Note del corso di Geometria 1

Gabriel Antonio Videtta

25 marzo 2023

Esercitazione: algoritmi per la ricerca del polinomio minimo

Definizione. Dato $f \in \mathrm{End}(V)$, si definisce come $\mathrm{val}_{f,\underline{v}}$ l'applicazione lineare da $\mathbb{K}[x]$ in V tale che $\mathrm{val}_{f,\underline{v}}(p) = p(f)(\underline{v})$.

Osservazione. Vi sono varie proprietà che legano $\ker \mathrm{val}_{f,\underline{v}}$ a $\ker \mathrm{val}_f$, ed in particolare il generatore monico di $\ker \mathrm{val}_{f,\underline{v}}$ $\varphi_{f,\underline{v}}$ a quello φ_f di $\ker \mathrm{val}_f$, ossia al polinomio minimo di f.

- $\varphi_{f,\underline{v}} \mid \varphi_f$, $\forall\, \underline{v} \in V$.
- $\varphi_f = \mathrm{mcm}(\varphi_{f,\underline{v_1}}, ..., \varphi_{f,\underline{v_n}})$., dove i $\underline{v_1}$, ..., $\underline{v_n}$ formano una base di V.

Esempio. Sia $A = \begin{pmatrix} 2 & 0 & 0 \\ 1 & -1 & 3 \\ 1 & 3 & -1 \end{pmatrix}$. Allora si possono considerare le seguenti catene:

- $\underline{e_1} \mapsto 2\underline{e_1} + \underline{e_2} + \underline{e_3} \mapsto 2(2\underline{e_1} + \underline{e_2} + \underline{e_3}) + (-\underline{e_2} + 3\underline{e_3}) + (3\underline{e_2} - \underline{e_3}) = 4\underline{e_1} + 4\underline{e_2} + 4\underline{e_3} = 4A\underline{e_1} - 4\underline{e_1}$. Pertanto $A^2\underline{e_1} - 4A\underline{e_1} + 4\underline{e_1} = \underline{0}$. Essendo $A\underline{e_1}$ e $\underline{e_1}$ linearmente indipendenti, si conclude che $\varphi_{A,\underline{e_1}}(x) = x^2 - 4x + 4 = (x-2)^2$.
- $\underline{e_2} \mapsto -\underline{e_2} + 3\underline{e_3} \mapsto -(-\underline{e_2} + 3\underline{e_3}) + 3(3\underline{e_2} - \underline{e_3}) = 10\underline{e_2} - 6\underline{e_3} = -2(-\underline{e_2} + 3\underline{e_3}) + 8\underline{e_2}$. Si conclude dunque che $\varphi_{A,\underline{e_2}}(x) = x^2 + 2x - 8 = (x-2)(x+4)$.
- $\underline{e_3} \mapsto 3\underline{e_2} - \underline{e_3} \mapsto 3(-\underline{e_2} + 3\underline{e_3}) - (3\underline{e_2} - \underline{e_3}) = -6\underline{e_2} + 10\underline{e_3} = -2(3\underline{e_2} - \underline{e_3}) + 8\underline{e_3}$. Dunque $\varphi_{A,\underline{e_3}}(x) = x^2 + 2x - 8 = \varphi_{A,\underline{e_2}}(x)$.

Pertanto $\varphi_A(x) = \mathrm{mcm}(\varphi_{A,\underline{e_1}}(x), \varphi_{A,\underline{e_2}}(x), \varphi_{A,\underline{e_3}}(x)) = (x-2)^2(x+4)$.

Definizione. Si dice che un vettore $\underline{v}$ è *ciclico* su f se il ciclo $\mathrm{Span}(\underline{v}, f(\underline{v}), f^2(\underline{v}), ...)$ coincide con V.

Osservazione. Riguardo all'esistenza di un vettore ciclico si possono fare alcune osservazioni.

▶ Se esiste un vettore $\underline{v}$ ciclico rispetto a f, i primi $n = \dim V$ vettori del suo ciclo devono essere linearmente indipendenti (altrimenti non potrebbe generare V), e quindi $\varphi_{f,\underline{v}}$ deve avere grado n. Allora anche φ_f deve avere grado n, ossia lo stesso grado di p_f. Allora, dal momento che $\varphi_f \mid p_f$ e $\deg \varphi_f = \deg p_f$, deve valere necessariamente $\varphi_f = \pm p_f$.
▶ Dal momento che $\varphi_{f,\underline{v}}$ è monico, ha lo stesso grado di φ_f e lo divide, deve anche valere che $\varphi_{f,\underline{v}} = \varphi_f$.
▶ Nella base ordinata $\mathcal{B}$ costituita dai primi n vettori del ciclo di $\underline{v}$, la matrice associata di f è della forma:

$$M_{\mathcal{B}}(f) = C_{\varphi_f} = \begin{pmatrix} 0 & 0 & \dots & \dots & 0 & -a_0 \\ 1 & 0 & \dots & \dots & 0 & -a_1 \\ 0 & 1 & \ddots & & \vdots & \vdots \\ \vdots & \vdots & & \ddots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix},$$

dove gli a_i sono i coefficienti di $\varphi_f(x) = \varphi_{f,\underline{v}} = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$. Tale matrice è detta **matrice compagna** del polinomio φ_f.
▶ Ogni polinomio $q \in \mathbb{K}[x]$ è il polinomio caratteristico, a meno del segno, della propria matrice compagna. In particolare $p_{C_q}(\lambda) = (-1)^n q(\lambda)$, dove $n := \deg q$. Infatti, se $n = 0$, $C_q = (-a_0) \implies p_{C_q}(\lambda) = -\lambda - a_0 = -(\lambda + a_0)$. Altrimenti, assumendo che la tesi sia vera per $i \leq n$, si osservi che:

$$p_{C_q}(\lambda) = (-1)^n a_0 - \lambda p_{C_{q'}}(\lambda), \qquad q'(\lambda) = \frac{q(\lambda) - a_0}{\lambda},$$

ossia, dacché $\deg q' = n - 1 < n \implies p_{C_{q'}}(\lambda) = (-1)^{n-1} q'(\lambda)$,

$$p_{C_q}(\lambda) = (-1)^n a_0 - \lambda(-1)^{n-1} q'(\lambda) = (-1)^n a_0 - \lambda(-1)^{n-1} \frac{q(\lambda) - a_0}{\lambda} = q(\lambda).$$

▶ Inoltre, osservando che $\mathcal{B} = (\underline{e_1}, C_q \underline{e_1} = \underline{e_2}, C_q^2 \underline{e_1} = \underline{e_3}, ..., C_q^{n-1} \underline{e_1} = \underline{e_n})$ è esattamente la base canonica di $\mathbb{K}^n$, essendo $\mathcal{B}$ una base ciclica di C_q su $\mathbb{K}^n$ deve valere che φ_{C_q} ha grado n, e quindi che $p_{C_q} = \pm \varphi_{C_q}$. Si conclude allora che $\varphi_{C_q} = q$.

Proposizione. Se $\mathbb{K}$ è un campo infinito[1], esiste sempre un vettore $\underline{v} \in V$ tale che $\varphi_{f,\underline{v}} = \varphi_f$.

Dimostrazione. Si definisce il seguente insieme:

$$S = \{\varphi_{f,\underline{v}} \mid \underline{v} \in V\}.$$

Poiché S è un sottoinsieme dei divisori di ϕ_f, S è finito. In particolare $\exists\, v_1$, ..., v_n tali che $S = \{\varphi_{f,\underline{v_1}}, ..., \varphi_{f,\underline{v_n}}\}$. Dal momento che ogni $\underline{v} \in V$ è associato ad un unico polinomio caratteristico, vale che $V = \bigcup_{i=1}^{n} \operatorname{Ker} \varphi_{f,\underline{v_i}}$. Tuttavia, se tutti i $\operatorname{Ker} \varphi_{f,\underline{v_i}}$ fossero propri, questo sarebbe impossibile, dal momento che uno spazio vettoriale fondato su un campo finito non può essere unione finita di sottospazi propri. Quindi $V = \operatorname{Ker} \varphi_{f,\underline{v_i}}$ per un i tale che $1 \leq i \leq n$. Allora $\varphi_f \mid \varphi_{f,\underline{v_i}}$, da cui si ricava l'uguaglianza. □

Teorema. Lo spazio V ammette un vettore ciclico su $f \in \operatorname{End}(V)$ se e solo se $p_f = \pm\varphi_f$.

Dimostrazione. Si dimostrano le due implicazioni separatamente.

($\Longrightarrow$) Dall'osservazione precedente.
($\Longleftarrow$) Dalla proposizione precedente esiste sicuramente un vettore $\underline{v}$ tale che $\varphi_{f,\underline{v}} = \varphi_f$. Allora, essendo $\varphi_f = \pm p_f$, deve valere che $p_f = \pm\varphi_{f,\underline{v}}$, ossia che la minima combinazione lineare linearmente dipendente di $\underline{v}$, ..., $f^k(\underline{v})$ si può ottenere coinvolgendo almeno $n+1$ termini (i.e. con $k \geq n$). Allora i vettori $\underline{v}$, ..., $f^{n-1}(\underline{v})$ sono linearmente indipendenti, ed essendo in totale n formano una base di V. Pertanto $V = \operatorname{Span}(\underline{v}, f(\underline{v}), ...)$. □

Esempio. Riprendendo l'esempio di prima, $\varphi_A(x) = (x-2)^2(x+4)$. Poiché $\deg p_A = 3$, allora $\varphi_A(x) - p_A(x)$. Allora per il teorema appena dimostrato deve necessariamente esistere un vettore ciclico di $\mathbb{R}^3$ su A.

In effetti, posto $\underline{v} = \begin{pmatrix} 4 \\ -3 \\ 5 \end{pmatrix}$, si ottiene che $\underline{v}$, $A\underline{v}$ e $A^2\underline{v}$ sono linearmente indipendenti, e sono dunque una base $\mathcal{B}$ di $\mathbb{R}^3$. In particolare, la matrice associata su questa base è la seguente:

[1] In realtà la tesi è vera per qualsiasi campo, benché la dimostrazione che è stata fornita sia valida solo per campi infiniti.

$$M_{\mathcal{B}}(A) = \begin{pmatrix} 0 & 0 & -16 \\ 1 & 0 & 12 \\ 0 & 1 & 0 \end{pmatrix},$$

proprio come ci aspettavamo che venisse da una delle osservazioni iniziali, dal momento che $\varphi_A(x) = (x-2)^2(x+4) = x^3 - 12x + 16$.