TEOR. 47. Sia V il $\mathbb{C}[x]$-modulo rispetto a $\varphi \in End_{\mathbb{C}}(V)$.
Sia $v \in V$ e $Ann(v) = ((x-\lambda)^r)$ ove $\lambda \in \mathbb{C}$, $r \in \mathbb{N}$, $r > 0$.
Allora:

a) $\mathcal{B} = \{v, (\varphi-\lambda id)(v), (\varphi-\lambda id)^2(v), \dots, (\varphi-\lambda id)^{r-1}(v)\}$
è una base del $\mathbb{C}$-sottospazio vettoriale $\langle v \rangle = \mathbb{C}[x]\cdot v$.

b) rispetto a $\mathcal{B}$ si ha

$$[\varphi_{|\langle v\rangle}]_{\mathcal{B}} = \begin{bmatrix} \lambda & 0 & \cdots & 0 & 0 \\ 1 & \lambda & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda & 0 \\ 0 & 0 & \cdots & 1 & \lambda \end{bmatrix} \in Mat_{r,r}(\mathbb{C})$$

DIM.

a) Per il teor. 43, $\dim_{\mathbb{C}} \langle v \rangle = r$: quindi basta provare che i vettori di $\mathcal{B}$ sono indipendenti su $\mathbb{C}$.
Sempre per il teor. 43 l'insieme $\mathcal{B}' = \{v, \varphi(v), \dots, \varphi^{r-1}(v)\}$ è una base del $\mathbb{C}$-spazio vett. $\langle v \rangle$ e le coordinate dei vettori di $\mathcal{B}$ rispetto a $\mathcal{B}'$ formano una matrice triangolare alta con gli elementi sulla diagonale $=1$ poiché:
$(v, (\varphi-\lambda id)v, \dots, (\varphi-\lambda id)^{r-1}(v)) = (v, \varphi(v)-\lambda v, \dots, \sum_{i=1}^{r-1} \binom{r-1}{i}(-\lambda)^{r-1-i}\varphi^i(v))$
Tale matrice è invertibile e quindi $\mathcal{B}$ è una base.

b) Pongo $(\varphi-\lambda id)^j(v) = v_j$ $\forall j = 0, 1, \dots, r-1$.
e quindi $\mathcal{B} = \{v_0, v_1, \dots, v_{r-1}\}$
Osservo che
- se $j < r-1$: $\varphi(v_j) = (\varphi-\lambda id)(v_j) + \lambda v_j = v_{j+1} + \lambda v_j$
- se $j = r-1$: $\varphi(v_{r-1}) = (\varphi-\lambda id)^r(v) + \lambda v_{r-1} = \lambda v_{r-1}$

  poiché $(\varphi-\lambda id)^r(v) = (x-\lambda)^r \cdot v = 0$,
  essendo $Ann(v) = ((x-\lambda)^r)$.

Dunque la matrice ha la forma indicata

c.v.d.

DEF. 48 La matrice trovata nel teor. 47 è detta

MATRICE ELEMENTARE di JORDAN

e viene indicata con $J(\lambda, r)$.

Tenendo presente il teorema di decomposizione primaria si ha allora il

TEOR. 49 Sia V uno spazio vettoriale su $\mathbb{C}$, $\dim_{\mathbb{C}} V = n$ e sia $\varphi \in End_{\mathbb{C}}(V)$. Allora esiste una base $\mathcal{B}$ (unione di basi del tipo indicato nel teor. 47 per ciascuno dei sottomoduli ciclici della decomposizione primaria) tale che

$$[\varphi]_{\mathcal{B}} = J(\lambda_1, r_1) \oplus J(\lambda_2, r_2) \oplus \dots \oplus J(\lambda_k, r_k)$$

ove $J(\lambda_i, r_i)$ è la matrice elementare di Jordan rispetto a $(x-\lambda_i)^{r_i}$, $r_i > 0$, $\sum_1^k r_i = n = \dim_{\mathbb{C}} V$.

La base $\mathcal{B}$ in questione è detta BASE di JORDAN di V e la matrice $[\varphi]_{\mathcal{B}}$ è detta FORMA CANONICA di JORDAN di φ.

NOTA 1. La forma di Jordan non è una forma razionale poiché la sua costruzione passa attraverso operazioni non razionali come "risolvere un'equazione polinomiale" che – anche se possibili: siamo in $\mathbb{C}$ – non è detto siano concretamente attuabili.

Nota 2. L'ipotesi $k = \mathbb{C}$ è servita solo a garantire che i fattori irriducibili del generatore di $Ann(V)$ siano polinomi di 1° grado.
Quindi si potrà trovare la forma canonica di Jordan, indipendentemente dal campo k, quando
$Ann\, V = (d)$ e $d = (x-\lambda_1)^{r_1} \cdot \ldots \cdot (x-\lambda_h)^{r_h}$.

10. ALGORITMO PER SCOMPORRE V.

Per poter trovare concretamente i fattori invarianti che entrano in gioco nella scomposizione di V in somma diretta di $k[x]$-sottomoduli ciclici servono alcune osservazioni preliminari.

Sia M un modulo libero di rango s su un anello comm. con 1, A. Sappiamo che <u>non è vero che</u> ogni sistema di s elementi di M linearmente indipendenti sia una base di M (vedi es. 2 pag. 18). MA VALE IL

LEMMA 50. Sia M un modulo LIBERO di rango s su un anello comm. con 1, A. Se $\{m_1, \dots, m_s\}$ è un insieme di generatori di M, allora $m_1, \dots, m_s$ sono linearmente indipendenti e quindi formano una base per M.

DIM. Sia $\{b_1, \dots, b_s\}$ una base di M. Allora:

$$(m_1, \dots, m_s)^T = X (b_1, \dots, b_s)^T$$ in quanto $\{b_1, \dots, b_s\}$ è un ins. di generatori di M

$$(b_1, \dots, b_s)^T = Y (m_1, \dots, m_s)^T$$ in quanto $\{m_1, \dots, m_s\}$ è un ins. di gen. di M

$$(b_1, \dots, b_s)^T = YX (b_1, \dots, b_s)^T \Rightarrow (I_s - YX)(b_1, \dots, b_s)^T = (0_M, \dots, 0_M)^T$$

$$\underset{\{b_1,\dots,b_s\}\text{ base}}{\Longrightarrow} \quad I_s - YX = 0_s \Rightarrow YX = I_s \Rightarrow X \text{ è invertibile.}$$

Sia ora $\sum_{i=1}^{s} a_i m_i = 0_M$. Poiché $\{b_1, \dots, b_s\}$ è una base,

$$\sum_{i=1}^{s} a_i m_i = (a_1, \dots, a_s)(m_1, \dots, m_s)^T = \big((a_1, \dots, a_s) X\big)(b_1, \dots, b_s)^T$$

può essere $= 0_M$ solo se

$$(a_1, \dots, a_s) X = (0, 0, \dots, 0)$$

cioè, dato che X è invertibile,

$$(a_1, \dots, a_s) = (0, \dots, 0).$$

c.v.d.

Sia ora $B = \{v_1, \dots, v_n\}$ una base del k-spazio vettoriale V.
Come nella dim. del teor. di struttura considero il $k[x]$-modulo libero $k[x]^n$ con la base standard $\{e_1, \dots, e_n\}$ e definisco

$$\sigma : k[x]^n \longrightarrow V$$

ponendo

$$\sigma(e_i) = v_i \qquad \forall i = 1, \dots, n$$

ed estendendo per linearità.
σ è un omomorfismo suriettivo di $k[x]$-moduli che agisce come segue:

$$\sigma(p_1(x), \dots, p_n(x)) = \sigma\Big(\sum_1^n p_i(x) \cdot e_i\Big) = \sum_1^n p_i(x) \cdot \sigma(e_i) = \sum_1^n p_i(x) \cdot v_i$$

e induce un isomorfismo di $k[x]$-moduli

$$\frac{k[x]^n}{\ker \sigma} \longrightarrow V$$

ponendo

$$[\ker \sigma + (p_1(x), \dots, p_n(x))] \longmapsto \sum_1^n p_i(x) \cdot v_i .$$

Per il teor. 21 sappiamo che $\ker \sigma$ è un $k[x]$-sottomodulo LIBERO; ne vogliamo trovare una base utilizzando il LEMMA 50: quindi serve conoscerne il RANGO.
Per il teor. 21', il rango di $\ker \sigma$ è $\leq n$.
Se fosse $\mathrm{rk}(\ker \sigma) < n$, per il teor. 24, $\frac{k[x]^n}{\ker \sigma}$ avrebbe una componente libera: ciò non può succedere poiché V è un $k[x]$-modulo di torsione (teor. 40).
Dunque

$\ker \sigma$ <u>è libero di rango n.</u>

Per il lemma 50, allora, un qualunque insieme di n generatori di $\ker \sigma$ è una sua base.

TEOR. 51. Denotiamo con A la matrice $[\varphi]_{B}$ che rappresenta l'endomorfismo φ del k-spazio vettoriale V rispetto alla base $B=\{v_1,\dots,v_n\}$. I vettori colonna della matrice

$$xI_n - A$$

sono un sistema di generatori (e quindi una base) per $\ker\sigma$.

DIM. Denoto con H il sottomodulo del $k[x]$-modulo $k[x]$ generato dalle colonne di xI_n-A e mostro che $H\equiv\ker\sigma$.

1) $H\subseteq\ker\sigma$

Infatti la i-esima colonna di A contiene le coordinate di $\varphi(v_i)$ rispetto a B, cioè

$$\varphi(v_i)=\sum_{j=1}^{n} a_{ji}v_j$$

cioè, poiché $x\cdot v_i=\varphi(v_i)$,

$$x\cdot v_i-\sum_{j=1}^{n} a_{ji}v_j=0$$

e quindi

$$\sigma(-a_{1i},\dots,x-a_{ii},\dots,-a_{ni})=0$$

Dunque tutte le colonne di xI_n-A stanno in $\ker\sigma \Rightarrow H\subseteq\ker\sigma$.

2) $\ker\sigma\subseteq H$.

Osservo che gli elementi di H sono combinazioni lineari (con coefficienti a sinistra) mediante polinomi $q_1,\dots,q_n$ delle colonne di $xI-A$:

$$(q_1,\dots,q_n)(xI_n-A)^T=(q_1,\dots,q_n)(xI_n-A^T)$$

al variare di $(q_1,\dots,q_n)$ in $k[x]^n$.

Se mostro che ogni elemento $\alpha=(f_1,\dots,f_n)\in k[x]^n$ si può scrivere come somma di un elemento di k^n e di un elemento di H

$$\alpha=(k_1,\dots,k_n)+\beta$$

posso concludere che, se $\alpha\in\ker\sigma$:

$$0=\sigma(\alpha)=\sigma(k_1+\dots+k_n)+\sigma(\beta)\underset{\text{poiché }\beta\in H\subseteq\ker\sigma}{=}\sigma(k_1,\dots,k_n)=\sum_{i=1}^{n}k_iv_i$$

e, dato che $\{v_1,\dots,v_n\}$ è una base dello spazio vettoriale V, ciò implica

$$(k_1,\dots,k_n)=(0,\dots,0)\qquad\Rightarrow\ \alpha=\beta$$

cioè $\ker\alpha\subseteq H$ che è la nostra tesi.

Mostriamo quindi che – come gruppi – risulta

$$k[x]^n=k^n+H$$

Applicando l'algoritmo della divisione, con divisore x, ad ogni componente f_i di α si ha

$$f_i=c_i+q_i\cdot x \qquad \text{ove } c_i\in k \text{ e } q_i(x)=0 \text{ oppure } \deg q_i<\deg f_i.$$

Dunque

$$\alpha=(f_1,\dots,f_n)=(c_1,\dots,c_n)+(q_1x,\dots,q_nx)=$$

$$=(c_1,\dots,c_n)+(q_1,\dots,q_n)\,xI_n=$$

$$=(c_1,\dots,c_n)+\underbrace{(q_1,\dots,q_n)(xI_n-A^T)}_{\in H}+(q_1,\dots,q_n)A^T$$

I polinomi della n-upla $(q_1,\dots,q_n)A^T$ o sono nulli o hanno grado $<$ del più grande dei polinomi $f_1,\dots,f_n$.
Quindi iterando la procedura su $(q_1,\dots,q_n)A^T$, in un numero finito di passi si arriva a scrivere

$$\alpha=(f_1,\dots,f_n)=(k_1,\dots,k_n)+(\tilde q_1,\dots,\tilde q_n)(xI_n-A^T)$$

con $(k_1,\dots,k_n)\in k^n$ e $(\tilde q_1,\dots,\tilde q_n)\in k[x]^n$ e quindi $(\tilde q_1,\dots,\tilde q_n)(xI_n-A^T)\in H$.

c.v.d.

Torniamo al teorema di struttura.

Denotiamo con $\{h_1, \dots, h_n\}$ la base di $\ker \sigma$ formata dalle colonne di $xI_n - A$. Allora, usando la notazione introdotta nel teor. delle due basi, avremmo:

$$(h_1, \dots, h_n)^T = (xI_n - A)^T (e_1, \dots, e_n)^T$$

e, posto $N = (xI_n - A)^T$, calcolando la forma normale di Smith di N:

$$\Delta = \operatorname{diag}(f_1, \dots, f_n) \quad \text{con} \quad f_i \mid f_{i+1} \quad , \quad \Delta = XNY$$

potremmo trovare la base

$$(e_1', \dots, e_n')^T = Y^{-1} (e_1, \dots, e_n)^T$$

di $k[x]^n$ e la base

$$(h_1', \dots, h_n')^T = X (h_1, \dots, h_n)^T$$

di $\ker \sigma$ legate tra loro dal fatto che $h_i' = f_i e_i' \quad \forall i = 1, \dots, n$

e per il teor. 24 potremmo dire che

$$V = \langle \sigma(e_1') \rangle \oplus \dots \oplus \langle \sigma(e_n') \rangle$$

con $\operatorname{Ann}(\sigma(e_i')) = (f_i)$, $\forall i = 1, \dots, n$

e l'avvertenza che se f_i è invertibile (cioè è un elemento di $k \setminus (0)$) allora $\langle \sigma(e_i') \rangle = 0$.

La notazione con i "trasposti" è però inutilmente noiosa a livello pratico (anche se serve a ricordare che lavoriamo con un $k[x]$-modulo sinistro).

È chiaro che $\Delta = \Delta^T = Y^T N^T X^T = Y^T (xI_n - A) X^T$

e

$$(h_1, \dots, h_n) X^T = (e_1, \dots, e_n)(Y^T)^{-1} \Delta .$$

Conviene quindi trovare direttamente la forma normale di Smith di $xI_n - A$: $\boxed{\Delta = P(xI_n - A)Q}$, ove si è posto $P = Y^T$ e $Q = X^T$. I vettori $e_1', \dots, e_n'$ saranno le colonne della matrice P^{-1}.

Riepiloghiamo il procedimento per trovare le forme canoniche di un endomorfismo $\varphi \in \operatorname{End}_k V$.

Data una matrice che rappresenti φ rispetto a una qualunque base $B = \{v_1, \dots, v_n\}$ dello spazio vett. V : $\quad A = [\varphi]_B$

1) si trova la forma normale di Smith di $xI_n - A$, con operazioni elementari sulle righe e sulle colonne:
$$\Delta = \operatorname{diag}(f_1, \dots, f_n) \quad \text{con } f_i \mid f_{i+1} \quad \text{e } f_i \text{ (ove non } = 0) \text{ monico;}$$
2) se P è la matrice che riassume le operazioni fatte sulle righe $(\Delta = P(xI_n - A)Q)$, si calcola P^{-1}.
3) le colonne di P^{-1} danno una base di $k[x]^n$, che denoto con $\{e_1', \dots, e_n'\}$, $e_i' \in k[x]^n \ \forall i$.
4) V come $k[x]$-modulo si decompone come
$$V = \langle \sigma(e_1') \rangle \oplus \dots \oplus \langle \sigma(e_n') \rangle$$
ove $\sigma : k[x]^n \to V$ è l'omomorfismo di $k[x]$-moduli
$$\sigma(p_1, \dots, p_n) = \sum_1^n p_i \cdot v_i$$
se $B = \{v_1, \dots, v_n\}$.

5) le forme canoniche di φ si deducono dai fattori invarianti, cioè dai polinomi f_i di grado ≥ 1, eventualmente scomponendo tali fattori in fattori irriducibili.

Vediamo come su un esempio.

ESEMPIO

Sia $\varphi : (\mathbb{Z}_2)^3 \to (\mathbb{Z}_2)^3$ l'endomorfismo di spazi vettoriali su $\mathbb{Z}_2$ definito da

$$\varphi\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} c \\ a+c \\ a \end{pmatrix}$$

Trovare le forme canoniche di φ e le basi corrispondenti.

Sol.

Sia $\mathcal{B}$ la base canonica di $(\mathbb{Z}_2)^3$: $\left\{\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right\} = \{v_1, v_2, v_3\}$. Allora

$$[\varphi]_{\mathcal{B}} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = A \in Mat_{3,3}(\mathbb{Z}_2)$$

Trovo la forma normale di Smith di $xI_3 - A$ (attenzione: $-1=1$) e per comodità indico ogni passaggio con la matrice che trasforma la matrice che precede in quella successiva; R_i denota una matrice che opera sulle righe (e quindi moltiplica a sinistra), C_i una che opera sulle colonne.

$$\begin{pmatrix} x & 0 & 1 \\ 1 & x & 1 \\ 1 & 0 & x \end{pmatrix} \xrightarrow{C_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}} \begin{pmatrix} 1 & 0 & x \\ 1 & x & 1 \\ x & 0 & 1 \end{pmatrix} \xrightarrow{C_2 = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}} \begin{pmatrix} 1 & 0 & 0 \\ 1 & x & 1+x \\ x & 0 & 1+x^2 \end{pmatrix} \longrightarrow$$

$$\xrightarrow{R_1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ x & 0 & 1 \end{pmatrix}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x & 1+x \\ 0 & 0 & 1+x^2 \end{pmatrix} \xrightarrow{C_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x & 1 \\ 0 & 0 & 1+x^2 \end{pmatrix} \longrightarrow$$

$$\xrightarrow{C_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & x \\ 0 & 1+x^2 & 0 \end{pmatrix} \xrightarrow{C_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1+x^2 & x+x^3 \end{pmatrix} \xrightarrow{R_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1+x^2 & 1 \end{pmatrix}}$$

$$\longrightarrow \mathrm{diag}(1, 1, x+x^3) = \Delta$$

Si ha $R_2 R_1 (xI_3 - A) C_1 C_2 C_3 C_4 C_5 = \Delta \Rightarrow P = R_2 R_1$, $Q = C_1 C_2 C_3 C_4 C_5$

Sulla diagonale c'è un solo polinomio di grado ≥ 1: quindi $V = (\mathbb{Z}_2)^3$ è un modulo ciclico su $\mathbb{Z}_2[x]$ con annullatore $Ann(V) = (x^3+x)$.

Per trovarne un generatore, guardiamo le colonne della matrice

$$P^{-1} = R_1^{-1} R_2^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ x & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1+x^2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ x & 1+x^2 & 1 \end{pmatrix}$$

esse sono la nuova(*) base $\{e_1', e_2', e_3'\}$ di $\mathbb{Z}_2[x]^3$ e

$$V = \langle \sigma(e_1') \rangle \oplus \langle \sigma(e_2') \rangle \oplus \langle \sigma(e_3') \rangle \simeq$$

$$\simeq \frac{\mathbb{Z}_2[x]}{(1)} \oplus \frac{\mathbb{Z}_2[x]}{(1)} \oplus \frac{\mathbb{Z}_2[x]}{(x+x^3)} = \frac{\mathbb{Z}_2[x]}{(x+x^3)}$$

quindi i primi due addendi sono nulli e come $\mathbb{Z}_2[x]$-modulo

$$V = \langle \sigma(e_3') \rangle = \langle \sigma\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \rangle = \langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \rangle.$$

La cosa può anche essere verificata concretamente (passiamo alla scrittura trasposta per indicare correttamente il prodotto per scalare a sinistra): ricordando che $\varphi(v_1) = v_2+v_3$, $\varphi(v_2) = 0$, $\varphi(v_3) = v_1+v_2$,

$$\begin{pmatrix} 1 & 1 & x \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = v_1 + v_2 + x \cdot v_3 = v_1 + v_2 + \varphi(v_3) = 0$$

$$\begin{pmatrix} 0 & 1 & 1+x^2 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = v_2 + v_3 + x^2 \cdot v_3 = v_2 + v_3 + \varphi^2(v_3) = v_2 + v_3 + \varphi(v_1+v_2) =$$

$$= v_2 + v_3 + v_2 + v_3 + 0 = 0.$$

Ne consegue che la forma canonica razionale di φ è

$$\mathcal{C}(x^3+x) = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

essendo $a_0 = a_2 = 0$ nel polinomio minimo: $x + x^3$.

La base corrispondente di V come spazio vettoriale è

$$\mathcal{B}' = \left\{\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \varphi\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \varphi^2\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right\} = \left\{\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}\right\}$$

(*) La base di partenza $\{e_1, e_2, e_3\}$ di $\mathbb{Z}_2[x]^3$ si scrive come quella di $\mathbb{Z}_2^3$ solo che 0 e 1 vanno pensati come polinomi.

Per trovare la forma primaria osserviamo che in $\mathbb{Z}_2[x]$

$$x^3+x = x\,(x^2+1) = x\,(x+1)^2$$

e quindi lo $\mathbb{Z}_2[x]$-modulo V è somma diretta di due ciclici:

$$V = V_1 \oplus V_2$$

ove

$$V_1 = \langle (x^2+1)\cdot\begin{pmatrix}0\\0\\1\end{pmatrix}\rangle = \langle (\varphi^2+id)\begin{pmatrix}0\\0\\1\end{pmatrix}\rangle = \langle \begin{pmatrix}0\\1\\0\end{pmatrix}\rangle \qquad \text{e } \mathrm{Ann}\, V_1 = (x)$$

$$V_2 = \langle x\cdot\begin{pmatrix}0\\0\\1\end{pmatrix}\rangle = \langle \varphi\begin{pmatrix}0\\0\\1\end{pmatrix}\rangle = \langle \begin{pmatrix}1\\1\\0\end{pmatrix}\rangle \qquad \text{e } \mathrm{Ann}\, V_2 = (x^2+1).$$

Ricordare: $[\varphi]_{\mathcal{B}} = \begin{bmatrix}0&0&1\\1&0&1\\1&0&0\end{bmatrix}$

Quindi la forma canonica primaria è

$$C(x)\oplus C(x^2+1) = \left[\begin{array}{c|cc}0&0&0\\ \hline 0&0&1\\0&1&0\end{array}\right]$$

e la corrispondente base di V è

$$\mathcal{B}'' = \left\{\begin{pmatrix}0\\1\\0\end{pmatrix};\begin{pmatrix}1\\1\\0\end{pmatrix},\ \varphi\begin{pmatrix}1\\1\\0\end{pmatrix}\right\} = \left\{\begin{pmatrix}0\\1\\0\end{pmatrix};\begin{pmatrix}1\\1\\0\end{pmatrix},\begin{pmatrix}0\\1\\1\end{pmatrix}\right\}.$$

Anche se il campo non è $\mathbb{C}$, si può trovare anche la forma canonica di Jordan poiché il generatore di $\mathrm{Ann}(V)$ si scompone nel prodotto di 3 polinomi irriducibili di 1° grado:

$$x+x^3 = x\,(x+1)^2$$

$\Rightarrow$ due "autovalori": $\lambda=0$ e $\lambda=-1=1$.

La forma canonica di Jordan proviene dalla scomposizione

$$V = V_1\oplus V_2$$

con una diversa scelta della base:

$$\mathcal{B}''' = \left\{\begin{pmatrix}0\\1\\0\end{pmatrix};\begin{pmatrix}1\\1\\0\end{pmatrix},\ (\varphi-id)\begin{pmatrix}1\\1\\0\end{pmatrix}\right\} = \left\{\begin{pmatrix}0\\1\\0\end{pmatrix},\begin{pmatrix}1\\1\\0\end{pmatrix},\begin{pmatrix}1\\0\\1\end{pmatrix}\right\}$$

$\Rightarrow$ forma canonica di Jordan: $\left[\begin{array}{c|cc}0&0&0\\ \hline 0&1&0\\0&1&1\end{array}\right]$

11. POLINOMIO MINIMO E POLINOMIO CARATTERISTICO

Nell'esempio precedente sono stati chiamati "autovalori" le radici dell'ultimo fattore invariante $f_3 = x(x+1)^2$.

In tale esempio è chiaro, vista una qualunque delle matrici canoniche rappresentative di φ che f_3 (che è il polinomio minimo di φ) è il polinomio caratteristico di φ, ove si dia la seguente:

DEF. 52. Sia φ un endomorfismo di uno spazio vettoriale V di dimensione n su k. Si dice POLINOMIO CARATTERISTICO di φ il polinomio

$$ch_\varphi(x) = \det\left[x I_n - [\varphi]\right]$$

ove $[\varphi]$ è una qualsiasi matrice rappresentativa di φ.

Più in generale:

TEOR. 53. Siano $f_1,\dots,f_s$ i fattori invarianti di V su $k[x]$ rispetto a φ: $\forall i$, f_i monico e $f_i \mid f_{i+1}$. Allora

(a) $m_\varphi(x) = f_s(x)$

(b) $ch_\varphi(x) = f_1(x)\cdot f_2(x)\cdot\ldots\cdot f_s(x)$.

Dim. (a) è già stato provato che $\mathrm{Ann}_{k[x]} V = (f_s)$ e dato che tanto m_φ che f_s sono monici i due generatori devono coincidere.

(b) Per la riduzione a forma normale di Smith, esistono $P, Q \in GL_n(k[x])$ tali che

$$P\,(xI_n - [\varphi])\,Q = \mathrm{diag}(1,\dots,1,f_1,\dots,f_s)$$

$$\Rightarrow \det P\cdot\det Q\cdot ch_\varphi(x) = f_1\cdot\ldots\cdot f_s$$

Ma $P,Q\in GL_n(k[x]) \Rightarrow \det P, \det Q \in k\setminus(0)$: essendo ch_φ, $f_1,\dots,f_s$ polinomi monici si deve avere $\det P\cdot\det Q = 1$ (in quanto coeff. del termine di grado max a sin. dell'$=$)

c.v.d.