$p_f(f)\, v_i = 0 \quad \forall i = 1 \dots n$

$\Rightarrow \quad p_f(f) = 0 \quad !!$

$A \in M_n(\mathbb{K})$

$\mathbb{K}' \supseteq \mathbb{K}$ t.c. $p_A(x)$ ha tutte le radici in $\mathbb{K}'$. $\Rightarrow A$ è triangol. se considerata come matrice in $M_n(\mathbb{K}')$.

Esiste $C \in Gl_n(\mathbb{K}')$ t.c.

CAC^{-1} è triangolare $= T^{\in M_n(\mathbb{K}')}$

$p_T = p_A$ perché T è simile ad A

$$p_A(A) = p_T(A)$$

$0 = p_T(T)$ perché T triangol.

$$0 = p_T(T) = p_T(CAC^{-1}) = p_A(CAC^{-1})$$

$$= C\, p_A(A)\, C^{-1}$$

ma C inv.

$\Rightarrow p_A(A) = 0$ $\square$

<u>Corollario</u> $A \in M_n(\mathbb{K})$

$$\operatorname{Span}\{A^\ell\}_\ell = \operatorname{Span}\{I, A, A^2, \dots\}$$

prima stima ing. $\dim \operatorname{Span}\{A^\ell\} \leq n^2$

CH! se $p_A(X) = \pm X^n + a_1 X^{n-1} + \dots$

$$A^n = -a_1 A^{n-1} - \dots - a_n I, \text{ cioè}$$

A^n è comb. lin. di $I, A, \dots A^{n-1}$

analogg A^{n+1} " — — — — $I, A, \dots$

$$\Rightarrow \quad \dim \operatorname{Span}\{A^k\}_k \le n$$

$$\wr$$

$$\deg q_A \, .$$

Le radici di 1 in $\mathbb{C}$.

Vogliamo risolvere $x^n = 1$ cioè trovare tutti i numeri compl. la cui n-ma potenza è 1.

<u>oss. 1</u> Se $x^n = 1 \Rightarrow |x| = 1$

infatti $|x^n| = |1| = 1$ ma

$|x^n| = |x|^n$ e $|x| \in \mathbb{R}_{>0} \Rightarrow |x| = 1$

<u>oss. 2.</u> Le radici n-me di 1 formano un gruppo risp. alla moltipl.: (vero in ogni campo)

se $x_1^n = 1$ e $x_2^n = 1$

$\Rightarrow (x_1 x_2)^n = x_1^n x_2^n = 1.$

inoltre se $x^n = 1 \Rightarrow x \neq 0$

quindi esiste x^{-1}, e

$$(x^{-1})^n = \frac{1}{x^n} = \frac{1}{1} = 1.$$

In $\mathbb{C}$: se $|x| = 1$

$$\Rightarrow x = (\cos\theta + i\sin\theta).$$

$$x^n = (\cos\theta + i\sin\theta)^n =$$

$$\cos(\underbrace{\theta + \dots + \theta}_{n \text{ volte}}) + i\sin(\underbrace{\theta + \dots + \theta}_{n \text{ volte}})$$

$$= \cos(n\theta) + i\sin(n\theta) = 1$$

se e solo se $\cos(n\theta) = 1$
$\sin(n\theta) = 0$

cioè se $n\theta$ è multiplo di 2π: esiste $K \in \mathbb{Z}$ t.c. $n\theta = 2K\pi$, vale a dire le radici n-me sono della forma

$$\cos\left(\frac{2K\pi}{n}\right) + i \sin\left(\frac{2K\pi}{n}\right) =: \mu_K$$

$K \in \mathbb{Z}$. Adesso osserviamo che: $K_1 - K_2$ divisibile per $n \Leftrightarrow \mu_{K_1} = \mu_{K_2}$.

quindi, per non ripeterci, prendiamo $K = 0, 1, 2, \ldots n-1$

(più canonicamente questo mostra che il gruppo delle radici n-me (in $\mathbb{C}$!) è isomorfo al gruppo ciclico $\mathbb{Z}/_{n\mathbb{Z}}$.)

$\mu_0 = 1 \quad \mu_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$

...

oss. anche che $\mu_k = \mu_1^k$, cioè μ_1 è un generatore del gruppo ciclico.

<u>Es.</u> μ_k è un gen. del gruppo delle radici n-me $\iff$ k è primo con n

(si dice che μ_k è una radice primitiva)

e.g. $n=4$ $\mu_0 = 1$ $\mu_1 = i$

$\mu_2 = -1$ $\mu_3 = -i$

i e $-i$ sono primitive

1 e -1 NO.

Più dettagli sulla dim del corollario:

$f \in End(V)$, $p \in \mathbb{K}[X]$

t.c. $p(f) = 0$; $p = p_1 \cdot \ldots \cdot p_k$

$p_i \in \mathbb{K}[X]$, p_i sono a due a due primi tra loro

$$\Rightarrow V = \bigoplus_{i=1}^{k} \underbrace{\operatorname{Ker} p_i(f)}_{\text{ssv } f\text{-invarianti}}.$$

$$p_i(f)\big|_{\operatorname{Ker} p_i(f)} = 0$$

$= \{ v : p_i(f) v = 0 \}$.

<u>Dim</u>. $k=2$ è il Teor. già visto.

Supponiamo vero l'enunciato per $k-1$:

Se $q \in \mathbb{K}[X]$ $q = \underbrace{q_2 \cdot \ldots \cdot q_k}_{k-1 \text{ pol.}}$

$q_2 \ldots q_k$ a due a due primi tra loro

$g \in End(W)$: $q(g)=0$

$\Rightarrow W = \bigoplus_{i=2}^{k} Ker\, q_i(g)$.

per k. (Torniamo alla not. dell'enunciato).

Scrivo $p = p_1 \cdot (p_2 \cdot \ldots \cdot p_k)$

p_1 e $p_2 \cdot \ldots \cdot p_k$ sono primi tra loro. (Se esistesse $r \in \mathbb{K}[x]$ che divide p_1 e $p_2 \cdot \ldots \cdot p_k$ allora dovrebbe dividere o p_2 o p_3 o ... p_k.)

per il Teor.

$$V = \operatorname{Ker} p_1(f) \oplus \underline{\operatorname{Ker} p_2 \cdot \ldots \cdot p_k}(f) \quad (*)$$

Applichiamo l'ipotesi indutt. come scritto sopra a

$$W = \operatorname{Ker}\left(p_2 \cdot \ldots \cdot p_k(f)\right)$$

$$g = f_{|W} : W \longrightarrow W$$

(ok perchè W è f-invariante)

$q = p_2 \cdot \ldots \cdot p_k \qquad q_2 = p_2 \ \ldots$

Trovo (ipotesi induttiva)

$$\underline{\operatorname{Ker}\left(p_2 \cdot \ldots \cdot p_k(f)\right)} = \bigoplus_{i=2}^{k} \operatorname{Ker} p_i(f)$$

Sostituendo in (*) troviamo

l'enunciato.

Riepiloghiamo:

$f \in End(V)$. vogliamo scomporre V in somma diretta di ssv f-invarianti.

- Se ho un polinomio p t.c. $p(f)=0$ $\quad p = p_1 \cdot \ldots \cdot p_k$

posso scomporre ad esempio in prodotto di (potenze) di pol irriducibili.

L'importante è che $p_1, \ldots p_k$ siano a due a due primi tra loro

$$\Rightarrow V = \bigoplus \underbrace{\ker p_i(f)}_{\text{ssv } f\text{-invarianti}} \qquad p_i(f)\big|_{\ker p_i} = 0$$

Il problema è trovare polinomi (non nulli) p t.c. $p(f)=0$.

- poiché l'appl. $\mathbb{K}[X] \longrightarrow End(V)$
$$p \longmapsto p(f)$$

è un om. di anelli, il suo nucleo è un ideale di $\mathbb{K}[X]$. Poiché ogni ideale in $\mathbb{K}[X]$ è principale $\exists!$ q_f generatore MONICO di questo ideale che si chiama il polinomio minimo.

$$q_f(f) = 0$$

e se $p(f)=0 \Rightarrow p$ è divisibile per q.

- Teor. di C-H. se p_f è il pol. caratteristico di $f \Rightarrow$
  $p_f(f)=0$ cioè

il pol. minimo divide il pol. caratteristico.

Ipotesi: $\mathbb{K}$ contenga tutte le radici di p_f.

questo è automatico se $\mathbb{K}$ è alg. chiuso.

$$\Rightarrow q_f = \prod_{i=1}^{k} \underbrace{(X-\lambda_i)}^{r_i}.$$

come corollario

$$V = \bigoplus_i \underbrace{\operatorname{Ker}(f-\lambda_i I)^{r_i}}.$$

OSS. Per il Teor. di C-H i λ_i devono essere autovalori di f.

Perché $p_f(X) = \prod_{j=1}^{s} \underbrace{(X-\lambda_j)}^{m_j}$

dove $\lambda_1 \dots \lambda_s$ sono gli autoval. distinti e

$m_1 \dots m_s$ le loro molteplic. algebriche.

Ma siccome il pol. minimo divide quello car.

<u>OSS</u>. A priori q_f potrebbe non contenere qualche $X-\lambda_i$. In realtà sì:

<u>Teor</u>. Se λ_1 è un autovalore di $f \Rightarrow q_f$ è div. per $X-\lambda_1$

quindi, nelle not introdotte

$K = S$ e l' unica cosa in

cui q_f può differire

da p_f sono le molt.

cioè $1 \leq r_i \leq m_i$.

<u>Dim.</u> λ_1 è autovalore di f

scelgo $v_1 \neq 0$ t.c. $f(v_1) = \lambda_1 v_1$

Se $q_f(X)$ non fosse divisibile per λ_1

$$\underbrace{q_f(X) = \prod_{i=2}^{s} (X - \lambda_i)^{r_i}}$$

(cioè manca il fattore $X - \lambda_1$

$q_f(f) = 0 \qquad q_f(f)(v_1) = 0$

$$\parallel$$

$$\prod_{i=2}^{s} (f - \lambda_i)^{r_i} (v_1)$$

$$(f - \lambda_i)(v_1) = f(v_1) - \lambda_i v_1$$

cioè $(\lambda_1 - \lambda_i)\, v_1$

$$(f - \lambda_i I)^a (v_1) = (\lambda_1 - \lambda_i)^a v_1$$

$$\prod_{i=2}^{s} (f - \lambda_i)^{r_i} (v_1) =$$

$$\Big(\prod_{i=2}^{s} (\lambda_1 - \lambda_i)^r \Big) v_1 \neq 0.$$

scalari $\neq 0$

assurdo perché $q_f(f)(v_1) = 0$.

$\square$