots, W_n) = \bigoplus_{i=1}^{n} W_i$$

ESEMPIO Sia $V, W \underset{SSP}{\subseteq} \mathbb{R}^5$

$$V = \mathrm{span}(\underline{e}_1, \underline{e}_2) \qquad W = \mathrm{span}(\underline{e}_3, \underline{e}_4, \underline{e}_5)$$

V, W sono in somma diretta e $V \oplus W = \mathbb{R}^5$

PROPOSIZIONE

Sia V un $\mathbb{K}$-spazio e $W_1, \dots, W_m \underset{SSP}{\subseteq} V$

1. W_1, W_2 sono in somma diretta $\iff W_1 \cap W_2 = \{0\}$ $\dim = 0$

2. $W_1, \dots, W_n$ sono in somma diretta se e solo se:

$$\dim(W_1, \dots, W_n) = \dim W_1 + \dots + \dim W_m$$

$$\dim \sum_{i=1}^{m} W_i = \sum_{i=1}^{m} \dim W_i$$

DIMOSTRAZIONE PER INDUZIONE

Passo base: $n=2$ $\Rightarrow$ Grassman

Passo induttivo: Suppongo vero per n: $\dim \sum_{i=1}^{n} W_i = \sum_{i=1}^{n} \dim W_i$

Voglio dimostrare che $\dim \sum_{i=1}^{n+1} W_i = \sum_{i=1}^{n+1} \dim W_i$

$$\dim \sum_{i=1}^{n+1} W_i = \dim \left(\sum_{i=1}^{n} W_i + W_{n+1} \right) = \dim \sum_{i=1}^{n} W_i + \dim W_{n+1}$$

Uso l'ipotesi induttiva:

$$\sum_{i=1}^{n} \dim W_i + \dim W_{n+1} = \sum_{i=1}^{n+1} \dim W_i$$

DESCRIZIONI CARTESIANE E PARAMETRICHE

Sia $V = \{(a+b, b, c, a-c, a) \mid a, b, c \in \mathbb{K}\} \underset{ssp}{\subseteq} \mathbb{R}^5$

È una descrizione parametrica di V.

Si $U = \{(x, y, z, t) \mid x - y - z = 0\}$

È una descrizione cartesiana

Il suo vettore generico è: $(y+z, y, z, t)$

$y(1,1,0,0) + z(1,0,1,0) + t(0,0,0,1)$

Possiamo scrivere U in forma parametrica:

$U = \{(a+b, a, b, c) \mid a, b, c \in \mathbb{K}\}$

ESEMPIO

$V = \text{span}\{(3,1,0,5)(1,2,0,6)(0,0,0,1)\} \underset{ssp}{\subseteq} \mathbb{R}^4$

Condizione $\in V$: $z = 0$

$V \underset{ssp}{\subseteq} \{(x, y, z, t) \in \mathbb{R}^4 \mid z = 0\}$

dim = # variabili - # condizioni di appartenenza

$3 = 4 - 1$

$\dim V = 3$

$W_1 = \text{span}(1,2,2)(1,0,2)(2,1,4)$ $\quad x = 2z \quad$ dim = 2

$W_2 = \text{span}(1,1,1)(2,2,0)(3,3,2)$ $\quad x = y \quad$ dim = 2

$$x\begin{pmatrix}1\\2\\2\end{pmatrix} + y\begin{pmatrix}1\\0\\2\end{pmatrix} + z\begin{pmatrix}2\\1\\4\end{pmatrix} + a\begin{pmatrix}1\\1\\1\end{pmatrix} + b\begin{pmatrix}2\\2\\0\end{pmatrix} + c\begin{pmatrix}3\\3\\2\end{pmatrix} = 0$$

$$\begin{pmatrix}1 & 1 & 2 & 1 & 2 & 3\\ 2 & 0 & 1 & 1 & 2 & 3\\ 2 & 2 & 4 & 1 & 0 & 2\end{pmatrix} \quad \begin{array}{c} \\ -2I^1 \\ -2I^1 \end{array} \begin{array}{c} \begin{array}{cccccc} x & y & z & a & b & c \end{array} \\ \begin{pmatrix}1 & 1 & 2 & 1 & 2 & 3\\ 0 & -2 & -3 & -1 & -2 & -3\\ 0 & 0 & 0 & -1 & -4 & -4\end{pmatrix}\end{array}$$

$$\boxed{-a - 4b - 4c = 0} \Rightarrow a = -4b - 4c$$

$$-4b-4c\begin{pmatrix}1\\1\\1\end{pmatrix} + b\begin{pmatrix}2\\2\\0\end{pmatrix} + c\begin{pmatrix}3\\3\\2\end{pmatrix} = \begin{pmatrix}-4b-4c+2b+3c\\ -4b-4c+2b+3c\\ -4b-4c+2c\end{pmatrix} = \begin{pmatrix}-2b-c\\ -2b-c\\ -4b-2c\end{pmatrix}$$

$\{(-2b-c, -2b-c, -4b-2c)\}$ vettore generico di $W_1 \cap W_2$

$b(-2,-2,-4) + c(-1,-1,-2)$

Una base di $W_1 \cap W_2 = (1,1,2)$

$\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim W_1 \cap W_2$

$x = 2+2-1$

$x = 3$

- Le basi di $W_1 + W_2$ sono le colonne con pivot.

$W_1 + W_2 = \text{span}(1,0,0)(1,-2,0)(1,-1,1)$

PROPOSIZIONE $\quad A \xrightarrow{GAUSS} S$

Sia $A \in Mat_{m \times n}(\mathbb{K})$ e S una riduzione a scala di A, senza scambi di colonne. Allora il $rk(A) = r = rk(S)$, in più se:

$S^{i_1}, \dots, S^{i_r}$ sono le colonne S con pivot, allora $A^{i_1}, \dots, A^{i_r}$ sono una base di $span(A^1, \dots, A^m)$

DIMOSTRAZIONE

Dato che $rk(A) = rk(S) = r$ per dimostrare che $A^{i_1}, \dots, A^{i_r}$ sono base di $span(A^1, \dots, A^m)$, basta dimostrare che sono linearmente indipendenti.

Quindi:

$$\alpha_1 A^{i_1} + \dots + \alpha_R A^{i_r} = \underline{0} \Rightarrow \underline{\alpha} = \underline{0}$$

Applichiamo alla matrice associata al sistema la stessa riduzione che porta da A a S otteniamo una matrice triangolare superiore con r pivot, che ha un'unica soluzione, quella nulla.

$$A' \longrightarrow S' \text{ quadrata } (S^{i_1}, \dots, S^{i_R})$$

$$\Rightarrow Sol(A'\underline{x} = \underline{0})$$
$$\parallel$$
$$\underline{0}$$

MORFISMI DI SPAZI VETTORIALI

Siano V, W $\mathbb{K}$-spazi e $F: V \to W$ una funzione.

1. $F(\underline{v}_1 + \underline{v}_2) = F(\underline{v}_1) + F(\underline{v}_2) \quad \forall \underline{v}_1, \underline{v}_2 \in V$ (diremo che F è additiva)

2. $F(\lambda \underline{v}) = \lambda F(\underline{v}) \quad \forall \underline{v} \in V, \lambda \in \mathbb{R}$ (diremo che F è omogenea)

Diciamo che la funzione F è un applicazione lineare, o morfismo.

ESEMPI

$F: \mathbb{R}^2 \to \mathbb{R}^2$
$(x, y) \to (x+y, x-y)$ è lineare

$F: \mathbb{R}^2 \to \mathbb{R}^2$
$(x, y) \to (x+5y-2, 3x)$ non lo è

$F: \mathbb{R}^2 \to \mathbb{R}^2$
$(x, y) \to (x^2, y)$ non lo è

OSS: Le funzioni lineari ovvie $F: V \to W$ sono:

- quella nulla $\underline{v} \to 0$
- quella identità $\underline{v} \to \underline{v}$
- il prodotto scalare $\underline{w} \to \underline{v} \cdot \underline{w}$
- la derivata formale $p[x] \to p'[x]$

<u>Definizione</u>: L'inverso di un morfismo è un morfismo.

Sia $F: V \to W$ lineare, invertibile

Allora $F^{-1}: W \to V$ è lineare

DIMOSTRAZIONE

Dobbiamo dimostrare che:

$$\forall \lambda, \mu \in \mathbb{K},\ \underline{w}_1, \underline{w}_2 \in W \quad F^{-1}(\lambda \underline{w}_1 + \mu \underline{w}_2) = \lambda F^{-1}(\underline{w}_1) + \mu F^{-1}(\underline{w}_2)$$

Dato che F è invertibile, è surgettiva. Quindi $\exists\, \underline{v}_1, \underline{v}_2 \in V$ t.c.

$$\begin{cases} F(\underline{v}_1) = \underline{w}_1 \\ F(\underline{v}_2) = \underline{w}_2 \end{cases} \iff \begin{cases} v_1 = F^{-1}(\underline{w}_1) \\ v_2 = F^{-1}(\underline{w}_2) \end{cases}$$

Quindi

$$\begin{aligned} F^{-1}(\lambda \underline{w}_1 + \mu \underline{w}_2) &= F^{-1}(\lambda F(\underline{v}_1) + \mu F(\underline{v}_2)) \\ &= F^{-1}(F(\lambda \underline{v}_1 + \mu \underline{v}_2)) && F \text{ lineare} \\ &= \lambda \underline{v}_1 + \mu \underline{v}_2 && F \text{ inversa di } F^{-1} \\ &= \lambda F^{-1}(\underline{w}_1) + \mu F^{-1}(\underline{w}_2) \end{aligned}$$

ESEMPIO

Sia $A \in Mat_{m \times n}(\mathbb{K})$. La funzione

$$\begin{aligned} L_A : \mathbb{K}^n &\longrightarrow \mathbb{K}^m \\ \underline{v} &\longrightarrow A \cdot \underline{v} \end{aligned}$$

è lineare.

UNICITÀ

Siano V, W due $\mathbb{K}$-spazi, B base di V $B = v_1, \dots, v_n$ e $w_1, \dots, w_n \in W$. Allora esiste un'unica applicazione lineare $T: V \to W$ tale che $F(\underline{v}_i) = \underline{w}_i$ per $i: 1, \dots, n$

questa applicazione si dice definita su B.

UNICITÀ: Sia $G: V \to W$ lineare t.c. $F(\underline{v}_i) = w_i$

$F \equiv G \iff \forall \underline{v} \in V \quad F(\underline{v}) = G(\underline{v})$

$$F\left(\sum_{i=1}^{n} \alpha_i \underline{v}_i\right) = G\left(\sum_{i=1}^{n} \alpha_i v_i\right)$$

$$\sum_{i=1}^{n} \alpha_i \underbrace{F(\underline{v}_i)}_{\underline{w}_i} = \sum_{i=1}^{n} \alpha_i \underbrace{G(\underline{v}_i)}_{\underline{w}_i}$$

OSSERVAZIONI

- Posso definire un morfismo su una base.
- Due funzioni lineari che assumano gli stessi valori su una base del dominio sono uguali come funzioni.
- Un'applicazione lineare è completamente determinata dai valori che assume su una base.

PROPOSIZIONE MATRICE ASSOCIATA

Dato il morfismo di $\mathbb{K}$-spazi $T: \mathbb{K}^m \longrightarrow \mathbb{K}^n$ esiste un'unica matrice $A \in Mat_{n \times m}(\mathbb{K})$ tale che $T \equiv L_A$

Costruiamo la matrice A che ha come colonne $T(\underline{e}_1), \dots, T(\underline{e}_m)$

$$A = \begin{pmatrix} T(\underline{e}_1) & \dots & T(\underline{e}_m) \\ \vdots & & \vdots \end{pmatrix}$$

Quindi ogni applicazione lineare è legata a una matrice, appena ho una base.

ESEMPIO

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

$$B \begin{cases} (1,1,1) \longrightarrow (1,1) \\ (1,1,0) \longrightarrow (0,1) \\ (1,0,0) \longrightarrow (0,1) \end{cases}$$

parto da B

$$(M_F)^B_{E_2} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

arrivo in E

NUCLEO E IMMAGINE

Dato un morfismo di $\mathbb{K}$-spazi $T: V \to W$, possiamo associare due sottoinsiemi:

1. Il nucleo, $\ker T = \{ \underline{v} \in V \mid T(\underline{v}) = 0 \} \underset{SSP}{\subseteq} V$
2. L'immagine, $\operatorname{Im} T = \{ T(\underline{v}) \mid \underline{v} \in V \} \underset{SSP}{\subseteq} W$

DIMOSTRAZIONE

Dobbiamo verificare se $\underline{v}_1, \underline{v}_2 \in \ker T$, $\lambda, \mu \in \mathbb{K}$

$$\Rightarrow \lambda \underline{v}_1 + \mu \underline{v}_2 \in \ker T$$

Infatti se $\underline{v}_1, \underline{v}_2 \in \ker T$

$$T(\underline{v}_1) = T(\underline{v}_2) = \underline{0}$$

$$T(\lambda \underline{v}_1 + \mu \underline{v}_2) = \lambda \underbrace{T(\underline{v}_1)}_{\underline{0} \,=\, \in \ker T \,=\, \underline{0}} + \mu \underbrace{T(\underline{v}_2)}_{\underline{0}}$$

OSSERVAZIONE

Data $A \in \mathrm{Mat}_{m \times n}(\mathbb{K})$ $\quad L_A : V \to W$

$$\ker A = (\mathrm{Sol}(A\underline{x} = \underline{0}))$$

PROPOSIZIONE

Dato $F: V \to W$ morfismo di $\mathbb{K}$-spazi e $\underline{v}_1, \dots, \underline{v}_p \in V$

Allora: Se $\underline{v}_1, \dots, \underline{v}_p$ sono linearmente dipendenti,

lo sono anche $F(\underline{v}_1, \dots, \underline{v}_p)$

DIMOSTRAZIONE

Sappiamo che esistono $\alpha_1, \dots, \alpha_p$ con $\underline{\alpha} \neq \underline{0}$ tali che $\sum_{i=1}^{p} \alpha_i \underline{v}_i = \underline{0}$. Ma allora

$$F\left(\sum_{i=1}^{p} \alpha_i \underline{v}_i\right) = \underline{0}$$

$$\sum_{i=1}^{p} \alpha_i F(\underline{v}_i) = \underline{0} \quad \text{è sempre } \alpha \neq \underline{0}$$

PROPOSIZIONE

Dato $T: V \to W$ morfismo di $\mathbb{K}$-spazi iniettivo

Allora: Se $\underline{v}_1, \dots, \underline{v}_p \in V$ sono linearmente indipendenti,

lo sono anche $T(\underline{v}_1, \dots, \underline{v}_p)$

DIMOSTRAZIONE

$$\alpha_1 T(\underline{v}_1) + \dots + \alpha_m T(\underline{v}_m) = \underline{0} \implies \underline{\alpha} = \underline{0}$$

$$T(\alpha_1 \underline{v}_1 + \dots + \alpha_m \underline{v}_m) = \underline{0}$$

$$\alpha_1 \underline{v}_1 + \dots + \alpha_m \underline{v}_m = \underline{0}$$

Però se T è iniettiva $\ker T = \{0\}$

$$\implies \underline{\alpha} = \underline{0}$$

PROPOSIZIONE

Sia $T: V \to W$ un'applicazione lineare. Allora

1. $\ker T$ è un sottospazio di V
2. $\operatorname{Im} T$ è un sottospazio di W
3. T è surgettiva se e solo se $\operatorname{Im} T = \{W\}$
4. T è iniettiva se e solo se $\ker T = \{\underline{0}\}$

Se T è iniettiva, il $\ker T = \underline{0}$

$$T(\underline{v}) = \underline{0} \implies \underline{v} = \underline{0}$$

Per assurdo suppongo che

$$T(\underline{v}_1) = \underline{0}$$

$$\underline{v}_1 \neq 0$$

Allora: $T(\underline{v}_1) = T(\underline{v}) = \underline{0}$ ASSURDO, perché T è iniettiva, quindi $\underline{v}_1 = \underline{v} = \underline{0}$

LEMMA

Sia $T: V \to W$ un applicazione lineare, e $\underline{v}_1, \dots, \underline{v}_m$ una sua base di V.

Allora:

$$\operatorname{Im} T = \operatorname{span}(T(\underline{v}_1) \dots T(\underline{v}_m))$$

ESEMPIO

$F: \mathbb{R}^3 \to \mathbb{R}^4$

$(1,2,1) \to (1,0,0,0)$

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

$(0,3,2) \to (2,0,1,0)$

Determiniamo una base di $\ker F$ e $\operatorname{Im} F$

F è ben definita? $\begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 1 \\ 0 & 3 & 2 \end{pmatrix}$ $\det \neq 0$ sì

Vediamo se F è iniettiva.

$F((x,y,z)) = \underline{0} \iff x(1,0,0,0) + y(1,0,1,0) + z(2,0,1,0) = \underline{0}$

$$\begin{cases} x + y + 2z = 0 \\ y + z = 0 \end{cases} \qquad \begin{cases} x = -z \\ y = -z \end{cases}$$

Un vettore generico di $\ker F = (-z, -z, z) = (-1, -1, 1)$

È una base di $\operatorname{Im} F$: $\begin{pmatrix} 1 & 1 & 2 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ $rk = 2 = \dim \operatorname{Im} F$

$\operatorname{Im} T = (1,0,0,0)(1,0,1,0)$

OSSERVAZIONI

Sia $L_A: V \to W$

1. $\operatorname{Im} T = \operatorname{span}(A^1, \dots, A^n)$ le colonne di A
2. $\dim \operatorname{Im} T = rk(A)$

il rango di A è proprio il numero massimo di colonne indipendenti, che è per definizione $\dim \operatorname{Im} T$.

TEOREMA DELLA DIMENSIONE

Sia $T: V \longrightarrow W$ un'applicazione lineare. Allora

$\dim V = n$

$$\dim V = \dim \ker T + \dim \operatorname{Im} T$$

DIMOSTRAZIONE

Sia $\underline{\underline{u}} = \underline{u}_1, \dots, \underline{u}_R$ base del $\ker T$.

La completo a base di V, aggiungendo $n-R$ vettori, $\underline{\underline{v}} = \underline{v}_{R+1}, \dots, \underline{v}_n$. Diamo un nome alle immagini di $\underline{\underline{v}}$

$$\underline{\underline{w}}_j = T(\underline{v}_i) \qquad i: R+1, \dots, n$$

Voglio dimostrare che $\underline{\underline{w}}$ è una base di $\operatorname{Im} T$, il che completerebbe la dimostrazione, dato che avremmo:

$$n = \dim \ker T + \dim \operatorname{Im} T$$

Sappiamo che $T(\underline{\underline{v}}) = \underline{\underline{w}}$ generano $\operatorname{Im} T$, mi basta dimostrare che sono linearmente indipendenti. Quindi:

$$\alpha_{R+1} \underline{w}_{R+1} + \dots + \alpha_n \underline{w}_n = \underline{0} \quad \Rightarrow \underline{\alpha} = \underline{0}$$

$$\alpha_{R+1} T(\underline{v}_{R+1}) + \dots + \alpha_n T(\underline{v}_n) = \underline{0}$$

$$T(\alpha_{R+1} \underline{v}_{R+1} + \dots + \alpha_n \underline{v}_n) = \underline{0}$$

ma questo implica che $\alpha_{R+1} \underline{v}_{R+1} + \dots + \alpha_n \underline{v}_n \in \ker T$

Quindi esistono $\underline{\beta}$ tali che:

$$\underline{\alpha} \cdot \underline{\underline{v}} = \underline{\beta} \cdot \underline{\underline{u}}$$

$$\underline{\alpha} \cdot \underline{\underline{v}} - \underline{\beta} \cdot \underline{\underline{u}} = \underline{0}$$

Però $\underline{\underline{v}}, \underline{\underline{u}}$ sono base di V, quindi sono linearmente indipendenti, quindi $\underline{\alpha} = \underline{0}$ e $\underline{\beta} = \underline{0}$. Questo mi da la lineare indipendenza di $\underline{\underline{w}}$.

OSSERVAZIONE

Data una matrice $A \in Mat_{m \times n}(\mathbb{K})$

$$n = \dim \ker A + rk(A)$$

Dato che la dimensione di $\ker A = Sol(A\underline{x} = \underline{0})$, non dipende dalla particolare riduzione di Gauss, neppure il rango ne dipende.

Il numero dei pivot quindi è invariante per A.

PROPOSIZIONE

Sia dato il sistema $A \cdot \underline{x} = b$, con $A \in Mat_{m \times n}(\mathbb{K})$.
Allora il sistema ha soluzione se e solo se:

$$\underline{b} \in Span(A^1, \dots, A^n)$$

DIMOSTRAZIONE

Per definizione

$$\underline{b} \in span(A^1, \dots, A^n) \iff \exists \ \underline{\alpha} \text{ t.c.}$$

$$\underline{b} = \alpha_1 A^1 + \dots + \alpha_n A_n \iff \alpha \in Sol(A \underline{x} = \underline{b})$$

OSSERVAZIONE

Sia dato il sistema $A \cdot \underline{x} = \underline{b}$ con $A \in Mat_{m \times n}(\mathbb{K})$.
Allora il numero il numero minimo di parametri necessario a descrivere $Sol(A \underline{x} = \underline{0})$ è:

$$\dim Sol(A \underline{x} = \underline{0}) = \dim \ker A = n - rk(A)$$

TEOREMA DI ROUCHÉ-CAPELLI

Sia dato il sistema $A\underline{x} = \underline{b}$, con $A \in Mat_{m \times n}(\mathbb{K})$

Allora se $A' = [A|\underline{b}]$

1. Se $rk([A|\underline{b}]) \neq rk(A)$ il sistema non ha soluzioni
2. Se $rk([A|\underline{b}]) = rk(A)$ il sistema ha $\infty^{n - rk A}$ soluzioni.

DIMOSTRAZIONE

Per la proposizione vista prima, una soluzione esiste se e solo se:

$$b \in span(A^1, \dots, A^n) = span(A^1, \dots, A^n, b)$$

Ma il primo span è l'immagine di L_A, mentre il secondo di $L_{A'}$. Siccome abbiamo sempre

$$span(A^1, \dots, A^n) \subseteq span(A^1, \dots, A^n, \underline{b})$$

Che è contenuto è sempre vero, però l'uguaglianza vale solo se: $\dim L_A = \dim L_{A'} \iff rk(A) = rk(A')$

L'unicità c'è se e solo se:

$$Sol(A\underline{x} = \underline{0}) = \ker A = \{0\} \iff \dim \ker A = 0 \iff rk A = \dim \mathbb{K}^n = n$$

Il minimo numero di parametri necessario per descrivere $Sol(A\underline{x} = \underline{b})$ è uguale al numero minimo di parametri necessari a descrivere $Sol(A\underline{x} = \underline{0})$, ovvero

$$\dim Sol(A\underline{x} = \underline{0}) = \dim \ker A = n - rk(A)$$

ISOMORFISMI

Dati V, W $\mathbb{K}$-spazi, l'insieme

$$\hom(V,W) = (T : V \to W \mid T \text{ lineare})$$

abbiamo che $(\hom(V,W), +, \cdot)$ è uno spazio vettoriale con:

$$+ : \hom(V,W) \times \hom(V,W) \to \hom(V+W) \qquad \text{con} \qquad V \to W$$
$$(f,g) \to (f+g) \qquad\qquad \underline{v} \to f(\underline{v}) + g(\underline{v})$$

e

$$\cdot : \mathbb{K} \times \hom(V,W) \to \hom(V,W) \qquad \text{con} \qquad V \to W$$
$$(\lambda, f) \to \lambda f \qquad\qquad \underline{v} \to \lambda f(\underline{v})$$

È immediato che $f+g$, λf siano morfismi.

PROPOSIZIONE

Dati $f: V \to W$ e $g: W \to U$ morfismi di $\mathbb{K}$-spazi.

Allora la composizione $g \circ f: V \to U$ è lineare.

DIMOSTRAZIONE

Ricordiamoci che $(g \circ f)(x) = g(f(x))$

Quindi
$$
\begin{aligned}
(g \circ f)(\lambda \underline{v}_1 + \mu \underline{v}_2) &= g(f(\lambda \underline{v}_1 + \mu \underline{v}_2)) \\
&= g(f(\lambda \underline{v}_1) + f(\mu \underline{v}_2)) \\
&= \lambda g(f(\underline{v}_1)) + \mu g(f(\underline{v}_2)) \\
&= \lambda g \circ f(\underline{v}_1) + \mu g \circ f(\underline{v}_2)
\end{aligned}
$$

OSSERVAZIONI

$f: V \to W$ morfismo
$g: W \to U$ morfismo
$\Rightarrow$ $f \circ g$ non è un morfismo in genere:

$f \circ g = \cancel{W \to U \to W \to W}$

$\Rightarrow$ $g \circ f$ è un morfismo perché:

$g \circ f: V \to W \to U$

Definizione:

Un morfismo di $\mathbb{K}$-spazi $T: V \to V$ è un endomorfismo

Definizione:

Siano V, W $\mathbb{K}$-spazi. Se esiste un morfismo biunivoco (invertibile) $T: V \to W$ diciamo che T è un isomorfismo e che V, W sono isomorfi ($V \simeq W$)

OSSERVAZIONE

La relazione $\simeq$ ha tutte le proprietà di uguaglianza:

- simmetrica: $V \simeq V$ basta prendere id_V come isomorfismo
- riflessiva: $V \simeq W \Leftrightarrow W \simeq V$. Perché esiste l'inversa
- transitiva: Se $V \simeq W$ e $W \simeq U$ allora $V \simeq U$.

Due spazi isomorfi sono sostanzialmente lo stesso spazio, a meno "dei nomi che diamo agli oggetti", dato che c'è una corrispondenza biunivoca che trasporta le operazioni sia da V a W e viceversa.

PROPOSIZIONE Dato $f: \mathbb{K}^n \longrightarrow \mathbb{K}^m$ morfismo di $\mathbb{K}$-spazi, abbiamo

$$L(M_f)^{E_m}_{E_m} = f$$

DIMOSTRAZIONE

$$f(e_j) = L(M_f)^E_E (e_j)$$

$$\hookrightarrow \begin{pmatrix} f(e_1) & \cdots & f(e_n) \end{pmatrix} \cdot e_j = f(e_j)$$

PROPOSIZIONE

$$Mat_{m \times n}(\mathbb{K}) \simeq hom(\mathbb{K}^n, \mathbb{K}_m)$$

$$T: Mat_{m \times n}(\mathbb{K}) \longrightarrow Hom(\mathbb{K}^n, \mathbb{K}^m)$$

$$A \longrightarrow L_A$$

1. È ben definita, perché L_A è un morfismo
2. T è un morfismo:

$$T(\lambda A + \mu B) = \lambda T(A) + \mu T(B)$$

$$L(\lambda A + \mu B)(\underline{v}) = (\lambda A + \mu B) \cdot \underline{v} = \lambda (A \cdot \underline{v}) + \mu (B \cdot \underline{v})$$

3. T è invertibile.

$$\underset{\substack{\uparrow \\ Hom(\mathbb{R}^n, \mathbb{R}^m)}}{f} \longrightarrow \underset{\substack{\shortparallel \\ (M_f)^E_E}}{\begin{pmatrix} f(\underline{e}_1) & \cdots & f(e_n) \end{pmatrix}}$$

$$T(G(f)) = f$$

$$T((M_f)^E_E)$$

$$L(M_f{}^E_E) = f$$

PROPOSIZIONE

Se $L_A : V \longrightarrow W$ $L_B : W \longrightarrow U$, morfismi. Allora

$$L_A \circ L_B = L_{A \cdot B}$$

Voglio dimostrare che

$$\forall \underline{v} \in V \quad L_A \circ L_B (\underline{v}) = L_{A \cdot B} (\underline{v})$$

$$\begin{aligned} L_A \circ L_B (\underline{v}) &= L_A (L_B (\underline{v})) \\ &= L_A (B \cdot \underline{v}) \\ &= A (B \cdot \underline{v}) \\ &= (A \cdot B) \underline{v} \\ &= L_{A \cdot B} (\underline{v}) \end{aligned}$$

e dalla proprietà associativa

TEOREMA

Sia $A \in Mat_{n \times n}(\mathbb{K})$, TFAE

$L_A : \mathbb{K}^n \longrightarrow \mathbb{K}^n$

1. A è invertibile
2. L_A è iniettiva ($\ker L_A = \{0\}$)
3. L_A è surgettiva ($\operatorname{Im} L_A = \mathbb{K}^n$) -> Dal T. DIM: $n = \dim \ker A + rk A$
4. $rk\, A = n$
5. Le colonne di A sono linearmente indipendenti.
6. Le righe di A sono linearmente indipendenti.
7. $Sol(A\underline{x} = \underline{0}) = \{\underline{0}\}$
8. $Sol(A\underline{x} = \underline{b}) = \{A^{-1} \cdot b\}$
9. $\det A \neq 0 \iff A$ ha n pivot

CAMBIO BASE PER VETTORI

Sia V $\mathbb{K}$-spazio, con $\dim V = n$ e

$B = \underline{v}_1, \dots, \underline{v}_n$; $B' = \underline{v}'_1, \dots, \underline{v}'_n$ basi di V

$$M^B_{B'} = \left((\underline{v}_1)_{B'} \cdots (\underline{v}_n)_{B'} \right) \qquad M^B_{B'} \cdot \underline{w}_B = \underline{w}_{B'}$$

OSSERVAZIONE

$$L_{M^B_{B'}} \circ L_{M^{B'}_B} = id = M^B_{B'} \cdot M^{B'}_B$$

L'applicazione $L_{M^{B'}_B}$ cambia le coordinate dalla base B' alla base B, ed è associata alla matrice $M^{B'}_B$, le cui colonne sono i vettori di B' espressi in base B

ESEMPIO

Data la base $B = (1,1,1)(0,1,-2)(1,2,0)$

$$\underline{v} = (0,1,3)_{E_3} \quad e \quad \underline{w} = (1,0,2)_B$$

Voglio determinare $M^B_{E_3}$, $M^{E_3}_B$, $\underline{v}_B$, $\underline{w}_{E_3}$

$$M^B_{E_3} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 2 \\ 1 & -2 & 0 \end{pmatrix}$$

$$M^B_{E_3} \cdot w_B = w_E \qquad \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 2 \\ 1 & -2 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} = (3 \quad 5 \quad 1)_{E_3}$$

$$M^{E_3}_B = (M^B_{E_3})^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 2 \\ 1 & -2 & 0 \end{pmatrix}^{-1} \longrightarrow \begin{pmatrix} 4 & -2 & -1 \\ 2 & -1 & -1 \\ -3 & 2 & 1 \end{pmatrix}$$

$$M^{E_3}_B \cdot \underline{v}_{E_3} = \underline{v}_B \qquad \begin{pmatrix} 4 & -2 & -1 \\ 2 & -1 & -1 \\ -3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix} = (-5 \quad -4 \quad 5)_B$$

CAMBIAMENTO DI BASE PER MORFISMI

Siano: $B = \underline{v}_1, \dots, \underline{v}_n$ base di $\mathbb{K}^n$ $\quad$ $C = \underline{w}_1, \dots, \underline{w}_m$ base di $\mathbb{K}^m$

$$T: (\mathbb{K}^n, B) \longrightarrow (\mathbb{K}^m, C)$$

$$\underline{v}_B \longrightarrow (T(\underline{v}_B))_C$$

un morfismo di $\mathbb{K}$-spazi che trasforma un vettore di $\mathbb{K}^n$ in coordinate B in vettore di $\mathbb{K}^m$ in coordinate C.

1. La matrice associata a T dalle base B, C

$$(M_T)_C^B = \begin{pmatrix} \vdots & & \vdots \\ T(\underline{v}_1)_C & \cdots & T(\underline{v}_n)_C \\ \vdots & & \vdots \end{pmatrix}$$

2. Al variare delle basi di $\mathbb{K}^n$, $\mathbb{K}^m$ la matrice associata al morfismo varia secondo la formula:

$$(M_T)_{C'}^{B'} = M_{C'}^{C} \cdot (M_T)_C^B \cdot M_B^{B'}$$

Definizione Siano V, W $\mathbb{K}$-spazi

$T: V \longrightarrow W$ morfismo

T, W sono una descrizione parametrica di V se

$$V = \operatorname{Im} T = \{T(\underline{w}) = w \in W\}$$

Definizione Siano V, W $\mathbb{K}$-spazi

$T: V \longrightarrow W$ morfismo

T, W sono una descrizione cartesiana di V se

$$V = \ker T = \{\underline{v} \in V \mid T(\underline{v}) = \underline{0}\}$$

MATRICI SIMILI

<u>Definizione</u> L'insieme:

$$M \in GL_n(\mathbb{K}) = \{ M \in Mat_{n \times n}(\mathbb{K}) \mid \det M \neq 0 \}$$

Si dice gruppo lineare di ordine n su $\mathbb{K}$.

<u>Definizione</u> Due matrici quadrata $A, B \in Mat_{n \times n}(\mathbb{K})$ sono simili se esiste una matrice $M \in GL_n(\mathbb{K})$ tali che:

$$A \cdot M = M \cdot B \iff M \cdot A = B \cdot M \iff A = M^{-1} \cdot B \cdot M$$

Questa relazione si indica con $A \sim B$

COROLLARIO

Date due matrici quadrate $A \sim B$ ho che:

1. $\det(A) = 0 \iff \det(B) = 0$
2. $rk\, A = rk\, B$
3. $\dim \ker A = \dim \ker B$

ESERCIZIO

$$A = \begin{pmatrix} 1 & 3 \\ 3 & 2 \end{pmatrix} \qquad B = \begin{pmatrix} 3 & 7 \\ 1 & 0 \end{pmatrix} \qquad A \sim B\,?$$

$$A \cdot X = XB \qquad A \cdot X - XB = \underline{0}$$

$$\begin{pmatrix} 1 & 3 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} x & y \\ z & t \end{pmatrix} - \begin{pmatrix} x & y \\ z & t \end{pmatrix}\begin{pmatrix} 3 & 7 \\ 1 & 0 \end{pmatrix} =$$

$$\begin{pmatrix} x+3z & y+3t \\ 3x+2z & 3y+2t \end{pmatrix} - \begin{pmatrix} 3x+y & 7x \\ 3z+t & 7z \end{pmatrix} = \begin{pmatrix} -2x-y+3z & -7x+y+3t \\ 3x-z-t & 3y-7z+2t \end{pmatrix}$$

$$\begin{pmatrix} -2 & -1 & 3 & 0 \\ -7 & 1 & 0 & 3 \\ 3 & 0 & -1 & -1 \\ 0 & 3 & -7 & 2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & -\frac{1}{3} & -\frac{1}{3} \\ 0 & 1 & -\frac{7}{3} & \frac{2}{3} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$X = \begin{pmatrix} -\frac{1}{3}z - \frac{1}{3}t & -\frac{7}{3}z + \frac{2}{3}t \\ z & t \end{pmatrix}$$

Se pongo $z = 0$ e $t = 3$

$$X = \begin{pmatrix} -1 & -7 \\ 3 & 0 \end{pmatrix} \longrightarrow A \sim B$$

OSSERVAZIONE

Se avessi avuto una sola matrice, il problema sarebbe stato molto più difficile se non impossibile.

PROPOSIZIONE

Sia $T: V \to V$ endomorfismo di $\mathbb{K}$-spazi.

con B base di V con $\dim B = n$. Allora

1. Se B' è una base di V, allora $(M_T)^B_B \sim (M_T)^{B'}_{B'}$
2. Se $A \in Mat_{n \times n}(\mathbb{K})$ e $A \sim (M_T)^B_B$ allora $\exists\, C$ base di V tale che:

$$A = (M_T)^C_C$$

DIMOSTRAZIONE

1. $(M_T)^{B'}_{B'} = M^B_{B'} \, (M_T)^B_B \, M^{B'}_B$ $\qquad$ M è invertibile

$$M^{B'}_B = (M^B_{B'})^{-1}$$

2. $A \sim (M_T)^B_B$

$\exists\, M$ t.c. $\quad A = M^{-1} (M_T)^B_B \cdot M \qquad L_M$ è un isomorfismo

<u>Definizione</u> Data $A \in Mat_{n \times n}$, la sua classe di similitudine $\mathcal{O}_A$ è $: \{ B \in Mat_{n \times n} \mid A \sim B \}$

$$\{ B \in Mat_{n \times n} \mid \exists\, M \in GL \text{ t.c. } A = M^{-1} B M$$

PROBLEMA

Dato un $\mathbb{K}$-spazio V di $\dim V = n$ ed un endomorfismo $T: V \to V$, vorrei identificare una base B di V tale che $(M_T)^B_B$ sia il più semplice possibile, al limite, diagonale.

DIAGONALIZZAZIONE

Sia $T: \mathbb{R}^3 \to \mathbb{R}^3$ endomorfismo di $\mathbb{K}$ spazi, :

$$e_1 \to 3e_1$$
$$e_2 \to 2e_2$$
$$e_3 \to \underline{0}$$

$$(M_T)^{E_3}_{E_3} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Questa è una matrice diagonale, composta da autovettori di V. $\Leftrightarrow T(\underline{v}_i) = \lambda \underline{v}_i$

AUTOVALORI E AUTOVETTORI

Sia $T: V \to V$ endomorfismo di $\dim V = n$

1) Un vettore non nullo $\underline{v} \in V$ è detto autovettore di T relativo all'autovalore $\lambda \in \mathbb{K}$ se:

$$T(\underline{v}) = \lambda \underline{v}$$

2) Si dice che un autovalore λ è associato all'autovettore $\underline{v}$.

3) L'insieme degli autovalori di T, cioè degli scalari λ, per cui esista un vettore non nullo v_0, è lo spettro di T, indicato con $sp(T)$

$$sp(T) = \{\lambda \in \mathbb{K} \mid \exists\, \underline{v} \in V \text{ t.c. } T(\underline{v}) = \lambda \underline{v}\}$$

4) Se $\lambda \in sp(T)$, l'insieme

$$V_\lambda = \{\underline{v} \in V \mid T(\underline{v}) = \lambda \underline{v}\}$$

è detto autospazio di T.

OSSERVAZIONI

1. $T(\underline{v}) = \lambda \underline{v} \iff T(\underline{v}) - \lambda \underline{v} = \underline{0}$

$$(M_T)_B^B \cdot (\underline{v}) - \lambda \underline{v} = \underline{0}$$

$$\left((M_T)_B^B - \lambda I_n\right) \cdot \underline{v} = \underline{0}$$

2. $V_0 = \ker T$ Quindi 0 è autovalore solo se T è singolare (Altrimenti l'unico elemento di $\ker T$ sarebbe il vettore nullo, che non è associato ad un autovalore

3. $\lambda_0 \in Sp(T)$ $V_{\lambda_0} \underset{SSP}{\subseteq} V$. Dato che $V_0 = \ker (M_T)_B^B$ è SSP di V

<u>Definizione</u> Un endomorfismo $T: V \to V$ è diagonalizzabile se esiste una base di V composta da autovettori di T.

IL POLINOMIO CARATTERISTICO

Sia $T: V \to V$ endomorfismo e $B = v_1, \dots, v_n$ base di V con $\dim B = n$. Allora

1. La funzione $p_T : \mathbb{K} \to \mathbb{K}$ non dipende dalla base B
$$\lambda \to \det\left((M_T)_B^B - \lambda I_n\right)$$

2. p_T è un polinomio di grado n, in cui il coefficente direttivo di p_T è $(-1)^n$, il termine noto di $p_T(\lambda) = \det(M_T)_B^B$ e il coefficente di λ^{n-1} è $(-1)^{n-1} tr(M_T)_B^B$.

3. λ_0 è un autovalore di $T \iff p_T(\lambda_0) = 0$

DIMOSTRAZIONE

1. Supponiamo di avere una base C rispetto a cui T è associato alla matrice $(M_T)_C^C$.

Voglio dimostrare:

$$\det\left((M_T)_C^C - \lambda I_n\right) = \det\left((M_T)_B^B - \lambda I_n\right)$$

Però: $(M_T)_C^C = (M_B^C)^{-1}(M_T)_B^B M_B^C$ Quindi

$$\det\left((M_T)_C^C \lambda I_n\right) = \det\left((M_B^C)^{-1}(M_T)_B^B M_B^C - \lambda I_n\right)$$

dato che $I_n = (M_B^C)^{-1} M_B^C$

$$= \det\left((M_B^C)^{-1}(M_T)_B^B M_B^C - \lambda (M_B^C)^{-1} M_B^C\right)$$

raccolgo $= \det\left((M_B^C)^{-1}, \left((M_T)_B^B - \lambda I_n\right) M_B^C\right)$

per Binet $= \det(M_B^C)^{-1} \cdot \det\left((M_T)_B^B - \lambda I_n\right) \cdot \det M_B^C$

$= \det\left((M_T)_B^B - \lambda I_n\right)$ dato che $\det(M_B^C)^{-1} = \dfrac{1}{\det M_B^C}$

2. Procediamo per induzione. Passo base $n=2$

$$p_T(\lambda) = \begin{vmatrix} a_{11}-\lambda & a_{12} \\ a_{21} & a_{22}-\lambda \end{vmatrix} = (a_{11}-\lambda)(a_{22}-\lambda) - a_{12}\cdot a_{21}$$

$$= \overbrace{\lambda^2}^{(-1)^2} - \underbrace{(a_{11}+a_{22})}_{Tr(M_T)_B^B}\lambda + \underbrace{a_{11}\cdot a_{22} - a_{21}a_{22}}_{\det(M_T)_B^B}$$

E ci siamo

Passo induttivo: suppongo vero per $n-1$, dimostro per n

$$p_T(\lambda) = \begin{vmatrix} a_{11}-\lambda & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22}-\lambda & \cdots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{n1} & \cdots & & a_{nn}-\lambda \end{vmatrix}$$

Sviluppo con Laplace per la prima colonna.

$$= (a_{11}-\lambda)\cdot \det[\dots] + \underbrace{(a_{21})\cdot\det[\dots] + \dots\dots + (a_{n1})\cdot\det[\dots]}_{\text{termini di grado al più } n-2}$$

Ho sviluppato lungo la 1ª colonna (il det.), il resto sono determinanti di matrici in cui λ appare $n-2$ volte. Per cui forniscono polinomi di grado al più $n-2$. Per l'ipotesi induttiva,

$$p_T(\lambda) = (a_{11}-\lambda)\left[(-1)^{n-1}\lambda^{n-1} + (-1)^{n-2}(a_{22}+\dots+a_{nn})\lambda^{n-2} + \dots\dots\right.$$

$$p_T(\lambda) = (-1)^n\lambda^n + (-1)^{n-1}(trA)\lambda^{n-1} + \dots\dots$$

Quindi ho dimostrato che p_T è un polinomio di grado esattamente n, con coefficente direttivo $(-1)^n$, e con $(-1)^{n-1}\cdot Tr(M_T)_B^B$ come coefficente λ^{n-1}.

ESEMPIO

$$A = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} \qquad p_T(\lambda) = \lambda^2 - 2\lambda - 5$$

$$e \quad \lambda = \frac{2 \pm \sqrt{24}}{2}$$

Definizione Il polinomio

$$p_T(\lambda) = \det\left((M_T)_B^B - \lambda I_n\right)$$

è detto polinomio caratteristico di T.

COROLLARIO

1. Il numero degli autovalori è minore o uguale al grado di p_T, ovvero alla dimensione di V
2. Il termine noto di $p_T(\lambda) = \det(M_T)_B^B$

PROPOSIZIONE

Sia $T: V \longrightarrow V$ e B base. Allora

B è composta da autovettori $\Longleftrightarrow (M_T)_B^B$ è diagonale.

COROLLARIO

Sia $A \in Mat_{n \times n}(\mathbb{K})$. Allora esiste una base di autovettori per $L_A \Longleftrightarrow \exists\, D$ diagonale $A \sim D$

$\Longleftrightarrow \mathcal{O}_A \ni D$ diagonale

<u>Definizione</u> Sia $T: V \longrightarrow V$ un morfismo di $\mathbb{K}$-spazi. Diciamo che T ha tutti gli autovalori in $\mathbb{K}$ se $p_T(\lambda)$ ha esattamente n radici in $\mathbb{K}$, contate con la loro molteplicità.

CRITERI DI DIAGONALIZZABILITÀ

Sia $T: V \to V$ endomorfismo e siano $\underline{v}_1, \dots, \underline{v}_k \neq 0$ autovettori di T corrispondenti ad autovalori distinti $\lambda_1, \dots, \lambda_k$. Allora $\underline{v}_1, \dots, \underline{v}_k$ sono linearmente indipendenti.

DIMOSTRAZIONE (induzione)

- Passo base: $k=1$ $\quad \underline{v}_1$ è indipendente da se stesso
- Passo induttivo: Suppongo vero per $k-1$, dimostro per k.

Sappiamo che $\underline{v}_1, \dots, \underline{v}_{k-1}$ sono linearmente indipendenti.

Voglio dimostrare che $\alpha_1 \underline{v}_1 + \dots + \alpha_k \underline{v}_k = \underline{0} \Rightarrow \underline{\alpha} = \underline{0}$

Applichiamo T:

$$T(\alpha_1 \underline{v}_1 + \dots + \alpha_k \underline{v}_k) = \underline{0}$$

$$\alpha_1 T(\underline{v}_1) + \dots + \alpha_k T(\underline{v}_k) = \underline{0}$$

Ma dato che $\underline{v}_i$ sono autovettori: $\quad T(\underline{v}) = \lambda \underline{v}$

$$\alpha_1 \lambda_1 \underline{v}_1 + \dots + \alpha_k \lambda_k \underline{v}_k = \underline{0}$$

Sfruttando la prima relazione

$$\alpha_1 \underline{v}_1 + \dots + \alpha_k \underline{v}_k = \underline{0} \iff \alpha_k \underline{v}_k = -\alpha_1 \underline{v}_1 - \dots - \alpha_{k-1} \underline{v}_{k-1}$$

$$\alpha_1 \lambda_1 \underline{v}_1 + \dots + \alpha_{k-1} + \lambda_{k-1} \underline{v}_{k-1} + \lambda_k (-\alpha_1 \underline{v}_1 - \dots - \alpha_{k-1} \underline{v}_{k-1}) = \underline{0}$$

$$\alpha_1 (\lambda_1 - \lambda_k) \underline{v}_1 + \dots + \alpha_{k-1} (\lambda_{k-1} - \lambda_k) \underline{v}_{k-1} = \underline{0}$$

E dato che $\underline{v}_1, \dots, \underline{v}_{k-1}$ sono indipendenti. Questo implica che:

$$\alpha_1 (\lambda_1 - \lambda_k) = \dots = \alpha_{k-1} (\lambda_{k-1} - \lambda_k) = 0$$

Ma tutti i λ_i sono distinti per ipotesi, quindi

$\alpha_1 = \dots = \alpha_{k-1} = 0$

Quindi ricordando $\alpha_1 \underline{v}_1 + \dots + \alpha_k \underline{v}_k = \underline{0}$ abbiamo che

$\alpha_k \underline{v}_k = 0 \Rightarrow \alpha_k = 0$ dato che $\underline{v}_k$ è un autovettore, $\underline{v}_k \neq 0$ e quindi $\alpha_k = 0$. Dunque $\underline{v}_1, \dots, \underline{v}_k$ sono linearmente indipendenti.

COROLLARIO

Sia $T: V \to V$. Se T ha esattamente n valori distinti, T è diagonalizzabile.

Perché $\underline{v}_1, \dots, \underline{v}_n$ formano una base di V, dato che sono linearmente indipendenti.

Cosa accade quando le radici del polinomio caratteristico non sono tutte distinte.

MOLTEPLICITÀ ALGEBRICA E GEOMETRICA

Sia $T: V \to V$ con $\dim V = n$ e $\lambda_0 \in sp\,T$. Allora

1. la molteplicità algebrica di λ_0 è la sua molteplicità come radice del polinomio caratteristico p_T. (ma_{λ_0})
2. la molteplicità geometrica di λ_0 è la dimensione del relativo autospazio V_{λ_0}. (mg_{λ_0})

$$\dim V_{\lambda_0} = \dim V - rk(T - \lambda_0 I_n)$$

ESEMPIO:

$$(M_T)^{E_3}_{E_3} = \begin{pmatrix} 3 & 1 & 1 \\ 2 & 4 & 2 \\ 3 & 3 & 5 \end{pmatrix} \qquad p_T(\lambda) = \begin{pmatrix} 3-\lambda & 1 & 1 \\ 2 & 4-\lambda & 2 \\ 3 & 3 & 5-\lambda \end{pmatrix}$$

$$p_T = -\lambda^3 + 12\lambda^2 - 36\lambda + 32 = (2-\lambda)^2(8-\lambda)$$

$sp(T) = \{2, 8\}$ $\quad \lambda_1 = 2 \quad ma = 2$

$\lambda_2 = 8 \quad ma = 1$

$$mg_2 = \left((M_T)^{E_3}_{E_3} - 2I_3\right) = 3 - rk\begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{pmatrix} = 3 - 1 = 2$$

$$mg_8 = \left((M_T)^{E_3}_{E_3} - 8I_3\right) = 3 - rk\begin{pmatrix} -5 & 1 & 1 \\ 2 & -4 & 2 \\ 3 & 3 & -3 \end{pmatrix} = 3 - 2 = 1$$

PROPOSIZIONE

La molteplicità algebrica di un autovalore è sempre maggiore o uguale della sua molteplicità geometrica

DIMOSTRAZIONE

Sia $T: V \to V$ endomorfismo, con $\dim V = n$ e $\lambda_0 \in Sp\,T$ e sia h la molteplicità geometrica di λ_0.

Sia $\{v_1, \dots, v_h\}$ una base di V_{λ_0}, la completiamo a base di V: $\{v_1, \dots, v_h, v_{h+1}, \dots, v_n\}$. Quindi

$$(M_T)_B^B = \left(\begin{array}{c|c} \lambda_0 I_h & B \\ \hline 0 & C \end{array}\right)$$

$$(M_T)_B^B - \lambda I_n = \left(\begin{array}{c|c} (\lambda_0 - \lambda) I_h & B \\ \hline 0 & C - \lambda I \end{array}\right)$$

Questa è una matrice a blocchi, quindi

$$p_T(\lambda) = \det((M_T)_B^B - \lambda I_n) = \det((\lambda_0 - \lambda) I_h) \det(C - \lambda I)$$
$$= (\lambda_0 - \lambda)^h p_C(\lambda)$$

Siccome la molteplicità algebrica è il più grande m per cui $(\lambda_0 - \lambda)^m \mid p_T(\lambda)$ ne segue che la molteplicità algebrica è sempre maggiore o uguale a quella geometrica.

CRITERIO DI DIAGONALIZZABILITÀ

Sia $T: V \to V$ endomorfismo e $\dim V = n$. $sp(T) = (\lambda_1, \dots, \lambda_h)$

Allora T.F.A.E:

1) T è diagonalizzabile
2) Ogni elemento di V si scrive come somma di autovettori di T relativi ad autovalori distinti.
3) $V = V_{\lambda_1} \oplus \dots \oplus V_{\lambda_h}$
4) T ha tutti gli autovalori in $\mathbb{K}$ e $ma_{\lambda_i} = mg_{\lambda_i}$ $i: 1 \dots h$
5) $mg_{\lambda_1} + \dots + mg_{\lambda_h} = n$

DIMOSTRAZIONE

$1 \Rightarrow 2$ T è dig. $\Leftrightarrow$ Ogni $v \in V$ è somma a.v. di T associati a a.val. distinti.

Per ipotesi esiste $B = \underline{v}_1, \dots, \underline{v}_n$ base di V, composta da autovettori, quindi $\forall \underline{v} \in V$ esiste $\alpha \in \mathbb{K}^n$ t.c.

$$\underline{v} = \sum_{i=1}^{n} \alpha_i \underline{v}_i$$

Se raggruppiamo i termini $\lambda_i \underline{v}_i$ corrispondenti agli ad autovettori relativi a uno stesso autovalore, abbiamo la teri.

$2 \Rightarrow 3$ Siano $\lambda_1, \dots, \lambda_h$ autovalori distinti per T. Per ipotesi abbiamo che $\forall \underline{v} \in V$ $\exists\, v_1, \dots, v_h$ $\in V_{\lambda_i}$ t.c.

$$\underline{v} = \underline{v}_1 + \dots + \underline{v}_h$$

Dobbiamo dimostrare che questa scrittura è unica:

$\exists\, \underline{w}_i \in \lambda_i$ t.c. $\underline{v}_1 + \dots \underline{v}_h = \underline{w}_1 + \dots + \underline{w}_h$

$$(\underline{v}_1 - \underline{w}_1) + \dots + (v_h - w_h) = 0 \quad \Rightarrow (v_i - w_i) = 0$$

$$\Rightarrow v_i = w_i \quad i: 1 \dots h$$

$3 \Rightarrow 4$ So che $V = V_{\lambda_1} \oplus \dots \oplus V_{\lambda_h}$ voglio dimostrare che T ha tutti gli autovalori in $\mathbb{K}$ e $ma_{\lambda_i} = mg_{\lambda_i}$

Abbiamo che

$$\dim V = n = \dim V_{\lambda_1} + \dots + \dim V_{\lambda_h} = mg_{\lambda_1} + \dots + mg_{\lambda_h}$$

Ma dato che la molteplicità algebrica sono le molteplicità algebriche delle radici $p_T(\lambda)$, si ha

$$\dim V = n \geq ma_{\lambda_1} + \dots + ma_{\lambda_h}$$

Siccome $ma_i \geq mg_i$

$$n = mg_{\lambda_1} + \dots + mg_{\lambda_h} \leq ma_{\lambda_1} + \dots + ma_{\lambda_h} \leq n$$

$$\Rightarrow ma = mg$$

$4 \Rightarrow 5$ Siccome T ha tutti gli autovalori in $\mathbb{K}$

POLINOMIO MINIMO

Data $A \in Mat_{n \times n}(\mathbb{K})$ l'insieme $I_A = \{ f \in \mathbb{K}[\lambda] \mid f(A) = 0 \}$

Abbiamo che:

1. Dal teorema Cayley-Hamilton: il polinomio caratteristico p_{LA}, appartiene all'insieme I_A.

$$p_{LA}(A) = 0$$

2. Esiste $p_{MA} \in I_A$ t.c: - p_{MA} è monico
   - $p_{MA} \mid p_{LA}(\lambda)$
   - $\partial\, p_{MA}$ è minimo in I_A

3. Se abbiamo una fattorizzazione in irriducibili di p_{LA}

$$p_{LA} = \prod_{i=1}^{k} f_i(x)^{\alpha_i} \qquad \alpha_i \geq 1$$

Allora $$p_M = \prod_{i=1}^{k} f_i(x)^{\beta_i} \qquad 1 \leq \beta_i \leq \alpha_i$$

4. Il polinomio minimo di L_A divide il p_T di L_A, ha le stesse radici ma con molteplicità minore od uguale.

5. Il p_M non dipende dalla base B. $p_M(\lambda)$ $[M_T]_B^B$

Deve essere squarefree

OSSERVAZIONI: la matrice è diagonalizzabile se e solo se il polinomio minimo è squarefree. Se fattorizzato il $p_T(\lambda)$, prendiamo i valori per cui non è sqr. e al posto di λ a sostituiamo la matrice. Se fa zero, il p_M è quello.

Quindi il polinomio minimo ci dice se un endomorfismo è diagonalizzabile. Dobbiamo avere un criterio per vedere se un polinomio ha radici multiple (metodo GCD) e un metodo per vedere se un polinomio ha tutte le radici in $\mathbb{K}$. Per $\mathbb{Q}$, $\mathbb{C}$ non è un problema, per $\mathbb{R}$, sì.

OSS: $GCD(p_T, p_T') = 1 \Rightarrow p_T(\lambda)$ è squarefree.

Non sempre siamo in grado di fattorizzare $p_T(\lambda)$, quindi dobbiamo trovare un nuovo metodo, senza calcolarne gli autovalori.

DEFINIZIONE SEQUENZA STANDARD

Sia: $p_0(t) = p(t)$

$p_1(t) = p'(t)$

allora: $p_0(t) = q_1(t)\, p_1(t) - p_2(t)$

$\vdots$

$p_{j-1}(t) = q_j(t)\, p_j(t) - p_{j+1}(t)$

$\vdots$

$p_{s-1}(t) \equiv 0 = q_s(t)\, p_s(t) + 0$

Si tratta della sequenza di Euclide per il calcolo di $GCD(p(t), p'(t))$ modificata: cambiando il segno al resto

Definizione

Sia $\underline{c} = c_0, \dots, c_s$ una sequenza in $\mathbb{R}$. Definiamo numero di variazioni $V(\underline{c})$ della successione il numero di cambi di segno non considerando lo zero.

ESEMPIO

$$V = (1, 0, 3, -1, -1, 2, 0, -2) = 3$$

Proposizione

Sia $p \in \mathbb{K}[t]$ Sia $p_0(t) \dots p_s(t)$ la sua sequenza standar

- Siano $a < b \in \mathbb{R}$, con $p(a), p(b)$ di segno opposto. Il numero di radici reali distinte nell'intervallo (a, b) sono:

$$V(p_0(a), p_1(a), \dots, p_s(a)) - V(p_0(b), p_1(b), \dots, p_s(b))$$

- Definiamo
  - $d_j = \partial p_j(t)$
  - c_j il coefficente di testa di $p_j(t)$
  - V_+ è il numero di variazioni nella sua successione $c_0, \dots, c_s$
  - V_- è il numero di variazioni della successione $(-1)^{d_0} \cdot c_0, \dots, (-1)^{d_s} \cdot c_s$
- Allora il numero di radici distinte in $\mathbb{R}$ è:

$$V_- - V_+$$

ESEMPIO

$p_0 = t^3 \qquad p_1 = 3t^2 \qquad p_2 = 2t \qquad p_3 = 1$

$V_+ = V(1, 3, 2, 1) = 0$

$V_- = V(-1, 3, -2, 1) = 3$

$V = 3 - 0 = 3$

Quindi ha 3 radici in $\mathbb{R}$. $\Rightarrow$ che T è diagonalizzabile in $\mathbb{R}$