Álgebra Lineal - Clase 14

Gabriela Jeronimo

FCEN-UBA

Segundo cuatrimestre 2020

Esquema de la clase

- Polinomio minimal de una transformación lineal.
- Teorema de Hamilton-Cayley.
- Criterio de diagonalización vía polinomio minimal.
- Subespacios invariantes.

Bibliografía recomendada.

G. Jeronimo, J. Sabia, S. Tesauri. *Algebra Lineal*. Cursos de Grado. Fascículo 2. Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, 2008.

Capítulo 6 (Secciones 6.3 y 6.4).

Polinomio minimal de una transformación lineal

Proposición.

Sean $A, B \in K^{n\times n}$, $A \sim B$. Entonces, $\forall P \in K[X]$, $P(A) \sim P(B)$.
En particular, $P(A) = 0 \iff P(B) = 0$.

Demostración.

$A \sim B \Rightarrow \exists C \in GL(n, K)$ tal que $A = C.B.C^{-1}$.
$\Rightarrow \forall k \in \mathbb{N}$, $A^k = C.B^k.C^{-1}$
(inducción: $A^{k+1} = A.A^k = C.B.C^{-1}.C.B^k.C^{-1} = C.B^{k+1}.C^{-1}$)
Sea $P \in K[X]$, $P = \sum\limits_{i=0}^{r} a_i X^i$.

$$\begin{aligned} P(A) &= P(C.\,B.\,C^{-1}) = \sum_{i=0}^{r} a_i.(C.\,B.\,C^{-1})^i \\ &= \sum_{i=0}^{r} a_i.\,C.\,B^i.\,C^{-1} = C.\Big(\sum_{i=0}^{r} a_i B^i\Big).\,C^{-1} \\ &= C.\,P(B).\,C^{-1}. \end{aligned}$$

$\Rightarrow P(A) \sim P(B)$. $\square$

Corolario.
Sean $A, B \in K^{n\times n}$, $A \sim B$. Entonces $m_A = m_B$.

No vale la recíproca:

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \text{ y } B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

cumplen que $m_A = m_B = X^2 - 1$, pero $A \not\sim B$.

Observación.
Sea V un K-e.v. de dimensión finita, y sea $f : V \to V$ una t.l.
El polinomio minimal de f se obtiene como $m_f = m_{|f|_B}$ para B una base (cualquiera) de V.

Polinomio minimal de un vector

Sea $A \in K^{n\times n}$. Para $v \in K^n$, dado $P \in K[X]$, definimos $P(v) = P(A).v$. Decimos que P anula a v si $P(v) = 0$.

Observación.
Para todo $v \in K^n$, m_A anula a v: en efecto,
$m_A(v) = m_A(A).v = 0.v = 0$.

Definición.
Sea $A \in K^{n\times n}$ y sea $v \in K^n$. El polinomio minimal de v (asociado a A), que notaremos $m_{A,v}$ o simplemente m_v, es el polinomio mónico de grado mínimo en $K[X]$ que anula a v.

Existencia y unicidad se prueban como para m_A.

Ejemplos.

1. Sean $A \in K^{n\times n}$ y $v \in K^n$ un autovector de A de autovalor λ.
   Entonces $m_v = X - \lambda$.
   En efecto, si $P = X - \lambda$, entonces $P(v) = (A - \lambda I).v = 0$.

2. Sean $A = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} \in \mathbb{R}^{2\times 2}$ y $e_1 = (1,0)$. Calcular m_{e_1}.

- $\mathrm{gr}(P) = 1$: $P = X + a_0 \in \mathbb{R}[X]$.

$$\begin{aligned} P(e_1) = 0 &\iff (A + a_0 I_2).e_1 = 0 \\ &\iff A.e_1 + a_0.e_1 = 0 \\ &\iff (-1,1) + a_0(1,0) = (0,0). \quad \text{Abs!} \end{aligned}$$

$\Rightarrow \nexists P$ tal que $P(e_1) = 0$ y $\mathrm{gr}(P) = 1$.

- $\mathrm{gr}(P) = 2$: $P = X^2 + a_1 X + a_0$.

$$\begin{aligned} P(e_1) = 0 \quad &\iff \quad (A^2 + a_1 A + a_0 I_2).e_1 = 0 \\ &\iff \quad A^2 e_1 + a_1.Ae_1 + a_0.e_1 = 0 \\ &\iff \quad (1,-2) + a_1(-1,1) + a_0(1,0) = (0,0) \\ &\iff \quad a_1 = 2,\ a_0 = 1. \end{aligned}$$

$\Rightarrow m_{e_1} = X^2 + 2X + 1.$

Proposición.

Sean $A \in K^{n \times n}$, $v \in K^n$ y $P \in K[X]$. Entonces:
$P(v) = 0 \iff m_v \mid P$. En particular, $m_v \mid m_A$.

Proposición.

Sea $A \in K^{n \times n}$ y sea $B = \{v_1, \dots, v_n\}$ una base de K^n. Entonces $m_A = \text{mcm}\{m_{v_i} : i = 1, \dots, n\}$ (mcm = mínimo común múltiplo).

Demostración.

Sea $P = \text{mcm}\{m_{v_i} : i = 1, \dots, n\}$.

$m_{v_i} \mid m_A \ \forall 1 \leq i \leq n \Rightarrow P \mid m_A$.

$\forall 1 \leq i \leq n$, $m_{v_i} \mid P \Rightarrow P(A).v_i = 0$.
Sea $v \in K^n$ y sean $\alpha_1, \dots, \alpha_n \in K$ tales que $v = \sum_{i=1}^n \alpha_i v_i$.
$P(A).v = P(A)\Big(\sum_{i=1}^n \alpha_i . v_i\Big) = \sum_{i=1}^n \alpha_i P(A).v_i = 0$.

$P(A) \in K^{n \times n}$ y $P(A).v = 0 \ \forall\, v \in K^n \Rightarrow P(A) = 0 \Rightarrow m_A \mid P$.

m_A y P son mónicos y se dividen mutuamente $\Rightarrow m_A = P$. $\square$

Ejemplo. Calcular m_A para $A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$.

Sea $E = \{e_1, e_2, e_3\}$ la base canónica de $\mathbb{R}^3$.

$m_A = \text{mcm}\{m_{e_1}, m_{e_2}, m_{e_3}\}$.

m_{e_1}: $\{e_1, Ae_1\} = \{e_1, e_1 + e_2\}$ es l.i.,

$\{e_1, Ae_1, A^2e_1\} = \{e_1,\ e_1 + e_2,\ e_1 + 2e_2\}$ es l.d:

$0 = (e_1 + 2e_2) - 2.(e_1 + e_2) + e_1 = A^2e_1 - 2.Ae_1 + e_1$.

$\Rightarrow m_{e_1} = X^2 - 2X + 1 = (X-1)^2$.

m_{e_2}: $Ae_2 = e_2 \Rightarrow m_{e_2} = X - 1$.

m_{e_3}: $Ae_3 = 2.e_3 \Rightarrow m_{e_3} = X - 2$.

$\Rightarrow m_A = \text{mcm}\{(X-1)^2, X-1, X-2\} = (X-1)^2(X-2)$.

Teorema de Hamilton-Cayley

Teorema (Hamilton-Cayley)

Sea $A \in K^{n\times n}$. Entonces $m_A \mid \mathcal{X}_A$. (Es decir, $\mathcal{X}_A(A) = 0$).

Demostración.

Sea $v \in K^n$, $v \neq 0$. Supongamos que $\{v, Av, \dots, A^k v\}$ es l.i. y que $A^{k+1}v + a_k A^k v + \cdots + a_1 Av + a_0 v = 0$.
$\Rightarrow m_v = X^{k+1} + a_k X^k + \cdots + a_1 X + a_0$.
Sea $f_A : K^n \to K^n$, $f_A(x) = A.x$.
$\{v, Av, \dots, A^k v\} = \{v, f_A(v), \dots, f_A^k(v)\}$ es l.i.
Extendemos a $B = \{v, f_A(v), \dots, f_A^k(v), w_{k+2}, \dots, w_n\}$ base de K^n.

$$|f_A|_B = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 & \\ 1 & 0 & & 0 & -a_1 & \\ 0 & 1 & & \vdots & \vdots & M \\ \vdots & & \ddots & 0 & -a_{k-1} & \\ 0 & \dots & 0 & 1 & -a_k & \\ & & \mathbb{O} & & & N \end{pmatrix}.$$

$\mathcal{X}_A = \mathcal{X}_{f_A} = \mathcal{X}_{|f_A|_B} =$

$$
\begin{aligned}
&= \det \left(\begin{array}{ccccc|c}
X & 0 & \dots & 0 & a_0 & \\
-1 & X & & 0 & a_1 & \\
0 & -1 & & \vdots & \vdots & -M \\
\vdots & & \ddots & X & a_{k-1} & \\
0 & \dots & & -1 & X + a_k & \\
 & & \mathbb{O} & & & X.\, I_{n-k-1} - N
\end{array} \right) \\
&= (X^{k+1} + a_k X^k + \cdots + a_1 X + a_0).\, \det(X.I_{n-k-1} - N) \\
&= m_v.\, \det(X.I_{n-k-1} - N).
\end{aligned}
$$

$\Rightarrow m_v \mid \mathcal{X}_A \ \forall v \in K^n$.

$E = \{e_1, \dots, e_n\}$ base canónica de K^n.

$m_{e_i} \mid \mathcal{X}_A \ \forall 1 \leq i \leq n \Rightarrow m_A = \mathrm{mcm}\{m_{e_1}, \dots, m_{e_n}\} \mid \mathcal{X}_A$. $\square$

Consecuencias.

Sea $A \in K^{n\times n}$. Entonces:

- $\mathrm{gr}(m_A) \leq n$.
- $\mathrm{gr}(m_A) = n \Rightarrow m_A = \mathcal{X}_A$.
- $\exists v \in K^n$ tal que $\mathrm{gr}(m_v) = n \Rightarrow m_v = m_A = \mathcal{X}_A$.

Observación.

$A \in GL(n, K) \Rightarrow A^{-1} \in < I_n, A, A^2, \dots, A^{n-1} >$.

Si $\mathcal{X}_A = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$, por el Teorema de Hamilton-Cayley,

$$A^n + a_{n-1}A^{n-1} + \cdots + a_1 A + a_0 I_n = 0.$$

$a_0 = \mathcal{X}_A(0) = \det(0.I_n - A) = \det(-A) = (-1)^n \det(A) \neq 0$, porque A es inversible.

$$\begin{aligned} I_n &= -a_0^{-1}.(A^n + a_{n-1}A^{n-1} + \cdots + a_2A^2 + a_1A) \\ &= \underbrace{-a_0^{-1}.(A^{n-1} + a_{n-1}A^{n-2} + \cdots + a_2A + a_1 I_n)}_{=A^{-1}}.A. \end{aligned}$$

Criterio de diagonalización vía polinomio minimal

Si $A \in K^{n\times n}$ y $\mathcal{X}_A \in K[X]$ se factoriza linealmente en $K[X]$ y tiene todas sus raíces simples, entonces A es diagonalizable.
No vale la recíproca: por ejemplo, $A = I_n$ es diagonalizable y $\mathcal{X}_A = (X-1)^n$ tiene raíces múltiples.

Proposición.

Sea $A \in K^{n\times n}$. Entonces A es diagonalizable en $K^{n\times n}$ si y sólo si m_A se factoriza linealmente en $K[X]$ y todas sus raíces son simples.

Demostración.
$(\Rightarrow)$ Supongamos que A es diagonalizable.
Sean $\lambda_1, \ldots, \lambda_r$ los autovalores de A, $\lambda_i \neq \lambda_j$ si $i \neq j$ y sea $\{v_1, \ldots, v_n\}$ base de K^n de autovectores de A.

$$\begin{aligned} m_A &= \mathrm{mcm}\{m_{v_1}, \ldots, m_{v_n}\} \\ &= \mathrm{mcm}\{X-\lambda_1, \ldots, X-\lambda_1, \ldots, X-\lambda_r, \ldots, X-\lambda_r\} \\ &= (X-\lambda_1)(X-\lambda_2)\ldots(X-\lambda_r) \end{aligned}$$

$(\Leftarrow)$ Supongamos $m_A = (X-\lambda_1)\dots(X-\lambda_r)$ con $\lambda_i \neq \lambda_j$ si $i \neq j$.
$\Rightarrow \lambda_1, \dots, \lambda_r$ son todos los autovalores de A en K.
Veamos que $K^n = \bigoplus_{i=1}^{r} E_{\lambda_i}(A)$, con $E_{\lambda_i}(A) = \{v \in K^n \mid Av = \lambda_i v\}$.
Sea $v \in K^n - \{0\}$. Consideremos el subespacio
$S = < v, Av, A^2v, \dots, A^m v, \dots > \subseteq K^n$.

Supongamos que $m_v = X^{k+1} + a_k X^k + \dots + a_1 X + a_0$.
$\Rightarrow \{v, Av, \dots, A^k v\}$ es l.i. y $A^{k+1}v \in < v, Av, A^2v, \dots, A^k v >$
$\Rightarrow A^j v \in < v, Av, \dots, A^k v > \forall j \in \mathbb{N}$
$\Rightarrow B_S = \{v, Av, \dots, A^k v\}$ es una base de S.

Sea $f_A : S \to S$, $f_A(x) = A.x$ $(x \in S \Rightarrow Ax \in S)$.

$$|f_A|_{B_S} = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & & \vdots & -a_1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \vdots & \ddots & 0 & -a_{k-1} \\ 0 & 0 & \dots & 1 & -a_k \end{pmatrix}.$$

$\mathcal{X}_{f_A} = X^{k+1} + a_k X^k + \dots + a_1 X + a_0 = m_v$.

$\mathcal{X}_{f_A} = m_v \mid m_A$ y $m_A = (X - \lambda_1) \dots (X - \lambda_r)$ con $\lambda_i \neq \lambda_j$ si $i \neq j$
$\Rightarrow \mathcal{X}_{f_A} = (X - \lambda_{i_1}) \dots (X - \lambda_{i_{k+1}})$ en $K[X]$ y sus raíces son simples.

$\Rightarrow f_A : S \to S$ es diagonalizable $\Rightarrow S = \bigoplus_{j=1}^{k+1} E_{\lambda_{i_j}}(f_A)$

$v \in S \Rightarrow \exists\ v_{i_j} \in E_{\lambda_{i_j}}(f_A)$, $1 \leq j \leq k+1$: $v = v_{i_1} + \dots + v_{i_{k+1}}$.
$v_{i_j} \in E_{\lambda_{i_j}}(f_A)$ (autovector de f_A de autovalor λ_{i_j})
$\Rightarrow Av_{i_j} = f_A(v_{i_j}) = \lambda_{i_j} v_{i_j} \Rightarrow v_{i_j} \in E_{\lambda_{i_j}}(A)$ (autovector de A).

$\Rightarrow v \in \bigoplus_{i=1}^{r} E_{\lambda_i}(A)$.

Luego, $K^n = \bigoplus_{i=1}^{r} E_{\lambda_i}(A)$. $\square$

Ejemplo.
Sea $A \in \mathbb{C}^{n \times n}$ tal que $A^k = I_n$ para algún $k \in \mathbb{N}$. Entonces A es diagonalizable.

$A^k - I_n = 0 \Rightarrow X^k - 1$ anula a $A \Rightarrow m_A \mid X^k - 1$.
$X^k - 1$ tiene todas sus raíces en $\mathbb{C}$ y son simples $\Rightarrow m_A$ también.
Luego, A es diagonalizable.

Subespacios invariantes

Definición.
Sea V un K-e.v. y sea $f : V \to V$ una t.l. Un subespacio $S \subseteq V$ se dice invariante por f o f-invariante si $f(S) \subseteq S$.

Ejemplo.

$$A = \begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & -1 & 3 \end{pmatrix}, \ f_A : \mathbb{R}^4 \to \mathbb{R}^4, \ f_A(x) = A.x.$$

Si $E = \{e_1, e_2, e_3, e_4\}$ es la base canónica de $\mathbb{R}^4$, algunos subespacios invariantes por f_A son:

- $S_1 = < e_1 >$, ya que $f_A(e_1) = -e_1 \in S_1$
- $S_2 = < e_1, e_2 >$:
  $f_A(e_1) = -e_1 \in S_2$ y $f_A(e_2) = e_1 - e_2 \in S_2$
- $S_3 = < e_3, e_4 >$:
  $f_A(e_3) = 2e_3 - e_4 \in S_3$ y $f_A(e_4) = e_3 + 3e_4 \in S_3$
- $S_4 = < e_1, e_3, e_4 > = S_1 + S_3$.

Proposición.

Sean V un K-e.v y $f : V \to V$ una t.l. Entonces:

- $\mathrm{Nu}(f)$ e $\mathrm{Im}(f)$ son subespacios f-invariantes de V.
- S subespacio f-invariante de V de dimensión 1 $\iff$ $S = < v >$ con $v \in V$ autovector de f.
- S y T subespacios f-invariantes de $V \Rightarrow S \cap T$ y $S + T$ subespacios f-invariantes de V.

Observación.

$f : V \to V$ t.l., $S \subset V$ subespacio invariante por f
$\Rightarrow$ la restricción de f a S, que notamos $f_{|_S}$, es una t.l. de S en S.

Proposición.

Sean V un K-.v. de dimensión finita, $f : V \to V$ una t.l. y $S \subseteq V$ un subespacio invariante por f. Si $f_{|_S} : S \to S$ es la restricción:

i) $m_{f_{|_S}} \mid m_f$.

ii) $\mathcal{X}_{f_{|_S}} \mid \mathcal{X}_f$.

Demostración.

Sean $n = \dim V$ y $s = \dim S$. Sean $B_S = \{v_1, \dots, v_s\}$ una base de S y $v_{s+1}, \dots, v_n \in V$ tales que $B = \{v_1, \dots, v_s, v_{s+1}, \dots, v_n\}$ es una base de V.

i) $m_{f_{|S}} = \text{mcm}\{m_{v_1}, \dots, m_{v_s}\}$.
$m_{v_i} \mid m_f \ \forall 1 \leq i \leq s \Rightarrow$ el mcm de estos polinomios también lo divide, es decir, $m_{f_{|S}} \mid m_f$.

ii) Para la base B, se tiene que

$$|f|_B = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \in K^{n\times n}, \text{ con } A = |f_{|S}|_{B_S} \in K^{s\times s}.$$

$$\begin{aligned} \mathcal{X}_f = \mathcal{X}_{|f|_B} &= \det \begin{pmatrix} X.I_s - A & -B \\ 0 & X.I_{n-s} - C \end{pmatrix} \\ &= \det(X.I_s - A).\det(X.I_{n-s} - C) \ = \ \mathcal{X}_{f_{|S}}.Q, \end{aligned}$$

$\Rightarrow \mathcal{X}_{f_{|S}} \mid \mathcal{X}_f$. □