Decomposizione di uno spazio vettoriale definito su un generico campo

La decomposizione in sottospazi invarianti rispetto ad un endomorfismo di uno spazio vettoriale definito su un campo non algebricamente chiuso motiva le definizioni e i teoremi che seguono.

Sia A un endomorfismo di uno spazio vettoriale $\mathcal{U}$ definito su un campo Γ. In corrispondenza di ogni polinomio f sul campo Γ

$$f(t) = a_0 + a_1 t^1 + a_2 t^2 + \ldots \qquad a_i \in \Gamma$$

si consideri l'endomorfismo di $\mathcal{U}$

$$f(A) := a_0 I + a_1 A^1 + a_2 A^2 + \ldots$$

Per qualunque polinomio f il sottospazio

$$\ker f(A)$$

è invariante rispetto ad A. Infatti

$$\forall u \in \ker f(A) \quad f(A)Au = Af(A)u = o$$

Siano f e g due polinomi tali che g divida f. Allora

$$\ker g(A) \subset \ker f(A)$$

Infatti, ponendo $f = gh$, si ha

$$\forall u \in \ker g(A) \quad f(A)u = g(A)h(A)u = h(A)g(A)u = o$$

Si possono inoltre dimostrare (si veda [1] pp. 384–385, oppure [3] pp. 148–149) i seguenti teoremi.

T1. Siano f e g due polinomi non nulli e d il massimo comun divisore. Allora

$$\ker d(A) = \ker f(A) \cap \ker g(A)$$

T2. Siano f e g due polinomi non nulli e v il minimo comune multiplo. Allora

$$\ker v(A) = \ker f(A) + \ker g(A)$$

T3. Siano f e g due polinomi primi tra loro e $w := fg$. Allora

$$\ker w(A) = \ker f(A) \oplus \ker g(A)$$

Tra tutti i polinomi su Γ particolarmente interessanti sono quei polinomi f tali che

$$f(A) = O$$

poiché per essi risulta

$$\ker f(A) = \ker O = \mathcal{U}$$

Indicando con $\mathcal{P}$ l'insieme di tali polinomi, si dimostra che:

T4. Esiste almeno un polinomio in $\mathcal{P}$ diverso dal polinomio nullo ([1] p. 367, [3] p. 146).

T5. Esiste un polinomio $p \in \mathcal{P}$, con il coefficiente del termine di grado più alto uguale ad uno, tale che $\mathcal{P}$ è costituito da tutti i suoi multipli; tale polinomio, detto *polinomio minimo* di A, è unico ([3] pp. 146–147).

T6. Il polinomio caratteristico P appartiene a $\mathcal{P}$ (*teorema di Cayley–Hamilton*, [1] p. 148, [3] pp. 129–130).

Si consideri il polinomio minimo di A e la sua decomposizione in fattori primi

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

Per uno dei teoremi precedenti risulta

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

Ponendo

$$\mathrm{V}_\alpha := \ker f_\alpha^{k_\alpha}(A)$$

si ha dunque

$$\mathcal{U} = \mathrm{V}_1 \oplus \ldots \oplus \mathrm{V}_r$$

I sottospazi V_α si dicono *autospazi generalizzati*.
Indicando con P_α la proiezione canonica su V_α, si dimostra che l'endomorfismo

$$f_\alpha(A)P_\alpha$$

è nilpotente di indice k_α. Si osservi infatti che, essendo V_α invariante rispetto ad A, e dunque anche rispetto a $f_\alpha(A)$, risulta per ogni intero m

$$(f_\alpha(A)P_\alpha)^m = f_\alpha^m(A)P_\alpha$$

e perciò

$$\{\ \forall u \in \mathcal{U} \quad (f_\alpha(A)P_\alpha)^{k_\alpha} u = f_\alpha^{k_\alpha}(A)P_\alpha u = o\ \} \quad \Rightarrow \quad f_\alpha^{k_\alpha}(A)P_\alpha = O$$

L'indice di nilpotenza non può dunque essere maggiore di k_α. Non può però neppure essere inferiore a k_α, altrimenti si negherebbe che p sia il polinomio minimo. Infatti se q_α è l'indice di nilpotenza si ha

$$f_\alpha^{q_\alpha}(A)P_\alpha = O$$
$$f_\alpha^{q_\alpha - 1}(A)P_\alpha \neq O$$

Questo implica che il polinomio $f := f_1^{q_1} \ldots f_2^{q_2}$ è tale che $f(A) = O$, come si ottiene dalla espressione

$$f(A) = f_1^{q_1}(A) \ldots f_2^{q_2}(A)(P_1 + \ldots + P_r)$$

applicando la proprietà
$$\forall \alpha, \beta \quad f_\alpha^{q_\alpha}(A) P_\beta = P_\beta f_\alpha^{q_\alpha}(A)$$
Se qualche q_α fosse inferiore al corrispondente k_α il polinomio f sarebbe un divisore del polinomio minimo p. Risulta dunque $q_\alpha = k_\alpha$.
Da questo deriva che il polinomio minimo della restrizione di A all'autospazio generalizzato V_α è
$$f_\alpha^{k_\alpha}$$
Infatti, per la invarianza di V_α, si ha
$$\begin{aligned} f_\alpha^{k_\alpha}(A|_{\mathrm{V}_\alpha}) P_\alpha = f_\alpha^{k_\alpha}(A) P_\alpha = O \quad &\Rightarrow \quad f_\alpha^{k_\alpha}(A|_{\mathrm{V}_\alpha}) = O \\ f_\alpha^{k_\alpha - 1}(A|_{\mathrm{V}_\alpha}) P_\alpha = f_\alpha^{k_\alpha - 1}(A) P_\alpha \neq O \quad &\Rightarrow \quad f_\alpha^{k_\alpha - 1}(A|_{\mathrm{V}_\alpha}) \neq O \end{aligned}$$
Si consideri ora un polinomio
$$f := f_1^{p_1} \dots f_r^{p_r} \qquad p_\alpha > k_\alpha$$
e la corrispondente decomposizione di $\mathcal{U}$
$$\mathcal{U} = \ker f_1^{p_1}(A) \oplus \dots \oplus \ker f_r^{p_r}(A)$$
Essendo in generale per ogni intero m
$$\ker f_\alpha^{m-1}(A) \subseteq \ker f_\alpha^{m}(A)$$
deve essere
$$\ker f_\alpha^{k_\alpha}(A) = \ker f_\alpha^{p_\alpha}(A)$$
poiché la somma delle dimensioni dei sottospazi V_α è già uguale alla dimensione di $\mathcal{U}$. Essendo poi k_α l'indice di nilpotenza di $f_\alpha(A) P_\alpha$ deve essere anche
$$\ker f_\alpha^{k_\alpha - 1}(A) \neq \ker f_\alpha^{k_\alpha}(A)$$
Risulta dunque che k_α è tale che
$$\forall m < k_\alpha \;, \; \forall q > k_\alpha \quad \ker f_\alpha^{m}(A) \subset \ker f_\alpha^{k_\alpha}(A) = \ker f_\alpha^{q}(A)$$
Si noti che nel caso in cui i fattori primi f_α del polinomio minimo siano di grado uno ($\nu_\alpha = 1$) le proprietà descritte corrispondono esattamente a quelle derivanti dalla decomposizione di uno spazio vettoriale definito su un campo algebricamente chiuso, ottenuta a partire dalla definizione degli autospazi generalizzati anziché dalla definizione del polinomio minimo.

Si dimostrano inoltre i seguenti importanti teoremi ([1] Chap. XIII)

- T7. Se lo spazio $\mathcal{U}$ è ciclico rispetto all'endomorfismo A allora la dimensione di $\mathcal{U}$ è uguale al grado del polinomio minimo p di A.
- T8. Esiste una decomposizione di $\mathcal{U}$ nella somma diretta di sottospazi ciclici rispetto all'endomorfismo A.
- T9. Se lo spazio $\mathcal{U}$ è irriducibile rispetto all'endomorfismo A allora è anche ciclico.

T10. Lo spazio $\mathcal{U}$ è irriducibile rispetto all'endomorfismo A se e solo se è ciclico e il polinomio minimo di A si può esprimere come $p = f^k$, con f irriducibile.

T11. Se lo spazio $\mathcal{U}$ è ciclico rispetto all'endomorfismo A e $n := \dim \mathcal{U}$, allora il polinomio minimo p e il polinomio caratteristico P di A hanno la seguente proprietà

$$P = (-1)^n p$$

T12. Il polinomio caratteristico P e il polinomio minimo p hanno gli stessi fattori primi.

Naturalmente questi teoremi si estendono a qualsiasi sottospazio di $\mathcal{U}$ invariante rispetto all'endomorfismo A.

Si osservi che, poiché il polinomio caratteristico è un multiplo del polinomio minimo e ha i suoi stessi fattori primi, il polinomio caratteristico di $A|_{\mathrm{V}_\alpha}$ sarà $f_\alpha^{h_\alpha}$, con $h_\alpha \geq k_\alpha$. Essendo il grado di tale polinomio uguale alla dimensione di V_α, risulta

$$m_\alpha := \dim \mathrm{V}_\alpha = h_\alpha \nu_\alpha \geq k_\alpha \nu_\alpha$$

avendo indicato con ν_α il grado del polinomio f_α.

È semplice poi dimostrare il seguente teorema.

T13. Se V è un sottospazio di $\mathcal{U}$ invariante rispetto all'endomorfismo A, p_V il polinomio minimo di $A|_{\mathrm{V}}$ e p il polinomio minimo di A allora p_V divide p.

Infatti

$$p(A) = 0 \quad \Rightarrow \quad p(A|_{\mathrm{V}}) = 0$$

Essendo p_V il polinomio minimo in V esso è un divisore di qualsiasi polinomio f tale che $f(A|_{\mathrm{V}}) = 0$, quindi è anche un divisore di p.

È utile infine definire una proprietà corrispondente alla diagonalizzabilità di un endomorfismo di uno spazio vettoriale definito su un campo chiuso.

Si dice *semisemplice* un endomorfismo il cui polinomio minimo è il prodotto di polinomi irriducibili primi tra loro. Il polinomio minimo ha dunque, per un endomorfismo semisemplice, la seguente decomposizione in fattori primi

$$p = f_1 \dots f_r$$

a cui corrispondono gli autospazi generalizzati

$$\mathrm{V}_\alpha = \ker f_\alpha(A)$$

Un ultimo utile teorema è il seguente.

T14. Condizione necessaria e sufficiente affinché un endomorfismo sia semisemplice è che per ogni sottospazio invariante esista un complemento invariante ([1] p. 427).