Minimálpolinom

Def. $A \in K^{n\times n}$, $p(x) = c_0 + c_1x + \cdots + c_mx^m \in K[x]$-re $p(A) := c_0I + c_1A + \cdots + c_mA^m$.

Állítás. $A \in K^{n\times n}$-hez $\exists\ 0 \neq p(x) \in K[x]$, amelyre $p(A) = 0$ (ahol 0 a csupa nullából álló mátrix).

Bizonyítás. $I, A, A^2, \ldots, A^{n^2} \in K^{n\times n}$, de $\dim K^{n\times n} = n^2 \Rightarrow$ ezek lineárisan összefüggők $\Rightarrow \exists\ c_0, \ldots, c_{n^2}$ nem mind 0: $c_0I + c_1A + \ldots + c_{n^2}A^{n^2} = 0$. □

Cayley–Hamilton-tétel. $k_A(A) = 0$.

Nem biz.

Def. $m_A(x) \in K[x]$ az $A \in K^{n\times n}$ mátrix minimálpolinomja az a minimális fokú, 1 főegyütthatós polinom, amelyre $m_A(A) = 0$. (A Cayley–Hamilton-tételből következik, hogy $\deg m_A(x) \leq n$.)

Megjegyzés. Bővebb test fölött is ugyanaz a minimálpolinom, tehát pl. $A \in \mathbb{R}^{n\times n}$ minimálpolinomja ugyanaz $\mathbb{R}$ és $\mathbb{C}$ fölött, mert $c_0 + c_1A + \cdots + c_mA^m = 0$ lineáris egyenletrendszer a c_i-kre, és ha az együtthatók K-beliek, és egy bővebb test fölött van nem triviális megoldás, akkor a Gauss-módszer miatt K fölött is van.

Állítás. $p(x) \in K[x]$-re $p(A) = 0 \Leftrightarrow m_A(x)|p(x)$, azaz $\exists\ q(x) \in K[x]$, hogy $p(x) = m_A(x)q(x)$.

Bizonyítás. $\Leftarrow$: $p(A) = m_A(A)q(A) = 0q(A) = 0$

$\Rightarrow$: Maradékos osztással: $p(x) = m(x)q(x) + r(x)$, ahol $\deg r(x) < \deg m(x)$. De $0 = p(A) = m(A)q(A) + r(A) = 0 \cdot q(A) + r(A) = r(A)$ és $\deg m(x)$ minimalitása miatt $r(x) = 0$. □

Állítás. Ⓑ $m_A(x)$-nek gyöke az A minden sajátértéke (bővebb test fölött is).

Bizonyítás. Legyen $\mathbf{v}$ sajátvektor λ sajátértékkel.

$$\begin{aligned}
A\mathbf{v} =& \lambda\mathbf{v} \\
A^2\mathbf{v} =& A(\lambda\mathbf{v}) = \lambda A\mathbf{v} = \lambda^2\mathbf{v} \\
&\vdots \\
A^k\mathbf{v} =& \lambda^k\mathbf{v} \\
p(A)\mathbf{v} =& p(\lambda)\mathbf{v}\ \forall p(x) \in K[x] \\
\mathbf{0} = m_A(A)\mathbf{v} =& m_A(\lambda)\mathbf{v} \\
m_A(\lambda) =& 0, \text{ mert } \mathbf{v} \neq \mathbf{0}.
\end{aligned}$$

□

Következmény. $A \in \mathbb{C}^{n\times n}$-re $k_A(x) = (-1)^n(x-\lambda_1)^{a_1}\cdots(x-\lambda_k)^{a_k}$, ahol $\lambda_1, \ldots, \lambda_k$ különbözők $\Rightarrow m_A(x) = (x-\lambda_1)^{b_1}\cdots(x-\lambda_k)^{b_k}$, ahol $1 \leq b_i \leq a_i\ \forall i$.

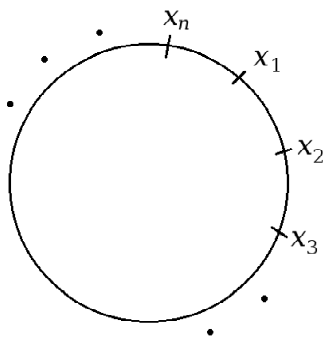
Pl. Határozzuk meg az $A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}$ mátrix karakterisztikus és minimálpolinomját!

Megoldás: $k_A(x) = |A - xI| = -(x-1)^2(x-2)$, tehát $m_A(x)$ csak $(x-1)(x-2)$ vagy $(x-1)^2(x-2)$ lehet. Ellenőrizzük, hogy az elsőnek gyöke-e az A:

$$(A-I)(A-2I) = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} -1 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \neq 0,$$

tehát a minimálpolinom $m_A(x) = (x-1)^2(x-2)$.

Pl.: A pénzérmés feladat megoldása:



$x_i = \quad 0$ v. $1 \in \mathbb{F}_2$
(írás vagy fej)
Egy lépés: $\quad x_1 \mapsto x_n + x_1$
$\quad x_i \mapsto x_{i-1} + x_i$

Ez lineáris transzformáció, a mátrixa: $\begin{bmatrix} 1 & 0 & 0 & \dots & 1 \\ 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 1 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & \\ 0 & 0 & \dots & 1 & 1 \end{bmatrix}$.

k lépés: $\mathbf{x} \mapsto A^k\mathbf{x}$, véget ér a játék: $\exists k$: $A^k\mathbf{x} = \mathbf{0}$.

$\forall \mathbf{x}$-re véget ér $\Leftrightarrow$ $\forall$ bázisvekorra véget ér
$\Leftrightarrow \forall i\ \exists k_i :\ A^{k_i}\mathbf{e}_i = \mathbf{0}$
$\Leftrightarrow \exists k :\ \forall i\ A^k\mathbf{e}_i = \mathbf{0}$ (k a legnagyobb k_i)
$\Leftrightarrow \exists k :\ 0 = A^k[\mathbf{e}_1|\cdots|\mathbf{e}_n] = A^kI = A^k$
$\Leftrightarrow \exists k :\ m_A(x)|x^k$
$\Leftrightarrow$ 0 az egyetlen sajátérték
$\Leftrightarrow k_A(x) = (-1)^n x^n = x^n$ ($\mathbb{F}_2$-ben)

Viszont $|A - xI|$-t az első oszlop szerint kifejtve azt kapjuk, hogy

$$|A - xI| = \begin{vmatrix} 1 & 0 & 0 & \dots & 1 \\ 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 1 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & \\ 0 & 0 & \dots & 1 & 1 \end{vmatrix} = (1-x)^n + (-1)^{n+1} \cdot 1 = (x+1)^n + 1$$

$\mathbb{F}_2$-ben, tehát azok az n számok jók, amelyekre $(x+1)^n + 1 = x^n$, azaz $(x+1)^n = x^n + 1$ $\mathbb{F}_2$ fölött. Ha n 2-hatvány, akkor ez igaz. Ha viszont $n = m \cdot 2^t$, ahol $m > 1$ páratlan szám, akkor $(x+1)^n = (x^{2^t}+1)^m = 1 + mx^{2^t} + \dots$, tehát x^{2^t} együtthatója nem 0, és emiatt $(x+1)^n \neq x^n + 1$.

Azt kaptuk, hogy a játék pontosan akkor ér véget minden kezdeti állásból, ha n 2-hatvány.

Mátrixok invariánsai

Ha $A, B \in K^{n\times n}$, és $A \sim B \Rightarrow A$-ra és B-re ugyanaz:

a) karakterisztikus polinom (láttuk)
b) determináns (a kar. pol.-ból levezethető)
c) nyom (a kar. pol.-ból levezethető)
d) minimálpolinom ($g(P^{-1}AP) = P^{-1}g(A)P$ minden $g(x)$ polinomra)
e) rang ($\dim \operatorname{Im} f$ nem függ a bázistól)
f) spektrum (a kar. pol. gyökei)
g) a sajátaltér dimenziója ($A \sim B \Rightarrow (A-\lambda I) \sim (B-\lambda I)$, és $\dim V_\lambda = n - \operatorname{rang}(A-\lambda I)$)

Vektorterek direkt összege

Jelölés: $U, W \le V$-re $U + W = \langle U \cup W \rangle = \{ \mathbf{u} + \mathbf{w} \mid \mathbf{u} \in U, \mathbf{w} \in W \} \le V$.
$V_i \le V$-re $(i = 1, \dots, k)$ $\sum\limits_{i=1}^{k} V_i = \langle \cup V_i \rangle = \{ \mathbf{v}_1 + \ldots + \mathbf{v}_k \mid \mathbf{v}_i \in V_i \} \le V$.

Def. Legyen $V_1, \dots, V_k \le V$. A V vektortér a $V_1, \dots, V_k$ alterek **direkt összege** (jele: $V = V_1 \oplus \cdots \oplus V_k = \bigoplus\limits_{i=1}^{k} V_i$), ha az alábbi ekvivalens állítások bármelyike teljesül:

(i) $\sum V_i = V$ és $V_i \cap \sum\limits_{j\ne i} V_j = 0$;
(ii) $\forall \mathbf{v} \in V$ egyértelműen felírható $\mathbf{v} = \mathbf{v}_1 + \ldots + \mathbf{v}_k$ alakban, ahol $\mathbf{v}_i \in V_i$ minden i-re;
(iii) $\exists \mathcal{B} = \dot\cup \mathcal{B}_i$ (diszjunkt unió) bázisa V-nek, ahol $\mathcal{B}_i$ bázisa V_i-nek minden i-re.

Állítás. $\forall U \le V$-re $\exists W \le V$: $V = U \oplus W$.

Bizonyítás. U bázisa független V-ben, így kiterjeszthető V bázisává. □

Def. f lineáris transzformáció V-n, $U \le V$. Az U altér f-**invariáns**, ha $f(U) := \{ f(\mathbf{u}) \mid \mathbf{u} \in U \} \le U$.

Állítás. Legyen $V = U \oplus W$, $\mathcal{B} = \mathcal{B}_1 \oplus \mathcal{B}_2$ bázisokkal, és $f : V \to V$ lineáris transzformáció.

1) Ha U f-invariáns $\Rightarrow [f]_{\mathcal{B}} = \begin{bmatrix} * & * \\ 0 & * \end{bmatrix}$ blokk-háromszögmátrix.
2) Ha U és W f-invariánsok $\Rightarrow [f]_{\mathcal{B}} = \begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix}$ blokkdiagonális mátrix.

Blokkmátrixok műveletei

Azonos méretű és felosztású blokkmátrixok összege:

$$\begin{bmatrix} A_{11} & \dots & A_{1m} \\ \dots & \dots & \dots \\ A_{n1} & \dots & A_{nm} \end{bmatrix} + \begin{bmatrix} B_{11} & \dots & B_{1m} \\ \dots & \dots & \dots \\ B_{n1} & \dots & B_{nm} \end{bmatrix} = \begin{bmatrix} A_{11}+B_{11} & \dots & A_{1m}+B_{1m} \\ \dots & \dots & \dots \\ A_{n1}+B_{n1} & \dots & A_{nm}+B_{nm} \end{bmatrix}.$$

Az összeillő méretű és felosztású (azaz A oszlopai ugyanannyi, egyenként ugyanannyi oszlopból álló részre vannak osztva, mint B sorai)

$$A = \begin{bmatrix} A_{11} & \dots & A_{1m} \\ \dots & \dots & \dots \\ A_{n1} & \dots & A_{nm} \end{bmatrix} \qquad \text{és} \qquad \begin{bmatrix} B_{11} & \dots & B_{1k} \\ \dots & \dots & \dots \\ B_{m1} & \dots & B_{mk} \end{bmatrix}$$

mátrixok szorzata $AB = C$, ahol $C_{ij} = \sum_{t=1}^{m} A_{it}B_{tj}$. (A felosztás "összeillő" volta miatt léteznek az $A_{it}B_{tj}$ mátrixszorzatok, és nyilván összeadhatók is.)

Pl. Az $AB = \left[\begin{array}{cc|cc} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \hline -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{array}\right] \cdot \left[\begin{array}{cc} 1 & 2 \\ 3 & -1 \\ \hline 0 & 1 \\ 2 & 1 \end{array}\right] = \left[\begin{array}{cc} 0 & 1 \\ 2 & 1 \\ \hline -1 & -1 \\ -1 & 2 \end{array}\right]$ szorzat

kiszámítható egyszerűbben, ha az A és B mátrixokat blokkmátrixoknak tekintjük, 2×2-es blokkokkal: $AB = \begin{bmatrix} 0 & I \\ -I & I \end{bmatrix} \cdot \begin{bmatrix} B_1 \\ B_2 \end{bmatrix} = \begin{bmatrix} B_2 \\ -B_1 + B_2 \end{bmatrix} = \left[\begin{array}{cc} 0 & 1 \\ 2 & 1 \\ \hline -1 & -1 \\ -1 & 2 \end{array}\right]$.

Köv.: Blokkdiagonális mátrixok szorzatát (négyzetes mátrixokról van szó, amelyeknek a sorait és oszlopait ugyanúgy osztjuk fel, és csak a főátló mentén lehetnek nem 0 blokkok) úgy kapjuk meg, hogy a megfelelő diagonális blokkjaikat szorozzuk össze:

$$\begin{bmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ & & \ddots & \\ 0 & 0 & \dots & A_n \end{bmatrix} \cdot \begin{bmatrix} B_1 & 0 & \dots & 0 \\ 0 & B_2 & \dots & 0 \\ & & \ddots & \\ 0 & 0 & \dots & B_n \end{bmatrix} = \begin{bmatrix} A_1B_1 & 0 & \dots & 0 \\ 0 & A_2B_2 & \dots & 0 \\ & & \ddots & \\ 0 & 0 & \dots & A_nB_n \end{bmatrix}.$$

Def. $f(x), g(x) \in K[x]$-re $f(x)$ és $g(x)$ relatív prímek, ha nincs olyan legalább elsőfokú $h(x) \in K[x]$, ami mindkettőnek osztója.

Állítás. $f(x)$ és $g(x)$ relatív prímek $\Leftrightarrow \exists\ a(x), b(x) \in K[x]$: $a(x)f(x) + b(x)g(x) = 1$.

Bizonyítás. Mint $\mathbb{Z}$-ben, euklideszi algoritmussal.

Tétel. Legyen $A \in K^{n\times n}$, $m_A(x) = f(x)g(x)$ az A minimálpolinomja, ahol $f(x), g(x) \in K[x]$ 1 főegyütthatós, relatív prím polinomok. Ekkor A hasonló egy $\begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}$ blokkmátrixhoz, ahol $m_{A_1}(x) = f(x)$ és $m_{A_2}(x) = g(x)$.

(Bizonyítás a jövő órán)