$L: V \longrightarrow V$, $\dim_K V = n$

1) DEF. L diagonalizzabile se $\exists\, \mathcal{B}$ base di V t.c. $M_{\mathcal{B}}(L)$ è diagonale

2) TEOR. L diagonalizzabile $\iff \exists\, \mathcal{B}$ base di V costituita da autovettori di L.

COR. Se L ha n autovalori distinti, allora è diagonalizzabile.

3) Ristudiare il seguente esempio:

$$L: \mathbb{R}^3 \longrightarrow \mathbb{R}^3, \quad L(x,y,z) = (x+2z,\, 2y,\, 2x+z)$$

Gli autovalori di L sono $\lambda_1 = -1$, $\lambda_2 = 2$, $\lambda_3 = 3$.

Allora L è diagonalizzabile.

Gli autospazi relativi sono:

$$V_{\lambda_1} = \langle (1,0,-1) \rangle, \quad V_{\lambda_2} = \langle (0,1,0) \rangle, \quad V_{\lambda_3} = \langle (1,0,1) \rangle$$

Allora $\mathcal{B} = \{(1,0,-1), (0,1,0), (1,0,1)\}$ è una base di autovettori per L.

Si ha

$$M_{\mathcal{B}}(L) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Ricordare che

1) ogni matrice $A \in M_n(K)$ induce un endomorfismo

$$L_A : K^n \longrightarrow K^n$$

definito come segue:

Se $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in K^n$, allora

$$L_A(X) = AX$$

Inoltre abbiamo visto che

$$M_{\mathscr{E}}(L_A) = A,$$

essendo $\mathscr{E}$ la base canonica di K^n.

2) <u>DEF.</u> $A \in M_n(K)$ è diagonalizzabile se L_A è diagonalizzabile.

3) <u>TEOR.</u> $A \in M_n(K)$ è diagonalizzabile $\Longleftrightarrow$ A è simile ad una matrice diagonale

<u>DIM.</u> A diagonalizzabile $\Longleftrightarrow$ L_A diagonalizzabile $\Longleftrightarrow$ $\exists B$ base di K^n t.c. $M_B(L_A)$ è diagonal

./.

Ma matrici di uno stesso endomorfismo su basi distinte sono simili, pertanto

$$M_{\mathcal{B}}(L_A) \sim M_{\mathcal{E}}(L_A) = A$$

Viceversa: sia B una matrice diagonale simile ad A, allora

$$B = N^{-1}AN \,, \quad \text{con } N \in \mathcal{M}_n(K) \text{ invertibile}$$

Essendo N invertibile, le sue colonne $N^1, \dots, N^n$ costituiscono una base $\mathcal{B}$ di K^n e si ha $N = M^{\mathcal{B}}_{\mathcal{E}}(id)$ e anche $N^{-1} = M^{\mathcal{E}}_{\mathcal{B}}(id)$. Allora

$$\begin{tikzcd} K^n_{\mathcal{B}} \arrow[r, "id"] \arrow[rrr, bend right, "L_A"'] & K^n_{\mathcal{E}} \arrow[r, "L_A"] & K^n_{\mathcal{E}} \arrow[r, "id"] & K^n_{\mathcal{B}} \end{tikzcd}$$

quindi

$$M_{\mathcal{B}}(L_A) = M^{\mathcal{E}}_{\mathcal{B}}(id)\, M_{\mathcal{E}}(L_A)\, M^{\mathcal{B}}_{\mathcal{E}}(id) =$$
$$= N^{-1}AN = B,$$

cioè, la matrice di L_A sulla base $\mathcal{B}$ è diagonale $\Rightarrow L_A$ diagonalizzabile $\Rightarrow$
$\Rightarrow A$ diagonalizzabile.

Il seguente teorema, detto anche Teorema Spettrale fornisce una condizione necessaria e sufficiente per la diagonalizzabilità.

<u>Teor.</u> Sia $A \in M_n(K)$ e siano $\lambda_1, \dots, \lambda_r$ i suoi autovalori distinti, aventi molteplicità rispettive $m_1, \dots, m_r$.
Allora A è diagonalizzabile se e solo se sono verificate le seguenti condizioni

$$(1)\ \dim V_{\lambda_i} = m_i, \quad \forall i = 1, \dots, r$$

$$(2)\ \sum_{i=1}^{r} m_i = n.$$

<u>DIM.</u> Siano vere (1) e (2). Sia B_i una base di V_{λ_i}, $\forall i = 1, \dots, r$. Allora

$$B = \bigcup_{i=1}^{r} B_i$$

è un insieme di autovettori linearmente indipendenti. Da (1) e (2) segue allora che B è costituita da n autovettori, quindi è una base di K^n. Allora A è diagonalizzabile.
Viceversa, sia A diagonalizzabile. Allora esiste una base B di K^n costituita da autovettori. Da ciò si ricava che

$$K^n = V_{\lambda_1} \oplus \dots \oplus V_{\lambda_r}$$

Segue allora:

$$n = \dim K^n = \sum_{i=1}^{r} \dim V_{\lambda_i} \leq \sum_{i=1}^{r} m_i \leq n$$

quindi $\sum_{i=1}^{r} m_i = n$, cioè la (2) e necessariamente anche la (1). $\#$

<u>Esempi</u>

(1) Consideriamo la matrice

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

Il suo polinomio caratteristico è

$$P_A(t) = \begin{vmatrix} 1-t & 2 & 0 \\ 0 & 3-t & 0 \\ 2 & -4 & 2-t \end{vmatrix} = (1-t)(2-t)(3-t)$$

Pertanto A ha tre autovalori distinti

$$\lambda_1 = 1, \quad \lambda_2 = 2, \quad \lambda_3 = 3$$

ed è diagonalizzabile.
L'autospazio di λ_1 si ottiene risolvendo il sistema $AX = \lambda_1 X = X$, cioè

$$\begin{cases} x + 2y = x \\ 3y = y \\ 2x - 4y + 2z = z \end{cases} \Rightarrow \begin{cases} y = 0 \\ z = -2x \end{cases}$$

quindi $V_{\lambda_1} = \langle (1, 0, -2) \rangle$

Analogamente per gli altri autospazi, si ha

$V_{\lambda_2} = \langle (0,0,1) \rangle$, $V_{\lambda_3} = \langle (1,1,-2) \rangle$

Allora $\mathcal{B} = \{ (1,0,-2), (0,0,1), (1,1,-2) \}$ è una base di autovettori di L_A per $\mathbb{R}^3$.

Si ha

$$M^{\mathcal{B}}_{\mathcal{E}}(id) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ -2 & 1 & -2 \end{pmatrix} \quad e \quad M^{\mathcal{E}}_{\mathcal{B}} = \begin{pmatrix} 1 & -1 & 0 \\ 2 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Posto $N = M^{\mathcal{B}}_{\mathcal{E}}(id)$ si ottiene

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

Cioè la matrice N <u>diagonalizza</u> la matrice A. Si noti che

$$M_{\mathcal{B}}(L_A) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

è la matrice diagonale con gli autovalori sulla diagonale, secondo l'ordine considerato.

$\#$

(2) Si consideri la matrice

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

In questo, per il polinomio caratteristico si ha $p_A(t)=(1-t)(1+t)^2$, pertanto gli autovalori sono $\lambda_1=1$ e $\lambda_2=-1$, il secondo con molteplicità 2:

$$\lambda_1=1 \;,\; m_1=1$$
$$\lambda_2=-1 \;,\; m_2=2$$

Calcolando gli autospazi otteniamo

$V_{\lambda_1}=\langle(1,-1,0)\rangle$, $V_{\lambda_2}=\langle(1,0,-2),(0,1,0)\rangle$,

quindi $\dim V_{\lambda_1}=m_1=1$, $\dim V_{\lambda_2}=m_2=2$, e, in base al teorema spettrale, la matrice A è diagonalizzabile.

Se $\mathcal{B}=\{(1,-1,0),(1,0,-2),(0,1,0)\}$ è la base di autovettori, la matrice diagonalizzante è

$$N=M_{\mathcal{E}}^{\mathcal{B}}(id)=\begin{pmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -2 & 0 \end{pmatrix}, \text{ con } N^{-1}= M_{\mathcal{B}}^{\mathcal{E}}(id)=$$

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

Infine $N^{-1}AN=\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}=M_{\mathcal{B}}(L_A)$.

$L: V \longrightarrow V$ endomorfismo, $\dim_K V = n$

DEF. Un VENTAGLIO in V risp. ad L è una famiglia $\{V_1, \dots, V_n\}$ di sottospazi di V che soddisfa le seguenti richieste:

(1) $\dim V_i = i$, $\forall i = 1, \dots, n$

(2) $V_i \subset V_{i+1}$, $\forall i = 1, \dots, n-1$

(3) $L(V_i) \subset V_i$, $\forall i = 1, \dots, n$.

Nota che da (1) segue $\dim V_n = n$, pertanto $V_n = V$.

Dato un Ventaglio $\{V_1, \dots, V_n\}$ in V risp. L, si costruisce una BASE A VENTAGLIO per V, come segue:

- Sia $V_1 = \langle v_1 \rangle$ per (1).
- $v_1 \in V_2$ per (2) e $\dim V_2 = 2$. Allora si può scegliere $v_2 \in V_2$ in modo tale che $V_2 = \langle v_1, v_2 \rangle$
- $v_1, v_2 \in V_3$, quindi si può scegliere $v_3 \in V_3$ in modo tale che $V_3 = \langle v_1, v_2, v_3 \rangle$
- si continua in questo modo fino ad ottenere una base $\langle v_1, \dots, v_n \rangle$ di $V_n = V$ con la proprietà che $\langle v_1, \dots, v_i \rangle$ è base di V_i, $\forall i = 1, \dots, n$.

DEF l'endomorfismo $L: V \to V$ si dice TRIANGOLABILE se esiste una base $\mathcal{B}$ di V tale che $M_{\mathcal{B}}(L)$ sia una matrice triangolare superiore (= al disotto della diagonale principale tutti gli elementi sono nulli). (9)

TEOR. L è triangolabile se e solo se esiste un ventaglio in V risp. L.

DIM. Sia $\{V_1, \dots, V_n\}$ un ventaglio in V risp. L, e sia $\{v_1, \dots, v_n\} = \mathcal{B}$ una base a ventaglio per V. Dalle tre proprietà di ventaglio segue che

$$L(v_1) = a_{11} v_1$$
$$L(v_2) = a_{12} v_1 + a_{22} v_2$$
$$\vdots$$
$$L(v_n) = a_{1n} v_1 + \dots + a_{nn} v_n$$

pertanto

$$M_{\mathcal{B}}(L) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & 0 & & a_{nn} \end{pmatrix}$$

è triangolare superiore.

%

Viceversa, sia $\mathcal{B} = \{v_1, \dots, v_n\}$ una base di V tale che $M_{\mathcal{B}}(L)$ è matrice triangolare superiore (come la precedente). Poniamo $V_1 = \langle v_1 \rangle, \dots, V_n = \langle v_1, \dots, v_n \rangle$. Si ottiene un ventaglio in V risp. L, infatti: le proprietà (1), (2) sono immediatamente vere. Proviamo che $L(V_i) \subset V_i$, $\forall i = 1, \dots, n$.

Se $v \in V_i$, allora $v = \alpha_1 v_1 + \dots + \alpha_i v_i$ e

$$L(v) = \alpha_1 L(v_1) + \dots + \alpha_i L(v_i) =$$

$$= \alpha_1 a_{11} v_1 + \dots + \alpha_i (a_{1i} v_1 + \dots + a_{ii} v_i)$$

quindi $L(v)$ è combinazione lineare di $v_1, \dots, v_i$, cioè $L(v) \in V_i$. $\#$

NOTA Sia $V = U \oplus W$. Allora se $v \in V$, $v = u + w$, $u \in U$, $w \in W$, in un unico modo. Consideriamo le applicazioni lineari

$$P_1 : V \longrightarrow U, \quad P_1(v) = u$$

$$P_2 : V \longrightarrow W, \quad P_2(v) = w$$

Si ha $(P_1 + P_2)(v) = P_1(v) + P_2(v) =$

$$= u + w = v$$

cioè $P_1 + P_2 = id_V$.

Consideriamo $P_2 \circ L : V \longrightarrow W$, si ha $(P_2 \circ L)(w) \in W$, $\forall w \in W$, così si può considerare $P_2 \circ L : W \longrightarrow W$.

Equivalentemente:

$$P_1(v) = \begin{cases} v & \text{se } v \in U \\ \bar{0} & \text{se } v \notin U \end{cases}$$

$$P_2(v) = \begin{cases} v & \text{se } v \in W \\ \bar{0} & \text{se } v \notin W \end{cases}$$

TEOR. Sia V uno spazio vettoriale su $\mathbb{C}$ con $\dim_{\mathbb{C}} V = n$. Ogni endomorfismo $L: V \to V$ è triangolabile.

DIM. Per il teorema precedente basta provare che esiste un ventaglio per V risp. L.
Dimostrazione per induzione su $\dim V$.
Se $\dim V = 1$, $\{V\}$ è esso stesso un ventaglio.
Ipotesi induttiva: assumiamo che esiste un ventaglio per ogni endomorfismo $L: V \to V$ con $\dim V = n-1$.

Sia ora $\dim V = n$ e sia B una base per V.
Il polinomio caratteristico della matrice $M_B(L)$ è un polinomio di grado n a coefficienti complessi, quindi ammette certamente una radice $\lambda \in \mathbb{C}$ (autovalore della matrice e quindi di L). Sia $v_1 \in V$ un autovettore relativo a λ e poniamo $V_1 = \langle v_1 \rangle$.
Consideriamo $W < V$ tale che $V = V_1 \oplus W$ si ha $\dim_{\mathbb{C}} W = n-1$

Notiamo che $P_2 \circ L : \overline{W} \longrightarrow \overline{W}$ è un endomorfismo di $\overline{W}$. Pertanto, per l'ipotesi induttiva esiste un ventaglio in $\overline{W}$ rispett. a $P_2 \circ L$. Sia esso $\{\overline{W}_1, \dots, \overline{W}_{n-1}\}$.

A questo punto poniamo, $\forall\, i = 2, \dots, n$

$$\overline{V}_i = \overline{V}_1 \oplus \overline{W}_{i-1} .$$

Proviamo che $\{\overline{V}_1, \overline{V}_2, \dots, \overline{V}_n\}$ è un ventaglio in $\overline{V}$ risp. L, verificando le tre proprietà.

(1) $\dim \overline{V}_i = \dim \overline{V}_1 + \dim \overline{W}_{i-1} = i$ <u>OK</u>

(2) poiché $\overline{W}_{i-1} \subset \overline{W}_i$ segue che

$$\overline{V}_i = \overline{V}_1 \oplus \overline{W}_{i-1} \subset \overline{V}_1 \oplus \overline{W}_i = \overline{V}_{i+1}$$ <u>OK</u>

(3) da provare $L(\overline{V}_i) \subset \overline{V}_i$.

Ricordiamo che

$$L = id_{\overline{V}} \circ L = (P_1 + P_2) \circ L =$$
$$= P_1 \circ L + P_2 \circ L ,$$

allora se $u \in \overline{V}_i$, $u = v + w$, $v \in \overline{V}_1$, $w \in \overline{W}_{i-1}$

si ha: $L(u) = P_1 L(u) + P_2 L(u)$

dove:

$P_1 L(u) \in V_1 \subset V_i$ e

$P_2 L(u) = P_2 L(v) + P_2 L(w)$

ma $P_2 L(v) = P_2(\alpha v_1) = \alpha P_2(v_1) = \overline{0}$

quindi $P_2 L(u) = P_2 L(w) \in W_{i-1} \subseteq V_i$.

In fine $L(u) \in V_i$. Questo completa la dimostrazione

//

DEF. Una matrice $A \in M_n(K)$ si dice triangolabile se è triangolabile l'endomorfismo indotto

$$L_A : K^n \to K^n .$$

PROP. A è triangolabile se e solo se è simile ad una matrice triangolare superiore (Stessa dimostrazione del caso della diagonalizzazione)

TEOR Ogni matrice complessa $A \in M_n(\mathbb{C})$ è triangolabile.

In particolare ogni matrice reale $A \in M_n(\mathbb{R})$ è triangolabile nel campo dei complessi.

Esercizio 1 Si consideri la matrice

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

Il suo polinomio caratteristico:

$$P_A(t) = (2-t)\left[\left(\tfrac{3}{2}-t\right)^2 - \tfrac{1}{4}\right] = (2-t)(t-2)(t-1).$$

Allora gli autovalori di A sono

$\lambda_1 = 1$ con molteplicità $m_1 = 1$

$\lambda_2 = 2$ " " $m_2 = 2$

Calcoliamo l'autospazio V_{λ_1} risolvendo il sistema

$$AX = \lambda_1 X \iff AX = X \iff \begin{cases} \frac{3}{2}x - \frac{1}{2}y + \frac{1}{2}z = x \\ -\frac{1}{2}x + \frac{3}{2}y - \frac{1}{2}z = y \\ 2z = z \end{cases}$$

$\iff z = 0,\ x = y$

$\Rightarrow V_{\lambda_1} = \langle (1,1,0) \rangle$

calcoliamo l'autospazio V_{λ_2}:

$$AX = \lambda_2 X \iff AX = 2X \iff \begin{cases} \frac{3}{2}x - \frac{1}{2}y + \frac{1}{2}z = 2x \\ -\frac{1}{2}x + \frac{3}{2}y - \frac{1}{2}z = 2y \\ 2z = 2z \end{cases}$$

$\iff -x = y,\ z = 0$

$\Rightarrow V_{\lambda_2} = \langle (1,-1,0) \rangle$

%

Allora la dimensione di V_2 non coincide con la molteplicità dell'autovalore, quindi la matrice A <u>non</u> è diagonalizzabile.
Essa è però triangolabile sul campo $\mathbb{C}$.
Considerati i due autovettori $(1,1,0)$ e $(1,-1,0)$ aggiungiamo un vettore di $\mathbb{C}^3$ per ottenere una base di $\mathbb{C}^3$, ad es.

$$\mathcal{B} = \{(1,1,0),(1,-1,0),(0,0,1)\}$$

e notiamo che

$$L_A(1,1,0) = 1(1,1,0)+0(1,-1,0)+0(0,0,1)$$
$$L_A(1,-1,0) = 0(1,1,0)+2(1,-1,0)+0(0,0,1)$$
$$L_A(0,0,1) = \tfrac{1}{2}(1,1,0)-\tfrac{1}{2}(1,-1,0)+2(0,0,1)$$

cioè

$$M_{\mathcal{B}}(L_A) = \begin{pmatrix} 1 & 0 & 1/2 \\ 0 & 2 & -1/2 \\ 0 & 0 & 2 \end{pmatrix}$$

è la matrice triangolare con gli autovalori sulla diagonale principale secondo la loro molteplicità.
Determiniamo la matrice che triangola A, usando il solito diagramma

$$\begin{tikzcd} \mathbb{C}^n_{\mathcal{B}} \arrow[r, "id"] \arrow[rrr, bend right, "L_A"'] & \mathbb{C}^n_{\mathcal{E}} \arrow[r, "L_A"] & \mathbb{C}^n_{\mathcal{E}} \arrow[r, "id"] & \mathbb{C}^n_{\mathcal{B}} \end{tikzcd}$$

%

che fornisce

$$\circledast \quad M_{\mathcal{B}}(L_A) = M_{\mathcal{B}}^{\mathcal{C}}(id)\, \underset{\displaystyle A}{\overset{\|}{M_{\mathcal{C}}(L_A)}}\, M_{\mathcal{C}}^{\mathcal{B}}(id).$$

Si deve solo determinare la matrice $M_{\mathcal{B}}^{\mathcal{C}}(id)$; si ha

$$(1,0,0) = 1(1,1,0) + 1(1,-1,0) + 0(0,0,1)$$
$$(0,1,0) = \tfrac{1}{2}(1,1,0) - \tfrac{1}{2}(1,-1,0) + 0(0,0,1)$$
$$(0,0,1) = 0(1,1,0) + 0(1,-1,0) + 1(0,0,1)$$

così $M_{\mathcal{B}}^{\mathcal{C}}(id) = \begin{pmatrix} 1 & 1/2 & 0 \\ 1 & -1/2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Infine la $\circledast$ diventa:

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

#

Sia $A \in \mathcal{M}_n(\mathbb{C})$. Proviamo, per induzione su n, che essa è triangolabile.
Se $n = 1$, non c'è niente da provare.
Supponiamo per ipotesi induttiva che siano triangolabili tutte le matrici di $\mathcal{M}_{n-1}(\mathbb{C})$.

Caso $A \in \mathcal{M}_n(\mathbb{C})$. Il polinomio caratteristico $p_A(t)$ è un polinomio di grado n a coefficienti complessi, pertanto ammette una radice $\lambda_1 \in \mathbb{C}$. Sia $Z_1 \in \mathbb{C}^n$ un autovettore di λ_1 e costruiamo una base

$$\mathcal{B} = \{ Z_1, Y_2, \dots, Y_n \}$$

di $\mathbb{C}^n$. Consideriamo poi la matrice $B = M_{\mathcal{B}}(L_A)$. Questa è necessariamente della forma

$$B = \begin{pmatrix} \lambda_1 & * \cdots * \\ \vdots & B_{11} \\ 0 & \end{pmatrix}$$

Per l'ipotesi induttiva B_{11} è triangolabile, pertanto esiste una matrice invertibile $U_1 \in M_{n-1}(\mathbb{C})$ che triangola B_{11}, cioè

$$U_1^{-1} B_{11} U_1 = T_1$$

con T_1 matrice triangolare superiore di dimensione $n-1$.

A questo punto si pone

$$U = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & U_1 & \\ 0 & & \end{pmatrix}.$$

Segue che

$$U^{-1} B U = T = \begin{pmatrix} \lambda_1 & \cdots & * \\ \vdots & T_1 & \\ 0 & & \end{pmatrix}$$

è triangolare superiore.

Dal fatto poi che

$$B = M_{\mathcal{B}}^{\mathcal{E}} A M_{\mathcal{E}}^{\mathcal{B}}$$

segue subito

$$(U^{-1} M_{\mathcal{B}}^{\mathcal{E}}) A (M_{\mathcal{E}}^{\mathcal{B}} U) = T$$

cosicché $M_{\mathcal{E}}^{\mathcal{B}} U$ è la matrice che triangola A.

Come applicazione di quanto visto, consideriamo la matrice

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

Il suo polinomio caratteristico è

$$p_A(t) = (2-t)^3,$$

quindi A ammette come unico autovalore $\lambda = 2$ con molteplicità $m = 3$.

L'autospazio corrispondente:

$$AX = 2X \iff \begin{cases} 2x - 2y + 2z = 2x \\ 2y = 2y \\ 2y + 2z = 2z \end{cases}$$

$$\iff \begin{cases} 2y = 2z \\ y = 0 \end{cases} \iff \begin{cases} y = z = 0 \\ \forall x \end{cases}$$

Allora $V_\lambda = \langle (1,0,0) \rangle$.

Costruiamo una base di $\mathbb{C}^3$ a partire da tale autovettore, ad es.:

$$\mathcal{B} = \{(1,0,0), (0,1,0), (1,0,1)\}$$

<u>Nota</u>: è necessario che $\mathcal{B}$ non sia la base canonica.

Si ha:

$L_A(1,0,0) = 2(1,0,0) = 2(1,0,0) + 0(0,1,0) + 0(1,0,1)$

$L_A(0,1,0) = (-2,2,2) = -4(1,0,0) + 2(0,1,0) + 2(1,0,1)$

$L_A(1,0,1) = (4,0,2) = 2(1,0,0) + 0(0,1,0) + 2(1,0,1)$

allora

$$B = M_{\mathcal{B}}(L_A) = \begin{pmatrix} 2 & -4 & 2 \\ 0 & 2 & 0 \\ 0 & 2 & 2 \end{pmatrix}$$

Consideriamo la sottomatrice

$$B_{11} = \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix}$$

la quale ha come unico autovalore $\lambda = 2$ con molteplicità $m = 2$ ed autospazio

$$B_{11}X = 2X \iff \begin{cases} 2x = 2x \\ 2x + 2y = 2y \end{cases} \iff \begin{cases} x = 0 \\ \forall y \end{cases}$$

quindi $V_\lambda = \langle (0,1) \rangle$.

Costruiamo una base di $\mathbb{C}^2$ a partire dal tale autovettore, ad es.

$$\mathcal{B}' = \{(0,1), (-1,0)\}$$

Allora la matrice che triangola B_{11} è la matrice $M^{\mathcal{B}'}_{\mathcal{C}}(id) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = U_1$

Si noti che $U_1^{-1} = M^{\mathcal{C}}_{\mathcal{B}'}(id) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

e che

$$U_1^{-1} B_{11} U_1 = \begin{pmatrix} 2 & -2 \\ 0 & 2 \end{pmatrix} = T_1$$

Poniamo ora

$$U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & & \\ 0 & \multicolumn{2}{c}{U_1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$

con

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

Si ottiene che

$$U^{-1} B U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} 2 & -4 & 2 \\ 0 & 2 & 0 \\ 0 & 2 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} =$$

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

$\longrightarrow T_1$

Poiché $B = M^{\mathcal{C}}_{\mathcal{B}}(id)\, A\, M^{\mathcal{B}}_{\mathcal{C}}(id)$.

Verifichiamo che la matrice che triangola A è la matrice $M^{\mathcal{B}}_{\mathcal{C}}(id)\,U$; si ha

$$M^{\mathcal{B}}_{\mathcal{C}}(id)\,U = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix},$$

poiché $U^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$

e $M^{\mathcal{C}}_{\mathcal{B}}(id) = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

si ottiene

$$U^{-1} M^{\mathcal{C}}_{\mathcal{B}}(id) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$$

ed infine

$$\left(U^{-1} M^{\mathcal{C}}_{\mathcal{B}}(id)\right) A \left(M^{\mathcal{B}}_{\mathcal{C}}(id)\, U\right) =$$

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

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

PRODOTTI SCALARI.

Sia V uno spazio vettoriale sul campo K, con $\dim_K V = n$

<u>DEF.</u> Un prodotto scalare su V è una funzione $V \times V \to K$, $(v, w) \mapsto v \cdot w$
($v \cdot w$ si legge "v scalare w" !)
che verifica le seguenti richieste:

(1) $v \cdot w = w \cdot v$, $\forall v, w \in V$

(2) $v \cdot (w + u) = v \cdot w + v \cdot u$, $\forall u, v, w \in V$

(3) $(\alpha v) \cdot w = v \cdot (\alpha w) = \alpha (v \cdot w)$, $\forall \alpha \in K, \forall v, w \in V$

<u>Nota</u>: è un esercizio provare che (1) e (2) implicano che

(*) $(v + w) \cdot u = v \cdot u + w \cdot u$, $\forall u, v, w \in V$

Un prodotto scalare su V si dice poi <u>non degenere</u> se vale inoltre la

(4) $v \cdot w = 0, \forall w \in V \Rightarrow v = \overline{0}$.

Esempio Fondamentale.

Su K^n, per $X=(x_1,\dots,x_n)$, $Y=(y_1,\dots,y_n)$ si ponga

$$X\cdot Y = x_1y_1+\dots+x_ny_n .$$

Si ottiene un prodotto scalare non degenere sullo spazio K^n.

La verifica delle (1), (2), (3) è immediata.

Per la (4) si ha:

poiché $X\cdot Y=0$, $\forall Y\in K^n$, allora in particolare, detto $E_i=(0,\dots,1,\dots,0)$ l'i-esimo vettore della base canonica si ha

$$X\cdot E_i = x_i = 0, \ \forall i=1,\dots,n$$

quindi $X=\bar{0}$.

Su uno spazio vettoriale V dotato di un prodotto scalare due vettori $v, w\in V$ si definiscono ortogonali, scritto $v\perp w$, se $v\cdot w=0$

Una base $\mathcal{B}$ si dice ortogonale se i vettori che la compongono sono a due a due ortogonali.

la base canonica di K^n è una base ortogonale.

Sia ora V uno spazio vettoriale reale, cioè su $\mathbb{R}$. Un prodotto scalare su V è definito positivo se verifica la richiesta

$$(P) \quad v \cdot v \geq 0, \ \forall v \in V \ \text{e}$$
$$v \cdot v = 0 \iff v = \bar{0}.$$

Def. Uno spazio vettoriale reale munito di un prodotto scalare definito positivo si dice uno spazio Euclideo.

Esempio Fondamentale

Consideriamo su $\mathbb{R}^n$, $n > 0$, il prodotto scalare $X \cdot Y = x_1 y_1 + \dots x_n y_n$.
Tale prodotto scalare è definito positivo poichè $X \cdot X = x_1^2 + \dots + x_n^2 \geq 0$, e tale quantità è nulla se e solo se $x_i = 0$, $\forall i = 1, \dots, n$.
Allora $\mathbb{R}^n$ è, con tale prodotto scalare, uno spazio Euclideo.

<u>Notazioni</u>:

in $\mathbb{R}^n$ scriveremo $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, e quindi

$X^t = (x_1, \dots, x_n)$. Allora

$$X \cdot Y = X^t Y = (x_1, \dots, x_n) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

come prodotto righe x colonne.

Un altro esempio noto di spazio Euclideo è lo spazio dei vettori geometrici $V(\Sigma)$, con il prodotto scalare $v \cdot w = |v|\,|w| \cos \widehat{vw}$.

<u>Esercizio</u>: ogni prodotto scalare definito positivo è non degenere. Il viceversa non vale.

Se V è uno spazio Euclideo e

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

è una base ortogonale per V, allora

$v \in V \Rightarrow v = \alpha_1 v_1 + \dots + \alpha_n v_n$, $\alpha_i \in \mathbb{R}$.

$\forall\, i = 1, \dots, n$ si ha

$$v \cdot v_i = (\alpha_1 v_1 + \dots + \alpha_n v_n) \cdot v_i = \alpha_i (v_i \cdot v_i)$$

da cui $\alpha_i = \dfrac{v \cdot v_i}{v_i \cdot v_i}$, $\forall\, i = 1, \dots, n$.

<u>Coefficienti</u> di <u>Fourier</u> di v rispetto a $\mathcal{B}$.

TEOR. Ogni spazio Euclideo V ammette una base ortogonale.

DIM. Sia $\mathcal{B} = \{v_1, \dots, v_n\}$ una base qualunque di V. Poniamo

$$w_1 = v_1$$

$$w_2 = v_2 - \frac{v_2 \cdot w_1}{w_1 \cdot w_1} w_1$$

$$\vdots$$

$$w_n = v_n - \frac{v_n \cdot w_1}{w_1 \cdot w_1} w_1 - \dots - \frac{v_n \cdot w_{n-1}}{w_{n-1} \cdot w_{n-1}} w_{n-1},$$

allora $\{w_1, \dots, w_n\}$ è una base ortogonale per V.

Proviamo per induzione (finita) che ciascun w_i è ortogonale a tutti i vettori che lo precedono.

- primo passo: $w_2 \perp w_1$, infatti:

$$\left(v_2 - \frac{v_2 \cdot w_1}{w_1 \cdot w_1} \cdot w_1 \right) \cdot w_1 =$$

$$= v_2 \cdot w_1 - \frac{v_2 \cdot w_1}{\cancel{w_1 \cdot w_1}} (\cancel{w_1 \cdot w_1}) =$$

$$v_2 \cdot w_1 - v_2 \cdot w_1 = 0$$

- secondo passo: supponiamo che w_r sia ortogonale a tutti i precedenti.

- terzo passo: proviamo che allora w_{r+1} è ortogonale a tutti i precedenti:

$\forall\, i = 1, \dots, r$ si ha

$$w_{r+1} \cdot w_i = \left(v_{r+1} - \frac{v_{r+1} \cdot w_1}{w_1 \cdot w_1} w_1 - \dots - \frac{v_{r+1} \cdot w_r}{w_r \cdot w_r} \cdot w_r \right) \cdot w_i =$$

$$= v_{r+1} \cdot w_i - \frac{v_{r+1} \cdot w_1}{w_1 \cdot w_1} (w_1 \cdot w_i) - \dots - \frac{v_{r+1} \cdot w_r}{w_r \cdot w_r} (w_r \cdot w_i) =$$

$$= v_{r+1} \cdot w_i - \frac{v_{r+1} \cdot w_i}{\cancel{w_i \cdot w_i}} \cancel{(w_i \cdot w_i)} = 0 .$$

Allora $w_1, \dots, w_n$ sono vettori a due a due ortogonali. Per provare che essi forniscono una base di V basta provare che sono linearmente indipendenti.

Se $\alpha_1 w_1 + \dots + \alpha_n w_n = \bar{0}$, allora $\forall\, i = 1, \dots, n$ si ha

$$0 = (\alpha_1 w_1 + \dots + \alpha_n w_n) \cdot w_i =$$

$$\alpha_1 w_1 \cdot w_i + \dots + \alpha_i w_i \cdot w_i + \dots + \alpha_n w_n \cdot w_i =$$

$$= \alpha_i w_i \cdot w_i \quad , \text{ ma } w_i \cdot w_i > 0$$

quindi $\alpha_i = 0$, $\forall\, i = 1, \dots, n$.

#

Il teorema che abbiamo appena dimostrato prende il nome di

processo di ortogonalizzazione di Gram - Schmidt.

Esempio Ortogonalizziamo la base

$$\mathcal{B} = \{(2,1,1),(1,0,1),(0,0,2)\}$$

di $\mathbb{R}^3$.

Si ha

$$w_1 = (2,1,1)$$

$$w_2 = (1,0,1) - \frac{(1,0,1)\cdot(2,1,1)}{(2,1,1)\cdot(2,1,1)}(2,1,1) =$$

$$= (1,0,1) - \frac{3}{6}(2,1,1) =$$

$$= (1,0,1) - (1, 1/2, 1/2) = (0, -1/2, 1/2)$$

$$w_3 = (0,0,2) - \frac{(0,0,2)\cdot(2,1,1)}{(2,1,1)\cdot(2,1,1)}(2,1,1) - \frac{(0,0,2)\cdot(0,-1/2,1/2)}{(0,-1/2,1/2)\cdot(0,-1/2,1/2)}(0,-1/2,1/2)$$

$$= (0,0,2) - \frac{2}{6}(2,1,1) - \frac{1}{1/2}(0,-1/2,1/2) =$$

$$= (0,0,2) - (2/3, 1/3, 1/3) - (0,-1,1) =$$

$$= (-2/3, 2/3, 2/3)$$

La base ortogonalizzata di $\mathcal{B}$ è allora

$$\{(2,1,1),(0,-1/2,1/2),(-2/3,2/3,2/3)\}$$

$$(2,1,1)\cdot(0,-1/2,1/2)=0$$
$$(2,1,1)\cdot(-2/3,2/3,2/3)=0$$
$$(0,-1/2,1/2)\cdot(-2/3,2/3,2/3)=0 \quad .$$

\#

In uno spazio Euclideo V possiamo introdurre il concetto di metrica o misura come segue.

Se $v\in V$, poiché $v\cdot v\geq 0$ e $v\cdot v=0 \Leftrightarrow v=\bar{0}$, definiamo <u>norma di v</u> il numero reale

$$\|v\|=\sqrt{v\cdot v}\ .$$

Proprietà della norma.

1. $\forall \alpha\in\mathbb{R}, \forall v\in V$

$$\boxed{\|\alpha v\|=|\alpha|\,\|v\|}$$

$$\|\alpha v\|=\sqrt{(\alpha v)\cdot(\alpha v)}=\sqrt{\alpha^2(v\cdot v)}=|\alpha|\sqrt{v\cdot v}=|\alpha|\,\|v\|$$

(2) Disuguaglianza di Schwartz

$$\boxed{|v \cdot w| \leq \|v\| \, \|w\|}$$

Posto $\alpha = w \cdot w$, $\beta = -v \cdot w$ si ha

$$(\alpha v + \beta w) \cdot (\alpha v + \beta w) \geq 0 \quad \Rightarrow$$

$$\Rightarrow \alpha^2 (v \cdot v) + \beta^2 (w \cdot w) + 2\alpha\beta (v \cdot w) \geq 0$$

$$\Rightarrow (w \cdot w)^2 (v \cdot v) + (v \cdot w)^2 (w \cdot w) - 2 (w \cdot w)(v \cdot w)^2 \geq 0$$

se $w = \bar{0}$ $\underline{\text{OK}}$ se $w \neq \bar{0}$

$$\Rightarrow (w \cdot w)(v \cdot v) + (v \cdot w)^2 - 2(v \cdot w)^2 \geq 0$$

$$\Rightarrow (w \cdot w)(v \cdot v) \geq (v \cdot w)^2$$

e passando alle radici quadrate si ottiene l'asserto.

(3) Disuguaglianza Triangolare

$$\boxed{\|v + w\| \leq \|v\| + \|w\|}$$

si ha

$$\|v+w\|^2 = (v+w)\cdot(v+w) =$$

$$= v\cdot v + 2\,v\cdot w + w\cdot w =$$

$$= \|v\|^2 + \|w\|^2 + 2\,v\cdot w$$

ma $v\cdot w \leq |v\cdot w| \leq \|v\|\,\|w\|$, quindi

$$\leq \|v\|^2 + \|w\|^2 + 2\|v\|\|w\| =$$

$$= (\|v\| + \|w\|)^2$$

e passando alle radici quadrate, segue l'asserto.

Sia V uno spazio Euclideo e $v \in V$, un vettore non nullo. v è un vettore unità o unitario se $\|v\| = 1$.

Si noti che, dato $v \in V$, poiché $\|v\| > 0$, se $v \neq \bar{0}$, in base alla prima proprietà della norma è

$$\left\| \frac{1}{\|v\|} v \right\| = \frac{1}{\|v\|} \|v\| = 1.$$

Allora, $\forall\, v \in V$, $v \neq \bar{0}$, $\frac{v}{\|v\|}$ è un vettore unitario.

pertanto

$$\left\{ \left(\frac{2}{\sqrt{6}}, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}\right), \left(0, \frac{-1/2}{\sqrt{1/2}}, \frac{1/2}{\sqrt{1/2}}\right), \left(\frac{-2/3}{\sqrt{12/9}}, \frac{2/3}{\sqrt{12/9}}, \frac{2/3}{\sqrt{12/9}}\right) \right\}$$

è una base ortonormale di $\mathbb{R}^3$, ottenuta dalla base $\mathcal{B}$.

Per quanto visto, se V è uno spazio Euclideo e $\mathcal{B} = \{v_1, \dots, v_n\}$, tale base può essere ortogonalizzata con il processo di Gram-Schmidt, ottenendo una base ortonormale $\{w_1, \dots, w_n\}$ e poi si può normalizzare tale base ottenendo la base ortonormale

$$\left\{ \frac{w_1}{\|w_1\|}, \dots, \frac{w_n}{\|w_n\|} \right\}.$$

Allora: uno spazio Euclideo V ammette sempre una base ortonormale, cioè costituita da vettori a due a due ortogonali e ciascuno di norma 1.

Nell'esempio precedente abbiamo ortogonalizzato la base $\mathcal{B} = \{(2,1,1), (1,0,1), (0,0,2)\}$ di $\mathbb{R}^3$, ottenendo la base ortogonale

$$\{(2,1,1), (0,-1/2,1/2), (-2/3, 2/3, 2/3)\}.$$

Si ha

$$\|(2,1,1)\| = \sqrt{(2,1,1)\cdot(2,1,1)} = \sqrt{6}$$

$$\|(0,-1/2,1/2)\| = \sqrt{(0,-1/2,1/2)\cdot(0,-1/2,1/2)} = \sqrt{1/2}$$

$$\|(-2/3,2/3,2/3)\| = \sqrt{(-2/3,2/3,2/3)\cdot(-2/3,2/3,2/3)} = \sqrt{12/9}$$

Da notare quanto segue.

Sia V uno spazio Euclideo e sia $\mathcal{B}=\{v_1,\dots,v_n\}$ una base ortonormale per V. Siano poi

$$v=\alpha_1 v_1+\dots+\alpha_n v_n\,,\quad w=\beta_1 v_1+\dots+\beta_n v_n$$

due vettori qualunque di V. Si ha

$$v\cdot w=(\alpha_1 v_1+\dots+\alpha_n v_n)\cdot(\beta_1 v_1+\dots+\beta_n v_n)=$$

$$=\alpha_1\beta_1\, v_1\cdot v_1+\alpha_1\beta_2\, v_1\cdot v_2+\dots+\alpha_n\beta_n\, v_n\cdot v_n=$$

$$=\alpha_1\beta_1+\dots+\alpha_n\beta_n$$

poiché $v_i\cdot v_j=0$ se $i\neq j$ e $v_i\cdot v_i=\|v_i\|^2=1$ $\forall i=1,\dots,n$.

Allora, in presenza di una base ortonormale, comunque sia definito il prodotto scalare in V, esso si può esprimere attraverso il prodotto scalare usuale in $\mathbb{R}^n$ tra le coordinate dei vettori su tale base:

$$v\cdot w=\alpha_1\beta_1+\dots+\alpha_n v_n=v_{\mathcal{B}}^t\cdot w_{\mathcal{B}}$$

$$v_{\mathcal{B}}=\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix},\quad w_{\mathcal{B}}=\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix}.$$

Alcuni esercizi:

(1) Provare che, in $\mathbb{R}^3$, si ottiene un prodotto scalare definito positivo ponendo

$$X\cdot Y = 2x_1y_1 + x_1y_2 + x_2y_1 + 3x_2y_2 + x_2y_3 + \\ + x_3y_2 + 2x_3y_3$$

ove $X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$, $Y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$.

Basta verificare le proprietà (1), (2), (3) e (P).

- si noti che $X\cdot Y = Y\cdot X$ è evidente per il fatto che la definizione è simmetrica rispetto alle variabili x_i e y_i.
- le altre due proprietà $X\cdot(Y+Z) = X\cdot Y + X\cdot Z$ e $(\alpha X)\cdot Y = X\cdot(\alpha Y) = \alpha(X\cdot Y)$ sono immediate

Per la (P):

$$X\cdot X = 2x_1^2 + x_1x_2 + x_2x_1 + 3x_2^2 + x_2x_3 + \\ + x_3x_2 + 2x_3^2 =$$

$$= 2x_1^2 + 2x_1x_2 + 3x_2^2 + 2x_2x_3 + 2x_3^2 =$$
$$= (x_1+x_2)^2 + (x_2+x_3)^2 + x_1^2 + x_2^2 + x_3^2$$

Tale quantità è sempre ≥ 0 e vale 0 esattamente quando $x_1 = x_2 = x_3 = 0$, cioè $X = \overline{0}$.

(2) Determinare, se esiste, un prodotto scalare rispetto al quale la base

$$\mathcal{B} = \{(1,1,0), (1,-1,1), (0,0,1)\}$$

risulti una base ortonormale.

Posto $v_1 = (1,1,0)$, $v_2 = (1,-1,1)$, $v_3 = (0,0,1)$, se un tale prodotto scalare "$*$" esiste, si deve avere

$$v_1 * v_2 = v_1 * v_3 = v_2 * v_3 = 0 \quad e$$

$$v_1 * v_1 = v_2 * v_2 = v_3 * v_3 = 1.$$

Se $X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3$, si ha

$$\cancel{X = \frac{x+y}{2} v_1 + \frac{x-y}{2} v_2 + \frac{-x+y+2z}{2} v_3}$$

$$X = \frac{x_1+x_2}{2} v_1 + \frac{x_1-x_2}{2} v_2 + \frac{-x_1+x_2+2x_3}{2} v_3$$

Allora

$$X * Y = X^t Y = \left(\frac{x_1+x_2}{2}, \frac{x_1-x_2}{2}, \frac{-x_1+x_2+2x_3}{2} \right) \begin{pmatrix} \frac{y_1+y_2}{2} \\ \frac{y_1-y_2}{2} \\ \frac{-y_1+y_2+2y_3}{2} \end{pmatrix}$$

$$= \frac{x_1+x_2}{2} \cdot \frac{y_1+y_2}{2} + \frac{x_1-x_2}{2} \cdot \frac{y_1-y_2}{2} +$$

$$+ \frac{-x_1+x_2+2x_3}{2} \cdot \frac{-y_1+y_2+2y_3}{2} = - - -$$

La Traccia.

Sia $A \in \mathcal{M}_n(\mathbb{R})$. Definiamo traccia di A la somma degli elementi della diagonale principale di A,

se $A = (a_{ij})$, $Tr(A) = a_{11} + a_{22} + \cdots + a_{nn}$.

Si ottiene un'applicazione lineare

$$Tr : \mathcal{M}_n(\mathbb{R}) \to \mathbb{R}$$

infatti:

(1) $Tr(A+B) = Tr(A) + Tr(B)$.

(2) $Tr(\lambda A) = \lambda Tr(A)$.

Vale inoltre la seguente proprietà:

(3) $Tr(AB) = Tr(BA)$.

Infatti, se $A = (a_{ij})$, $B = (b_{ij})$, si ha per definizione di prodotto righe × colonne

$$AB = (A_i B^j)$$

quindi

$$Tr(AB) = \sum_{i=1}^{n} A_i B^i = (a_{i1}, \dots, a_{in}) \begin{pmatrix} b_{1i} \\ \vdots \\ b_{ni} \end{pmatrix} =$$

$$= a_{i1} b_{1i} + \cdots + a_{in} b_{in} = \sum_{j=1}^{n} a_{ij} b_{ji}$$

Segue che

$$\mathrm{Tr}(AB) = \sum_{i=1}^{n} A_i B^i = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} b_{ji} =$$
$$= \sum_{j=1}^{n} \sum_{i=1}^{n} b_{ji} a_{ij} = \sum_{j=1}^{n} B_j A^j =$$
$$= \mathrm{Tr}(BA).$$

Quanto visto ci permette di definire un prodotto scalare nello spazio $\mathcal{M}_n(\mathbb{R})$ delle matrici, ponendo

$$A \cdot B = \mathrm{Tr}(AB).$$

Si noti, ad es., che

$$A \cdot (B+C) = \mathrm{Tr}(A(B+C)) = \mathrm{Tr}(AB + AC) =$$
$$= \mathrm{Tr}(AB) + \mathrm{Tr}(AC) = A \cdot B + A \cdot C.$$

Le altre proprietà sono immediate.

Il prodotto scalare definito in $\mathcal{M}_n(\mathbb{R})$ è poi nondegenere. Infatti:

supponiamo $A \cdot B = 0$, $\forall B \in \mathcal{M}_n(\mathbb{R})$. Ciò equivale a

$$\mathrm{Tr}(AB) = 0, \ \forall B,$$

quindi, in particolare $\mathrm{Tr}(AE_{ij}) = 0$, $\forall i, j = 1, \ldots, n$.

E_{ij} è la matrice ad elementi tutti nulli, tranne $a_{ij} = 1$. Si ha:

$$Tr(AE_{ij}) = \sum_{k=1}^{n} A_k E_{ij}^{k} = A_j E_{ij}^{j} =$$

$$= (a_{j1}, \dots, a_{jn}) \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \to \text{i-esimo posto}$$

$$= a_{ji} \quad //$$

Il prodotto scalare definito dalla traccia non è definito positivo. Infatti, considerata la matrice

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

si ha

$$A \cdot A = Tr \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & 0 \\ -2 & -1 & -1 \end{pmatrix} = -1 \quad //$$

Alcune osservazioni:

(1) Matrici simili hanno la stessa traccia. Se $A \sim B$ allora $B = N^{-1}AN$, e si ha

$$Tr(B) = Tr(N^{-1}AN) = Tr(N^{-1}(AN)) =$$

$$= Tr(ANN^{-1}) = Tr(A)$$

(2) Se A è diagonalizzabile, si ha:

2.1) $Tr(A)$ è la somma degli autovalori di A.

2.2) Il prodotto degli autovalori di A è pari a $\det(A)$

Entrambe le affermazioni discendono dal fatto che matrici simili hanno stessi autovalori e stesso determinante.

<u>PROP.</u> Sia $A \in M_n(\mathbb{R})$. Allora

$$P_A(t) = (-1)^n t^n + (-1)^{n-1} Tr(A)\, t^{n-1} + \dots$$
$$\dots + \det(A)$$

Consideriamo il caso in cui

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

È $$p_A(t) = (a_{11}-t)(a_{22}-t) - a_{12}a_{21} =$$
$$= t^2 - (a_{11}+a_{22})\,t + a_{11}a_{22} - a_{12}a_{21} =$$
$$= t^2 - \mathrm{Tr}(A)\,t + \det(A).$$

La formula generale si dimostra per induzione su n, con passo iniziale quello appena visto, sviluppando $\det(A - tI)$ secondo la prima colonna.

<u>Esempio</u>

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

e $p_A(t) = (1-t)(2-t)(3-t)$, quindi

$$p_A(t) = -t^3 + 6t^2 + \text{—} + 6$$

#

In questa lezione V sarà uno spazio vettoriale complesso, cioè costruito su $\mathbb{C}$.

<u>DEF.</u> Un prodotto Hermitiano su V è una funzione

$$V \times V \to \mathbb{C} \,, \quad (v, w) \mapsto v \cdot w$$

(in tal caso $v \cdot w$ si legge: "v Hermitiano w") che verifica le seguenti richieste:

(1) $v \cdot w = \overline{w \cdot v}$

(2) $v \cdot (w + u) = v \cdot w + v \cdot u$

(3) $(\alpha v) \cdot w = \alpha (v \cdot w)$ e $v \cdot (\alpha w) = \overline{\alpha} (v \cdot w)$

$$\forall u, v, w \in V \,, \forall \alpha \in \mathbb{C}.$$

Si noti che:

$$(v + w) \cdot u = \overline{u \cdot (v + w)} = \overline{u \cdot v + u \cdot w} =$$

$$= \overline{u \cdot v} + \overline{u \cdot w} = v \cdot u + w \cdot u \,,$$

quindi vale anche la distributività destra.

Se V è uno spazio Hermitiano e $v \in V$ allora $v \cdot v$ è sempre un numero reale, quindi ha senso dichiarare che il prodotto Hermitiano di V è <u>definito positivo</u> se

(P) $v \cdot v \geq 0$ e $v \cdot v = 0 \iff v = \overline{0}$.

Def. Uno spazio Vettoriale complesso munito di un prodotto Hermitiano definito positivo si dice uno spazio Hermitiano.

Esempio Fondamentale

$\mathbb{C}^n$ è spazio Hermitiano con il prodotto

$$X \cdot Y = x_1 \overline{y_1} + \dots + x_n \overline{y_n} = X^t \overline{Y}$$

con $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{C}^n$.

Proprietà del prodotto Hermitiano:

Se $v \in V$ spazio Hermitiano, allora è possibile definire la norma di v

$$\|v\| = \sqrt{v \cdot v}$$

Si hanno le seguenti proprietà:

(1) $\|\alpha v\| = |\alpha| \, \|v\|$

(2) disuguaglianza di Schwartz

$$|v \cdot w| \leq \|v\| \cdot \|w\|$$

(3) disuguaglianza Triangolare

$$\|v + w\| \leq \|v\| + \|w\|$$

che sono formalmente uguali a quella della norma in uno spazio Euclideo.
Da notare però, che nella (2) $|v \cdot w|$ è il modulo del numero complesso $v \cdot w$.

Proviamo ora la (3):

$$\|v+w\|^2 = (v+w)\cdot(v+w) = v\cdot v + v \cdot w + w \cdot v + w \cdot w =$$

$$= v \cdot v + v \cdot w + \overline{v \cdot w} + w \cdot w \leq$$

Posto $v \cdot w = a + ib$ si ha

$$v \cdot w + \overline{w \cdot v} = 2a \leq 2\sqrt{a^2+b^2} = 2|v \cdot w|$$

$$\leq \|v\|^2 + \|w\|^2 + 2|v \cdot w| \leq \text{ per la (2)}$$

$$\leq \|v\|^2 + \|w\|^2 + 2\|v\|\,\|w\| = (\|v\| + \|w\|)^2.$$

Passando alle radici quadrate si ottiene l'asserto.

In uno spazio Hermitiano V si definisce nel modo ovvio il concetto di <u>base ortonormale</u>.

Il processo di ortonormalizzazione di una base si ottiene da quello che si è visto in uno spazio Euclideo, considerando il prodotto Hermitiano invece di quello

Esercizio. Ortonormalizzare la base

$$\mathcal{B}=\{\overset{v_1}{(1,i,0)},\overset{v_2}{(1,0,2i)},\overset{v_3}{(0,0,1)}\}$$

di $\mathbb{C}^3$.

Come nel caso Euclideo poniamo

- $w_1 = v_1$
- $w_2 = v_2 - \dfrac{v_2 \cdot w_1}{w_1 \cdot w_1} w_1$

$$v_2 \cdot w_1 = (1,0,2i)\cdot(1,i,0) = 1$$

$$w_1 \cdot w_1 = (1,i,0)\cdot(1,i,0) = 2$$

allora

$$w_2 = (1,0,2i) - \tfrac{1}{2}(1,i,0) = (\tfrac{1}{2}, -\tfrac{1}{2}i, 2i)$$

- $w_3 = v_3 - \dfrac{v_3 \cdot w_1}{w_1 \cdot w_1} w_1 - \dfrac{v_3 \cdot w_2}{w_2 \cdot w_2} w_2$

$$v_3 \cdot w_1 = (0,0,1)\cdot(1,i,0) = 0$$

$$v_3 \cdot w_2 = (0,0,1)\cdot(\tfrac{1}{2}, -\tfrac{1}{2}i, 2i) = -2i$$

$$w_2 \cdot w_2 = (\tfrac{1}{2}, -\tfrac{1}{2}i, 2i)\cdot(\tfrac{1}{2}, -\tfrac{1}{2}i, 2i) =$$

$$= (\tfrac{1}{4}+\tfrac{1}{4}+4) = \frac{18}{4} = \frac{9}{2}$$

allora

$$w_3 = (0,0,1) - \frac{-2i}{9/2}(\tfrac{1}{2}, -\tfrac{1}{2}i, 2i)$$

$$= (0,0,1) + \frac{4}{9}i(\tfrac{1}{2}, -\tfrac{1}{2}i, 2i) =$$

$$= (0,0,1) + (\tfrac{2}{9}i, \tfrac{2}{9}, -\tfrac{8}{9}) = (\tfrac{2}{9}i, \tfrac{2}{9}, \tfrac{1}{9})$$

Segue che la base ortogonalizzata è

$$w_1 = (1, i, 0), \quad w_2 = (1/2, -1/2\, i, 2i)$$

$$w_3 = (2/9\, i, 2/9, 1/9)$$

La base ortonormalizzata sarà:

$$\left\{ \frac{w_1}{\|w_1\|}, \frac{w_2}{\|w_2\|}, \frac{w_3}{\|w_3\|} \right\}$$

$$\|w_1\| = \sqrt{w_1 \cdot w_1} = \sqrt{2}$$

$$\|w_2\| = \sqrt{w_2 \cdot w_2} = \sqrt{9/2}$$

$$\|w_3\| = \sqrt{w_3 \cdot w_3} = \sqrt{(2/9\, i, 2/9, 1/9) \cdot (2/9\, i, 2/9, 1/9)} =$$

$$= \sqrt{\frac{4}{81} + \frac{4}{81} + \frac{1}{81}} = \sqrt{1/9}$$

quindi:

$$\left\{ \left(1/\sqrt{2}, i/\sqrt{2}, 0\right), \left(\frac{1/2}{\sqrt{9/2}}, -\frac{1/2}{\sqrt{9/2}}\, i, \frac{2}{\sqrt{9/2}}\, i\right), \right.$$

$$\left. \left(\frac{2/9}{\sqrt{1/9}}\, i, \frac{2/9}{\sqrt{1/9}}, \frac{1/9}{\sqrt{1/9}}\right) \right\}$$

#

Nota: anche nel caso di uno spazio Hermitiano V, con una base ortonormale $\mathcal{B}$, si verifica facilmente che, comunque sia definito il prodotto Hermitiano, si ha

$$v \cdot w = v_{\mathcal{B}}^t \cdot \overline{w_{\mathcal{B}}} = x_1 \overline{y_1} + \dots + x_n \overline{y_n}$$

per $v_{\mathcal{B}} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $w_{\mathcal{B}} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$

Sia ora V uno spazio Euclideo oppure Hermitiano e sia $W < V$ un suo sottospazio.
Poniamo

$$W^\perp = \{ v \in V \mid v \perp w, \ \forall w \in W \}$$

ove $v \perp w \iff v \cdot w = 0$, in ogni caso.
$W^\perp$ si chiama ortogonale di W.

<u>Prop</u> $\dim V = \dim W + \dim W^\perp$

<u>Dim</u> Sia $\{w_1, \dots, w_r\}$ una base ortonormale di W. Allora è possibile determinare $w_{r+1}, \dots, w_n$ in modo tale che $\{w_1, \dots, w_n\}$ sia una base ortonormale di V. Segue $W^\perp$ è il sottospazio generato da $\{w_{r+1}, \dots, w_n\}$. #

<u>Coroll.</u> $V = W \oplus W^\perp$.

<u>Esempio</u> Determinare l'ortogonale del sottospazio di $\mathbb{R}^4$

$$W = \langle (1,0,1,1), (2,0,0,1) \rangle .$$

Si ha $(x,y,z,t) \in W^\perp$ se e solo se

$$(x,y,z,t)\cdot(1,0,1,1) = 0$$
$$(x,y,z,t)\cdot(2,0,0,1) = 0$$

le due relazioni forniscono il sistema

$$\begin{cases} x+z+t=0 \\ 2x+t=0 \end{cases}$$

di 2 equazioni in 4 incognite. Le quaterne soluzioni del sistema sono della forma

$$(z, y, z, -2z).$$

pertanto $W^\perp = \langle (1,0,1,-2), (0,1,0,0) \rangle$.

Sia V uno spazio Euclideo e sia
$$L : V \longrightarrow V$$
un endomorfismo

TEOR. Sono equivalenti:

(1) $L(v)\cdot L(w) = v\cdot w$

(2) $\|L(v)\| = \|v\|$ $\qquad \forall v, w \in V$

(3) $\|v\| = 1 \Rightarrow \|L(v)\| = 1$

(4) L porta basi ortonormali in basi ortonormali.

Dim.

(1) $\Rightarrow$ (2) $\|L(v)\| = \sqrt{L(v)\cdot L(v)} = \sqrt{v\cdot v} = \|v\|$.

(2) $\Rightarrow$ (1) $\forall v, w \in V$ si ha

$$L(v+w)\cdot L(v+w) = (v+w)\cdot(v+w) \Rightarrow$$

$$[L(v)+L(w)]\cdot[L(v)+L(w)] = (v+w)\cdot(v+w) \Rightarrow$$

$$L(v)\cdot L(v) + L(w)\cdot L(w) + 2L(v)\cdot L(w) = v\cdot v + w\cdot w + 2v\cdot w \Rightarrow$$

$$\cancel{\|L(v)\|^2} + \cancel{\|L(w)\|^2} + 2L(v)\cdot L(w) = \cancel{\|v\|^2} + \cancel{\|w\|^2} + 2v\cdot w$$

$$\Rightarrow L(v)\cdot L(w) = v\cdot w$$

(2) $\Rightarrow$ (3) evidente.

(3) $\Rightarrow$ (2) $\forall v \in V$ si ha che $\frac{v}{\|v\|}$ è un vettore unitario, quindi

$$\left\|L\left(\frac{v}{\|v\|}\right)\right\| = 1 \text{ per (3)}$$

$$\Rightarrow \frac{1}{\|v\|}\|L(v)\| = 1 \Rightarrow \text{la (2)}.$$

Allora (1) e (3) sono equivalenti ed implicano la (4), cioè

se $\mathcal{B}=\{v_1,\dots,v_n\}$ è tale che
$v_i\cdot v_j=0\ \forall i\neq j$ et $v_i\cdot v_i=1,\ \forall i=1,\dots,n$
segue
$L(v_i)\cdot L(v_j)=0,\ \forall i\neq j$ et $L(v_i)\cdot L(v_i)=1,\ \forall i=1,\dots,n$
$\Rightarrow L(\mathcal{B})=\{L(v_1),\dots,L(v_n)\}$ è base ortonormale.

(4) $\Rightarrow$ (1) Sia $\mathcal{B}=\{v_1,\dots,v_n\}$ base ortonormale, e siano

$$v=\sum_{i=1}^{n}a_i v_i\ ,\quad w=\sum_{i=1}^{n}b_i v_i$$

$$\Rightarrow\qquad L(v)=\sum a_i L(v_i),\ L(w)=\sum b_i L(v_i),$$

in ogni caso si ha

$$v\cdot w=\sum a_i b_i\ ,\quad L(v)\cdot L(w)=\sum a_i b_i$$

#

DEF. Un endomorfismo $L:V\to V$ di uno spazio Euclideo si dice unitario se verifica una delle condizioni equivalenti del Teorema.

Nota: Se L è unitario, allora conserva l'ortogonalità. Il viceversa non vale:

$$L:V\to V,\ L(v)=2v$$

è lineare e conserva l'ortogonalità, ma

$$L(v)\cdot L(w)=4\,v\cdot w.$$

#

Se L è unitaria allora è un isomorfismo:

$v\in\ker L\Rightarrow L(v)=\bar{0}$, quindi

$$L(v)\cdot L(v)=v\cdot v=\bar{0}\quad\Longrightarrow v=\bar{0}$$

#

Osservazione:
Sia $\mathcal{E} = \{e_1, \dots, e_n\}$ la base canonica di $\mathbb{R}^n$ e sia $A \in M_n(\mathbb{R})$, $A = (a_{ij})$.
Si ha, $\forall\, i, j = 1, \dots, n$

$$e_i^t A e_j = (0, \dots, \underset{i\text{-esimo}}{1}, \dots, 0)\, A \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} \\ \\ \to j\text{-esimo} \\ \\ \\ \end{matrix} =$$

$$= (0, \dots, 1, \dots, 0) \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix} = a_{ij}$$

$$\Rightarrow \boxed{e_i^t A e_j = a_{ij}} \quad \forall\, i, j = 1, \dots, n.$$

DEF. Una matrice $A \in M_n(\mathbb{R})$ si dice unitaria se $A^t A = I_n$.

Se A è unitaria, allora A è invertibile e $A^t = A^{-1}$.
Infatti:
- A invertibile: $\det(A)^2 = \det(A^t A) = 1$
  $\Rightarrow \det(A) = \pm 1$
- $A^t A A^{-1} = I A^{-1} = A^{-1} \Rightarrow A^t = A^{-1}$

Inoltre: A unitaria $\Leftrightarrow \{A^1, \dots, A^n\}$ è una base ortonormale per $\mathbb{R}^n$.

Se A è unitaria, allora $A^t A = (A_i^t A^j) = (A^i A^j) = I_n$, quindi

$$A^i A^j = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

e viceversa.

<u>TEOR</u> Sia V Euclideo, $L: V \to V$ un endomorfismo. Sia $\mathcal{B}$ una base ortonormale di V e

$$A = M_{\mathcal{B}}(L).$$

Allora L è unitaria $\Leftrightarrow$ A è unitaria.

<u>DIM.</u>

$\forall\, v, w \in V$ è $v \cdot w = v_{\mathcal{B}}^t \cdot w_{\mathcal{B}}$.

Allora

$$L(v) \cdot L(w) = L(v)_{\mathcal{B}}^t \cdot L(w)_{\mathcal{B}} = (A v_{\mathcal{B}})^t (A w_{\mathcal{B}}) =$$

$$= v_{\mathcal{B}}^t (A^t A) w_{\mathcal{B}}.$$

Pertanto, se A è unitaria, L è unitaria.

Viceversa, se L è unitaria, allora

$$v_{\mathcal{B}}^t \cdot w_{\mathcal{B}} = v_{\mathcal{B}}^t (A^t \cdot A)\, w_{\mathcal{B}}, \quad \forall\, v, w \in V.$$

In particolare, se $v = e_i$, $w = e_j$, vettori della base canonica, si ottiene:

$$e_i^t (A^t A)\, e_j = e_i^t e_j = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{altrimenti} \end{cases}$$

ma (pag. 54, Osservazione)

$$e_i^t (A^t A)\, e_j = x_{ij}$$

cioè, l'elemento di posto (i, j) della matrice $A^t A$.

$$x_{ij} = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{altrimenti} \end{cases}$$

$$\Rightarrow A^t A = I_n$$

#

Considerazioni analoghe in ambito complesso.

Una matrice $A \in M_n(\mathbb{C})$ si dice <u>unitaria</u> se

$$A^t \bar{A} = I_n$$

ove, se $A = (a_{ij})$, $\bar{A} = (\bar{a}_{ij})$.

- A è invertibile:

$$1 = \det(A^t \bar{A}) = \det(A^t)\det(\bar{A}) =$$
$$= \det(A)\overline{\det(A)}$$
$$\Rightarrow |\det(A)| = 1$$

- $A^t = A^t \bar{A} \bar{A}^{-1} = \cancel{A^t \bar{A} \bar{A}^{-1}} = (A^t \bar{A})\bar{A}^{-1} = \bar{A}^{-1}$

$$\Rightarrow A^t = \bar{A}^{-1}$$

- A è unitaria $\Leftrightarrow \{A^1, \dots, A^n\}$ è una base ortonormale di $\mathbb{C}^n$.

<u>DEF</u> Se V è uno spazio Hermitiano e $L: V \to V$ è un endomorfismo, L è unitario se $L(v) \cdot L(w) = v \cdot w$, $\forall\, v, w \in V$

(Vale il Teorema analogo a quello di pag 55 $\mathcal{F}$, cioè

$$v \cdot w = v_B^t \overline{w_B}$$
$$L(v) \cdot L(w) = L(v)_B^t \cdot \overline{L(w)_B} = (A v_B)^t (\overline{A w_B}) =$$
$$= v_B^t (A^t \bar{A}) \overline{w_B}$$

e $v_B^t \overline{w_B} = v_B^t (A^t \bar{A}) \Leftrightarrow A^t \bar{A} = I_n$)

Sia ora V uno spazio Euclideo oppure uno spazio Hermitiano e siano

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

due basi ortonormali di V.

Poniamo $$A = M^{\mathcal{B}}_{\mathcal{B}'}(id)$$

essere la matrice del cambiamento di base.

In ogni caso A risulta essere una matrice unitaria. Infatti; posto

$$v_1 = a_{11}v_1' + \dots + a_{n1}v_n'$$
$$\vdots$$
$$v_n = a_{1n}v_1' + \dots + a_{nn}v_n'$$

si ha:

caso Euclideo:

$$\cancel{A^t_i A^j = (a_{i1},\dots,a_{in})\begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj}\end{pmatrix} =}$$
$$\cancel{= a_{i1}a_{1j}+\dots+a_{in}a_{nj} =}$$

$$A^t_i A^j = A^i A^j = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni}\end{pmatrix}\cdot\begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj}\end{pmatrix} =$$

$$= a_{1i}a_{1j}+\dots+a_{ni}a_{nj} = v_i\cdot v_j = \begin{cases} 1 & \text{se } i=j \\ 0 & \text{se } i\neq j\end{cases}$$

caso Hermitiano:

$$A^t_i \overline{A^j} = A^i\overline{A^j} = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni}\end{pmatrix}\cdot\begin{pmatrix} \overline{a}_{1j} \\ \vdots \\ \overline{a}_{nj}\end{pmatrix} =$$

$$= a_{1i}\overline{a}_{1j}+\dots+a_{ni}\overline{a}_{nj} = v_i\cdot v_j = \begin{cases} 1 & \text{se } i=j \\ 0 & \text{se } i\neq j\end{cases}$$

TEOR. Sia V Hermitiano, $\dim_{\mathbb{C}} V = n$, e sia $L : V \to V$ unitario. Esiste una base ortonormale di V costituita da autovettori di L.

DIM.

Dalle ipotesi segue:

(1) esiste un ventaglio $\{V_1, \dots, V_n\}$ in V risp. L.

(2) esiste una base a ventaglio $\{v_1, \dots, v_n\}$ per V

(3) ortonormalizziamo tale base ottenendo la base ortonormale

$$\{u_1, \dots, u_n\}$$

(4) $\{u_1, \dots, u_n\}$ è ancora una base a ventaglio in V risp. al ventaglio $\{V_1, \dots, V_n\}$, infatti, $\forall\, i = 1, \dots, n$, risulta

$$u_i = \frac{v_i - \alpha_1 v_1 - \dots - \alpha_{i-1} v_{i-1}}{\| v_i - \alpha_1 v_1 - \dots - \alpha_{i-1} v_{i-1} \|} \in V_i$$

Allora $L(u_1) \in V_1 \Rightarrow L(u_1) = \lambda_1 u_1$, $\lambda_1 \in \mathbb{C}$, così u_1 è autovettore di λ_1.

Supponiamo, per induzione, che $u_1, \dots, u_{k-1}$ siano autovettori di $\lambda_1, \dots, \lambda_{k-1}$.

Consideriamo

$$L(u_k) \in V_k \Rightarrow L(u_k) = \alpha_1 u_1 + \dots + \alpha_k u_k$$

e che, $\forall\, i = 1, \dots, k-1$ si ha

$$L(u_i) \cdot L(u_k) = u_i \cdot u_k = 0$$

quindi anche $L(u_i)\cdot L(u_K) = u_i\cdot u_K = 0$ e

$$\lambda_i u_i \cdot L(u_K) = \overline{\lambda_i}[u_i\, L(u_K)] = 0$$

Si noti che l'autovalore λ_i non è 0, poiché L è biiettiva, quindi dall'ultima relazione segue

$$0 = u_i\, L(u_K) = u_i\cdot(\alpha_1 u_1 + \dots + \alpha_K u_K) =$$

$$= u_i\cdot(\alpha_i u_i) = \overline{\alpha_i}\,(u_i\cdot u_i)$$

ed essendo $u_i\cdot u_i \neq 0$, si deve avere $\alpha_i = \overline{\alpha_i} = 0$, $\forall\, i = 1,\dots,K-1$.
Infine $L(u_K) = \alpha_K u_K$, cosicché anche u_K è un autovettore. #

<u>TEOR.</u> Ogni matrice unitaria complessa si diagonalizza per mezzo di una matrice unitaria.

<u>Dim.</u>

Sia $\mathcal{C}$ la base canonica di $\mathbb{C}^n$ e sia $A \in M_n(\mathbb{C})$ unitaria. Per il Teor. di pag 55 segue che

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

è unitaria. Quindi esiste una base ortonormale $\mathcal{B}$ di $\mathbb{C}^n$, costituita da autovettori di A.
Posto $M = M_{\mathcal{B}}(L_A)$, M è diagonale e simile ad A, pertanto

$$M = N^{-1}AN \quad \text{con } N = M^{\mathcal{B}}_{\mathcal{C}}(id).$$

Essendo $\mathcal{C}$ e $\mathcal{B}$ basi ortogonali, N è unitaria.
* Si noti che $N^{-1} = \overline{A}^t = \overline{A}^t$.

Esempio: Sia
$$A = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$
A è unitaria infatti
$$A^tA = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$P_A(t) = \begin{vmatrix} -t & 1 & 0 \\ -1 & -t & 0 \\ 0 & 0 & 1-t \end{vmatrix} = (1-t)(t^2+1)$$
e gli autovalori sono
$$\lambda_1 = 1, \quad m_1 = 1$$
$$\lambda_2 = i, \quad m_2 = 1$$
$$\lambda_3 = -i, \quad m_3 = 1$$
pertanto A è diagonalizzabile e simile a
$$M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -i \end{pmatrix}.$$

Autospazi:

$\underline{\lambda_1 = 1}$ $\quad AX = X \iff \begin{cases} y = x \\ -x = y \\ z = z \end{cases} \Rightarrow V_{\lambda_1} = \langle (0,0,1) \rangle.$

$\underline{\lambda_2 = i}$ $\quad AX = iX \iff \begin{cases} y = ix \\ -x = iy \\ z = iz \end{cases} \iff \begin{cases} ix - y = 0 \\ x - iy = 0 \\ (1-i)z = 0 \end{cases} \iff \begin{matrix} z = 0 \\ y = ix \end{matrix}$

$$\Rightarrow V_{\lambda_2} = \langle (1, i, 0) \rangle.$$

$\underline{\lambda_3 = -i}$ $\quad AX = -iX \iff \begin{cases} y = -ix \\ -x = -iy \\ z = -iz \end{cases} \iff \begin{cases} ix + y = 0 \\ x + iy = 0 \\ (1+i)z = 0 \end{cases} \iff \begin{matrix} z = 0 \\ y = -ix \end{matrix}$

$$\Rightarrow V_{\lambda_3} = \langle (1, -i, 0) \rangle$$

la base di autovettori di $\mathbb{C}^3$

$$\{(0,0,1),(1,i,0),(1,-i,0)\}$$

è già ortogonale.

$$\|(0,0,1)\| = \sqrt{(0,0,1)\cdot(0,0,1)} = 1$$
$$\|(1,i,0)\| = \sqrt{(1,i,0)\cdot(1,i,0)} = \sqrt{2}$$
$$\|(1,-i,0)\| = \sqrt{(1,-i,0)\cdot(1,-i,0)} = \sqrt{2}$$

Segue che $\mathcal{B} = \{(0,0,1),(1/\sqrt{2}, i/\sqrt{2}, 0),(1/\sqrt{2}, -i/\sqrt{2}, 0)\}$ è una base ortonormale di autovettori.

Considerato

$$N = M^{\mathcal{B}}_{\mathcal{C}}(id) = \begin{pmatrix} 0 & 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & i/\sqrt{2} & -i/\sqrt{2} \\ 1 & 0 & 0 \end{pmatrix}$$

che è unitaria, si ha

$$N^{-1} = \bar{N}^t = \begin{pmatrix} 0 & 0 & 1 \\ 1/\sqrt{2} & -i/\sqrt{2} & 0 \\ 1/\sqrt{2} & i/\sqrt{2} & 0 \end{pmatrix}$$

ed infine

$$\bar{N}^t A N = \begin{pmatrix} 0 & 0 & 1 \\ 1/\sqrt{2} & -i/\sqrt{2} & 0 \\ 1/\sqrt{2} & i/\sqrt{2} & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & i/\sqrt{2} & -i/\sqrt{2} \\ 1 & 0 & 0 \end{pmatrix} =$$

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

#

Sia ora V uno spazio Euclideo e $L: V \to V$ un endomorfismo.

<u>DEF</u> L è simmetrico se vale
$$L(v) \cdot w = v \cdot L(w), \ \forall v, w \in V$$

<u>TEOR.</u> Sia $L: V \to V$ e sia $\mathcal{B}$ una base ortonormale di V. Posto $A = M_{\mathcal{B}}(L)$, allora L è simmetrico se e solo se A è simmetrica.

<u>DIM.</u>
$\forall v, w \in V$ si ha $v \cdot w = v_{\mathcal{B}}^t \cdot w_{\mathcal{B}}$. Quindi:
$$L(v) \cdot w = L(v)_{\mathcal{B}}^t \cdot w_{\mathcal{B}} = (A v_{\mathcal{B}})^t w_{\mathcal{B}} = v_{\mathcal{B}}^t A^t w_{\mathcal{B}}$$

$$v \cdot L(w) = v_{\mathcal{B}}^t \cdot L(w)_{\mathcal{B}} = v_{\mathcal{B}}^t A w_{\mathcal{B}}$$

Segue che se A è simmetrica $A = A^t$, allora $L(v) \cdot w = v \cdot L(w)$ e L è simmetrico.
Viceversa, supponiamo che L sia simmetrico, allora vale
$$v_{\mathcal{B}}^t A^t w_{\mathcal{B}} = v_{\mathcal{B}}^t A w_{\mathcal{B}}$$
$\forall v, w \in V$. Con un argomento analogo a quello del teorema di pag. 55 si ottiene $A = A^t$
#

<u>TEOR.</u> Una matrice reale simmetrica $A \in M_n(\mathbb{R})$ ha n autovalori reali.

<u>DIM.</u> Sia $p_A(t)$ il polinomio caratteristico di A e sia $\lambda \in \mathbb{C}$ una sua radice.

Sia $Z \in \mathbb{C}^n$ un autovettore di λ, cioè $AZ = \lambda Z$.
Si ha:

$$\lambda(Z\cdot Z) = (\lambda Z)\cdot Z = (AZ)\cdot Z = (AZ)^t\,\bar{Z} =$$

$$= (Z^t A^t)\bar{Z} = Z^t\cdot(A\bar{Z}) = Z^t\,\overline{(AZ)} =$$

$$= Z\cdot(AZ)$$

$$\overline{\lambda(Z\cdot Z)} = \overline{(\lambda Z)\cdot Z} = \overline{(AZ)\cdot Z} = Z\cdot(AZ) \quad \#$$

$$= \cancel{Z\cdot(AZ) = \bar{\lambda}(Z\cdot Z)\lambda} =$$

$$= \cancel{\bar{\lambda}(Z\cdot Z)}$$

Allora $\lambda(Z\cdot Z) = \overline{\lambda(Z\cdot Z)} = \bar{\lambda}(Z\cdot Z)$.

Poiché $Z\cdot Z \in \mathbb{R}$, segue $\lambda = \bar{\lambda}$, così $\lambda \in \mathbb{R}$.
#

<u>COROLL.</u> Se $L: V \to V$ è simmetrica, essa ha n autovalori reali.

<u>TEOR.</u> Se $L: V \to V$ è simmetrica, esiste una base di V ortonormale, costituita da autovettori di L.

<u>DIM.</u> Per induzione sulla dimensione di V. Se $\dim V = 1$, non c'è niente da provare. Supponiamo il teorema vero per tutti gli spazi Euclidei di dimensione $n-1$.

Sia $\dim V = n$, e sia λ un autovalore di L

con autovettore relativo v. Allora $w = \frac{v}{\|v\|}$ è ancora un autovettore di λ.
Poniamo $U = \langle w \rangle^\perp$, con $\dim U = n-1$.
Si noti che $\forall\, u \in U$ si ha:

$$L(u)\cdot w = u \cdot L(w) = u(\lambda w) = \lambda(u \cdot w) = 0$$

così $L(u) \in U$, quindi $L: U \to U$, e per l'ipotesi induttiva esiste una base ortonormale di U costituita da autovettori di L.
Sia essa $\{u_1, \dots, u_{n-1}\}$.
Allora $\{u_1, \dots, u_{n-1}, w\}$ è una base ortonormale di V, di autovettori di L.

//

TEOR Ogni matrice reale simmetrica $A \in M_n(\mathbb{R})$ si diagonalizza per mezzo di una matrice unitaria reale.

DIM. $L_A : \mathbb{R}^n \to \mathbb{R}^n$ è simmetrica. Allora esiste una base ortonormale $\mathcal{B}$ di $\mathbb{R}^n$ costituita da autovettori di A.
Sia $N = (B^1, \dots, B^n)$ la matrice i cui vettori colonne sono i vettori di $\mathcal{B}$ $(N = M^{\mathcal{B}}_{\mathcal{C}}(id))$.
N è una matrice reale unitaria e vale

$$N^{-1}AN = M_{\mathcal{B}}(L_A) \text{ che è diagonale}$$

//

Esempio. Sia

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

$$P_A(t) = -t(1-t) - 1/4 = t^2 - t - 1/4$$

$$\Rightarrow \quad t = \frac{1 \pm \sqrt{2}}{2}$$

$\Rightarrow$ due autovalori reali

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

Gli autovettori:

$\underline{\lambda_1}$ $\quad Ax = \frac{1+\sqrt{2}}{2} x \iff \begin{cases} x - \frac{1}{2} y = \frac{1+\sqrt{2}}{2} x \\ -\frac{1}{2} x = \frac{1+\sqrt{2}}{2} y \end{cases} \Rightarrow \begin{cases} \frac{1-\sqrt{2}}{2} x - \frac{1}{2} y = 0 \\ \frac{1}{2} x + \frac{1+\sqrt{2}}{2} y = 0 \end{cases}$

$$\iff V_{\lambda_1} = \langle (1, 1+\sqrt{2}) \rangle$$

$\underline{\lambda_2}$ .... $V_{\lambda_2} = \langle (1, 1-\sqrt{2}) \rangle$

Base di autovettori $\{(1, 1+\sqrt{2}), (1, 1-\sqrt{2})\}$:

È ortogonale $(1, 1+\sqrt{2}) \cdot (1, 1-\sqrt{2}) = 1 + (1-2) = 0$

$\|(1, 1+\sqrt{2})\| = \sqrt{(1+\sqrt{2}) \cdot (1+\sqrt{2})} = \sqrt{4 + 2\sqrt{2}} =$

$\|(1, 1-\sqrt{2})\| = \sqrt{(1, 1-\sqrt{2}) \cdot (1, 1-\sqrt{2})} = \cancel{\sqrt{\ldots}} = \sqrt{4 - 2\sqrt{2}}$

$\Rightarrow$ base ortonormale

$$B = \left\{ \left(\frac{1}{\sqrt{4+2\sqrt{2}}}, \frac{1+\sqrt{2}}{\sqrt{4+2\sqrt{2}}} \right), \left(\frac{1}{\sqrt{4-2\sqrt{2}}}, \frac{1-\sqrt{2}}{\sqrt{4-2\sqrt{2}}} \right) \right\}$$

Si ha

$$N = M_{\mathcal{B}}^{B}(id) = \begin{pmatrix} \frac{1}{\sqrt{4+2\sqrt{2}}} & \frac{1}{\sqrt{4-2\sqrt{2}}} \\ \frac{1+\sqrt{2}}{\sqrt{4+2\sqrt{2}}} & \frac{1-\sqrt{2}}{\sqrt{4-2\sqrt{2}}} \end{pmatrix}$$

unitaria, e $N^{-1} = N^t$.

Basta verificare che

$$N^t A N = \begin{pmatrix} \frac{1+\sqrt{2}}{2} & 0 \\ 0 & \frac{1-\sqrt{2}}{2} \end{pmatrix}$$

#

Esercizi.

(1) Studiare la matrice $A = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

Si ha:

$$P_A(t) = \begin{vmatrix} 2-t & 0 & 1 \\ 1 & 1-t & 1 \\ 0 & 0 & 1-t \end{vmatrix} = (2-t)(1-t)^2 \#$$

$\Rightarrow$ autovalori
$$\lambda_1 = 1, \quad m_1 = 2$$
$$\lambda_2 = 2, \quad m_2 = 1$$

Autospazi:

$\underline{\lambda_1 = 1}$ $\quad AX = X \iff \begin{cases} 2x + z = x \\ x + y + z = y \\ z = z \end{cases} \iff \begin{cases} x + z = 0 \\ z = z \end{cases}$

$$\Rightarrow V_{\lambda_1} = \{(-z, y, z) \mid y, z \in \mathbb{R}\} =$$
$$= \{(-z, 0, z) + (0, y, 0) \mid y, z \in \mathbb{R}\} =$$
$$= \{z(-1, 0, 1) + y(0, 1, 0) \mid y, z \in \mathbb{R}\} =$$
$$= \langle (-1, 0, 1), (0, 1, 0) \rangle$$

$\underline{\lambda_2 = 2}$ $\quad AX = 2X \iff \begin{cases} 2x + z = 2x \\ x + y + z = 2y \\ z = 2z \end{cases} \iff \begin{cases} z = 0 \\ x - y = 0 \end{cases}$

$$\Rightarrow V_{\lambda_2} = \{(x, x, 0) \mid x \in \mathbb{R}\} = \langle (1, 1, 0) \rangle$$

La matrice è diagonalizzabile poiché la molteplicità degli autovalori coincide con la dimensione dei relativi autospazi.
Allora
$$\mathcal{B} = \{(-1, 0, 1), (0, 1, 0), (1, 1, 0)\}$$
è una base di autovettori di A per $\mathbb{R}^3$.

si ha subito

$$M^{\mathcal{B}}_{\mathcal{C}}(id) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ -1 & 0 & 0 \end{pmatrix},$$

calcoliamo la sua inversa:

$$(1,0,0) = 0(1,0,-1) - 1(0,1,0) + 1(1,1,0)$$
$$(0,1,0) = 0(1,0,-1) + 1(0,1,0) + 0(1,1,0)$$
$$(0,0,1) = -1(1,0,-1) - 1(0,1,0) + 1(1,1,0)$$

quindi

$$M^{\mathcal{C}}_{\mathcal{B}}(id) = \begin{pmatrix} 0 & 0 & -1 \\ -1 & 1 & -1 \\ 1 & 0 & 1 \end{pmatrix}.$$

E' inoltre evidente che $M_{\mathcal{B}}(L_A) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$.

In base al solito diagramma

$$\begin{tikzcd} \mathbb{R}^3_{\mathcal{B}} \arrow[r, "id"] \arrow[rrr, bend right, "L_A"'] & \mathbb{R}^3_{\mathcal{C}} \arrow[r, "L_A"] & \mathbb{R}^3_{\mathcal{C}} \arrow[r, "id"] & \mathbb{R}^3_{\mathcal{B}} \end{tikzcd}$$

si ottiene
$$M^{\mathcal{C}}_{\mathcal{B}}(id)\, A\, M^{\mathcal{B}}_{\mathcal{C}}(id) = M_{\mathcal{B}}(L_A),$$

infatti

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

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

(2) Studiare la matrice $A = \begin{pmatrix} 3 & 4 & 7 \\ -2 & -3 & -8 \\ 1 & 2 & 5 \end{pmatrix}$

Si ha

$$P_A(t) = \begin{vmatrix} 3-t & 4 & 7 \\ -2 & -3-t & -8 \\ 1 & 2 & 5-t \end{vmatrix} = -t^3+5t^2-8t+4$$

Poiché $t^3-5t^2+8t-4 = (t-1)(t-2)^2$
si ottengono gli autovalori

$$\lambda_1 = 1 \ , \ m_1 = 1$$

$$\lambda_2 = 2 \ , \ m_2 = 2$$

Gli autospazi:

$\underline{\lambda_1 = 1}$ $\quad AX = X \iff \begin{cases} 3x+4y+7z = x \\ -2x-3y-8z = y \\ x+2y+5z = z \end{cases} \iff \begin{cases} 2x+4y+7z=0 \\ 2x+4y+8z=0 \\ x+2y+4z=0 \end{cases}$

$\iff \begin{cases} z=0 \\ 2x+4y=0 \end{cases} \iff \begin{cases} z=0 \\ x=-2y \end{cases}$

$$\Rightarrow V_{\lambda_1} = \langle (-2,1,0) \rangle$$

$\underline{\lambda_2 = 2}$ $\quad AX = 2X \iff \begin{cases} 3x+4y+7z = 2x \\ -2x-3y-8z = 2y \\ x+2y+5z = 2z \end{cases} \iff \begin{cases} x+4y+7z = 0 \\ 2x+5y+8z = 0 \\ x+2y+3z = 0 \end{cases}$

$\iff \begin{cases} 2x+5y = -8z \\ x+2y = -3z \end{cases} \quad \Rightarrow \quad x = \dfrac{\begin{vmatrix} -8z & 5 \\ -3z & 2 \end{vmatrix}}{-1}, \ y = \dfrac{\begin{vmatrix} 2 & -8z \\ 1 & -3z \end{vmatrix}}{-1}$

$\Rightarrow \quad V_{\lambda_2} = \langle (1,-2,1) \rangle$

La matrice A non è diagonalizzabile. Si può però triangolare sul campo dei complessi. Consideriamo, ad es., il vettore $(1,0,0) \in \mathbb{C}^3$ per ottenere la base

$$\mathcal{B} = \{ (-2,1,0), (1,-2,1), (1,0,0) \}$$

di $\mathbb{C}^3$.

Si ha subito $M^{\mathcal{B}}_{\mathcal{E}}(id) = \begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, ed essendo

$$L_A(-2,1,0) = 1(-2,1,0)$$
$$L_A(1,-2,1) = 2(1,-2,1)$$
$$L_A(1,0,0) = (3,-2,1) = 0(-2,1,0) + 1(1,-2,1) + 2(1,0,0)$$

si ha

$$M_{\mathcal{B}}(L_A) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

Calcoliamo $M^{\mathcal{E}}_{\mathcal{B}}(id)$:

$$(1,0,0) = 0(2,-1,0) + 0(1,-2,1) + 1(1,0,0)$$
$$(0,1,0) = -1(2,-1,0) + 0(1,-2,1) + 2(1,0,0)$$
$$(0,0,1) = -2(2,-1,0) + 1(1,-2,1) + 3(1,0,0)$$

$$\Rightarrow \quad M^{\mathcal{E}}_{\mathcal{B}}(id) = \begin{pmatrix} 0 & -1 & -2 \\ 0 & 0 & 1 \\ 1 & 2 & 3 \end{pmatrix}$$

Si deve allora avere

$$M^{\mathcal{E}}_{\mathcal{B}}(id)\, A\, M^{\mathcal{B}}_{\mathcal{E}}(id) = M_{\mathcal{B}}(L_A)\,, \quad \text{cioè}$$

$$\begin{pmatrix} 0 & -1 & -2 \\ 0 & 0 & 1 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 3 & 4 & 7 \\ -2 & -3 & -8 \\ 1 & 2 & 5 \end{pmatrix} \begin{pmatrix} -2 & 1 & 1 \\ -1 & -2 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} \quad /\!/$$

(3) Studiare la matrice $A = \begin{pmatrix} 0 & 1 & -1 \\ -3 & 3 & -1 \\ -1 & 1 & 0 \end{pmatrix}$.

Si ha $p_A(t) = \begin{vmatrix} -t & 1 & -1 \\ -3 & 3-t & -1 \\ -1 & 1 & -t \end{vmatrix} = (t-1)^3$

$\lambda = 1, \quad m = 3$

$\underline{V_\lambda}$ $\quad AX = X \iff \begin{cases} y - z = x \\ -3x + 3y - z = y \\ -x + y = z \end{cases} \iff \begin{cases} x - y + z = 0 \\ 3x - 2y + z = 0 \\ x - y + z = 0 \end{cases}$

$\iff \begin{cases} x - y = -z \\ 3x - 2y = -z \end{cases} \qquad \Rightarrow V_\lambda = \langle (1,2,1) \rangle$

La matrice data si può triangolare sul campo dei complessi.
A partire dall'autovettore $(1,2,1)$ costruiamo una base di $\mathbb{C}^3$, ad es.

$$\mathcal{B} = \{(1,2,1), (1,0,0), (0,1,0)\}$$

Si ha $M_{\mathcal{E}}^{\mathcal{B}}(id) = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}$, poi essendo

$L_A(1,2,1) = 1(1,2,1) + 0(1,0,0) + 0(0,1,0)$
$L_A(1,0,0) = (0,-3,-1) = -1(1,2,1) + 1(1,0,0) - 1(0,1,0)$
$L_A(0,1,0) = (1,3,1) = 1(1,2,1) + 0(1,0,0) + 1(0,1,0)$

segue che

$$M_{\mathcal{B}}(L_A) = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} = B$$

Consideriamo la sottomatrice $B_{11} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$
la quale ha come autovalore $\lambda = 1$, $m = 2$.
Triangoliamo tale matrice.

$$B_{11} X = X \iff \begin{cases} x = x \\ -x+y = y \end{cases} \iff \begin{cases} x = 0 \\ \forall\, y \end{cases}$$

$$\Rightarrow V_1 = \langle (0,1) \rangle$$

Costruiamo la base di $\mathbb{C}^2$, $B' = \{(0,1),(1,1)\}$, quindi

$$M^{B'}_{\mathcal{C}}(id) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = U_1$$

Poniamo

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

e calcoliamo la sua inversa; si ha:

$$(1,0,0) = 1(1,0,0) + 0(0,0,1) + 0(0,1,1)$$
$$(0,1,0) = 0(1,0,0) - 1(0,0,1) + 1(0,1,1)$$
$$(0,0,1) = 0(1,0,0) + 1(0,0,1) + 0(0,1,1)$$

pertanto

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

Si ha

$$U^{-1} B U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} =$$

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

Dal fatto che

$$B = M^{\mathcal{C}}_{B}(id)\, A\, M^{B}_{\mathcal{C}}(id)$$

segue allora che

$$\left(U^{-1} M^{\mathcal{C}}_{B}(id)\right) A \left(M^{B}_{\mathcal{C}}(id)\, U\right) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

è triangolare superiore.

(4) Studiare la matrice $A=\begin{pmatrix} 1 & 0 & 3 \\ 0 & 3 & 0 \\ 3 & 0 & 1 \end{pmatrix}$.

La matrice è reale simmetrica, pertanto ha tre autovalori reali e si diagonalizza per mezzo di una matrice unitaria.
Si ha

$$P_A(t) = \begin{vmatrix} 1-t & 0 & 3 \\ 0 & 3-t & 0 \\ 3 & 0 & 1-t \end{vmatrix} = -t^3+5t^2+2t-24 =$$

$$= -(t+2)(t-3)(t-4)$$

Allora gli autovalori sono $\lambda_1=-2$, $\lambda_2=3$, $\lambda_3=4$
Gli autospazi

$\underline{\lambda_1=-2}$ $AX=-2X \iff \begin{cases} x+3z=-2x \\ 3y=-2y \\ 3x+z=-2z \end{cases} \iff \begin{cases} y=0 \\ x+z=0 \end{cases}$

$$\Rightarrow V_{\lambda_1} = \langle (1,0,-1) \rangle$$

$\underline{\lambda_2=3}$ $AX=3X \iff \begin{cases} x+3z=3x \\ 3y=3y \\ 3x+z=3z \end{cases} \iff \begin{cases} \forall y \\ 2x+3z=0 \\ 3x-2z=0 \end{cases}$

$$\Rightarrow V_{\lambda_2} = \langle (0,1,0) \rangle$$

$\underline{\lambda_3=4}$ $AX=4X \iff \begin{cases} x+3z=4x \\ 3y=4y \\ 3x+z=4z \end{cases} \iff \begin{cases} \forall y \\ x-z=0 \\ x-z=0 \end{cases}$

$$\Rightarrow V_{\lambda_3} = \langle (1,0,1) \rangle$$

$\Rightarrow$ base di autovettori $\{(1,0,-1),(0,1,0),(1,0,1)\}$

tale base è ortogonale, normalizziamola:

$$\mathcal{B} = \left\{ \left(1/\sqrt{2}, 0, -1/\sqrt{2}\right), (0, 1, 0), \left(1/\sqrt{2}, 0, 1/\sqrt{2}\right) \right\}$$

Allora la matrice

$$M^{\mathcal{B}}_{\mathcal{C}}(id) = \begin{pmatrix} 1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 0 & 1 & 0 \\ -1/\sqrt{2} & 0 & 1/\sqrt{2} \end{pmatrix}$$

è unitaria e la sua inversa coincide con la sua trasposta. Si ha infine

$$M^{\mathcal{C}}_{\mathcal{B}}(id)\, A\, M^{\mathcal{B}}_{\mathcal{C}} = \begin{pmatrix} 1/\sqrt{2} & 0 & -1/\sqrt{2} \\ 0 & 1 & 0 \\ 1/\sqrt{2} & 0 & 1/\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} 1 & 3 & 0 \\ 0 & 3 & 0 \\ 3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 0 & 1 & 0 \\ -1/\sqrt{2} & 0 & 1/\sqrt{2} \end{pmatrix}$$

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

(5) Ortonormalizzare la base di $\mathbb{C}^3$

$$B = \{(0,1,-1),(1,0,i),(1,i,0)\}$$

Posto $v_1=(0,1,-1)$, $v_2=(1,0,i)$, $v_3=(1,i,0)$, si ha

$$w_1 = v_1$$

$$w_2 = v_2 - \frac{v_2 \cdot w_1}{w_1 \cdot w_1} w_1 = (1,0,i) - \frac{(1,0,i)\cdot(0,1,-1)}{(0,1,-1)\cdot(0,1,-1)}(0,1,-1) =$$

$$= (1,0,i) - \frac{-i}{2}(0,1,-1) = (1, i/2, i/2)$$

$$w_3 = v_3 - \frac{v_3 \cdot w_1}{w_1 \cdot w_1} w_1 - \frac{v_3 \cdot w_2}{w_2 \cdot w_2} w_2 =$$

$$= (1,i,0) - \frac{i}{2}(0,1,-1) - \frac{(1,i,0)\cdot(1,i/2,i/2)}{(1,i/2,i/2)\cdot(1,i/2,i/2)}(1,i/2,i/2) =$$

$$= (1,i,0) - (0,i/2,-i/2) - (4/3, 2/3\, i, 2/3\, i) =$$

$$= (-1/3, -1/6\, i, -1/6\, i)$$

$$\Rightarrow \{w_1, w_2, w_3\} \text{ base ortogonale}$$

$$\|w_1\| = \sqrt{2}$$

$$\|w_2\| = \sqrt{(1, i/2, i/2)\cdot(1, i/2, i/2)} = \sqrt{3/2}$$

$$\|w_3\| = \sqrt{(-1/3, -1/6\, i, -1/6\, i)\cdot(-1/3, -1/6\, i, -1/6\, i)} = \sqrt{1/6}$$

$$\Rightarrow \left\{ \frac{w_1}{\|w_1\|}, \frac{w_2}{\|w_2\|}, \frac{w_3}{\|w_3\|} \right\}$$

la base ortonormalizzata.

Siano V, W spazi vettoriali sul campo K

DEF. Una funzione $f : V \times W \to K$ si dice una applicazione bilineare se verifica le seguenti richieste:

(1) $f(v+v', w) = f(v, w) + f(v', w)$ $\quad \forall\, v, v' \in V$

(2) $f(v, w+w') = f(v, w) + f(v, w')$ $\quad \forall\, w, w' \in W$

(3) $f(\alpha v, w) = \alpha f(v, w) = f(v, \alpha w)$ $\quad \forall\, \alpha \in K$

Notiamo che, se $f, g : V \times W \to K$ sono applicazioni bilineari e definiamo

$$(f+g)(v, w) = f(v, w) + g(v, w)\ ,\ (\alpha f)(v, w) = \alpha f(v, w)$$

allora le applicazioni

$$f+g : V \times W \to K \quad e \quad \alpha f : V \times W \to K$$

sono ancora bilineari. Questo ci permettere di dire che l'insieme $\mathcal{B}(V \times W, K)$ di tutte le applicazioni bilineari $V \times W \to V$ è a sua volta uno spazio vettoriale su K.

In seguito scriveremo $\mathcal{B}(V, K) = \mathcal{B}(V \times V, K)$ ed i suoi elementi si dicono forme bilineari su V

Esempi:

(1) ogni prodotto scalare su V è una forma bilineare
(scrivere $f(v, w) = v \cdot w$ ...)

(2) Se $A \in M_n(K)$, essa definisce una forma bilineare su K^n
$$f_A : K^n \times K^n \to K^n$$

definita ponendo
$$f(X,Y) = X^t A Y$$
per $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in K^n$.

Verifichiamo solo la prima proprietà, le altre si verificano in modo analogo.
$$f(X+X', Y) = (X+X')^t A Y = (X^t + X'^t) A Y =$$
$$= X^t A Y + X'^t A Y = f(X,Y) + f(X',Y).$$

Sia poi $\dim_K V = n$ e $\mathcal{B} = \{v_1, \dots, v_n\}$ è una base di V. Se $f \in \mathcal{B}(V, K)$, e
$$v = a_1 v_1 + \dots + a_n v_n, \quad w = b_1 v_1 + \dots + b_n v_n$$
si ha
$$f(v,w) = f(a_1 v_1 + \dots + a_n v_n, b_1 v_1 + \dots + b_n v_n) =$$
$$= a_1 b_1 f(v_1, v_1) + a_1 b_2 f(v_1, v_2) + \dots + a_n b_n f(v_n, v_n) =$$
$$= \sum_{i,j=1}^{n} a_i b_j f(v_i, v_j).$$

Poniamo $M_{\mathcal{B}}(f) = (f(v_i, v_j))$ essere la matrice della forma bilineare f.

Si ottiene poi
$$f(v,w) = v_{\mathcal{B}}^t M_{\mathcal{B}}(f) w_{\mathcal{B}} =$$
$$= (a_1, \dots, a_n) \begin{pmatrix} f(v_1,v_1) & \cdots & f(v_1,v_n) \\ \vdots & & \\ f(v_n,v_1) & \cdots & f(v_n,v_n) \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

TEOR La corrispondenza $f \mapsto M_B(f)$ definisce un isomorfismo

$$\Phi : \mathcal{B}(V,K) \longrightarrow \mathcal{M}_n(K).$$

DIM

(1) Φ è lineare, cioè $\begin{cases} \Phi(f+g) = \Phi(f)+\Phi(g) \\ \Phi(\alpha f) = \alpha\, \Phi(f) \end{cases}$

Si ha:

$$\begin{aligned} \Phi(f+g) &= M_B(f+g) = \big((f+g)(v_i, v_j)\big) = \\ &= \big(f(v_i,v_j) + g(v_i,v_j)\big) = \\ &= \big(f(v_i,v_j)\big) + \big(g(v_i,v_j)\big) = \\ &= M_B(f) + M_B(g) = \Phi(f) + \Phi(g). \end{aligned}$$

Analogamente per la seconda proprietà.

(2) Φ è iniettiva. Sia $f \in \mathcal{B}(V,K)$ tale che $\Phi(f) = \overline{O}$ (matrice nulla).

Allora $f(v_i, v_j) = 0$, $\forall\, i,j = 1,\dots,n$, pertanto $f(v,w) = 0$, $\forall\, v,w \in V$, cioè f è la forma bilineare nulla.

(3) Φ è suriettiva. Sia $A = (a_{ij}) \in \mathcal{M}_n(K)$ e sia $f_A : V \times V \longrightarrow K$ definita da

$$f_A(v,w) = v_B^{\,t} A\, w_B.$$

Allora f è bilineare e $M_B(f_A) = A$ #

COROLL. $\dim \mathcal{B}(V,K) = n^2$.

Siano V, W spazi vettoriali sul campo K

<u>DEF.</u> Una funzione $f: V \times W \to K$ si dice una applicazione <u>bilineare</u> se verifica le seguenti richieste:

(1) $f(v+v', w) = f(v,w) + f(v',w) \quad \forall\, v,v' \in V$

(2) $f(v, w+w') = f(v,w) + f(v,w') \quad \forall\, w,w' \in W$

(3) $f(\alpha v, w) = \alpha f(v,w) = f(v, \alpha w) \quad \forall\, \alpha \in K$

Notiamo che, se $f, g: V \times W \to K$ sono applicazioni bilineari e definiamo

$$(f+g)(v,w) = f(v,w) + g(v,w), \quad (\alpha f)(v,w) = \alpha f(v,w)$$

allora le applicazioni

$$f+g: V \times W \to K \quad e \quad \alpha f: V \times W \to K$$

sono ancora bilineari. Questo ci permette di dire che l'insieme $\mathcal{B}(V \times W, K)$ di tutte le applicazioni bilineari $V \times W \to V$ è a sua volta uno spazio vettoriale su K.

In seguito scriveremo $\mathcal{B}(V,K) = \mathcal{B}(V \times V, K)$ ed i suoi elementi si dicono <u>forme bilineari</u> su V

Esempi:

(1) ogni prodotto scalare su V è una forma bilineare
(scrivere $f(v,w) = v \cdot w$ ...)

(2) Se $A \in M_n(K)$, essa definisce una forma bilineare su K^n

$$f_A: K^n \times K^n \to K$$

definita ponendo

$$f_A(X,Y) = X^t A Y$$

per $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in K^n$.

Verifichiamo solo la prima proprietà, le altre si verificano in modo analogo.

$$f(X+X', Y) = (X+X')^t A Y = (X^t + X'^t) A Y =$$

$$= X^t A Y + X'^t A Y = f(X,Y) + f(X', Y).$$

Sia poi $\dim_K V = n$ e $B = \{v_1, \dots, v_n\}$ una base di V. Se $f \in B(V, K)$, e

$$v = a_1 v_1 + \dots + a_n v_n \quad , \quad w = b_1 v_1 + \dots + b_n v_n$$

si ha

$$f(v, w) = f(a_1 v_1 + \dots + a_n v_n, b_1 v_1 + \dots + b_n v_n) =$$

$$= a_1 b_1 f(v_1, v_1) + a_1 b_2 f(v_1, v_2) + \dots + a_n b_n f(v_n, v_n) =$$

$$= \sum_{i,j=1}^{n} a_i b_j f(v_i, v_j).$$

Poniamo $M_B(f) = (f(v_i, v_j))$ essere la matrice della forma bilineare f.

Si ottiene poi

$$f(v, w) = v_B^t M_B(f) w_B =$$

$$= (a_1, \dots, a_n) \begin{pmatrix} f(v_1, v_1) & \cdots & f(v_1, v_n) \\ \vdots & & \\ f(v_n, v_1) & \cdots & f(v_n, v_n) \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

TEOR La corrispondenza $f \mapsto M_B(f)$ definisce un isomorfismo
$$\Phi: \mathcal{B}(V,K) \longrightarrow \mathcal{M}_n(K).$$

DIM
(1) Φ è lineare, cioè $\begin{cases} \Phi(f+g) = \Phi(f)+\Phi(g) \\ \Phi(\alpha f) = \alpha\,\Phi(f) \end{cases}$

Si ha:
$$\Phi(f+g) = M_B(f+g) = \big((f+g)(v_i,v_j)\big) =$$
$$= \big(f(v_i,v_j) + g(v_i,v_j)\big) =$$
$$= \big(f(v_i,v_j)\big) + \big(g(v_i,v_j)\big) =$$
$$= M_B(f) + M_B(g) = \Phi(f)+\Phi(g).$$
Analogamente per la seconda proprietà.

(2) Φ è iniettiva. Sia $f \in \mathcal{B}(V,K)$ tale che $\Phi(f) = \bar{0}$ (matrice nulla).
Allora $f(v_i,v_j) = 0$, $\forall\, i,j = 1,\dots,n$, pertanto $f(v,w) = 0$, $\forall\, v,w \in V$, cioè f è la forma bilineare nulla.

(3) Φ è suriettiva. Sia $A = (a_{ij}) \in \mathcal{M}_n(K)$ e sia $f_A : V\times V \to K$ definita da
$$f_A(v,w) = v_B^t\, A\, w_B.$$
Allora f è bilineare e $M_B(f_A) = A$ #

COROLL. $\dim \mathcal{B}(V,K) = n^2$.

NOTA Sia $f \in \mathcal{B}(V, K)$ e siano $\mathcal{B}, \mathcal{B}'$ due basi di V.
Poniamo $A = M_{\mathcal{B}}(f)$ e $A' = M_{\mathcal{B}'}(f)$, $N = M^{\mathcal{B}}_{\mathcal{B}'}(id)$.
Allora risulta:

$$\boxed{A = N^t A' N}.$$

Infatti:
se $v, w \in V$, allora

$$f(v, w) = v_{\mathcal{B}}^t A w_{\mathcal{B}} = v_{\mathcal{B}'}^t A' w_{\mathcal{B}'}$$

e poiché

$$v_{\mathcal{B}'} = N v_{\mathcal{B}}, \quad w_{\mathcal{B}'} = N w_{\mathcal{B}}$$

segue

$$v_{\mathcal{B}}^t A w_{\mathcal{B}} = (N v_{\mathcal{B}})^t A (N w_{\mathcal{B}}) =$$
$$= v_{\mathcal{B}}^t (N^t A N) w_{\mathcal{B}}$$

$\forall v, w \in V$. Con il solito argomento basato su l'Osservazione pag. 54, si ottiene l'asserto. #

ESEMPIO (1) Sia $f: \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$ definita da

$$f(X, Y) = -2x_1y_1 + x_1y_2 + x_2y_3 + x_3y_1 - 3x_2y_2$$

e sia $\mathcal{B} = \{(1,1,0), (0,-1,0), (0,0,-1)\}$ una base di $\mathbb{R}^3$.
Se $\mathcal{C}$ è la base canonica, si ottiene

$$M_{\mathcal{C}}(f) = \begin{pmatrix} -2 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -3 & 0 \end{pmatrix}$$

Dalla Nota precedente si ha allora

$$M_{\mathcal{B}}(f) = (M^{\mathcal{B}}_{\mathcal{E}})^t M_{\mathcal{E}}(f) M^{\mathcal{B}}_{\mathcal{E}} ,$$

cioè

$$M_{\mathcal{B}}(f) = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} -2 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -3 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

(2) Determinare $f, g \in \mathcal{B}(V, K)$ tali che

$$M_{\mathcal{E}}(f) = A \quad , \quad M_{\mathcal{B}}(g) = A$$

essendo $\mathcal{B}$ come sopra e

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

* si ha $f(X,Y) = X_{\mathcal{E}}^t A Y_{\mathcal{E}} = (x_1, x_2, x_3) A \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} =$

$$= (x_1, x_2, x_3) \begin{pmatrix} y_1 - y_2 - y_3 \\ -y_2 \\ 2y_1 - 3y_2 \end{pmatrix} =$$

$$= x_1 y_1 - x_1 y_2 - x_1 y_3 - x_2 y_2 + 2x_3 y_1 - 3x_3 y_2$$

* calcoliamo $X_{\mathcal{B}}$:

da $(x_1, x_2, x_3) = \frac{x_1 + x_2}{2}(1,1,0) + \frac{x_1 - x_2}{2}(1,-1,0) + x_3(0,0,-1)$

si ottiene

$$g(X,Y) = X_{\mathcal{B}}^t A Y_{\mathcal{B}} = \left(\frac{x_1+x_2}{2}, \frac{x_1-x_2}{2}, x_3\right) A \begin{pmatrix} \frac{y_1+y_2}{2} \\ \frac{y_1-y_2}{2} \\ y_3 \end{pmatrix} = \dots$$

Def. Una forma bilineare $f : V \times V \to K$ si dice simmetrica se verifica

$$(4)\ f(v,w) = f(w,v),\ \forall v, w \in V.$$

Le forme bilineari simmetriche definite su V costituiscono un sottospazio

$$\mathcal{B}_s(V,K) < \mathcal{B}(V,K).$$

TEOR. Sia $\mathcal{B}$ una base di V e $f \in \mathcal{B}(V,K)$. Posto $A = M_{\mathcal{B}}(f)$, si ha

$$f \text{ è simmetrica} \iff A \text{ è simmetrica.}$$

DIM. Per $v, w \in V$ si ha:

$$f(v,w) = v_{\mathcal{B}}^t A w_{\mathcal{B}}, \quad f(w,v) = w_{\mathcal{B}}^t A v_{\mathcal{B}}$$

Poiché $w_{\mathcal{B}}^t A v_{\mathcal{B}} \in K$ risulta $w_{\mathcal{B}}^t A v_{\mathcal{B}} = (w_{\mathcal{B}}^t A v_{\mathcal{B}})^t$ da cui segue

$$f(w,v) = v_{\mathcal{B}}^t A^t w_{\mathcal{B}},$$

allora $f(v,w) = f(w,v) \iff v_{\mathcal{B}}^t A w_{\mathcal{B}} = v_{\mathcal{B}}^t A^t w_{\mathcal{B}}$.

Con le solite considerazioni si ottiene l'asserto. $\cancel{}$

(*) Le forme bilineari simmetriche su V sono esattamente i prodotti scalari definibili su V.

NOTE.

(1) Sia $f \in \mathcal{B}_s(\bar{V}, K)$ e sia $\mathcal{B}$ una base ortogonale di $\bar{V}$. Allora

$$A = M_{\mathcal{B}}(f)$$

è una matrice diagonale.
Qui l'ortogonalità si intende rispetto al prodotto scalare f. cioè $f(v_i, v_j) = 0, \forall i \neq j$.
Allora se

$$v_{\mathcal{B}}^t = (x_1, \dots, x_n) \quad e \quad w_{\mathcal{B}}^t = (y_1, \dots, y_n)$$

$$f(v, w) = v_{\mathcal{B}}^t A w_{\mathcal{B}} = \sum_{i=1}^{n} x_i y_i f(v_i, v_i)$$

In particolare se $\bar{V}$ è Euclideo risp. ad f, si ha

$$f(v, w) = \sum_{i=1}^{n} x_i y_i .$$

(2) Sia $f \in \mathcal{B}_s(\bar{V}, \mathbb{R})$ e $\mathcal{B}$ una base di $\bar{V}$ allora $A = M_{\mathcal{B}}(f)$ è reale simmetrica ed ha n autovalori reali $\lambda_1, \dots, \lambda_n$.
Allora esiste una base ortonormale di $\bar{V}$, $\mathcal{B}'$ tale che

$$M_{\mathcal{B}'}(f) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

In tal caso

$$f(v, w) = \lambda_1 x_1' y_1' + \dots + \lambda_n x_n' y_n'$$

ove l'apice denota coordinate su $\mathcal{B}'$.

DEF. Sia $f \in \mathcal{B}_s(V, K)$. Si dice forma quadratica associata ad f la funzione

$$q: V \to K \quad , \quad q(v) = f(v, v), \ \forall v \in V.$$

Nel caso si dice anche che f è la forma polare di q. (cfr. p.77)

NOTA Se q è una forma quadratica allora la sua forma polare si può ricavare come segue:

$$f(v, w) = \frac{1}{2}\left[q(v+w) - q(v) - q(w)\right].$$

Infatti:

$$\frac{1}{2}\left[q(v+w) - q(v) - q(w)\right] =$$

$$\frac{1}{2}\left[f(v+w, v+w) - f(v, v) - f(w, w)\right] =$$

$$\frac{1}{2}\left[f(v, v+w) + f(w, v+w) - f(v, v) - f(w, w)\right] =$$

$$\frac{1}{2}\left[\cancel{f(v, v)} + f(v, w) + \cancel{f(w, v)} + f(w, w) - \cancel{f(v, v)} - \cancel{f(w, w)}\right] =$$

$$= \frac{1}{2}\left[2 f(v, w)\right] = f(v, w).$$

Si osservi che nel caso della NOTA (2) precedente si ha

$$q(v) = v_{B'}^t M_{B'}(f) v_{B'} = \sum_{i=1}^{n} \lambda_i x_i^2 \quad \text{è}$$

la forma canonica di q.

Se B è una base di V poniamo

$$M_B(q) = M_B(f).$$

Riduzione a forma canonica di una forma quadratica

Da quanto visto nella pagina precedente e dalle NOTE di pag. 82 si ricava quanto segue.

(*) se V è uno spazio Euclideo e $q: V \to \mathbb{R}$ è una forma quadratica su V, allora esiste una base ortonormale di V rispetto alla quale q assume una forma canonica.

Illustriamo quanto detto con un

ESEMPIO. Sia $q: \mathbb{R}^3 \to \mathbb{R}$ definita da

$$q(X) = 2x_1x_2 + 2x_3^2 .$$

Qui $X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3$ e $Y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \in \mathbb{R}^3$.

(1) Calcoliamo la forma polare di q:

$$f(X,Y) = \frac{1}{2}\left[q(X+Y) - q(X) - q(Y)\right] =$$

$$\frac{1}{2}\left[2(x_1+y_1)(x_2+y_2) + 2(x_3+y_3)^2 - 2x_1x_2 - 2x_3^2 - 2y_1y_2 - 2y_3^2 \right] =$$

$$\frac{1}{2}\left[\cancel{2x_1x_2} + \cancel{2y_1y_2} + 2x_1y_2 + 2x_2y_2 + 2x_3^2 + 2y_3^2 + 4x_3y_3 - \cancel{2x_1x_2} - 2x_3^2 - \cancel{2y_1y_2} - 2y_3^2 \right] =$$

$$= x_1y_2 + x_2y_2 + 2x_3y_3$$

(2) Calcoliamo $A = M_{\mathcal{E}}(f)$

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

che è simmetrica (reale) come ci si aspettava.

(3) Autovalori ed autovettori di A.

$$p_A(t) = \begin{vmatrix} -t & 1 & 0 \\ 1 & -t & 0 \\ 0 & 0 & 2-t \end{vmatrix} = (2-t)(t^2-1)$$

$$\Rightarrow \lambda_1 = 2,\ m_1 = 1;\ \lambda_2 = 1,\ m_2 = 1$$
$$\lambda_3 = -1,\ m_3 = 1$$

$\underline{\lambda_1 = 2}$

$$AX = 2X \Longleftrightarrow \begin{cases} y = 2x \\ x = 2y \\ 2z = 2z \end{cases} \Longleftrightarrow x = y = 0,\ \forall z$$

$$\Rightarrow V_{\lambda_1} = \langle (0,0,1) \rangle$$

$\underline{\lambda_2 = 1}$ $$AX = X \Longleftrightarrow \begin{cases} y = x \\ x = y \\ 2z = z \end{cases} \Longleftrightarrow z = 0,\ x = y$$

$$\Rightarrow V_{\lambda_2} = \langle (1,1,0) \rangle$$

$\underline{\lambda_3 = -1}$ $$AX = -X \Longleftrightarrow \begin{cases} y = -x \\ x = -y \\ 2z = -z \end{cases} \Longleftrightarrow z = 0,\ y = -x$$

$$\Rightarrow V_{\lambda_3} = \langle (1,-1,0) \rangle$$

$\Rightarrow$ base di autovettori

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

(4) Ortonormalizziamo la base di autovettori. Poiché essa è già ortogonale, si ha

$$\mathcal{B} = \{ (0,0,1),\ (1/\sqrt{2}, 1/\sqrt{2}, 0),\ (1/\sqrt{2}, -1/\sqrt{2}, 0) \}$$

Si ha

$$M_{\mathcal{B}}(f) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

(3) Calcoliamo ~~...~~ $M^{\mathcal{B}}_{\mathcal{C}}(id)$

$$\Rightarrow \quad M^{\mathcal{B}}_{\mathcal{C}}(id) = \begin{pmatrix} 0 & 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 1/\sqrt{2} & -1/\sqrt{2} \\ 1 & 0 & 0 \end{pmatrix}$$

Allora se $X \in \mathbb{R}^3$ e denotiamo con

$$X_{\mathcal{C}} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \quad e \quad X_{\mathcal{B}} = \begin{pmatrix} x'_1 \\ x'_2 \\ x'_3 \end{pmatrix}$$

si deve avere

$$X_{\mathcal{C}} = M^{\mathcal{B}}_{\mathcal{C}}(id)\, X_{\mathcal{B}} \qquad \text{cioè}$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 & 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 1/\sqrt{2} & -1/\sqrt{2} \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x'_1 \\ x'_2 \\ x'_3 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2}\, x'_2 + 1/\sqrt{2}\, x'_3 \\ 1/\sqrt{2}\, x'_2 - 1/\sqrt{2}\, x'_3 \\ x'_1 \end{pmatrix}$$

$$\Leftrightarrow \begin{cases} x_1 = 1/\sqrt{2}\, x'_2 + 1/\sqrt{2}\, x'_3 \\ x_2 = 1/\sqrt{2}\, x'_2 - 1/\sqrt{2}\, x'_3 \\ x_3 = x'_1 \end{cases}$$

queste sono le equazioni del cambiamento di coordinate di un vettore $X \in \mathbb{R}^3$ quando si passa dalla base $\mathcal{B}$ a quella canonica.

(4) Infine da $q(X) = 2x_1x_2 + 2x_3^2$, per cambio di coordinate si ha:

$$q(X) = 2\left(\tfrac{1}{\sqrt{2}}x_2' + \tfrac{1}{\sqrt{2}}x_3'\right)\left(\tfrac{1}{\sqrt{2}}x_2' - \tfrac{1}{\sqrt{2}}x_3'\right) + 2x_1'^2 =$$

$$= 2\left(\tfrac{1}{2}x_2'^2 - \tfrac{1}{2}x_3'^2\right) + 2x_1'^2 =$$

$$= 2x_1'^2 + 1x_2'^2 - 1x_3'^2$$

la forma canonica di q.

DEFINIZIONI

(1) Se $f \in \mathcal{B}_s[V, K]$ si pone

$$\mathrm{Ker}\, f = \{ v \in V \mid f(v, w) = 0,\ \forall w \in V \}$$

Se poi $q : V \to K$ è la forma quadratica associata ad f si dice che q è

non degenere $:\Longleftrightarrow K(f) = \bar{0}$

(ovvero: il prodotto scalare f è non degenere)

(2) Se $f \in \mathcal{B}_s(V, \mathbb{R})$ si dice

- q definita positiva se $q(v) \geq 0\ \forall v \in V$ e $q(v) = 0 \Longleftrightarrow v = \bar{0}$
- q definita negativa se $q(v) \leq 0\ \forall v \in V$ e $q(v) = 0 \Longleftrightarrow v = \bar{0}$
- non definita: altrimenti

(3) Il discriminante di $f \in \mathcal{B}_s(V, K)$ e/o della forma quadratica associata q è

$$\mathrm{Det}(M_{\mathcal{B}}(f)) = \mathrm{Det}(M_{\mathcal{B}}(q))$$

essendo $\mathcal{B}$ una base di V.

Il discriminante si denota $\Delta f = \Delta q$

Teor. Sia $f \in B_s(V, K)$ e q la forma quadratica associata ad f.

$$q \text{ degenere} \Leftrightarrow \Delta q = 0$$

Dim. Sia $B = \{v_1, \dots, v_n\}$ una base di V e sia
$$v = a_1 v_1 + \dots + a_n v_n, \quad v \neq \bar{0}$$

Se $v \in \operatorname{Ker} f$ allora $f(v, w) = 0$, $\forall w \in V$, quindi anche
$$f(v, v_j) = 0, \; \forall j = 1, \dots, n$$

Questo si riscrive
$$0 = f\left(\sum a_i v_i, v_j\right) = \sum_{i=1}^{n} a_i f(v_i, v_j) =$$
$$= v_B{}^t A^j, \quad \forall j = 1, \dots n,$$
ove $A = M_B(f)$.

Segue che $v_B{}^t$ è una soluzione non nulla del sistema omogeneo $X^t A = \bar{0}$, e questo è possibile se e solo se $\operatorname{Det}(A) = 0$.

#

Nota: $X^t A = (X^t A^1, \dots, X^t A^n)$!

Teor. Siano f, q come sopra. Se q è definita positiva oppure negativa, allora q è non degenere.

Dim. q degenere $\Rightarrow \exists\, v \in V$, $v \neq \bar{0}$ tale che $f(v, w) = 0$, $\forall w \in V$. In particolare $f(v, v) = 0$

#

$\tau \in S_8$

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

$\tau = (2\,5\,3)(4\,8\,6\,7)$

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

$\tau^{-1} = (2\,3\,5)(4\,7\,6\,8)$

$\delta = (4\,3\,1)(2\,7\,5\,6)$

δ e τ sono coniugate perché hanno la stessa struttura in cicli disgiunti

$\Rightarrow \exists\, \alpha \in S_8$ tale che $\alpha^{-1} \tau \alpha = \delta$

$\delta = (8)(4\,3\,1)(2\,7\,5\,6)$

$\tau = (1)\ (2\,5\,3)(4\,8\,6\,7)$

α :
$8 \to 1$
$4 \to 2$
$3 \to 5$
$1 \to 3$
$2 \to 4$
$7 \to 8$
$5 \to 6$
$6 \to 7$

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

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

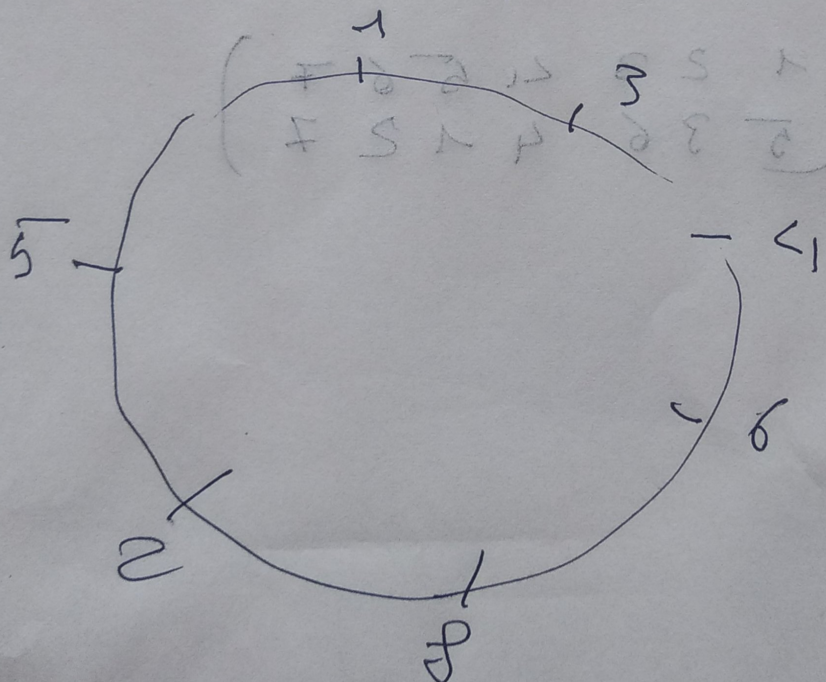
S_8 $\quad \alpha = (2\,5)$

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

$(2\,5)$

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

$$\tau = (1\,3\,4\,6\,8\,2\,5) = (6\,8\,2\,5\,1\,3\,4)$$



$(\mathbb{R}, +)$ gruppo additivo

$\mathbb{R}^+$ = reali positivi

$(\mathbb{R}^+, \cdot)$

$$\varphi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \cdot)$$
$$x \longmapsto e^x$$

$$x+y \longmapsto e^{x+y} = e^x \cdot e^y$$

$$\varphi(x+y) = \varphi(x)\varphi(y)$$

$$\log : (\mathbb{R}^+, \cdot) \longrightarrow (\mathbb{R}, +)$$
$$x \longmapsto \log x$$

$$\log(xy) = \log x + \log y$$

$\beta = (1\,5\,3) = (1\,3)(1\,5)$

$\alpha = (1\,7\,6)(2\,5)(4\,9\,8) =$

$= (1\,6)(1\,7)(2\,5)(4\,8)(4\,9)$

$\tau = (2\,3)(2\,5)(4\,7)(4\,6)(4\,8)$

$\tau = (3\,2\,5)(4\,1\,6)$

$\delta = (7\,8\,4)(1\,3\,5)$ $\in S_8$

$\exists\ \alpha \in S_8$ t.c $\alpha^{-1} \tau \alpha = \delta$

α?

$\tau \in S_8$

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

$\tau = (2\,5\,3)(4\,8\,6\,7)$

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

$\tau^{-1} = (2\,3\,5)(4\,7\,6\,8)$

$\delta = (4\,3\,1)(2\,7\,5\,6)$

δ e τ sono coniugate perché hanno la stessa struttura in cicli disgiunti

$\Rightarrow \exists\, \alpha \in S_8$ tale che $\alpha^{-1}\tau\alpha = \delta$

$\delta = (8)(4\,3\,1)(2\,7\,5\,6)$

$\tau = (1)\,(2\,5\,3)(4\,8\,6\,7)$

α:
$8 \to 1$
$4 \to 2$
$3 \to 5$
$1 \to 3$
$2 \to 4$
$7 \to 8$
$5 \to 6$
$6 \to 7$

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

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

$$\alpha^{-1}\tau\alpha = \begin{array}{l} \\ \\ \\ \\ \end{array}\left(\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 2 & 6 & 7 & 8 & 1 \\ 2 & 8 & 3 & 5 & 7 & 4 & 6 & 1 \\ 4 & 7 & 1 & 3 & 6 & 2 & 5 & 8 \end{array}\right)\begin{array}{l} \\ \longrightarrow \alpha \\ \longrightarrow \tau \\ \longrightarrow \tau^{-1} \end{array}$$

$$\Rightarrow \alpha^{-1}\tau\alpha = (1\,4\,3)(2\,7\,5\,6) = \sigma$$

<u>Nota</u>: $(1\,4\,3) = (3\,1\,4) = (4\,3\,1)$

11. CLASSI LATERALI

Sia G un gruppo e $H < G$ un sottogruppo.
H definisce una relazione di equivalenza in G ponendo, $\forall x, y \in G$

$$x \sim y \iff \exists h \in H : y = xh .$$

La classe di equivalenza di un elemento $x \in G$ si scrive:

$$\{ y \in G \mid y = xh , h \in H \} = xH$$

L'insieme xH prende il nome di LATERALE SINISTRO ~~di~~ H in G

Analogamente si definisce ~~un~~ laterale destra di H in G, della forma Hx'.
Nota che, in generale $xH \neq Hx$, poiché G non è necessariamente commutativo.
D'altra parte, anche nel caso che $xH = Hx$, questo significa che presa $xh \in xH$, esiste $h' \in H$ t.c. $xh = h'x$, e viceversa.

I laterali sinistri H in G, in quanto classi di equivalenza, determinano una partizione di G, cioè
1) laterali distinti sono disgiunti
2) ~~la~~ la loro unione dà G.

Stabiliu se $\langle \tau \rangle$ e normale in S_8

$$H \trianglelefteq G \iff \forall a \in G\ \forall h \in H,\ a^{-1} h a \in H$$

$$\langle \tau \rangle < S_8$$

$\alpha = (3\,6) \in S_8$ $\qquad \alpha^{-1} = (5\,6)$

$$\alpha^{-1} \tau \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 6 & 4 & 5 & 3 & 7 & 8 \\ 3 & 7 & 6 & 2 & 1 & 5 & 8 & 4 \\ 6 & 7 & 3 & 2 & 1 & 5 & 8 & 4 \end{pmatrix}$$

$$= (1\,6\,5)(2\,7\,8\,4) \notin \langle \tau \rangle$$

$\Rightarrow \langle \tau \rangle$ nu e normale

in S_8

$\tau^0 = id$

$\tau^1 = \tau$

$\tau^2 = (1\,3\,5)^2 (4\,2\,7\,8)^2 = (1\,5\,3)(4\,7)(2\,8)$

$\tau^3 = (1\,3\,5)^3 (4\,2\,7\,8)^3 = (2\,4\,8\,7)$

$\tau^4 = (1\,3\,5)^4 (4\,2\,7\,8)^4 = (1\,3\,5)$

$\tau^5 = (1\,3\,5)^5 (4\,2\,7\,8)^5 = (1\,5\,3)(4\,2\,7\,8)$

$\tau^6 = (1\,3\,5)^6 (4\,2\,7\,8)^6 = (4\,7)(2\,8)$

$\tau^7 = (1\,3\,5)^7 (2\,7\,8)^7 = (1\,3\,5)(2\,4\,8\,7)$

$\tau^8 = (1\,3\,5)^8 (4\,2\,7\,8)^8 = (1\,5\,3)$

$\tau^9 = (1\,3\,5)^9 (4\,2\,7\,8)^9 = (4\,2\,7\,8)$

$\tau^{10} = (1\,3\,5)^{10} (4\,2\,7\,8)^{10} = (1\,3\,5)(4\,7)(2\,8)$

$\tau^{11} = (1\,3\,5)^{11} (4\,2\,7\,8)^{11} = (1\,5\,3)(2\,4\,8\,7)$

$$\tau = (1\,3\,5)(4\,2\,7\,8) \qquad \tau \in S_8$$

$$o(\tau) = \mathrm{mcm}(3,4) = 12$$

$$\Rightarrow \quad o(\langle \tau \rangle) = 12$$

$$(1\,3\,5)^2 = (1\,5\,3)$$

$$(1\,3\,5)^3 = id$$

$$(4\,2\,7\,8)^2 = (4\,7)(2\,8) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 7 & 3 & 2 & 5 & 6 & 8 & 4 \\ 1 & 8 & 3 & 7 & 5 & 6 & 4 & 2 \end{pmatrix}$$

$$(4\,2\,7\,8)^3 = (4\,2\,7\,8)(4\,2\,7\,8)^2$$

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

$$(4\,2\,7\,8)^4 = id$$

$\tau = (135)(4678)$

<u>Esercizio</u>: calcolare $\langle \tau \rangle$

Sia $u \in D$ l'elemento unità

$\exists! x \in D$ t. c. $ax = u = xa$

In S_n l'ordine di una permutazione ciclica di lunghezza r è $\underline{\underline{r}}$.

$\tau = (1\,5)(4\,7\,2\,8)$

$\tau^4 = id$

$\tau = (1\,3\,5)(4\,2\,7\,8)$

$\tau^{12} = id$

$M \subset \mathcal{M}_{2\times 2}(K)$

M è un gruppo moltiplicativo abeliano

$\varphi : (K,+) \longrightarrow M$

$$\varphi(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

φ è biiettiva

1) $\varphi(a) = \varphi(b) \Longrightarrow \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$

$\Longrightarrow a = b$

2) è suriettiva

3) ~~[illegible]~~ omomorfismo

$$\varphi(a+b) = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

$\Rightarrow \varphi(a) \cdot \varphi(b)$

$= e_G$

$= b_K$

$\partial_a(y)$

$a =$

$a\, a^{-1} y)\, a$

$)\, (a^{-1} y$

$a(y)$

$a' \in aH \Rightarrow a' = a h \qquad h \in H$

$b' \in bH \Rightarrow b' = b k \qquad k \in H$

$a'b = a h b k$

$\delta_a(xy) = \delta_a(x) \cdot \delta_a(y)$

$\delta_a(xy) = a^{-1}(xy)a =$

$= a^{-1}(x a a^{-1} y) a =$

$= (a^{-1} x a)(a^{-1} y a)$

$= \delta_a(x)\, \delta_a(y)$

---

iniettivo $\delta_a(x) = \delta_a(y) \Rightarrow x = y$

$a^{-1} x a = a^{-1} y a \Rightarrow x = y$

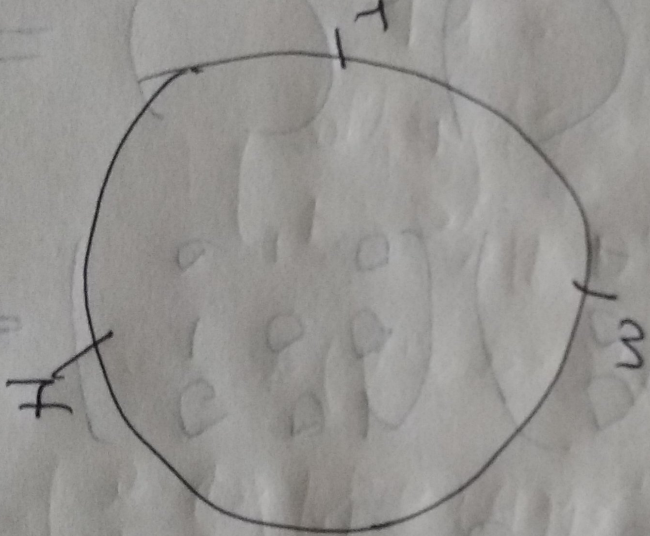
Se $z \in G \Rightarrow z = \delta_a(a z a^{-1})$

infatti $\delta_a(a z a^{-1}) = a^{-1} a z a^{-1} a = z$

$S_n \ni \tau \qquad \tau^k = id$

$\tau \in S_8$

$\tau = (1, 3, 7)$



$\tau^2 = (1\,7\,3)$

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

$= id$

(1)

$$\mathbb{Z}_p = \{[0], [1], \dots, [p-1]\}$$

$$\mathbb{Z}_p = \{0, 1, \dots, p-1\}$$

$$\mathbb{Z}_7 = \{0, 1, 2, \dots, 6\}$$

$$4 + 5 = 2$$

$$4 \cdot 5 = 6$$

p primo , $n > 0$

$$(\mathbb{Z}_p)^n = \mathbb{Z}_p \times \underbrace{\mathbb{Z}_p \times \cdots \times}_{n\text{-volte}} \mathbb{Z}_p$$

$\alpha \in (\mathbb{Z}_p)^n \quad \alpha = (a_0, a_1, \dots, a_{n-1})$

con $a_0, \dots, a_{n-1} \in \mathbb{Z}_p$

① Addizione

$$(a_0, \dots, a_{n-1}) + (b_0, \dots, b_{n-1}) =$$

$$\left(\overline{a_0 + b_0}, \dots, \overline{a_{n-1} + b_{n-1}}\right)$$

Es. $(\mathbb{Z}_3)^4$

$$(1, 0, 2, 1) + (2, 2, 2, 1) =$$

$$\left(\overline{1+2}, \overline{0+2}, \overline{2+2}, \overline{1+1}\right) =$$

$$= (0, 2, 1, 2)$$

$((\mathbb{Z}_p)^n, +)$

$\boxed{\begin{array}{l}\forall p \text{ primo}, \forall n>0 \\ \exists\, d(t) \in \mathbb{Z}_p[t] \\ \text{di grado } n, \text{ irriducibile}\end{array}}$

② Moltiplicazione:

$$(a_0, \dots, a_{n-1}), (b_0, \dots, b_{n-1}) \in (\mathbb{Z}_p)^n$$

$$f(t) = a_0 + a_1 t + \dots + a_{n-1} t^{n-1} \in \mathbb{Z}_p[t]$$

$$g(t) = b_0 + b_1 t + \dots + b_{n-1} t^{n-1} \in \mathbb{Z}_p[t]$$

$$\begin{array}{c|c} f(t) \cdot g(t) & d(t) \\ \hline r(t) & q(t) \end{array}$$

$$\Rightarrow \quad f(t) \cdot g(t) = q(t) \cdot d(t) + r(t)$$

$$0 \leq \deg r(t) < n$$

$$\Rightarrow \quad r(t) = c_0 + c_1 t + \dots + c_{n-1} t^{n-1}$$

Def $(a_0, \dots, a_{n-1}) \cdot (b_0, \dots, b_{n-1}) =$

$$= (c_0, \dots, c_{n-1})$$

$$(\mathbb{Z}_3)^3 = GF(3^3)$$

$(1,0,1) \longrightarrow 1+t^2 \qquad f(t)$

$(2,1,2) \longrightarrow 2+t+2t^2 \qquad g(t)$

$f(t)\cdot g(t) = (1+t^2)(2+t+2t^2) =$

$= 2+t+2t^2+2t^2+t^3+2t^4 =$

$= 2+t+4t^2+t^3+2t^4$

$= 2+t+t^2+t^3+2t^4$

$J(t) = 2+2t+t^3$

$$\begin{array}{l|l} 2t^4+t^3+t^2+t+2 & t^3+2t+2 \\ \hline 2t^4 \quad +4t^2+4t & 2t+1 \\ \hline t^3 - \cancel{3t^2} - \cancel{3t} + 2 & \\ t^3 \qquad\qquad +2 & \\ t^3 \quad +2t \quad \cancel{+2} & \\ \hline -2t = t & \end{array}$$

$r(t) = t \longrightarrow (0,1,0)$

$\Rightarrow (1,0,1)\cdot(2,1,2) = (0,1,0)$

$\mathbb{Z}_5 = GF(5^1)$

F, u unità

$\{ hu \mid \forall h \in \mathbb{Z} \}$

! $hu = \underbrace{u + u + \dots + u}_{h\text{-volte}}$

non sono tutti distinti

$(h \cdot k)u = (hu)(ku)$, $h, k \in \mathbb{N}$

$k = 1$ $(h1)u = (hu) = (hu)(1u)$

Vera per k

$[h(k+1)]u = (hk + h)u =$

$= (hk)u + hu =$

$= (hu)(ku) + hu =$

$= hu(ku + u) =$

$= (hu)[(k+1)u]$ #

CLASSI LATERALI

Sia G un gruppo e $H<G$ un sottogruppo.
H definisce una relazione di equivalenza in G ponendo, $\forall x, y \in G$

$$x \sim y \iff \exists h \in H : y = xh .$$

La classe di equivalenza di un elemento $x \in G$ si scrive:

$$\{ y \in G \mid y = xh ,\ h \in H \} = xH$$

L'insieme xH prende il nome di LATERALE SINISTRO ~~di~~ H in G

Analogamente si definisce ~~la~~ laterale destra di H in G, della forma Hx.
Nota che, in generale $xH \neq Hx$, perché G non è necessariamente commutativo.
D'altra parte, anche nel caso che $xH = Hx$, questo significa che presa $xh \in xH$, esiste $h' \in H$ t.c. $xh = h'x$, e viceversa.

I laterali sinistri di H in G, in quanto classi di equivalenza, determinano una partizione di G, cioè

1) laterali distinti sono disgiunti
2) la loro unione dà G.

$\tau = (7)(8)(3\,2\,5)(4\,1\,6)$

$\delta = (2)(6)(7\,8\,4)(1\,3\,5)$

$7 \to 2$
$8 \to 6$
$3 \to 7$
$2 \to 8$
$5 \to 4$
$4 \to 1$
$1 \to 3$
$6 \to 5$

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

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

$$\alpha^{-1}\delta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 7 & 1 & 4 & 5 & 2 & 6 \\ 5 & 4 & 8 & 3 & 7 & 1 & 2 & 6 \\ 6 & 5 & 2 & 1 & 3 & 4 & 7 & 8 \end{pmatrix} =$$

$$= (1\,6\,4)(2\,5\,3) = \tau$$

! $(1\,6\,4) = (4\,1\,6)$, $(2\,5\,3) = (3\,2\,5)$

Naturalmente anche

$$\delta = (\alpha^{-1})^{-1}\,\tau\,\alpha^{-1}.$$

11. CLASSI LATERALI

Sia G un gruppo e $H < G$ un sottogruppo. H definisce una relazione di equivalenza in G ponendo, $\forall x, y \in G$

$$x \sim y \iff \exists h \in H : y = xh .$$

La classe di equivalenza di un elemento $x \in G$ si scrive:

$$\{ y \in G \mid y = xh, \, h \in H \} = xH$$

L'insieme xH prende il nome di LATERALE SINISTRO ~~di~~ H in G

Analogamente si definisce ~~un~~ laterale destra di H in G, della forma Hx'.

Nota che, in generale $xH \neq Hx$, poiché G non è necessariamente commutativo.

D'altra parte, anche nel caso che $xH = Hx$, questo significa che presa $xh \in xH$, esiste $h' \in H$ t.c. $xh = h'x$, e viceversa.

I laterali sinistri H in G, in quanto classi di equivalenza, determinano una partizione di G, cioè

1) laterali distinti sono disgiunti

2) ~~la~~ loro unione dà G.

Stabiliți dacă $\langle \tau \rangle$ e normală în S_8

$$H \trianglelefteq G \iff \forall a \in G\ \forall h \in H,\ a^{-1} h a \in H$$

$$\langle \tau \rangle < S_8$$

$\alpha = (3\,6) \in S_8 \qquad \alpha^{-1} = (5\,6)$

$$\alpha^{-1} \tau \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 6 & 4 & 5 & 3 & 7 & 8 \\ 3 & 7 & 6 & 2 & 1 & 5 & 8 & 4 \\ 6 & 7 & 3 & 2 & 1 & 5 & 8 & 4 \end{pmatrix}$$

$$= (1\,6\,5)(2\,7\,8\,4) \notin \langle \tau \rangle$$

$\Rightarrow \langle \tau \rangle$ nu e normală în S_8

$\tau^0 = id$

$\tau^1 = \tau$

$\tau^2 = (1\,3\,5)^2 (4\,2\,7\,8)^2 = (1\,5\,3)(4\,7)(2\,8)$

$\tau^3 = (1\,3\,5)^3 (4\,2\,7\,8)^3 = (2\,4\,8\,7)$

$\tau^4 = (1\,3\,5)^4 (4\,2\,7\,8)^4 = (1\,3\,5)$

$\tau^5 = (1\,3\,5)^5 (4\,2\,7\,8)^5 = (1\,5\,3)(4\,2\,7\,8)$

$\tau^6 = (1\,3\,5)^6 (4\,2\,7\,8)^6 = (4\,7)(2\,8)$

$\tau^7 = (1\,3\,5)^7 (2\,7\,8)^7 = (1\,3\,5)(2\,4\,8\,7)$

$\tau^8 = (1\,3\,5)^8 (4\,2\,7\,8)^8 = (1\,5\,3)$

$\tau^9 = (1\,3\,5)^9 (4\,2\,7\,8)^9 = (4\,2\,7\,8)$

$\tau^{10} = (1\,3\,5)^{10} (4\,2\,7\,8)^{10} = (1\,3\,5)(4\,7)(2\,8)$

$\tau^{11} = (1\,3\,5)^{11} (4\,2\,7\,8)^{11} = (1\,5\,3)(2\,4\,8\,7)$

$\tau = (1\,3\,5)(4\,2\,7\,8) \quad \tau \in S_8$

$o(\tau) = \text{mcm}(3,4) = 12$

$\Rightarrow \quad o(\langle \tau \rangle) = 12$

$(1\,3\,5)^2 = (1\,5\,3)$

$(1\,3\,5)^3 = id$

$(4\,2\,7\,8)^2 = (4\,7)(2\,8) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 7 & 3 & 2 & 5 & 6 & 8 & 4 \\ 1 & 8 & 3 & 7 & 5 & 6 & 4 & 2 \end{pmatrix}$

$(4\,2\,7\,8)^3 = (4\,2\,7\,8)(4\,2\,7\,8)^2$

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

$(4\,2\,7\,8)^4 = id$

$\tau = (135)(4678)$

<u>Esercizio</u>: calcolare $\langle \tau \rangle$

Sia $u \in D$ l'elemento unità

$\exists! x \in D$ t. c. $ax = u = xa$

In S_n l'ordine di una permutazione ciclica di lunghezza r è $\underline{\underline{r}}$.

$\tau = (1\,5)(4\,7\,2\,8)$

$\tau^4 = id$

$\tau = (1\,3\,5)(4\,2\,7\,8)$

$\tau^{12} = id$

$M \subset \mathcal{M}_{2\times 2}(K)$

M è un gruppo moltiplicativo abeliano

$$\varphi : (K,+) \longrightarrow M$$

$$\varphi(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

φ è biettiva

1) $\varphi(a) = \varphi(b) \Longrightarrow \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$

$\Longrightarrow a = b$

2) è suriettiva

3) omomorfismo

$$\varphi(a+b) = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

$$= \varphi(a) \cdot \varphi(b)$$

$= aG$

$= bK$

$\lambda_a(y)$

$a \quad =$

$a a^{-1} y) a$

$) (a^{-1} y$

$\lambda_a(y)$

$a' \in aH \Rightarrow a' = a h \qquad h \in H$

$b' \in bH \Rightarrow b' = b k \qquad k \in H$

$a'b' = a h b k$

$\delta_a(xy) = \delta_a(x) \cdot \delta_a(y)$

$$\delta_a(xy) = a^{-1}(xy)a =$$

$$= a^{-1}(x a a^{-1} y) a =$$

$$= (a^{-1} x a)(a^{-1} y a)$$

$$= \delta_a(x)\, \delta_a(y)$$

---

iniettivo $\delta_a(x) = \delta_a(y) \Longrightarrow x = y$

$\cancel{a^{-1} x a\, a^{-1} y a \Rightarrow}$

$a^{-1} x a = a^{-1} y a \Longrightarrow x = y$

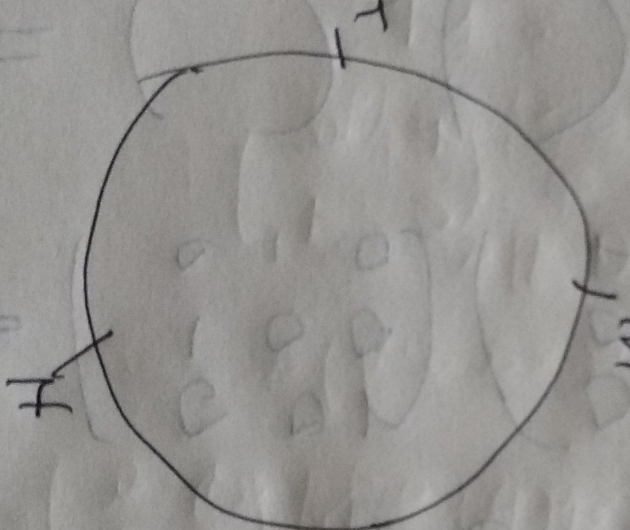
Se $z \in G \Rightarrow z = \delta_a(a z a^{-1})$

infatti $\delta_a(a z a^{-1}) = a^{-1} a z a^{-1} a = z$

$S_n \ni \tau \qquad \tau^k = id$

$\tau \in S_8$

$\tau = (1, 3, 7)$



$\tau^2 = (1\ 7\ 3)$

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

$= id$

①

$$\mathbb{Z}_p = \{[0], [1], \dots, [p-1]\}$$

$$\mathbb{Z}_p = \{0, 1, \dots, p-1\}$$

$$\mathbb{Z}_7 = \{0, 1, 2, \dots, 6\}$$

$$4 + 5 = 2$$
$$4 \cdot 5 = 6$$

p primo, $n > 0$

$$(\mathbb{Z}_p)^n = \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n\text{-volte}}$$

$\alpha \in (\mathbb{Z}_p)^n \quad \alpha = (a_0, a_1, \dots, a_{n-1})$

con $a_0, \dots, a_{n-1} \in \mathbb{Z}_p$

① Addizione

$$(a_0, \dots, a_{n-1}) + (b_0, \dots, b_{n-1}) =$$

$$\left(\overline{a_0 + b_0}, \dots, \overline{a_{n-1} + b_{n-1}}\right)$$

Es. $(\mathbb{Z}_3)^4$

$$(1, 0, 2, 1) + (2, 2, 2, 1) =$$

$$\left(\overline{1+2}, \overline{0+2}, \overline{2+2}, \overline{1+1}\right) =$$

$$= (0, 2, 1, 2)$$

$$((\mathbb{Z}_p)^n, +)$$

$\boxed{\text{$\forall p$ primo, $\forall n>0$ $\exists\, d(t) \in \mathbb{Z}_p[t]$ di grado n, irriducibile}}$

② Moltiplicazione:

$$(a_0, \dots, a_{n-1}), (b_0, \dots, b_{n-1}) \in (\mathbb{Z}_p)^n$$

$$f(t) = a_0 + a_1 t + \dots + a_{n-1} t^{n-1} \in \mathbb{Z}_p[t]$$

$$g(t) = b_0 + b_1 t + \dots + b_{n-1} t^{n-1} \in \mathbb{Z}_p[t]$$

$$\begin{array}{l|l} f(t)\cdot g(t) & d(t) \\ \hline r(t) & q(t) \end{array}$$

$$\Rightarrow \quad f(t)\cdot g(t) = q(t)\cdot d(t) + r(t)$$

$$0 \le \deg r(t) < n$$

$$\Rightarrow \quad r(t) = c_0 + c_1 t + \dots + c_{n-1} t^{n-1}$$

Def $(a_0, \dots, a_{n-1}) \cdot (b_0, \dots, b_{n-1}) =$

$$= (c_0, \dots, c_{n-1})$$

$$(\mathbb{Z}_3)^3 = GF(3^3)$$

$(1,0,1) \longrightarrow 1 + t^2 \qquad f(t)$

$(2,1,2) \longrightarrow 2 + t + 2t^2 \qquad g(t)$

$$f(t)\cdot g(t) = (1+t^2)(2+t+2t^2) =$$

$$= 2+t+2t^2+2t^2+t^3+2t^4 =$$

$$= 2+t+4t^2+t^3+2t^4$$

$$= 2+t+t^2+t^3+2t^4$$

$$J(t) = 2+2t+t^3$$

$$
\begin{array}{l|l}
2t^4 + t^3 + t^2 + t + 2 & t^3+2t+2 \\
\underline{2t^4 \qquad\quad + 4t^2 + 4t} & 2t+1 \\
\qquad t^3 - \cancel{3}t^2 - \cancel{3}t + 2 & \\
\qquad t^3 \qquad\qquad\quad + 2 & \\
\qquad \underline{t^3 \quad + 2t \quad \cancel{+2}} & \\
\qquad\qquad -2t = t &
\end{array}
$$

$r(t) = t \longrightarrow (0,1,0)$

$$\Rightarrow (1,0,1)\cdot(2,1,2) = (0,1,0)$$

$\mathbb{Z}_5 = GF(5^1)$

F, u unità

$\{ h u \mid \forall h \in \mathbb{Z} \}$

! $h u = \underbrace{u + u + \dots + u}_{h\text{-volte}}$

non sono tutti distinti

$(h \cdot k) u = (h u)(k u)$, $h, k \in \mathbb{N}$

$k = 1$ $(h 1) u = (h u) = (h u)(1 u)$

Vero per k

$[h(k+1)] u = (h k + h) u =$

$= (h k) u + h u =$

$= (h u)(k u) + h u =$

$= h u (k u + u) =$

$= (h u)[(k+1) u]$ #

(1)

$GF(3^4)$, $\nu(t) = t^4+t^2+2$

$(1,2,0,1) \sim 1+2t+t^3$

$(2,2,1,1) \sim 2+2t+t^2+t^3$

$(1+2t+t^3)(2+2t+t^2+t^3) =$

$$
\begin{array}{l|l}
= t^6+t^5+t^4+2t^3+2t^2+2 & t^4+t^2+2 \\ \hline
t^6 \quad\; +t^4 \quad\;\; +2t^2 & t^2+t \\ \cline{1-1}
\quad t^5 \;\; +2t^3 \quad\; +2 & \\
\quad t^5 \;\; +t^3 \;\; +2t & \\ \cline{1-1}
\qquad\quad t^3 \;\; +t+2 &
\end{array}
$$

$\Rightarrow (1,2,0,1)\cdot(2,2,1,1) = (2,1,0,1)$

$\# GF(3^4) = 81 \Rightarrow \# GF(3^4)^* = 80$

$\alpha \in GF(3^4)^*$, $\alpha = (1,0,1,0)$

$o(\alpha) = 2, 4, 8, 5, 10, 20, 40, 80$

$$\alpha^2 = (1,0,1,0)\cdot(1,0,1,0) \sim (1+t^2)^2 =$$

$$\begin{array}{rrrl|l}
= t^4 & +2t^2 & +1 & & t^4+t^2+2 \\ \cline{5-5}
t^4 & +t^2 & +2 & & 1 \\ \hline
 & t^2 & +2 & &
\end{array}$$

$$\Rightarrow \alpha^2 = (2,0,1,0)$$

$$\alpha^4 = \alpha^2\cdot\alpha^2 \sim (t^2+2)^2 =$$

$$\begin{array}{rrrl|l}
= t^4 & +t^2 & +1 & & t^4+t^2+2 \\ \cline{5-5}
t^4 & +t^2 & +2 & & 1 \\ \hline
 & & 2 & &
\end{array}$$

$$\Rightarrow \alpha^4 = (2,0,0,0)$$

$$\alpha^5 = \alpha^4\cdot\alpha \sim 2(1+t^2) = 2t^2+2$$

$$\Rightarrow \alpha^5 = (2,0,2,0)$$

$$\alpha^8 = \alpha^4\cdot\alpha^4 = 4 = 1$$

$$\Rightarrow \alpha^8 = (1,0,0,0)$$

$\Rightarrow \alpha$ ha periodo 8 !

$GF(2^4)$, $\# GF(2^4)^* = 15$

$J(t) \in \mathbb{Z}_2[t]$ irriducibile di 4° grado

Polinomi di 2° grado in $\mathbb{Z}_2[t]$

$$
\begin{tikzcd}[column sep=small]
 & t^2+at \arrow[r] \arrow[dr] & t^2 \\
 & & t^2+t \\
t^2+at+b \arrow[uur] \arrow[dr] & & \\
 & t^2+at+1 \arrow[r] \arrow[dr] & t^2+t+1 \\
 & & t^2+t
\end{tikzcd}
$$

$\Rightarrow$ l'unico polinomio irriducibile di 2° grado è t^2+t+1

Si ha $(t^2+t+1)(t^2+t+1) = t^4+t^2+1$

che è l'unico polinomio in $\mathbb{Z}_2[t]$ privo di radici ma riducibile

Per fissare $J(t)$ basterà scegliere un polinomio di 4° grado, privo di radici diverso da t^4+t^2+1. Ad es.:

$$J(t) = t^4+t+1$$

c

Determiniamo l'ordine di

$$\alpha = (1,1,0,1) \sim 1+t+t^3$$

$$\alpha^2 \sim (1+t+t^3)\cdot(1+t+t^3) = t^6+t^2+1$$

$$\begin{array}{cccc|l}
t^6 & & +t^2 & +1 & t^4+t+1 \\ \cline{5-5}
t^6 & +t^3 & +t^2 & & t^2 \\ \cline{1-4}
 & t^3 & & +1 &
\end{array}$$

$\Rightarrow \quad \alpha^2 = (1,0,0,1)$

$$\alpha^3 = \alpha^2\alpha \sim (t^3+1)(1+t+t^3) = t^3+t^4+t^6+1+t+t^3$$
$$= t^6+t^4+t+1$$

$$\begin{array}{cccccc|l}
t^6 & +t^4 & & & +t & +1 & t^4+t+1 \\ \cline{7-7}
t^6 & & +t^3 & +t^2 & & & t^2+1 \\ \cline{1-6}
 & t^4 & +t^3 & +t^2 & +t & +1 & \\
 & t^4 & & & +t & +1 & \\ \cline{1-6}
 & & t^3 & +t^2 & & &
\end{array}$$

$\Rightarrow \quad \alpha^3 = (0,0,1,1)$

$$\alpha^5 = \alpha^3 \cdot \alpha^2 = (t^3+t^2)(t^3+1) =$$

$$= t^6+t^3+t^5+t^2$$

$$\begin{array}{l|l}
t^6+t^5 \quad +t^3+t^2 & t^4+t+1 \\
\cline{2-2}
t^6 \quad\quad\; +t^3+t^2 & t^2+t \\
\cline{1-1}
\quad\; t^5 & \\
\quad\; t^5 \quad +t^2+t & \\
\cline{1-1}
\quad\quad\quad t^2+t &
\end{array}$$

$\Rightarrow \alpha^5 = (0,1,1,0)$

Allora necessariamente $o(\alpha) = 15$

cioè α è un generatore di $GF(2^4)^*$ //