

Polinomio minimal

Hemos visto que si $A \in K^{n \times n}$, entonces $\chi_A(\lambda)$ es un polinomio no nulo que anula a A , es decir, si $\chi(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \dots + a_0$,

Entonces $\chi_A(A) = A^n + a_{n-1}A^{n-1} + \dots + a_1A + a_0\text{Id}_n = 0$ en $K^{n \times n}$.

Este no es el único polinomio no nulo que anula a A . Está claro por ejemplo que cualquier múltiplo polinomial de χ_A también anula a A :

si $h = g \cdot \chi_A$, entonces $h(A) = (g \chi_A)(A) = g(A) \chi_A(A) = 0$.

También por ejemplo si, para $\lambda_1 \neq \lambda_2$,

$$A = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_1 & & \\ & & \lambda_2 & \\ & & & \lambda_2 \end{bmatrix}$$

$\begin{matrix} \uparrow & & \uparrow \\ r & & s \\ \downarrow & & \downarrow \end{matrix}$

$$\text{Entonces } \chi_A(\lambda) = (\lambda - \lambda_1)^r (\lambda - \lambda_2)^s$$

Pero está claro que si tomamos $m_A(\lambda) = (\lambda - \lambda_1)(\lambda - \lambda_2)$, se

tiene

$$m_A(A) = \begin{bmatrix} m_A(\lambda_1) & & \\ & m_A(\lambda_1) & \\ & & m_A(\lambda_2) & \\ & & & m_A(\lambda_2) \end{bmatrix} = 0 \quad \text{pues } \lambda_1, \lambda_2 \text{ son raíces de } m_A(\lambda)$$

Luego $m_A(\lambda)$ en este caso es un polinomio de grado menor que anula a A . Y de hecho es fácil ver que es el polinomio no nulo mónico

de grado menor que anula a A , pues si $h \in K[\lambda]$ es tal que

$$0 = h(A) = \begin{bmatrix} h(\lambda_1) & & \\ & h(\lambda_1) & \\ & & h(\lambda_2) & \\ & & & h(\lambda_2) \end{bmatrix} \Rightarrow \begin{aligned} &h(\lambda_1) = h(\lambda_2) = 0 \\ &\Rightarrow \lambda_1, \lambda_2 \text{ son raíces de } h \\ &\Rightarrow (\lambda - \lambda_1)(\lambda - \lambda_2) \mid h. \end{aligned}$$

↑
polinomio
minimal
de A

Proposición - Definición (Polinomio minimal de una matriz)

Sea $A \in K^{n \times n}$. Entonces existe un único polinomio m_A en $K[\lambda]$ no nulo y mónico que satisface $m_A(A) = 0$ y que además divide a cualquier

polinomio en $K[\lambda]$ que anula a A , es decir:

Si $h \in K[\lambda]$ es tal que $h(A) = 0$, entonces $m_A \mid h$ en $K[\lambda]$.

En particular $m_A \in K[\lambda]$ es el polinomio mónico de grado mínimo que anula a A . Se llama el polinomio minimal de A .

Demostación: Es una consecuencia del hecho que $K[\lambda]$ tiene algoritmo de división (es lo que se llama un dominio euclideo)

Sea $\mathcal{P} = \{ h \in K[\lambda] : h(A) = 0 \}$. Sabemos que $\mathcal{P} \neq \{0\}$

pues por ejemplo $\chi_A(\lambda) \in \mathcal{P}$. (observar $h \in \mathcal{P} \iff ch \in \mathcal{P}, \forall c \in K$)

Luego existe en $\mathcal{P}$ algún polinomio m_A no nulo (y mónico) de grado más chico (sentido entero) que todos los demás polinomios no nulos en $\mathcal{P}$. Es decir existe $m_A \in \mathcal{P}$ no nulo y mónico tq si $h \in \mathcal{P}$ es no nulo, entonces $\text{gr}(m_A) \leq \text{gr}(h)$.

Se afirma que $m_A \mid h, \forall h \in \mathcal{P}$:

Aplicando el algoritmo de división:

$$h = q \cdot m_A + r \quad \text{con} \quad r=0 \quad \text{ó} \quad r \neq 0 \text{ y } \text{gr}(r) < \text{gr}(m_A)$$

$$\begin{aligned} \text{Pero } h(A) &= (q \cdot m_A + r)(A) = q(A) \underbrace{m_A(A)}_{\leftarrow m_A \in \mathcal{P}} + r(A) \Rightarrow \\ h \in \mathcal{P} &\rightarrow 0 = 0 + r(A) \Rightarrow r(A) = 0 \end{aligned}$$

Pero si $r \neq 0$, $\text{gr}(r) \geq \text{gr}(m_A)$ pues m_A era uno de grado más chico

Luego la única posibilidad es $r=0$, o sea $m_A \mid h$.

En particular m_A es el único mónico de su grado que anula a A pues $m_A \mid h$ y $\text{gr}(m_A) = \text{gr}(h) \Rightarrow h = c m_A$ con $c \in K$ \(\square\)

Ejemplos

① $D = \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_r \\ & & & 0 \end{bmatrix} \in K^{n \times n}, \quad \text{con } d_i \neq d_j \text{ si } i \neq j.$

$\begin{matrix} \uparrow m_1 \\ \downarrow \\ \uparrow m_r \\ \downarrow \end{matrix}$

Entonces $m_D(\lambda) = (\lambda - d_1) \dots (\lambda - d_r)$
(Comparar con $\chi_D(\lambda) = (\lambda - d_1)^{m_1} \dots (\lambda - d_r)^{m_r}$)

② $N = \begin{bmatrix} 0 & & \\ 1 & \ddots & \\ & & 1 & 0 \end{bmatrix} \in K^{n \times n}$

Aquí $\chi_N(\lambda) = \lambda^n$ y sabemos $m_N(\lambda) \mid \chi_N(\lambda)$,
luego $m_N(\lambda) = \lambda^k$ para algún $k \leq n$

A mano (luego veremos otra forma de pensarlo)

(3)

$$N^2 = \begin{bmatrix} 0 & & & \\ 0 & \ddots & & \\ 1 & & \ddots & \\ & & & 0 \end{bmatrix}, N^3 = \begin{bmatrix} 0 & & & \\ 0 & \ddots & & \\ 0 & 1 & & \\ & & \ddots & \\ & & & 0 \end{bmatrix}, \dots, N^{n-1} = \begin{bmatrix} 0 & & & \\ & \ddots & & \\ & & 1 & \\ & & & 0 \end{bmatrix}, N^n = 0$$

(Se van cayendo los 1 a una diagonal más abajo cada vez)

Luego $N^n = 0$ pero $N^{n-1} \neq 0$. Es decir $\chi^m(N) = 0$ pero $\chi^{n-1}(N) \neq 0$.

Esto implica $m_N(\lambda) = \chi^n = \chi_N(\lambda)$.

③ Sea $J = \begin{bmatrix} \lambda_0 & & & \\ & \ddots & & \\ 1 & & \ddots & \\ & & & 1 & \lambda_0 \end{bmatrix} \in K^{n \times n}$ con $\lambda_0 \neq 0$

Entonces $m_J = \chi_J = (\lambda - \lambda_0)^n$ pues sabemos que $m_J \mid \chi_J$ y

si hacemos $N = J - \lambda_0 \text{Id}_n$ se tiene $m_N = \chi^m$: $N^m = 0$ y $N^{m-1} \neq 0$

$\Rightarrow (J - \lambda_0 \text{Id}_n)^m = 0$ y $(J - \lambda_0 \text{Id}_n)^{m-1} \neq 0$, i.e. $(\lambda - \lambda_0)^m(J) = 0$ y $(\lambda - \lambda_0)^{m-1}(J) \neq 0$.

El polinomio característico se comportaba bien con la semejanza. Pasa lo mismo con el polinomio minimal, y esto nos va a permitir hablar de minimal de un endomorfismo (en dimensión finita)

Proposición (Minimal y semejanza)

Sean $A, B \in K^{n \times n}$. Entonces: $A \simeq B \Rightarrow m_A = m_B$

Demostración

Ya vimos que si $A \simeq B$ y $h \in K[\lambda]$, entonces $h(A) \simeq h(B)$

Luego si $A \simeq B$, $h(A) = 0 \Leftrightarrow h(B) = 0$

(pues $0 = h(A) \simeq h(B) \Rightarrow h(B) = 0$ y vice-versa)

Luego $m_A = m_B$ (pues el polinomio mónico de grado mínimo que anula a los dos es el mismo). (Obviamente no vale la recíproca) $\square$

En particular si $A \simeq D$ o $A \simeq J$ arriba, $m_A = (\lambda - \lambda_1)^{m_1} \dots (\lambda - \lambda_r)^{m_r}$, o $m_A = \lambda^m$.

Definición (Minimal de un endomorfismo)

Sea V un K -e.v. de dim. finita y sea $f \in \text{End}_K(V)$. Entonces el polinomio minimal de f es el polinomio

$m_f := m_{[f]_{\mathcal{B}}} \in K[\lambda]$ donde $\mathcal{B}$ es cualquier base de V

El polinomio minimal de f cumple:

① $m_f(f)$ es el endomorfismo nulo, i.e. $m_f(f)(v) = 0, \forall v \in V$
pues sabemos que $\forall h \in K[\lambda], [h(f)]_{\beta} = h([f]_{\beta})$,
luego, si $A = [f]_{\beta}$, se tiene $[m_f(f)]_{\beta} = m_A(A) = 0 \in K^{n \times n}$,
o sea $m_f(f) = 0$.

② $m_f \mid h, \forall h \in K[\lambda] / h(f) = 0$.

pues $[h(f)]_{\beta} = 0 \Leftrightarrow h([f]_{\beta}) = 0$ luego $m_f = m_A \mid h$.
 m_f es el polinomio mónico (no nulo) de menor grado que anula a f

Subespacio cíclico generado por v y polinomio minimal de un vector

¿Cuál es el menor subespacio f -invariante que contiene a algún $v \in V$?

S f -invariante y $v \in S \Rightarrow f(v) \in S, f^2(v) \in S, \dots, f^k(v) \in S, \forall k \in \mathbb{N}$

Luego $\langle v, f(v), \dots, f^k(v), \dots \rangle \subseteq S$.

claramente f -invariante también. Luego:

Definición (Subespacio cíclico)

Sea V un K -e.v., $f \in \text{End}_K(V)$ y $v \in V$.

El **subespacio cíclico generado por v** para f es el subespacio

$$\langle v \rangle_f := \langle v, f(v), f^2(v), \dots, f^k(v), \dots \rangle \subseteq V$$

(Si $\langle v \rangle_f = V$, se dice que v es un **vector cíclico** de V)

Este es el menor subespacio f -invariante que contiene a $v \in V$.

Observación Si $\dim_K(V) = n$, como $\{v, f(v), \dots, f^n(v)\}$ es claramente l.d., existe $k \leq n$ t.q. $\{v, f(v), \dots, f^{k-1}(v)\}$ es l.i. pero $f^k(v) \in \langle v, f(v), \dots, f^{k-1}(v) \rangle$.

En ese caso, inductivamente, $f^{k+j}(v) \in \langle v, f(v), \dots, f^{k-1}(v) \rangle, \forall j \geq 0$

pues para $j=0$ ya lo sabemos, y para $j > 0$, si lo sabemos hasta $k+j-1$:

si $f^k(v) = a_0 v + a_1 f(v) + \dots + a_{k-1} f^{k-1}(v)$, entonces

$$f^{k+j}(v) = f^j \circ f^k(v) = a_0 f^j(v) + a_1 f^{j+1}(v) + \dots + a_{k-1} f^{j+k-1}(v)$$

Pero por HI, como $j = k+j-k, \dots, j+k-1 = k+j-1$,

$f^j(v), \dots, f^{j+k-1}(v) \in \langle v, \dots, f^{k-1}(v) \rangle$ luego $f^{k+j}(v) \in \langle v, \dots, f^{k-1}(v) \rangle$

Hemos probado:

Proposición (Subespacio cíclico)

Sea V un K -e.v. de dim finita, $f \in \text{End}_K(V)$ y $v \in V$. Sea k el menor número t.q. $\{v, f(v), \dots, f^{k-1}(v)\}$ es l.i. y $f^k(v) \in \langle v, \dots, f^{k-1}(v) \rangle$. Entonces

$$\langle v \rangle_f = \langle v, f(v), \dots, f^{k-1}(v) \rangle \text{ y } \{v, \dots, f^{k-1}(v)\} \text{ base de } \langle v \rangle_f.$$

Definición (Polinomio minimal de un vector para f)

(5)

Sea V un K -e.v. de dim finita, sea $f \in \text{End}_K(V)$ y $v \in V$.

Sea $\langle v \rangle_f = \{v, f(v), \dots, f^{k-1}(v)\}$, con $\{v, \dots, f^{k-1}(v)\}$ li,

y sean $a_0, \dots, a_{k-1} \in K$ t q $f^k(v) = a_{k-1}f^{k-1}(v) + \dots + a_1f(v) + a_0v$

Se define el **polinomio minimal de v para f** como el polinomio

$$m_v(\lambda) = \lambda^k - a_{k-1}\lambda^{k-1} - \dots - a_1\lambda - a_0 \in K[\lambda]$$

Propiedades

① $m_v(f)(v) = 0$, i.e. $(f^k - a_{k-1}f^{k-1} - \dots - a_1f - a_0\text{id}_V)(v) = 0$
pues $(f^k - a_{k-1}f^{k-1} - \dots - a_0\text{id}_V)(v) = f^k(v) - a_{k-1}f^{k-1}(v) - \dots - a_0v = 0$

② $m_v(\lambda)$ es el polinomio mónico (no nulo) de menor grado en $K[\lambda]$ t q $m_v(f)$ anula a v
pues si $h(\lambda) = \lambda^d + b_{d-1}\lambda^{d-1} + \dots + b_0 \in K[\lambda]$ es t q $h(f)(v) = 0$,
entonces $f^d(v) + b_{d-1}f^{d-1}(v) + \dots + b_0v = 0 \Rightarrow f^d(v) \in \langle v, \dots, f^{d-1}(v) \rangle$
 $\Rightarrow d \geq k$ (pues $\{v, \dots, f^{k-1}(v)\}$ era li.

③ Más que eso: $m_v(f)(w) = 0$, $\forall w \in \langle v \rangle_f$
pues $m_v(f)$ anula no solo a v sino también a $f(v), \dots, f^{k-1}(v)$:
 $m_v(f)(f^d(v)) = (m_v(f) \circ f^d)(v) = (f^d \circ m_v(f))(v) = f^d(m_v(f)(v)) = f^d(0) = 0$
Luego $m_v(f)$ se anula en todo $\langle v \rangle_f$, y al ser el de menor grado que se anula en v , es el de menor grado que se anula en todo $\langle v \rangle_f$.

④ Sea $h(\lambda) \in K[\lambda]$. Entonces $h(f)(v) = 0 \iff m_v \mid h$ en $K[\lambda]$
(En particular $m_v \mid m_f$ en $K[\lambda]$)

$(\Rightarrow)$ Nuevamente por el algoritmo de división en $K[\lambda]$: $h = q m_v + r$
con $r = 0$ ó $\text{gr}(r) < \text{gr}(m_v) \Rightarrow h(f) = q(f) \circ m_v(f) + r(f) \Rightarrow$

$h(f)(v) = (q(f) \circ m_v(f))(v) + r(f)(v)$. Luego $h(f)(v) = m_v(f)(v) = 0$
 $\Rightarrow r(f)(v) = 0$ pero m_v era de grado mínimo no nulo, luego $r = 0$

$(\Leftarrow)$ Está implícito arriba: si $h = q m_v$, entonces $h(f)(v) = q(f) \circ m_v(f)(v) = q(f)(0) = 0$. Finalmente está claro que $m_f(f)(v) = 0$ pues $m_f(f) = 0$.

Esto implica el resultado muy útil siguiente:

Proposición (Minimal de f vs minimal de base)

Sea V un K -e.v. de dim finita n , $f \in \text{End}_K(V)$ y $\mathcal{B} = \{v_1, \dots, v_n\}$ base de V .

Entonces

$$m_f = \text{mcm}(m_{v_1}, \dots, m_{v_n})$$

↑
mínimo común múltiplo

Demostración: Ambos polinomios son mónicos. Alcanza con probar que se (6)

dividen mutuamente. Sea $h := \text{mcm}(m_{v_1}, \dots, m_{v_n})$.

• $m_{v_1} \mid m_f, \dots, m_{v_n} \mid m_f \Rightarrow h \mid m_f$

• $v = k_1 v_1 + \dots + k_n v_n \Rightarrow h(f)(v) = k_1 h(f)(v_1) + \dots + k_n h(f)(v_n) = 0$
 pues $m_{v_i} \mid h, \forall i$, luego $h(f) = 0 \Rightarrow m_f \mid h$ □

Observación

Para $A \in K^{n \times n}$, $m_A = \text{mcm}(m_{e_1}, \dots, m_{e_n})$

Ejemplos

① Ejemplo 2 revisitado

$N = \begin{bmatrix} 0 & & & \\ 1 & & & \\ & \ddots & & \\ & & 1 & 0 \end{bmatrix} \in K^{n \times n}$. Entonces $m_N = \lambda^n = \chi_N$

pues sabemos que $m_N \mid \chi_N = \lambda^n$. Pero por otro lado $m_{e_1} \mid m_N$ y

como $e_1 \xrightarrow{N} e_2 \xrightarrow{N} \dots \xrightarrow{N} e_{n-1} \xrightarrow{N} e_n \xrightarrow{N} 0$, se tiene

$\langle e_1 \rangle_N = \langle e_1, e_2, \dots, e_n \rangle$ y recién $N^n \cdot e_1 = 0$, es decir $m_{e_1} = \lambda^n$
 luego $\lambda^n \mid m_N \mid \lambda^n \Rightarrow m_N = \lambda^n$.

Observación

• si $w \in \langle v \rangle_f$, entonces $m_w \mid m_v$

pues probamos antes que $\underbrace{m_v(f)}_h(w) = 0$, luego $m_w \mid m_v$

• si $V = \langle v \rangle_f \oplus \langle w \rangle_f$, entonces $m_f = \text{mcm}(m_v, m_w)$

② $A = \begin{bmatrix} 0 & & & \\ 1 & & & \\ & \ddots & & \\ & & 1 & 0 \end{bmatrix} \begin{matrix} \uparrow r \\ \downarrow s \end{matrix} \in K^{n \times n}$, con $r \geq s$

Entonces $m_A = \lambda^r$ pues $m_{e_1} = m_{\langle e_1 \rangle} = \lambda^r$ y $m_{e_{r+1}} = m_{\langle e_{r+1} \rangle} = \lambda^s$

③ Sea $A \simeq \begin{bmatrix} \lambda_1 & & & \\ 1 & & & \\ & \ddots & & \\ & & 1 & d_1 \end{bmatrix} \begin{matrix} \uparrow r \\ \downarrow s \end{matrix} \in K^{n \times n}$, con $r \geq s$

Entonces $m_A = (\lambda - d_1)^r$ (haciendo $N = A - d_1 \text{Id}$)

④ Sea $A = \begin{bmatrix} \lambda_1 & & & \\ & \ddots & & \\ & & \lambda_1 & \\ & & & \ddots \\ & & & & \lambda_2 \\ & & & & & \ddots \\ & & & & & & \lambda_2 \\ & & & & & & & \ddots \end{bmatrix}$ con $\lambda_1 \neq \lambda_2$, entonces $m_A = (\lambda - \lambda_1)^r (\lambda - \lambda_2)^s = \chi_A$

⑤ $N = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$. Entonces $\chi_N(\lambda) = \lambda^4$ y $m_N(\lambda) = \lambda^3$

$e_1 \xrightarrow{N} e_3 + e_4 \xrightarrow{N} e_4 \xrightarrow{N} 0 : N^3 e_1 = 0$ y $N^2 e_1 \neq 0 \Rightarrow m_{e_1} = \lambda^3$

$e_2 \xrightarrow{N} e_3 \xrightarrow{N} e_4 \xrightarrow{N} 0 : N^3 e_2 = 0$ y $N^2 e_2 \neq 0 \Rightarrow m_{e_2} = \lambda^3$

$e_3 \xrightarrow{N} e_4 \xrightarrow{N} 0 : m_{e_3} = \lambda^2$ y $e_4 \xrightarrow{N} 0 : m_{e_4} = \lambda$

luego $m_N = \text{mcm}(m_{e_1}, \dots, m_{e_4}) = \lambda^3$

⑥ La matriz compañera de un polinomio (Ejercicio 7 de la práctica)

Sea $h(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \dots + a_1\lambda + a_0 \in K[\lambda]$

y sea $\mathcal{C}_h \in K^{n \times n}$ la matriz compañera de h , i.e.

$$\mathcal{C}_h = \begin{bmatrix} 0 & & & -a_0 \\ 1 & & & -a_1 \\ & \ddots & & \vdots \\ & & 0 & -a_{n-2} \\ & & 1 & -a_{n-1} \end{bmatrix}$$

Entonces $m_{\mathcal{C}_h} = h = \chi_{\mathcal{C}_h}$

Para terminar:

Proposición (minimal y características)

Sea V un K -e.v. de dim. finita n y sea $f \in \text{End}_K(V)$

① Sea $\lambda_0 \in K$ un autovalor de f . Entonces $\lambda - \lambda_0 \mid m_f$

② Sup $\chi_f(\lambda) = (\lambda - \lambda_1)^{m_1} \dots (\lambda - \lambda_r)^{m_r}$ con $\lambda_1, \dots, \lambda_r \in K$ (distintos).

Entonces $m_f(\lambda) = (\lambda - \lambda_1)^{k_1} \dots (\lambda - \lambda_r)^{k_r}$ con $1 \leq k_i \leq m_i, \forall i$.

Demostación

① si $v \in K^n$ es autovector de λ_0 , $f(v) = \lambda_0 v \Rightarrow (f - \lambda_0 \text{id}_V)(v) = 0$

$\Rightarrow m_v \mid \lambda - \lambda_0$ pero $m_v \neq 1 \Rightarrow m_v = \lambda - \lambda_0 \mid m_f$.

② $\lambda - \lambda_1 \mid m_f, \dots, \lambda - \lambda_r \mid m_f \Rightarrow (\lambda - \lambda_1) \dots (\lambda - \lambda_r) \mid m_f$

Pero $m_f \mid \chi_f \Rightarrow k_i \leq m_i, \dots, k_r \leq m_r$. $\square$