Álgebra Lineal (R211 - CE9)
2024

4.3 El polinomio minimal

Para una matriz cuadrada tenemos asociado un very important polynomial, el polinomio característico, que nos sirve para hallar los autovalores (son sus raíces) y caracterizar diagonalización. En esta sección asociaremos otro very important polynomial: el *polinomio minimal*, que nos brindará más información y nos permitirá dar un otro criterio de diagonalización y en la unidad próxima será de enorme utilidad.

A lo largo de esta sección y de la unidad próxima estaremos dando una utilidad nueva a los polinomios: nos servirán para dar expresiones algebraicas a otros objetos. Es decir, utilizaremos mucho más su naturaleza algebraica. La siguiente es la primera definición donde un polinomio sirve para describir una expresión matricial de manera polinómica (y of course también a su traducción a endomorfismos en ev de dim finita):

Consideremos un polinomio $p(X) = a_0 + a_1 x + a_2 x^2 + \cdots + a_r x^r \in F[X]$. Definimos:

- Para $A \in F^{n\times n}$,
$$p(A) := a_0 I + a_1 A + a_2 A^2 + \cdots + a_r A^r \in F^{n\times n}.$$
Observemos que (EJERCICIO) si $q \in F[X]$ es otro polinomio:
  - $(p+q)(A) = p(A) + q(A)$,
  - $(pq)(A) = p(A)q(A)$.
- Si V F-ev con $dim V = n$ y $T \in L(V)$,
$$p(T) := a_0 id_V + a_1 T + a_2 T^2 + \cdots + a_r T^r \in L(V),$$
donde $T^k = T \circ \cdots \circ T$ (composición de k funciones).

Diremos además que un polinomio p **anula** a una matriz A si $p(A) = \mathbf{0} \in F^{n\times n}$ (la matriz nula) y **anula** a una transformación lineal T si $p(T) \equiv 0$ es la **función** constante igual a cero (es decir, la transformación nula $p(T)(v) = 0(v)$).

Lema 1 *Si $A \in F^{n\times n}$, existe $p(X) \in F[X]$, $p \neq \overline{0(X)}$ (el polinomio nulo) tal que $p(A) = \overline{0}$.*

Demostración: Consideremos el conjunto $\{I, A, A^2, \ldots, A^{n^2}\} \subset F^{n\times n}$. Este conjunto tiene n^2+1 elementos, luego es ld (porque?). Esto significa que existen escalares $a_0, a_1, \ldots, a_{n^2} \in F$ no todos nulos tq $a_0 I + a_1 A + \cdots + a_{n^2} A^{n^2} = \overline{0}$, esto es, el polinomio $p(X) = a_0 + a_1 X + \cdots + a_{n^2} X^{n^2} \in F[X]$ es no nulo y anula a A.

□

De la proposición anterior sigue trivialmente que no sólo existe un polinomio que anule A, sino que hay infinitos. En efecto, si $q(X)$ es cualquier otro polinomio (no nulo), el polinomio $r(X) = p(X)q(X)$ es no nulo y anula a A.

A título informativo (se puede saltear este párrafo y no pasa nada): el conjunto de todos los productos del polinomio $p(X)$ por un polinomio $q(X)$ cualquiera se llama ideal principal generado por $p(x)$ y se anota $(p(x))$. En álgebra abstracta, dentro de unos años, se verá que el conjunto de polinomios tiene estructura de anillo, y más aún, es un dominio de ideales principales. Esto nos garantizará dos cuestiones fundamentales: tener un algoritmo de la división y un teorema de factorización única. Los

fundamentos algebraicos son muy interesantes, por ahora con lo que sabemos de polinomios de Álgebra y Geometría Analítica I nos alcanza, pues justamente ambas herramientas nos son conocidas.

Volviendo al conjunto de polinomios que anulan a una matriz A: hay exactamente uno de estos polinomios que es mónico y de grado mínimo. En efecto:

- Veamos que existe tal polinomio. El argumento de existencia que utilizaremos ya lo hemos aplicado alguna vez (recuerdan la prueba del principio del palomar?). Probar existencia sin dar el objeto, sin construírlo, es difícil. Esta técnica sirve para estos casos.

  Sea $H_A = \{gr(p) : p \in F[X], p(A) = \mathbf{0} \text{ y } p \neq 0(X)\}$ el conjunto de todos los grados posibles de polinomios no nulos que anulen a A. Claramente $H_A \subset \mathbb{N}$. Luego, como $\mathbb{N}$ es un conjunto bien ordenado y H_A es no vacío (porqué?) y está acotado inferiormente, resulta que debe tener un primer elemento, digamos r.

  Consideremos entonces el polinomio $q \in F[X]$ tal que $q(A) = \mathbf{0}$ y $gr(q) = r$. Si $q(X)$ no es mónico, consideramos el polinomio $q'(x)$ obtenido al dividir $q(X)$ por su coeficiente principal (que es no nulo, porque?). Obtenemos así la existencia de un polinomio mónico de grado mínimo que anula a A.

- La unicidad sigue del argumento usual para unicidad: consideremos $q(x), q'(x)$ dos tales polinomios, y supongamos que son distintos. Obviamente tienen el mismo grado puesto que de lo contrario alguno no tendría grado mínimo. Entonces el polinomio $q(x) - q'(X) = (q - q')(X)$ es no nulo, anula a A, y por ser ambos mónicos resulta $gr(q - q') < r$. Esto contradice que q (y q') sean de grado mínimo. Luego, $q(X)$ y $q'(X)$ deben ser iguales.

Esto nos dice que la siguiente es una buena definición:

Definición 1 *$A \in F^{n\times n}$. Llamamos **polinomio minimal de A** y denotamos $m_A(X)$ al polinomio no nulo, mónico y de grado mínimo que anula a A.*

Veamos un ejemplo:

Ejemplo 1 *Para $A = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$ queremos hallar el polinomio minimal $m_A(X)$. Para esto observamos que el conjunto $\{I, A\}$ es li, luego $gr(m_A) > 1$. Nos preguntamos entonces acerca de la lineal dependencia del conjunto $\{I, A, A^2\}$. Veamos:*

Consideremos la ecuación matricial

$$a_0 I + a_1 A + a_2 X^2 = \overline{0},$$

si hacemos los cálculos, $A^2 = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$, de donde la ecuación matricial queda descripta como

$$a_0 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + a_1 \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} + a_2 \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Si planteamos el sistema asociado y lo resolvemos, resulta que tiene infinitas soluciones, luego el conjunto es ld. (EJERCICIO).

Para hallar el polinomio minimal, como dicho polinomio es mónico, podríamos haber planteado desde un principio la ecuación $a_0 I + a_1 A + X^2 = \mathbf{0}$. En efecto, si hacemos los cálculos, obtenemos que $a_0 = 1$ y $a_1 = 2$ son los coeficientes del polinomio buscado: $m_A(X) = X^2 + 2X + 1$.

Finalmente observemos que si calculamos el polinomio característico asociado a A, $\chi_A(X) = det(XI - A)$ tenemos que $\chi_A(X) = (X + 1)^2 = m_A(X)$.

Si bien no es algo que ocurra siempre, es cierto que ambos polinomios se relacionan. Exploraremos un poco esta relación.

Puesto que hemos tomado el polinomio minimal de A en el conjunto de todos los polinomios que anulan a A, mónico y de grado mínimo, tenemos que m_A divide a todos los polinomios de dicho conjunto. En efecto:

Proposición 1 *$A \in F^{n\times n}$, $p \in F[X]$. Entonces $p(A) = \mathbf{0}$ sii $m_A | p$.*

Demostración: Recordar que decimos que un polinomio q divide a un polinomio p y denotamos $q|p$ si existe otro polinomio c tales que $p(x) = c(x)q(x)$.

=>) Tenemos que p anula a A. Puesto que m_A tiene grado mínimo entre todos los que anulan a A debe ser $gr(m_A) \leq gr(p)$. Por el algoritmo de la división, existen polinomios $c(X), r(X) \in F[X]$ tales que $p(X) = c(X)m_A(X) + r(X)$ con $gr(r) < gr(m_A)$ o $r \equiv 0$. Ahora bien, $0 = p(A) = c(A)m_A(A) + r(A) = r(A)$, de donde resulta que $r \equiv 0$ (porqué?) y por lo tanto $m_A|p$.

<=) Si $m_A|p$ existe $c(X) \in F[X]$ tal que $p(X) = c(X)m_A(X)$. Luego $p(A) = c(A)m_A(A) = \mathbf{0}$.

□

Es nuestro objetivo siguiente poder definir el polinomio minimal de una transformación lineal abstracta en un ev de dimensión finita. Para esto, y como hay involucradas matrices, deberíamos ver cómo se comporta el polinomio minimal respecto de la relación de semejanza de matrices. Ya habíamos visto que matrices semejantes tienen el mismo polinomio característico, esto también será así para el polinomio minimal.

Recordemos que dos matrices $A, B \in F^{n\times n}$ se dicen semejantes si existe una matriz $C \in F^{n\times n}$ invertible tal que $A = CBC^{-1}$.

Desafío 1 *Cuando aplicamos un polinomio a una matriz trabajamos con potencias. Pobar que si $A \sim B$ entonces $A^k \sim B^k$ con la misma matriz de conjugación C. Help: inducir sobre k, observar que $A^{k+1} = A^kA = CB^kC^{-1}CBC^{-1} = CB^{k+1}C^{-1}$. Bueno, les hice la cuenta. Escribirlo bien.*

Lema 2 *$A, B \in F^{n\times n}$, $A \sim B$. Si $p \in F[X]$ entonces $p(A) \sim (B)$. En particular, $p(A) = \overline{0}$ sii $p(B) = \overline{0}$.*

Demostración: Como $A \sim B$, existe una matriz $C \in F^{n\times n}$ invertible tal que $A = CBC^{-1}$. Si $p(X) = \sum_{i=0}^{r} a_iX^i$, por lo que observamos recién respecto de las potencias, $p(A) = \sum_{i=0}^{r} a_iA^i = \sum_{i=0}^{r} a_iCB^iC^{-1} = C\left(\sum_{i=0}^{r} a_iB^i\right)C^{-1} = Cp(B)C^{-1}$, que es lo que queríamos probar.

□

Ahora sí probemos el resultado que nos permitirá pasar a ev abstractos (finito dimensionales).

Proposición 2 *$A, B \in F^{n\times n}$, $A \sim B$. Entonces $m_A = m_B$.*

Demostración: EJERCICIO. Ayuda: justificar que $m_B|m_A$ y que $m_A|m_B$.

□

A nivel de transformaciones lineales tenemos: si V F-ev con $dimV = n$, $T \in L(V)$ y B_1, B_2 bases de V entonces $m_{[T]_{B_1}} = m_{[T]_{B_2}}$. Queda entonces bien definido el polinomio minimal para T:

Definición 2 *V F-ev con $dimV = n$, $T \in L(V)$, B base de V. Definimos el **polinomio minimal de** T como el polinomio $m_T := m_{[T]_B}$.*

Volviendo a la relación entre el polinomio característico y el polinomio minimal (de una matriz), resulta que ambos tienen las mismas raíces: los autovalores de la matriz. Esto lo probamos en la siguiente proposición:

Proposición 3 *$A \in F^{n\times n}$, $\lambda \in F$. Entonces λ es un autovalor de A sii λ es raíz de m_A.*

Demostración:

=>) Si λ es un autovalor de A, por el algoritmo de la división, existen $c(X), r(X) \in F[X]$, con $r(X) \equiv r$ para una constante r (por qué?) tq $m_A(X) = (X - \lambda)c(X) + r$. Aplicando este polinomio a A tenemos $m_A(A) = (A - \lambda I)c(A) + rI$. Como λ es un autovalor de A, sigue que $\mathbf{0} = rI$, luego $r = 0$, de modo que λ es raíz de m_A (por qué?).

<=) Sea λ raíz de m_A. Luego $m_A(X) = (X - \lambda)q(X)$ para algún $q(X) \in F[X]$. Luego $\mathbf{0} = m_A(A) = (A - \lambda I)q(A)$ y como $gr(q) = gr(m_A) - 1$ debe ser $q(A) \neq \mathbf{0}$. Entonces existe $w \in F^n$ tq $q(A)w = v \neq \overline{0} \in F^n$. Luego, $(A - \lambda I)v = (A - \lambda I)q(A) = \overline{0} \in F^n$, de donde v es autovector de A asociado al autovalor λ.

□

Terminamos esta sección definiendo el polinomio minimal asociado a un vector, de manera análoga: si $A \in F^{n\times n}$, $v \in F^n$ y $p(X) \in F[X]$ definimos $p(v) = p(A)v$. Decimos entonces que p anula a v si $p(v) = \overline{0} \in F^n$.

En particular, como el polinomio minimal asociado a A anula a A, tenemos que $m_A(v) = m_A(A)v = \overline{0} \in F^n$, para todo $v \in V$. Así, si damos $v \in V$ resulta que existe un único polinomio mónico de grado mínimo que lo anula, y lo denotamos m_v. (EJERCICIO: escribir y probar esto con detalle, es igualita a la prueba para matrices).

Ejemplos 1 *1. $A \in F^{n\times n}$, $v \in F^n$ autovector de A asociado al autovalor λ. Entonces $m_v(X) = X - \lambda$. En efecto: $m_v(v) = m_v(A)v = (A - \lambda I)v = \overline{0} \in F^n$. Aquí $gr(m_v) = 1$.*

2. $A = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} \in \mathbb{R}^{2\times 2}$, $v = e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Calculemos m_{e_1}. Para esto planteamos un polinomio mónico, comenzando por el grado 1: $p(x) = x + a_0 \in [X]$. Queremos que $\overline{0} = p(e_1) = p(A)e_1 = (A + a_0 I)e_1 = Ae_1 + a_0 e_1 = \begin{pmatrix} -1 \\ 1 \end{pmatrix} + a_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 + a_0 \\ 1 \end{pmatrix}$, de donde sigue que $1 = 0$, luego el polinomio buscado no puede ser de grado 1. Veamos con grado 2: sea $p(X) = a_0 + a_1 X + X^2$. Luego, $p(e_1) = p(A)e_1 = \ldots$ EJERCICIO: $m_{e_1}(X) = 1 + 2X + X^2$.

¿Y en general cómo se calcula el polinomio minimal? Veamos: si $A \in F^{n\times n}$, $v \in F^n$ y $m_v(X) = a_0 + a_1 X + \cdots + X^m$ es el polinomio minimal de v, entonces debe ser

$$m_v(v) = m_v(A)v = a_0 v + a_1 Av + \cdots + A^m v = \overline{0} \in F^n.$$

Como el grado de m_v es mínimo entre los polinomios que satisfacen $p(v) = \overline{0}$, se tiene que el conjunto $\{v, Av, \ldots, A^{m-1}v\}$ es li. En efecto, si fuera ld existirían constantes $\beta_0, \ldots, \beta_{m-1}$ no todas nulas tales que $\sum_{i=0}^{m-1} \beta_i A^i v = \overline{0}$, luego el polinomio $p(X) = \sum_{i=0}^{m-1} \beta_i X^i$ es no nulo, anula a v y es de grado menor al minimal, lo cual es absurdo. Entonces, para hallar m_v empezamos buscando el primer $m \in \mathbb{N}$ tal que $\{v, Av, \ldots, A^m v\}$ es ld. Así, $A^m v = -a_0 v - a_1 Av + \cdots + (-1)a_{m-1}A^{m-1}v$. Entonces $m_v(X) = a_0 + a_1 X + \cdots + X^m$.

Veamos algunos resultados más antes del teorema de Cayley-Hamilton que veremos en la próxima sección. En primer lugar, al igual que lo que pasaba con las matrices, el polinomio minimal de v divide a todo polinomio que lo anule:

Proposición 4 *$A \in F^{n\times n}$, $v \in F^n$, $p(X) \in F[X]$. Entonces $p(v) = \overline{0}$ sii $m_v | p$. En particular, $m_v | m_A$.*

Demostración: Como el grado de m_v es mínimo, $gr(m_v) \leq gr(p)$. Por el algoritmo de la división existen $c(X), r(X) \in F[X]$ tq $p(X) = c(X)m_v(X) + r(X)$ con $r(X) \equiv 0$ o $gr(r) < gr(m_v)$. Ahora bien, $p(v) = m_v(v)c(v) + r(v)$. Entonces:

$$P \text{ anula a } v \text{ sii } r(v) = 0 \text{ sii } r \equiv 0 \text{ sii } m_v | p.$$

□

Veamos, finalmente, cómo calculamos el polinomio minimal de una matriz a partir de los polinomios minimales de una base:

Proposición 5 *$A \in F^{n\times n}$, $B = \{v_1, \ldots, v_n\}$ base de F^n. Entonces*

$$m_A = m.c.m.\{m_{v_1}, \ldots, m_{v_n}\}.$$

Demostración: Sea $p = m.c.m.\{m_{v_1}, \ldots, m_{v_n}\}$. Por la propiedad anterior, $m_{v_i}|m_A$, para cada $i = 1, \ldots, n$. Luego $p|m_A$ Además, $m_{v_i}|p$ para cada $i = 1, \ldots, n$ (por qué?). Luego $p(A)v_i = \overline{0}$ para cada $i = 1, \ldots, n$. Sea $v \in F^n$ y $\alpha_1, \ldots, \alpha_n \in F$ tq $v = \sum_{i=1}^{n} \alpha_i v_i$. Entonces $p(A)v = \sum_{i=1}^{n} \alpha_i p(A)v_i = \overline{0}$. Así, $p(A)v = \overline{0}$ para todo $v \in F^n$, de modo que $p(A) = \overline{0} \in F^{n\times n}$. Sigue que $m_A|p$, de donde $m_A = p$.

□

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

Para esto, consideremos la base canónica $E = \{e_1, e_2, e_3\}$ de $\mathbb{R}^3$. Por la proposición anterior $m_A = m.c.m.\{m_{e_1}, m_{e_2}, m_{e_3}\}$. Calculemos cada uno de estos polinomios:

- *Para calcular m_{e_1} observamos que $\{e_1, Ae_1\}$ es li y que $\{e_1, Ae_1, A^2e_1\}$ es ld. En efecto, $Ae_1 = e_1 + e_2$ y $A^2e_1 = e_1 + 2e_2$ (EJERCICIO). Planteando entonces $a_0e_1 + a_1Ae_1 + A^2e_1 = \overline{0}$ obtenemos que $a_1 = -2$ y $a_0 = 1$ (EJERCICIO). Resulta entonces $m_{e_1}(X) = 1 - 2X + X$.*
- *Análogamente calculamos (EJERCICIO) $m_{e_2}(X) = X - 1$.*
- *Análogamente calculamos (EJERCICIO) $m_{e_3}(X) = X - 2$.*

Entonces $m_A(X) = (X - 1)^2(X - 2$.