Teoria di HAMILTON-CAYLEY (secondo criterio di diagonalizzazione)

$\varphi: V \to V$

c'è corrispondenza tra
- divisori del pol. caratteristico di φ
- sottospazi di V invarianti e stabili per φ ($\Rightarrow$ scrittura a blocchi di $\alpha_\varphi(\varphi)$ diagonali)

$\varphi: V \to V$, $V = U \oplus W$, $\varphi(U) \subseteq U$, $\varphi(W) \subseteq W$ — allora usando basi di U, W otteniamo base di V in cui $\alpha_\varphi(\varphi) = \left(\begin{array}{c|c} * & 0 \\ \hline 0 & * \end{array}\right)$

teorema H-C: se $\varphi: V \to V$ allora $p_\varphi(\varphi) = 0$ come funzione $V \to V$

note: $p_\varphi(x) \in \mathbb{K}[x]$, $= x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$ (x^0, $\varphi^0 = id$)

allora $p_\varphi(\varphi) = \varphi^n + a_{n-1}\varphi^{n-1} + \dots + a_1\varphi + a_0 id \in End_{\mathbb{K}}(V)$

e $p_A(A) = A^n + a_{n-1}A^{n-1} + \dots + a_1 A + a_0 \mathbb{1}_n \in M_n(\mathbb{K})$

$(p_A(A) = \mathbb{0}_n)$

$\boxed{\text{ogni matrice annulla il suo pol. caratteristico}}$

dimostrazione:

① supponiamo che φ abbia tutti gli autovalori in $\mathbb{K}$ (certamente accade se $\mathbb{K}$)

allora usiamo una base $v_1, \dots, v_n$ in cui $T = \alpha_\varphi(\varphi) = \begin{pmatrix} a_1 & & * \\ & a_2 & \\ 0 & & \ddots \; a_n \end{pmatrix}$

Osserviamo che $p_\varphi(x) = (x-a_1)(x-a_2)\cdots(x-a_n)$

e che $p_\varphi(\varphi) = (\varphi - a_1)(\varphi - a_2)\circ \dots \circ (\varphi - a_n)$

si ha che $(\varphi - a_i)\langle v_1, \dots, v_i\rangle \subseteq \langle v_1, \dots, v_{i-1}\rangle$

$$\begin{pmatrix} a_1-a_i & & * & & \\ & a_2-a_i & & * & \\ & & \ddots & & \\ & & & 0 & \\ & & & & \ddots \; a_n - a_i \end{pmatrix}$$

$v_1, v_2, \dots, v_i \subseteq \langle v_1, \dots, v_{i-1}\rangle$ (coefficiente per v_i è sempre nullo...).

$$p_\varphi(\varphi)(V) = (\varphi - a_1)(\varphi - a_2)\cdots(\varphi - a_{n-1})\underbrace{(\varphi - a_n)\langle v_1, \dots, v_n\rangle}$$
$$\underbrace{(\varphi - a_{n-1})\langle v_1, \dots, v_{n-1}\rangle}_{\langle v_1, \dots, v_{n-2}\rangle}$$
$$= (\varphi - a_1)\langle v_1\rangle = 0$$

quindi $p_\varphi(\varphi) = 0$

altrimenti: $p_A(x) = \sum a_i x^i$

$$p_A(x)\mathbb{1}_n - p_A(A) = \left(\sum a_i x^i\right)\mathbb{1}_n - \sum a_i A^i$$
$$\sum a_i x^i \mathbb{1} - \sum a_i A^i$$
$$\sum a_i (x^i \mathbb{1} - A^i)$$
$$\sum a_i (x\mathbb{1} - A)(\dots)$$

$p_A(x)\mathbb{1}_n = (x\mathbb{1} - A)(x\mathbb{1} - A)^c$

$\boxed{\det(B)\mathbb{1}_n = B \cdot B^c}$, $p_A(x) = \det(x\mathbb{1} - A)$

$\Downarrow$

$(x^i - y^i) = (x-y)(x^{i-1} + x^{i-2}y + x^{i-3}y^2 + \dots + xy^{i-2} + y^{i-1})$ ($x = x\mathbb{1}$, $y = A$)

$$p_A(A) = (x\mathbb{1} - A)(x\mathbb{1} - A)^c - (x\mathbb{1} - A)\sum a_i(\dots)$$
$$= (x\mathbb{1} - A)\underbrace{\left((x\mathbb{1} - A)^c - \sum a_i(\dots)\right)}_{R(x)}$$

non dipende da x

se $R(x)$ fosse $\neq \mathbb{0}_n$ allora ci sarebbe la x nella parte destra dell'$=$.

$\Rightarrow R(x) = \mathbb{0}_n \Rightarrow p_A(A) = \mathbb{0}_n$ //

---

dato una matrice $A \in M_n(\mathbb{K})$

Osservazione: abbiamo una funzione:

$$\sigma_A: \mathbb{K}[x] \longrightarrow M_n(\mathbb{K})$$
$$F(x) \longmapsto F(A) = \sum a_i A^i$$

$F(x) = \sum a_i x^i$

è $\mathbb{K}$-lineare e rispetta il prodotto (= morfismo di $\mathbb{K}$ algebre)

non è iniettivo ($\ker(\sigma_A) \neq 0$): $\dim_{\mathbb{K}}(\mathbb{K}[x]) = \infty$, $\dim_{\mathbb{K}} M_n(\mathbb{K}) = n^2 < \infty$

in particolare $\boxed{p_A(x) \in \ker \sigma_A}$ T.H.C.

non è suriettiva perché $\mathbb{K}[x]$ è commutativo e σ_A morfismo algebre, $\sigma_A(\mathbb{K}[x])$ è sottoalgebra COMMUTATIVA di $M_n(\mathbb{K})$, e $\neq M_n(\mathbb{K})$ che non è commutativa!

$\ker(\sigma_A) \trianglelefteq \mathbb{K}[x]$
= tutti e soli i multipli di un certo polinomio ($\mathbb{K}[x]$ è DIP.)
$= (m_A(x))$

$\boxed{\text{definizione } m_A(x) = \text{generatore MONICO di } \ker(\sigma_A) = \text{polinomio monico di grado MINIMO che annulla } A.}$

Dunque: $\sigma_A: \mathbb{K}[x] \longrightarrow M_n(\mathbb{K})$, $F(x) \longmapsto F(A) = \sum a_i A^i$ ("valutazione in A") $A \in M_n(\mathbb{K})$

è morfismo di $\mathbb{K}$ algebre con:

$\mathbb{K}[x] \trianglerighteq \ker(\sigma_A) = (m_A(x))$ ideale generato dal pol. minimo di A

$\boxed{\text{T.H.C.: } m_A(x) \mid p_A(x) \quad \text{minimo divide caratteristico}}$

e (primo teorema isomorfismo):

$$\boxed{\operatorname{im}(\sigma_A) \simeq \mathbb{K}[x]/\ker(\sigma_A)} = \mathbb{K}[x]/(m_A(x))$$

ha dimensione = grado del pol. minimo

Def: $\boxed{\mathbb{K}[A] := \operatorname{im}(\sigma_A)}$, $\dim_{\mathbb{K}} \mathbb{K}[A] = \deg m_A(x)$.

"matrici polinomiali in A"

Osservazione: se A è invertibile allora $A^{-1} \in \mathbb{K}[A]$ (cioè A^{-1} è polinomiale in A)

perché da H.C. abbiamo

$p_A(A) = 0$ $\quad A^n + a_{n-1}A^{n-1} + \dots + a_1 A + a_0\mathbb{1} = 0$, $a_0 = (-)\det A \neq 0$

$$A^n + a_{n-1}A^{n-1} + \dots + a_1 A = -a_0\mathbb{1} \neq 0$$
$$A(A^{n-1} + a_{n-1}A^{n-2} + \dots + a_1) = -a_0\mathbb{1} \neq 0$$
$$A\underbrace{\left(\frac{A^{n-1} + a_{n-1}A^{n-2} + \dots + a_1}{-a_0}\right)}_{A^{-1} \in \mathbb{K}[A]} = \mathbb{1}$$

Esempi:

$A = \mathbb{1}_3 = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$, $p_A(x) = (x-1)^3$

divisori $p_A(x)$: $x-1$, $(x-1)^2$, $(x-1)^3$

$m_A(x) = x - 1$ perché $A - \mathbb{1} = \mathbb{0}$

$A = \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix}$, $p_A(x) = (x-1)^3$

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

$(A - \mathbb{1})^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $m_A(x) = (x-1)^2$

$A = \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix}$, $p_A(x) = (x-1)^3$

$A - 1 = \begin{pmatrix} 0 & 1 & 0 \\ & 0 & 1 \\ & & 0 \end{pmatrix}$, $(010)\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = 1$

$(A-1)^2 = \begin{pmatrix} 0 & 0 & 1 \\ & 0 & 0 \\ & & 0 \end{pmatrix} \neq \mathbb{0}$, $m_A(x) = p_A(x) = (x-1)^3$

Osservazioni sul pol. minimo:

① per def è generatore monico dell'ideale nucleo della mappa di valutazione
è polinomio monico di grado minimo che annulla la matrice

② per H.C. $m_A(x) \mid p_A(x)$

dunque ha grado $\leq n$
ha come zeri gli autovalori

perché:

se α è zero di $m_A(x)$ allora α è zero di $p_A(x)$ (perché $m_A(x) \mid p_A(x)$, $p_A(x) = m_A(x) \cdot q(x)$)

(α autovalore)

viceversa se α è autovalore, cioè è zero $p_A(x)$ allora DEVE essere zero di $m_A(x)$

altrimenti $\exists \alpha$: $p_A(\alpha) = 0$, $m_A(\alpha) \neq 0$

$\exists \underset{\neq 0}{v}: Av = \alpha v$

allora $m_A(A)v \neq 0$ assurdo perché $m_A(A) = 0$

infatti $m_A(A)v = \left(\sum a_i A^i\right)(v)$

$m_A(x) = \sum a_i x^i$ $\quad \overset{!}{=} \sum a_i A^i v$, $Av = \alpha v$, $A^2 v = Aav = \alpha^2 v$, $A^i v = \alpha^i v$

$= \sum a_i \alpha^i v$

$= \left(\sum a_i \alpha^i\right) v$

$= \underbrace{m_A(\alpha)}_{\neq 0} v \neq 0$ //

③ conclusione: il polinomio minimo è divisore del caratteristico, ha gli stessi fattori irriducibili eventualmente con molteplicità più basse.

Teorema di DECOMPOSIZIONE:

se $\varphi: V \to V$

e $F(x) \in \mathbb{K}[x]$: $F(\varphi) = 0: V \to V$

$F(x) = F_1(x)F_2(x)\cdots F_s(x)$

con $F_i(x)$ a 2 a 2 coprimi

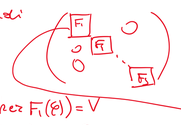
allora $V = V_1 \oplus V_2 \oplus \dots \oplus V_s$

dove $V_i := \ker(F_i(\varphi))$

e $\varphi(V_i) \subseteq V_i$ $\quad \forall i$

usiamo questo con $F(x) = p_\varphi(x)$, $m_\varphi(x)$.

$\boxed{\text{applicazione: in base dei } V_1, \dots, V_s \text{ (base di } V) \text{ abbiamo che } \varphi \text{ ha matrice a blocchi diagonali}}$



base $(\ker F_1(\varphi)) = V$

$v_1 \dots v_e$: $\varphi v_1 \in \langle v_1 \dots v_e\rangle$, $\varphi v_2 \in \langle v_1 \dots v_e\rangle$, $\vdots$

dopo aver dimostrato il teorema, vediamo applicazione:

SECONDO CRITERIO DI DIAGONALIZZAZIONE:

φ diagonalizzabile su $\mathbb{K}$ sse ① ha tutti gli autovalori in $\mathbb{K}$
② il polinomio minimo ha fattori (lineari) DISTINTI.

$\Rightarrow$ forte $A \sim \begin{pmatrix} \boxed{a_1 \cdots a_1} & & \\ & \boxed{a_2 \cdots a_2} & \\ & & \ddots \; \boxed{} \end{pmatrix}$ $\quad p_A(x) = \prod (x - a_i)^{m_i}$

e $m_A(x) = \prod (x - a_i)$ perché

$$(A - a_1\mathbb{1})(A - a_2\mathbb{1})\cdots(A - a_s\mathbb{1}) = \begin{pmatrix} \boxed{0} & & \\ & \boxed{} & \\ & & \ddots \; \boxed{} \end{pmatrix}\begin{pmatrix} \boxed{} & & \\ & \boxed{0} & \\ & & \ddots \; \boxed{} \end{pmatrix}\cdots\begin{pmatrix} \boxed{} & & \\ & \boxed{} & \\ & & \ddots \; \boxed{0} \end{pmatrix} = \begin{pmatrix} 0 & & 0 \\ & 0 & \\ 0 & & \ddots \; 0 \end{pmatrix}$$

$\Leftarrow$ usiamo il teorema di decomposizione:

$$m_A(x) = \prod_{i=1}^{s} (x - a_i)$$

siccome $m_A(A) = 0$ allora $V = V_1 \oplus V_2 \oplus \dots \oplus V_s$
dove $V_i = \ker(A - a_i\mathbb{1})$ AUTOSPAZIO di a_i

Quindi usando basi degli autospazi trovo base di V fatta di autovettori, quindi φ diagonalizzabile //

Possiamo applicare il Teo. Decomp anche al pol. caratteristico:

$p_A(x) = F_1(x)F_2(x)\cdots F_s(x)$ fattori 2 a 2 coprimi

allora $V = V_1 \oplus V_2 \oplus \dots \oplus V_s$

dove $V_i = \ker(F_i(A))$

$\varphi(V_i) \subseteq V_i \Longrightarrow \varphi_i = \varphi|_{V_i}: V_i \to V_i$

$p_{\varphi_i}(x) \overset{?}{=} F_i(x)$

Problemino: se $\varphi: V \to V$ diagonalizzabile e $W \leq V$ stabile per φ ($\varphi(W) \subseteq W$) allora $\varphi|_W$ è diagonalizzabile.

09/01/2024

Teorema di decomposizione:

$\varphi: V \to V$

$F(x) \in \mathbb{K}[x]$: $F(\varphi) = 0$ (appl. nulla $V \to V$)

e $F(x) = F_1(x)F_2(x)\cdots F_s(x)$

con $F_i(x)$ 2 a 2 coprimi

allora $V = V_1 \oplus V_2 \oplus \dots \oplus V_s$

dove $V_i = \ker(F_i(\varphi))$

$\varphi(V_i) \subseteq V_i$ sottospazi stabili per φ.

$\varphi_i := \varphi|_{V_i}: V_i \to V_i$ $\quad (F_i(\varphi_i) = 0)$

dimostrazione:

per induzione sul numero di fattori s

basta mostrare il caso $s = 2$:

$F(x) = F_1(x)F_2(x)$ con $(F_1(x), F_2(x)) = (1)$

cioè $\exists$ polinomi $G_1(x), G_2(x) \in \mathbb{K}[x]$ tali che $\boxed{F_1(x)G_1(x) + F_2(x)G_2(x) = 1}$ (*)

Vogliamo mostrare che $V = V_1 \oplus V_2$, $V_1 = \ker F_1(\varphi)$, $V_2 = \ker F_2(\varphi)$

e $\varphi(V_1) \subseteq V_1$, $\varphi(V_2) \subseteq V_2$

Allora: se $v \in V$ abbiamo da (*):

$F_1(\varphi)G_1(\varphi) + F_2(\varphi)G_2(\varphi) = id_V$ calcolato in v:

$\underbrace{F_1(\varphi)G_1(\varphi)v}_{v_2} + \underbrace{F_2(\varphi)G_2(\varphi)v}_{v_1} = v$

dove $v_1 \in \ker F_1(\varphi)$ perché

$F_1(\varphi)v_1 = F_1(\varphi)F_2(\varphi)G_2(\varphi)v = \underbrace{F(\varphi)}_{0}G_2(\varphi)v = 0$

e $v_2 \in \ker F_2(\varphi)$

dunque $V = V_1 + V_2$ $\quad \left(\forall v = \underset{V_1}{v_1} + \underset{V_2}{v_2}\right)$, $v_2 = F_1(\varphi)G_1(\varphi)v$

Mostriamo che $V_1 \cap V_2 = 0$ (allora $V = V_1 \oplus V_2$)

se $v \in V_1 \cap V_2$ ($\ker F_1(\varphi)$, $\ker F_2(\varphi)$)

(per (*)) $v = G_1(\varphi)\underbrace{F_1(\varphi)v}_{0} + G_2(\varphi)\underbrace{F_2(\varphi)v}_{0} = 0 + 0 = 0$

Inoltre: $\varphi(V_1) \subseteq V_1$

se $v \in V_1 = \ker F_1(\varphi)$

allora $\varphi(v) \in \ker F_1(\varphi) = V_1$

perché $F_1(\varphi)(\varphi v) = F_1(\varphi)\circ\varphi(v) = \varphi \circ \underbrace{F_1(\varphi)(v)}_{0} = 0$ //

Applicazioni:

polinomio minimo $m_\varphi(\varphi) = 0$

$\Rightarrow$ 2° diagonalizzazione
(φ diagonalizz./$\mathbb{K}$ $\Leftrightarrow$ ha tutti autov. in $\mathbb{K}$, $m_\varphi(x)$ ha fattori lineari DISTINTI)

polinomio caratteristico $p_\varphi(\varphi) = 0$

attenzione: fattorizzo $p_\varphi(x)$ $\Longrightarrow$ decomposizione V sottospazi stabili per φ

$\Leftarrow$

ma la corrispondenza

fattori p_φ $\longleftrightarrow$ sottospazi stabili

è LASCA perché # finito, non è detto che siano un # finito!

es. $\varphi = id_V$

$(x-1)^n$

$\ker(\varphi - 1) = \ker(\varphi - 1)^2 = \dots \ker(\varphi - 1)^n = V$