Costruzione del polinomio minimo

Sia A un endomorfismo di uno spazio vettoriale $\mathcal{U}$.

È possibile immaginare di costruire il polinomio minimo di A nel modo seguente.[1]

Si scelga un qualsiasi vettore $u \in \mathcal{U}$. Si applichi ripetutamente A al vettore u sino ad ottenere un vettore $A^h u$ che risulta essere una combinazione lineare dei vettori

$$u, Au, A^2u, \ldots, A^{h-1}u$$

Tali vettori costituiscono dunque una famiglia di vettori linearmente indipendenti. Sia V_1 il sottospazio da essi generato. Esso risulta essere invariante rispetto ad A, ciclico e di dimensione h.

Poiché il vettore $A^h u$ appartiene al sottospazio V_1 esistono degli scalari a_{ij} tali che

$$a_{10}u + a_{11}Au + a_{12}A^2u + \ldots + a_{1,h-1}A^{h-1}u + A^h u = o$$

Si osservi ora che il polinomio

$$p_1(t) := a_{10} + a_{11}t + a_{12}t^2 + \ldots + a_{1,h-1}t^{h-1} + t^h$$

è tale che

$$p_1(A|_{\mathrm{V}_1}) = O$$

È infatti

$$\begin{aligned}
&p_1(A)u = o\\
&p_1(A)Au = Ap_1(A)u = o\\
&\ldots\\
&p_1(A)A^h u = A^h p_1(A)u = o
\end{aligned}$$

Inoltre, poiché V_1 è ciclico, il grado del polinomio minimo di $A|_{\mathrm{V}_1}$ è uguale alla dimensione di V_1. Il polinomio p_1, essendo di grado pari alla dimensione di V_1 e avendo il coefficiente del termine di grado h uguale a 1, è dunque il polinomio minimo di $A|_{\mathrm{V}_1}$.

Si osservi che

$$\{\ \forall u \in \mathrm{V}_1 \quad p_1(A)u = o\ \} \quad \Rightarrow \quad \mathrm{V}_1 \subset \ker p_1(A)$$

Si scelga ora un qualsiasi vettore $u \notin \mathrm{V}_1$, si consideri lo spazio ciclico V_2 da esso generato e si costruisca il polinomio minimo di $A|_{\mathrm{V}_2}$ in modo analogo a p_1.

Si continui scegliendo un vettore u in un complemento di $\mathrm{V}_1 + \mathrm{V}_2$, e così via sino a che

$$\mathrm{V}_1 + \mathrm{V}_2 + \ldots + \mathrm{V}_s = \mathcal{U}$$

Poiché in generale

$$\mathrm{V}_\alpha \subset \ker p_\alpha(A)$$

risulta

$$\mathcal{U} = \ker p_1(A) + \ldots + \ker p_s(A)$$

[1] Da *Problem n. 6* in [1] p. 389.

Si considerino i fattori primi $f_i^{k_i}$ dei polinomi p_α. Scegliendo tra i fattori comuni solo quelli con esponente maggiore, si ottiene la decomposizione

$$\mathcal{U} = \ker f_1^{k_1} \oplus \ldots \oplus \ker f_r^{k_r}$$

Il polinomio

$$p := f_1^{k_1} \ldots f_r^{k_r}$$

è il minimo comune multiplo dei polinomi p_α e risulta tale che

$$p(A) = O$$

essendo

$$\ker p(A) = \ker f_1^{k_1} \oplus \ldots \oplus \ker f_r^{k_r} = \mathcal{U}$$

Poiché ciascun polinomio p_α, quale polinomio minimo della restrizione di A ad un sottospazio invariante, è un divisore del polinomio minimo di A, questo è diviso anche dal polinomio p, minimo comune multiplo dei polinomi p_α. Allora il polinomio p, essendo tale che $p(A) = O$ e avendo il coefficiente del termine di grado più alto pari ad 1, è il polinomio minimo di A.