Polinomio minimo

Nella definizione della decomposizione spettrale per un generico endomorfismo si può adottare un diverso punto di vista che risulta utile, tra l'altro, per trattare il caso in cui lo spazio vettoriale sia definito su un campo non algebricamente chiuso, in particolare sul campo dei numeri reali. Tale diverso punto di vista è suggerito dalle seguenti osservazioni.

Si consideri uno spazio vettoriale $\mathcal{U}$ definito sul campo dei numeri complessi $\mathbb{C}$, un generico endomorfismo A e la corrispondente decomposizione spettrale di $\mathcal{U}$

$$\mathcal{U} = \mathrm{V}_{\lambda_1} \oplus \ldots \oplus \mathrm{V}_{\lambda_r}$$

Gli autospazi generalizzati

$$\mathrm{V}_{\lambda_\alpha} := \ker\,(A - \lambda_\alpha I)^{\mu_\alpha}$$

hanno ciascuno dimensione uguale alla molteplicità algebrica m_α del corrispondente autovalore λ_α (si pensi al polinomio caratteristico ottenuto dalla matrice di A in una base costruita unendo delle basi dei sottospazi $\mathrm{V}_{\lambda_\alpha}$). Indicando con P_α la proiezione canonica su $\mathrm{V}_{\lambda_\alpha}$, è semplice dimostrare che l'endomorfismo

$$(A - \lambda_\alpha I)P_\alpha$$

è nilpotente di indice μ_α e che perciò

$$\mu_\alpha \leq m_\alpha$$

Si osservi infatti che, essendo $\mathrm{V}_{\lambda_\alpha}$ invariante rispetto ad A, risulta per ogni intero m

$$((A - \lambda_\alpha I)P_\alpha)^m = (A - \lambda_\alpha I)^m P_\alpha$$

e perciò

$$\{\, \forall u \in \mathcal{U} \quad ((A - \lambda_\alpha I)P_\alpha)^{\mu_\alpha} u = (A - \lambda_\alpha I)^{\mu_\alpha} P_\alpha u = o \,\} \quad \Rightarrow \quad (A - \lambda_\alpha I)^{\mu_\alpha} P_\alpha = O$$

L'indice di nilpotenza non può dunque essere maggiore di μ_α. Non può però neppure essere inferiore a μ_α, altrimenti si negherebbe la definizione di μ_α poiché

$$(A - \lambda_\alpha I)^{\mu_\alpha - 1} P_\alpha = O \quad \Rightarrow \quad \ker\,(A - \lambda_\alpha I)^{\mu_\alpha - 1} \supseteq \mathrm{V}_{\lambda_\alpha}$$

Si consideri ora l'endomorfismo

$$p(A) := (A - \lambda_1 I)^{\mu_1}(A - \lambda_2 I)^{\mu_2} \ldots (A - \lambda_r I)^{\mu_r}$$

È semplice dimostrare che

$$p(A) = O$$

osservando che

$$p(A) = (A - \lambda_1 I)^{\mu_1}(A - \lambda_2 I)^{\mu_2} \ldots (A - \lambda_r I)^{\mu_r}(P_1 + \ldots + P_r)$$

e applicando a tale espressione le seguenti proprietà

$$\forall\alpha \quad (A-\lambda_\alpha I)^{\mu_\alpha} P_\alpha = O$$
$$\forall\alpha,\beta \quad (A-\lambda_\alpha I)^{\mu_\alpha} P_\beta = P_\beta (A-\lambda_\alpha I)^{\mu_\alpha}$$

Si noti che se si sostituisse nella definizione di $p(A)$ un esponente μ_α con un intero più piccolo risulterebbe $p(A) \neq O$, essendo $(A-\lambda_\alpha I)^{\mu_\alpha - 1} P_\alpha \neq O$.

L'endomorfismo $p(A)$ si può vedere come corrispondente al polinomio su $\mathbb{C}$

$$p(\lambda) = (\lambda-\lambda_1)^{\mu_1}(\lambda-\lambda_2)^{\mu_2}\ldots(\lambda-\lambda_r)^{\mu_r}$$

Tale polinomio si dice *polinomio minimo* di A. Questo termine trae origine dalle seguenti proprietà.

Poiché $\mu_\alpha \le m_\alpha$, il polinomio minimo è un divisore del polinomio caratteristico P. Per tale ragione l'endomorfismo corrispondente a P

$$P(A) := (A-\lambda_1 I)^{m_1}(A-\lambda_2 I)^{m_2}\ldots(A-\lambda_r I)^{m_r}$$

risulta tale che (*teorema di Cayley–Hamilton*)

$$P(A) = O$$

Tra tutti i polinomi f tali che $f(A) = O$ non può esisterne uno che divide il polinomio p. Un tale polinomio sarebbe infatti esprimibile come prodotto dei fattori primi $(A-\lambda_\alpha I)$ di p di cui almeno uno avrebbe esponente inferiore al corrispondente esponente μ_α e questo implicherebbe $f(A) \neq O$.

Si osservi infine che a ciascuno dei fattori primi $(\lambda-\lambda_\alpha)$ del polinomio minimo p, che coincidono con quelli del polinomio caratteristico P, corrisponde un endomorfismo $(A-\lambda_\alpha I)$ e quindi un autospazio generalizzato $\mathrm{V}_{\lambda_\alpha} := \ker(A-\lambda_\alpha I)^{\mu_\alpha}$. Dunque alla decomposizione del polinomio minimo in fattori primi di grado uno corrisponde la decomposizione spettrale dello spazio vettoriale $\mathcal{U}$. Inoltre condizione necessaria e sufficiente affinché A sia diagonalizzabile è che risulti, per tutti gli autovalori λ_α, $\mu_\alpha = 1$. Infatti

$$\mu_\alpha = 1 \iff \mathrm{V}_{\lambda_\alpha} = \ker(A-\lambda_\alpha I) = \mathrm{U}_{\lambda_\alpha}$$

Tutto questo suggerisce, almeno nel caso in cui lo spazio $\mathcal{U}$ sia definito su un campo non algebricamente chiuso, di definire il polinomio minimo di un endomorfismo come quel polinomio che ha le proprietà qui sopra descritte e di costruire poi una decomposizione di $\mathcal{U}$ in sottospazi invarianti corrispondente alla decomposizione del polinomio minimo in fattori primi, in generale di grado maggiore o uguale ad uno.