① $a, b \in \mathbb{Z}$ (a osztója b-nek)

- $a \mid b$, ha $b = c \cdot a$ $\quad c \in \mathbb{Z}$

valódi osztó, ha $1 < |a| < |b|$

Prímszám: nincs valódi osztója, abszolútértéke nagyobb 1-nél, egész.

SzAT: Minden egész szám (-1, 0, 1 és inverzeivel) egyértelműen felbontható prímek szorzatára (előjelétől és sorrendjétől eltekintve)

- $x \longrightarrow x = a \cdot b \xrightarrow{a \vee b \text{ összetett}} x = a_1 a_2 b \longrightarrow \dots$

  $\downarrow$ prím $\quad \downarrow$ a, b prím ✓ $\quad \downarrow \dots$

Prímek száma végtelen

Legyen $p_1, p_2, p_3 \dots p_k$ prím (k db)

$N := p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_k + 1$

- N minden prímnél nagyobb (nem prím)
  N minden prímmel osztva 1 maradékot ad

  $\Rightarrow$ ellentmondás

Prímek száma n-ig: $\pi(n)$

$\pi(n) \approx \frac{n}{\ln n}$

$a \equiv b \pmod m$ $\qquad a, b, m \in \mathbb{Z}$

① a és b m szerinti osztási maradéka megegyezik

② m osztója $a-b$-nek

① $\Leftrightarrow$ ②

$a = c_1 \cdot m + r_1$

$b = c_2 \cdot m + r_2$

① $r_1 = r_2$ $\qquad (r_1 \geq r_2)$

② $m \mid m(c_1 - c_2) + (r_1 - r_2)$

$\Updownarrow$

$r_1 - r_2 = 0$

$r_1 = r_2$

$a \equiv b \pmod m$

$c \equiv d \pmod m$

$\Rightarrow$

$a + c \equiv b + d \pmod m$

$a - c \equiv b - d \pmod m$

$ac \equiv bd \pmod m$

$a^k \equiv b^k \pmod m$ $\qquad k \in \mathbb{Z}$

$m \mid a-b$ $\quad \oplus$

$m \mid c-d$

$\Rightarrow m \mid a-b+c-d$ $\qquad m \mid (a+c)-(b+d) \Leftrightarrow a+c \equiv b+d \pmod m$

$m \mid a-b$ $\quad \ominus$

$m \mid c-d$

$\Rightarrow m \mid a-b-c+d$ $\qquad m \mid (a+c)+(b+d) \Leftrightarrow a \cdot c \equiv b-d \pmod m$

$m \mid a-b \quad \cdot c$ $\quad \oplus$

$m \mid c-d \quad \cdot b$

$\Rightarrow m \mid ac-bc+bc-db$ $\qquad m \mid ac-bd \Leftrightarrow ac \equiv bd \pmod m$

$a \equiv b \pmod m \cdot (a \equiv b \pmod m)$

$a^2 \equiv b^2 \pmod m$ $\cdot$ — " —

$a^3 \equiv b^3 \pmod m$

$\vdots$

$a^k \equiv b^k \pmod m$

$ac \equiv bc \pmod m$ $\qquad d = (m, c)$

$m \mid ac - bc = c(a-b)$

$\frac{m}{d} \mid \frac{c}{d}(a-b)$ $\qquad$ (nincs közös prímtényező)

$a \equiv b \pmod{\frac{m}{d}}$

(2)

$a, b, n \in \mathbb{Z}$

$ax \equiv b \ (n)$ megoldható $\Leftrightarrow$ $(a,n) \mid b$

Biz $\Rightarrow$ tfh x_0 l.o. $\quad d = (a,n)$

$ax_0 \equiv b \ (n) \Rightarrow b = n \cdot \ell + a \cdot x_0$

$d \mid ? \quad d \mid ?$

$d \mid b \quad d \mid ?$

$\Leftarrow$ 1. eset $(a,n) = 1$

$x := a^{\varphi(n)-1} \cdot b$

$a \cdot x = a \cdot a^{\varphi(n)-1} \cdot b = a^{\varphi(n)} \cdot b \equiv b \ (n)$

$\uparrow$ E-F

2. eset $(a,b) \neq 0$

$ax \equiv b \ (n) \ / : (a,n)$

$a'x \equiv b' \ (n')$

$(a', n') = 1$

Megoldások száma (ha megoldható)

(modulo n) (a,n)

Euklideszi algoritmus : LNKO számítás (polinomiális lépésszám)

$(a,n) = ?$ $\quad n \geq a$ $\quad$ osztások száma: $\leq 2 \log_2 a \leq c \cdot n$

$n = \ell_1 \cdot a + r_1$

$a = \ell_2 \cdot r_1 + r_2$

$r_1 = \ell_3 \cdot r_2 + r_3$

$r_2 = \ell_4 \cdot r_3 + r_4$

$\vdots$

$r_n = \ell_{n+2} \cdot r_{n+1} + \boxed{r_{n+3}} \quad r_{n+3} = LNKO$

$r_{n+1} = \ell_{n+3} \cdot r_{n+3} + 0$

Lineáris kongruencia megoldása E.A.-vel

Alkalmazható, ha $(a, m) = 1$

① $mx \equiv 0 \pmod{m}$

② $ax \equiv b \pmod{m}$

③ : ① $- r_1$ ② $r_1 x \equiv c_1 \pmod{m}$

④ : ② $- r_2$ ③ $r_2 x \equiv c_2 \pmod{m}$

$\vdots$

$r_n x \equiv c_n \pmod{m}$

$\|$

1 $\hookrightarrow$ egyértelmű megoldás

3) $\varphi(n)$: relatív prímek száma 1-től n-ig

- $\varphi(p) = p-1$ (p prím)

$\underbrace{1, 2, 3, \dots, p-1}_{\text{mind relatív prím}}, p$

$\varphi(p^n) = p^n - p^{n-1}$

$1, 2, 3, \dots, p, \dots, 2p, \dots, 3p, \dots, (p^{n-1}-1)p, \dots, (p^{n-1})\cdot p$

- $\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) \qquad (p,q) = 1$

RMR mod n : $\{a_1, a_2, a_3, \dots, a_n\}$

$n = \varphi(n)$

$a_i \not\equiv a_j \ (n) \quad i \neq j$

- $(a_i, n) = 1$

Euler-Fermat tétel

$(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \ (n)$

Ill. tetsz. RMR mod n: $\{c_1, c_2, c_3 \dots, c_n\}$

$\{a\cdot c_1, a\cdot c_2, \dots, a\cdot c_n\}$ is RMR mod n

- A két RMR elemei páronként kongruensek, ezért

$c_1 \cdot c_2 \cdot c_3 \cdots c_n \equiv ac_1 \cdot ac_2 \cdots ac_n \ (n)$

$c_1 \cdot c_2 \cdot \ldots \cdot c_n \equiv a^n c_1 \cdot c_2 \cdot \ldots \cdot c_n \pmod{m} \quad / : c_1 \cdot c_2 \cdot \ldots \cdot c_n$

$(c_1 \cdot c_2 \cdot \ldots \cdot c_n, m) = 1$ (RMR def.)

$a^n = a^{\varphi(m)} \equiv 1 \pmod{m}$ ✓

Lemma: $\{c_1, c_2, c_3, \ldots, c_n\}$ RMR mod m

$(a,m)=1 \Rightarrow \{a \cdot c_1, a \cdot c_2, \ldots, a \cdot c_n\}$ is RMR mod m

Biz $\left.\begin{matrix}(a,m)=1 \\ (c_i,m)=1\end{matrix}\right\}$ SZAT $(a \cdot c_i, m) = 1$

$a \cdot c_i \not\equiv a \cdot c_j \pmod{m} \quad / : a \quad (a,m)=1 \quad i \neq j$

$c_i \not\equiv c_j \pmod{m}$ ✓

$n = \varphi(m)$ ✓

Kis-Fermat-tétel

p prím

$(a,p)=1 \quad (p \nmid a) \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

$\left.\begin{matrix} a^p \equiv a \pmod{p} \\ p \mid a \Rightarrow a^n \equiv a \pmod{p} \Rightarrow a^p \equiv a \pmod{p} \end{matrix}\right\} \Rightarrow a^p \equiv a \pmod{p} \quad \forall p$ prím

Következmények

$x \equiv b \pmod{m} \rightsquigarrow x = km + b$

$x \equiv d \pmod{m}$

$km + b \equiv d \pmod{m}$ ← Ell.

(4)

Polinomiális futásidejű algoritmus: olyan algoritmus, ami $c \cdot n^\varepsilon$ idő alatt fut le, ahol $c, \varepsilon \geq 1$ konstans és n az input mérete

összeadás, kivonás: $c \cdot n$

szorzás, osztás: $c \cdot n^2$

hatványozás (a^b): b db szorzás → exponenciális

mod. hatv.

a^b mod m $\quad 0 \leq c_i \leq m$

$a^1 \equiv c_1 \pmod m$

$a^2 \equiv c_2 \pmod m$

$a^4 \equiv c_3 \pmod m$

$a^8 \equiv c_4 \pmod m$

$\vdots$

$b = 1 \cdot n_1 + 2 n_2 + 4 n_3 + 8 n_4 + \dots + \dots$ $\quad n_i = 0, 1$

$a^b \equiv c_1^{n_1} \cdot c_2^{n_2} \cdot c_3^{n_3} \cdot c_4^{n_4} \dots \pmod m$

$\equiv ? \pmod m$

$\equiv ! \pmod m$

$\equiv ! \pmod m$

$\vdots$

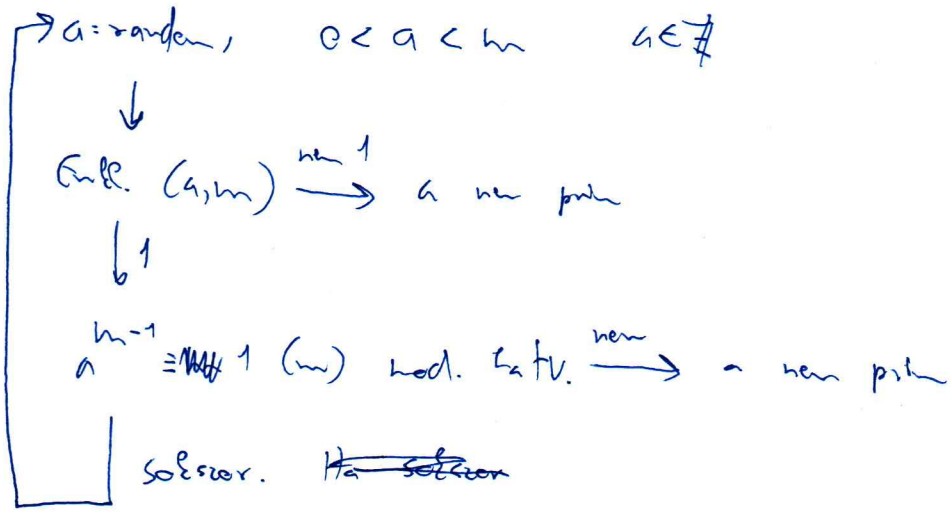
$a^b \equiv x \pmod m$ ✓

Címmunka: $\square^2$-re eső maradékos osztás, szorzás $\Big\}$ $c \cdot n^2$ $\Big\}$ összesen $c'' \cdot n^3$

$\log_2 b$-szer fut le $2 \cdot n$

Prímtesztelés

n prím-e? $\quad n \in \mathbb{N}$



Def.: a tanúja n-nek, ha $(a,n)=1$ és $a^{n-1} \not\equiv 1 \pmod n$

c cinkos n-nek, ha $(c,n)=1$ és $c^{n-1} \equiv 1 \pmod n$

Ha egy számnak van tanúja, akkor a Lucas relatív prímek segítségével fele tanú.

Riz.: $c_1, c_2, c_3, \dots, c_m$ cinkosok

a ~~fiktív~~ tanú

$a_i := a \cdot c_i$

$a_i^{n-1} \overset{?}{\equiv} 1 \pmod n$

$a^{n-1} \cdot c_i^{n-1} \overset{?}{\not\equiv} 1 \pmod n$

$1 \quad 1$

Carmichael-szám: összetett szám, de nincs tanúja

(4) Fogl.

$k \in \mathbb{Z}$

$\varphi(N) = (p-1)(q-1)$

- RSA p, q m-, $p \neq q$

$N = p \cdot q$ $\qquad x^{k\varphi(N)+1} \equiv x \ (N)$

1. eset $(N, x) = 1 \rightarrow$ E-F $\quad x^{\varphi(N)} \equiv 1 \ (N) \ / \uparrow k$

$x^{k\varphi(N)} \equiv 1 \ (N) \ / \cdot x$

$x^{k\varphi(N)+1} \equiv x$

2. eset $q \mid x$ $\qquad p \nmid x$

- $(x, p) = 1 \quad x^{p-1} \equiv 1 \ (p) \ / \uparrow (q-1)k$

$x^{\varphi(N) \cdot k} \equiv 1$

$x^{k\varphi(N)+1} \equiv x \ (p)$

$p \mid x^{k\varphi(N)+1} - x$

$q \mid x^{k\varphi(N)+1} - x$

$\Big\} \ p \cdot q = N \mid x^{k\varphi(N)+1} - x \Leftrightarrow x^{k\varphi(N)+1} \equiv x \ (N)$

3. eset $p \nmid x$, $q \mid x$, $p \mid x \Rightarrow p \cdot q = N \mid x \Rightarrow x^{k\varphi(N)+1} \equiv x \ (N)$

- Titkos: p, q $\qquad y \mapsto y^d \bmod N$

Nyilvános: $N (= p \cdot q)$, $c : (c, \varphi(N)) = 1 \qquad x \mapsto x^c = y$

cél $\quad (x^c)^d \equiv x \ (N) \qquad (\forall x)$

$cd = k\varphi(N) + 1 \Leftrightarrow cd \equiv 1 \ (\varphi(N))$ $\qquad (c, \varphi(N)) = 1 \,/\, 1$

Euler. $\downarrow$ $\qquad \exists$ m.o.

- $d = \ldots$

$(x^c)^d \equiv x \ (N)$ ✓

5) Sík egyenlete: $P_0(x_0, y_0, z_0)$ pont a síkban

$\underline{n}(a, b, c)$ normálvektor

$$ax + by + cz = ax_0 + by_0 + cz_0$$

Rövid: $P(x,y,z) \in S \Rightarrow \overrightarrow{PP_0} \in S$ és $\overrightarrow{PP_0} \perp \underline{n}$

$$\overrightarrow{P \cdot P_0} \cdot \underline{n} = 0$$

$$(x - x_0, y - y_0, z - z_0) \cdot (a, b, c) = (0, 0, 0)$$

$$(ax, by, cz) = (ax_0, by_0, cz_0) \checkmark$$

Egyenes egyenlete: $P_0(x_0, y_0, z_0)$ pont az egyenesen

$\underline{v}(a, b, c)$ irányvektor

$P(x, y, z)$ pont az egyenesen $\quad \forall \lambda \in \mathbb{R}$

$$P = P_0 + \underline{v} \cdot \lambda$$

$$(x, y, z) = (x_0 + a\lambda, y_0 + b\lambda, z_0 + c\lambda)$$

$$\begin{cases} x = x_0 + a\lambda \\ y = y_0 + b\lambda \\ z = z_0 + c\lambda \end{cases} \rightarrow \lambda = \frac{x - x_0}{a} \rightarrow \lambda = \frac{y - y_0}{b} \rightarrow \lambda = \frac{z - z_0}{c}$$

$$\frac{x - x_0}{a} = \frac{y - y_0}{b} = \frac{z - z_0}{c} = \lambda$$

$a, b, c \neq 0$

$$\frac{x - x_0}{a} = \frac{y - y_0}{b} \quad z = z_0 \qquad a, b \neq 0,\ c = 0$$

$$y = y_0,\ z = z_0 \qquad a \neq 0,\ b, c = 0$$

Skaláris szorzat: $\underline{a} \cdot \underline{b} = |\underline{a}| \cdot |\underline{b}| \cdot \cos(\underline{a} \sphericalangle \underline{b})$

Vektoriális szorzat: $|\underline{a} \times \underline{b}| = |\underline{a}| \cdot |\underline{b}| \cdot \sin(\underline{a} \sphericalangle \underline{b})$

$\underline{a} \times \underline{b} \perp \underline{a}$, $\underline{a} \times \underline{b} \perp \underline{b}$

$\underline{a}, \underline{b}, \underline{a} \times \underline{b}$ jobbsodrású rendszert alkot

Térbeli vektorok lineárisan függetlenek, ha nincs közöttük két egyenlő vektor

Térbeli vektorok $\mathbb{R}^3$-beli generátorrendszert alkotnak, ha van közöttük 3 olyan vektor ami lineárisan független

$\underline{a}, \underline{b}, \underline{c} \in \mathbb{R}^3$ bázis, ha $\underline{a}, \underline{b}, \underline{c}$ lin. ftlen és ## gen. rdsz. $\mathbb{R}^3$-ban

⑥ $\mathbb{R}^n$: n hosszú számoszlopok

- $\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$ $\quad \alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{R}$

V altér $\mathbb{R}^n$-ben ($V \leq \mathbb{R}^n$), ha

1. $\underline{u}, \underline{v} \in V \Rightarrow (\underline{u} + \underline{v}) \in V$
2. $\underline{u} \in V, \lambda \in \mathbb{R} \Rightarrow \underline{u} \cdot \lambda \in V$

- $\underline{v}_1, \underline{v}_2, \underline{v}_3, \dots, \underline{v}_\ell \in \mathbb{R}^n$

$\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_\ell \in \mathbb{R}$

$\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 + \alpha_3 \underline{v}_3 + \dots + \alpha_\ell \underline{v}_\ell$ ← Lineáris kombináció

$\underline{v}_1, \underline{v}_2, \underline{v}_3, \dots, \underline{v}_\ell \in \mathbb{R}^n$

$V = \{\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 + \alpha_3 \underline{v}_3 + \dots + \alpha_\ell \underline{v}_\ell : \alpha_1, \alpha_2, \alpha_3, \dots, \alpha_\ell \in \mathbb{R}\}$

ekkor $V \leq \mathbb{R}^n$

① $\underline{v} = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 \dots$

$\underline{u} = \beta_1 v_1 + \beta_2 v_2 + \beta_3 v_3 \dots$

- $\underline{u} + \underline{v} = (\alpha_1 + \beta_1) v_1 + (\alpha_2 + \beta_2) v_2 \dots \in V$

② $\beta \cdot \underline{v} = \alpha_1 \beta v_1 + \alpha_2 \beta v_2 \dots \in V$

Jele: $V = \langle \underline{v}_1, \underline{v}_2, \underline{v}_3, \dots, \underline{v}_\ell \rangle$

V generátorrendszere $\underline{v}_1, \underline{v}_2, \underline{v}_3, \dots \underline{v}_\ell$

Lin. ftlen. $\underline{v}_1, \underline{v}_2, \underline{v}_3 \dots, \underline{v}_\ell$

1, egyik vektor sem fejezhető ki a többi lineáris kombinációjából

2, csak a triviális lineáris kombinációjuk ad nullvektort ($\alpha_1 = \alpha_2 = \dots = 0$)

1 $\Rightarrow$ 2

Legyen $\underline{v}_\ell = \alpha_1 \cdot \underline{v}_1 + \alpha_2 \cdot \underline{v}_2 + \dots + \alpha_{\ell-1} \cdot \underline{v}_{\ell-1}$

ellen. $\underline{0} = \alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 + \dots + \alpha_{\ell-1} \underline{v}_{\ell-1} - 1 \cdot \underline{v}_\ell = \underline{0}$ $\rightarrow$ nem mind 0 együtthatós

Legyen $\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 + \dots + \alpha_\ell \underline{v}_\ell = \underline{0}$

Legyen $\alpha_\ell \neq 0$, ekkor

$$\underline{v}_\ell = -\frac{\alpha_1}{\alpha_\ell} \underline{v}_1 - \frac{\alpha_2}{\alpha_\ell} \underline{v}_2 - \dots$$ $\rightarrow$ egyik vektor kifejezhető a többi lin. kombinációval

ÚGVL $\underline{v}_1, \underline{v}_2, \underline{v}_3 \dots, \underline{v}_\ell \in \mathbb{R}^n$ lin. ftlen. $\Rightarrow \underline{v}_{\ell+1} \in \langle \underline{v}_1, \underline{v}_2, \dots, \underline{v}_\ell \rangle$

$\underline{v}_1, \underline{v}_2, \underline{v}_3, \dots, \underline{v}_\ell, \underline{v}_{\ell+1} \in \mathbb{R}^n$ lin. öf.

Biz. $\rightarrow$ def 2 $\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 + \dots + \alpha_\ell \underline{v}_\ell + \alpha_{\ell+1} \underline{v}_{\ell+1} = \underline{0}$ nem minden együtthatós 0

Ha $\alpha_{\ell+1} = 0$, akkor $\alpha_1, \dots, \alpha_\ell$ közül nem mind nulla, ami a lin. ftlenség miatt nem lehet, ezért $\alpha_{\ell+1} \neq 0$, ekkor

$$\underline{v}_{\ell+1} = -\frac{\alpha_1}{\alpha_{\ell+1}} \underline{v}_1 - \frac{\alpha_2}{\alpha_{\ell+1}} \underline{v}_2 - \dots \Rightarrow \underline{v}_{\ell+1} \in \langle \underline{v}_1, \underline{v}_2, \dots, \underline{v}_\ell \rangle$$

Kicserélési tétel $\underline{f}_1, \underline{f}_2, \dots, \underline{f}_\ell \in \mathbb{R}^n$ lin. ftlen. $\}$ $\forall \underline{f}_i$-hez létezik $\underline{g}_i$, hogy

$\underline{g}_1, \underline{g}_2, \dots, \underline{g}_m$ gen. rendszer $\mathbb{R}^n$-ben $\}$ $\underline{f}_1, \underline{f}_2, \dots, \underline{f}_{i-1}, \underline{g}_i, \underline{f}_{i+1}, \dots, \underline{f}_\ell$ lin. ftlen.

Biz. indirekt: Legyen $\underline{f}_\ell$ a kicserélendő vektor

$\underline{g}_1$ nem jó $\overset{\text{ÚGVL}}{\Rightarrow}$ $\underline{g}_1 \in \langle \underline{f}_1, \underline{f}_2, \underline{f}_3, \dots, \underline{f}_{\ell-1} \rangle$

$\vdots$

$\underline{g}_m$ nem jó $\Rightarrow$ $\underline{g}_m \in$ <—— " ——>

$\underline{f}_\ell \in \langle \underline{g}_1, \underline{g}_2, \dots, \underline{g}_m \rangle$ és $\forall \underline{g}_i \in \langle \underline{f}_1, \underline{f}_2, \dots, \underline{f}_{\ell-1} \rangle \Rightarrow \underline{f}_\ell \in \langle \underline{f}_1, \underline{f}_2, \dots, \underline{f}_{\ell-1} \rangle$ ellentm.

(6) Fogl.

F-G egyenlőtlenség

$F := \{f_1, f_2, f_3 \dots, f_\ell\}$ lin. független vektorok $\mathbb{R}^n$-ben

$G := \{g_1, g_2, \dots, g_n\}$ generátorrendszer $\mathbb{R}^n$-ben

$F \to F' \to F'' \to \dots F^*$

kicserélés: $f_i \to g_j$ ...

$F^* \subseteq G$

$|F^*| = |F|$

$k \leq n$

(7) $b_1, b_2, b_3 \dots, b_n$ bázis $\mathbb{R}^n$-ben, $c_1 \langle b_1, b_2, b_3, \dots, b_n \rangle = \mathbb{R}^n$ és

$b_1, b_2, b_3, \dots, b_n$ lin. ftlen.

$\dim V = n$, ha V-ben van n elemű bázis

1, $b_1, b_2, \dots, b_n$ bázis V-ben (lin. f. és g.r.)

2, $c_1, c_2, \dots, c_e$ bázis V-ben (—— n ——)

1, lin. f. és 2. g.r. $\Rightarrow$ $n \leq e$

2. —n— 1. —n— $\Rightarrow$ $e \leq n$

$\Rightarrow e = n$, $\dim V = e = n$

Standard bázis $\mathbb{R}^n$-ben: $\underbrace{\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}, \begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\\vdots\\0\end{pmatrix}, \dots, \begin{pmatrix}0\\0\\\vdots\\0\\1\end{pmatrix}}_{n \text{ db}}$

$\dim \mathbb{R}^n = n$, mivel a standard bázis n elemű

$B = \{b_1, b_2, \dots, b_e\}$ bázis V-ben, $V \leq \mathbb{R}^n$

$v \in V$

$v = \alpha_1 b_1 + \alpha_2 b_2 + \dots + \alpha_e b_e$

v koordinátavektora B, szerint $\begin{pmatrix}\alpha_1\\\alpha_2\\\vdots\\\alpha_e\end{pmatrix}$, jele $[v]_B = \begin{pmatrix}\alpha_1\\\alpha_2\\\vdots\\\alpha_e\end{pmatrix}$

Legyen $v = \alpha_1 b_1 + \alpha_2 b_2 + \dots + \alpha_e b_e$

$\ominus$ $v = \beta_1 b_1 + \beta_2 b_2 + \dots + \beta_e b_e$

$0 = (\alpha_1 - \beta_1) b_1 + (\alpha_2 - \beta_2) b_2 + \dots + (\alpha_e - \beta_e) b_e = 0$

$\downarrow$ $b_1, b_2, b_3, \dots, b_e$ lin. ftlen.

$\alpha_1 - \beta_1 = 0 \rightarrow \alpha_1 = \beta_1$, $\alpha_2 = \beta_2, \dots$, $\alpha_e = \beta_e$

(8) ~~Gauss-elim.~~

~~főbb felső elem girdlesztk~~

~~ha az nulla, sorcsere (legelső nemnulla sor)~~

$$a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \dots + a_{1k}x_k = b_1$$

$$\vdots$$

$$a_{n1}x_1 + a_{n2}x_2 + a_{n3}x_3 + \dots + a_{nk}x_k = b_n$$

$$A := \begin{pmatrix} a_{11} & a_{12} & \dots \\ \vdots & & \\ & & a_{nk} \end{pmatrix} \qquad B := \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

$(A|B)$ ~~gauss-elim~~ Gauss-elim.

$$\begin{pmatrix} a_{11} & a_{12} & \dots & & b_1 \\ & \vdots & & & b_2 \\ & & & & \vdots \\ & & & a_{nk} & b_n \end{pmatrix} \quad (x_1, x_2, \dots, x_n \text{ oszlopok})$$

$\rightarrow \begin{pmatrix} 1 & & 0 & c_1 \\ & 1 & & c_2 \\ & & 1 & c_3 \\ 0 & & 1 & \vdots \\ & & & c_n \end{pmatrix}$ → ~~egység~~ minden oszlopban # v.e.

→ egyértelmű m.o.

$x_1 = c_1,\ x_2 = c_2 \dots$

$\rightarrow \begin{pmatrix} 1 & a & & c_1 \\ 0 & 0 & 1 & \vdots \\ 0 & 0 & 0 & \vdots \\ 0 & 0 & 0 & \end{pmatrix}$ ↳ szabad paraméter

∞ sok m.o.

$x_n = \ell$

$x_1 = c_1 - a \cdot \ell$

$\vdots$

$\downarrow \begin{pmatrix} & & & & \\ 0 & 0 & 0 & 0 & c_n \neq 0 \end{pmatrix}$

↳ tilos sor

nincs m.o.

Lépcsős alak:

$$\begin{pmatrix} 1 & \cdot & a & \cdot & \vdots \\ 0 & 1 & b & & \vdots \\ 0 & 0 & 0 & 1 & \vdots \\ 0 & 0 & 0 & 0 & \end{pmatrix}$$

vezérles: sorban első nemnulla elem

minden vezéregyestől balra és lefele csak ~~0~~ 0-k vannak

RLA

$$\begin{pmatrix} 1 & 0 & a & 0 & \vdots \\ 0 & 1 & b & 0 & \vdots \\ 0 & 0 & 0 & 1 & \vdots \\ 0 & 0 & 0 & 0 & \end{pmatrix}$$

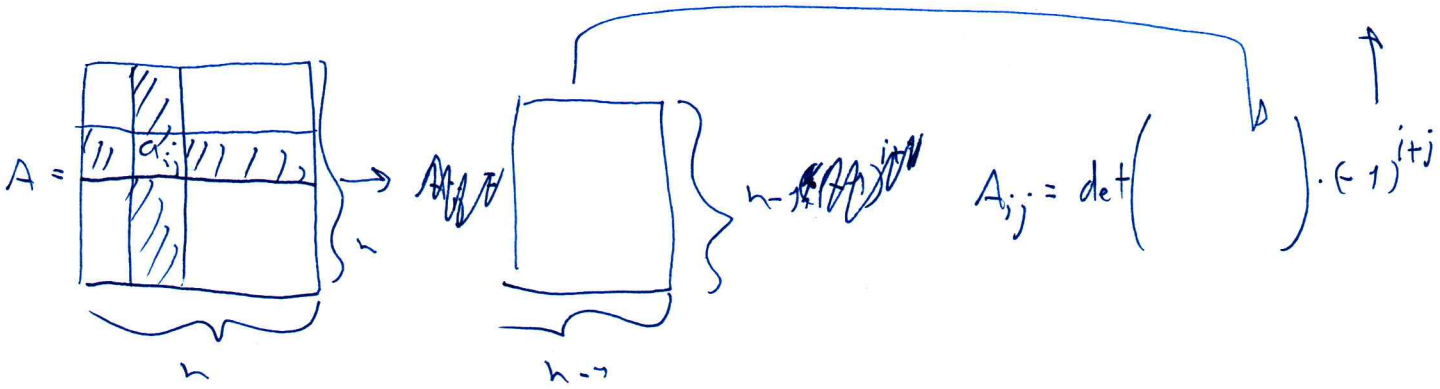
minden vezéregyestől ~~jobb~~ balra, lefele és felfele is 0-k vannak

Ha az egyenletek száma nem kevesebb az ismeretlenek számától, akkor lehet egyértelmű megoldása

①

$$\begin{vmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{vmatrix} = -e\begin{vmatrix} b & c & d \\ i & j & k \\ n & o & p \end{vmatrix} + f\begin{vmatrix} a & c & d \\ i & k & l \\ m & o & p \end{vmatrix} - g \dots$$

$$\begin{matrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ \vdots & & & \end{matrix} \dots$$



Sor szerint: kifejtés (i. sor)

$$\det A = a_{i1}A_{i1} + a_{i2}A_{i2} + \dots + a_{in}A_{in}$$

Oszlop szerint: kifejtés (j. oszlop)

$$\det A = a_{1j}A_{1j} + a_{2j}A_{2j} + \dots + a_{nj}A_{nj}$$

Mátrixműveletek

$A, B, C \in \mathbb{R}^{n \times k}$ $\quad \alpha, \beta \in \mathbb{R}$

$D \in \mathbb{R}^{k \times m}$

$$\begin{pmatrix} a_{11} & a_{12} & \dots \\ a_{21} & \ddots & \\ \vdots & & a_{nk} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \dots \\ b_{21} & \ddots & \\ \vdots & & b_{nk} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \dots \\ a_{21}+b_{21} & \ddots & \\ \vdots & & a_{nk}+b_{nk} \end{pmatrix}$$

① $A + B = B + A$

② $(A+B)C = AC + BC$

③ $\alpha \cdot A = A \cdot \alpha$

$$\alpha \begin{pmatrix} a_{11} & a_{12} & \dots \\ a_{21} & \ddots & \\ \vdots & & a_{nk} \end{pmatrix} = \begin{pmatrix} \alpha a_{11} & \alpha a_{12} & \dots \\ \alpha a_{21} & \ddots & \\ \vdots & & \alpha a_{nk} \end{pmatrix}$$

④ $(\alpha+\beta)A = \alpha A + \beta A$

⑤ $\alpha(\beta A) = (\alpha\beta)A$

⑥ $A(BC) = (AB)C$

$$\begin{pmatrix} d_{11} & d_{12} & \dots \\ d_{21} & \ddots & \\ \vdots & & d_{nm} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} & \dots \\ a_{21} & \ddots & \\ \vdots & & a_{nk} \end{pmatrix} \begin{pmatrix} \square \\ \vdots \\ \square \end{pmatrix} \rightarrow a_{11}d_{11} + a_{12}d_{21} + a_{1k}d_{k1} \dots$$

$$\square \rightarrow a_{n1} \cdot d_{n1} + \dots + a_{nk} \cdot d_{km}$$

$X \in \mathbb{R}^{k \times n}$

$A^T = X \quad a_{ij} = x_{ji} \quad \forall i, j$

$\det A = \det A^T$

$\det(A \cdot B) = \det A \cdot \det B$

(11)

- $(A|b)$ $\quad A \in \mathbb{R}^{n\times n}$

Az egyenletrendszer egyértelműen megoldható, ha $\det A \neq 0$

Biz.

$(A|b) \rightsquigarrow (A^*|b^*)$
Gauss ↳ egységtelű és minden oszlopban van vezéregy
↳ $A^* = E \quad \det E = 1$

Gauss eliminációs sorelemi lépései nem változtatják a determináns nullaságát

- Ekvivalens: $(A \in \mathbb{R}^{n\times n})$

① $Ax = 0$ egyértelműen megoldható

② $(A|\begin{smallmatrix}0\\ \vdots \\ 0\end{smallmatrix})$ egyértelműen megoldható

③ A oszlopai lin. ftlen

④ A sorai lin. ftlen

⑤ $\det A \neq 0$

① ⇔ ⑤

① ⇔ ②

$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$

$a_1 \cdot x = 0$
$a_2 \quad x$

$a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0$
$a_2 x_1 + \dots$
$\vdots$

$\Leftrightarrow (A|\begin{smallmatrix}0\\ \vdots \\ 0\end{smallmatrix})$

$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \end{pmatrix} \begin{pmatrix} x_1 & x_2 & \dots \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$

① ⇔ ③ $\quad (a_1 | a_2 | a_3 | \dots)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ $\quad a_1x_1 + a_2x_2 + \dots + a_nx_n = 0$

(12)

$A, B \in \mathbb{R}^{n \times n}$

B az A inverze, ha $A \cdot B = E = B \cdot A$

Jele: A^{-1}

$\exists$ inverze, $\Leftrightarrow \det A \neq 0$

Ha $\exists$ inverze, akkor az egyértelmű

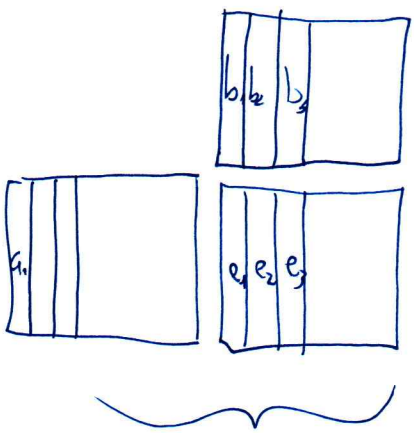
R=2

$A \cdot A^{-1} = E \quad / \det$

$\det (A \cdot A^{-1}) = \det E = 1$

$\det(A) \cdot \det A^{-1} = 1$

↳ egyéb sem csak c.



$A \cdot b_1 = e_1 \quad A b_2 = e_2 \ldots$

$(A|e_1) \quad (A|e_2) \ldots$

egyértelműen oldható ha $\det A \neq 0$

⇓

~~$x_1, x_2, \ldots, x_n$~~ egyértelmű

$b_1, b_2, \ldots, b_n \rightarrow B$ egyértelmű

Megoldás: ~~Gauss~~ Gauss-eliminációval

(több Gauss-t egyszerre)

$$\left(A \mid E \right) \rightsquigarrow \left(E \mid b_1, b_2 b_3, \ldots, b_n \right) = \left(E \mid A^{-1} \right)$$

$$\left(A \mid e_1 e_2 e_3 \ldots e_n \right)$$

$f: \mathbb{R}^n \to \mathbb{R}^n$ lin. tv.

$A := [f]$ $\quad x \longmapsto A \cdot x$ $\quad y = A \cdot x \quad / \cdot A^{-1}$

$A^{-1} y = A^{-1} A x = x$

$x = A^{-1} \cdot y$

① f^{-1} obstoj $\Leftrightarrow \det A \neq 0$

② Ko $\exists f^{-1} \Rightarrow f^{-1}$ lin. tv. $\quad [f^{-1}] = [f]^{-1}$

① $\Leftarrow$ ✓

① $\Rightarrow$ Lege- $\det A = 0 \Rightarrow$ A oslopni lin. od. $\Rightarrow \exists x \neq 0 \quad Ax = 0$

$\left.\begin{array}{l} f(x) = 0 \\ f(0) = 0 \end{array}\right\} x \neq 0 \Rightarrow f$ ne bij. inv.

(13)

$A \in \mathbb{R}^{n \times e}$

A sorrangja r, ha A-ban van r lineárisan független sora, de $r+1$ már nincs. Jele: $s(A) = r$

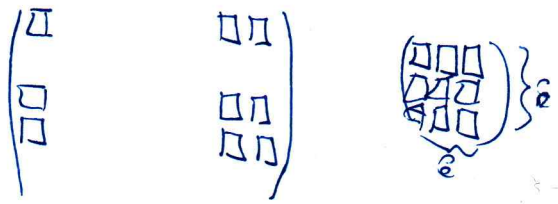
A oszloprangja r, ha ——— " ——— oszlopa, de

——— " ——— $o(A) = r$

A determinánsrangja r, ha van $r \times r$-es nemnulla determinánsú négyzetes részmátrixa, de $(r+1) \times (r+1)$-es már nincs

Jele: $d(A) = r$

Négyzetes részmátrix



Tétel: $s(A) = o(A) = d(A) = r(A)$

Jele: $r(A)$ = mátrix rangja

Biz: ✓

Kiszámítás $A \in \mathbb{R}^{n \times \ell}$ $a_1, a_2, a_3, \dots, a_n$ A-nak sorai

$r(A) = \dim \langle a_1, a_2, a_3, \dots, a_n \rangle$

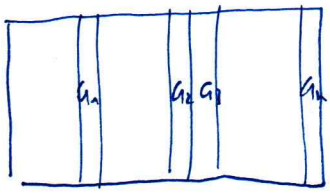
(vagyis a oszlopoké)

Kiszámítás $A \in \mathbb{R}^{n \times \ell}$

$A \overset{\text{Gauss}}{\rightsquigarrow}$ lépcsős alak $r(A) =$ lépcsős alak sorainak száma (nemnulla sor)

I.: elemi sorekvivalens lépések a rangot nem változtatják meg

→ Biz

$A =$ 

$M =$ 

M oszlopai lin. független

$\Leftrightarrow$

$\left(\boxed{M} \,\middle|\, \begin{matrix} * \\ \vdots \\ 0 \end{matrix} \right)$ egyértelműen, h.o. lefő

$r(A) = r(A')$

$A' = \begin{pmatrix} 1 & - & - & - & \cdot \\ 0 & 1 & & & \\ 0 & 0 & 1 & * & \cdot \\ \vdots & 0 & 0 & 0 & \\ & \vdots & \vdots & \vdots & \end{pmatrix}$ $r =$ sorok száma

→ Biz A-ban van r lin. független oszlop, legyen ez $\{a_1, \dots, a_r\} = V$

$a_1, \dots, a_r$ lin. független } ekkor $a_j \in \langle a_1, \dots, a_r \rangle$

$a_1, \dots, a_r, a_j$ lin. összef.

$\dim V = r(A) = r$

(14)

lin. Abb.: $f: \mathbb{R}^n \to \mathbb{R}^k \quad \underline{x} \mapsto f(\underline{x})$

- $\exists A \in \mathbb{R}^{k \times n}: \forall \underline{x} \in \mathbb{R}^n: \quad f(\underline{x}) = A \cdot \underline{x}$
- $k=n \Rightarrow$ lin. Abb.
- $A = [f]$

Def.: ~~f lin. Abb.~~ ~~[illegible]~~ $(f: \mathbb{R}^n \to \mathbb{R}^k)$

$f: \mathbb{R}^n \to \mathbb{R}^k$

f lin. Abb. $\Leftrightarrow$
$\begin{cases} \forall \underline{u}, \underline{v} \in \mathbb{R}^n: & f(\underline{u}+\underline{v}) = f(\underline{u}) + f(\underline{v}) \\ \forall \underline{u} \in \mathbb{R}^n \ \alpha \in \mathbb{R}: & f(\alpha \cdot \underline{u}) = f(\underline{u}) \cdot \alpha \end{cases}$

B.: $\Rightarrow$ $A = [f]$

$A(\underline{u}+\underline{v}) = A\underline{u} + A\underline{v}$ ✓

~~$\alpha \cdot A \cdot \underline{u} = \alpha \cdot A \cdot \underline{u}$~~

$A \cdot (\alpha \cdot \underline{u}) = A \cdot \underline{u} \cdot \alpha$ ✓

$f: \mathbb{R}^n \to \mathbb{R}^k$ $\quad g: \mathbb{R}^k \to \mathbb{R}^m$ $\quad A = [f]$ $\quad B = [g]$

$g \circ f = g(f(x)) = B \cdot (A \cdot x) \overset{T}{=} (B \cdot A)\, x$

$[g \circ f] = B \cdot A = [g] \cdot [f]$

$f: \mathbb{R}^2 \to \mathbb{R}^2$ forgatás α szöggel pl. π.

$$[f] = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

g: forgatás β szöggel

$g(f(x))$: forgatás $\alpha + \beta$ szöggel

$[g \circ f] = [g] \cdot [f]$

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

$$\begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \begin{pmatrix} \square & \\ \square & \end{pmatrix}$$

MX szerzés

$\cos\alpha\cos\beta - \sin\alpha\sin\beta = \cos(\alpha+\beta)$ ✓

$\cos\alpha\sin\beta + \cos\beta\sin\alpha = \sin(\alpha+\beta)$ ✓

(13)

$f: \mathbb{R}^n \to \mathbb{R}^e$ lin. lek.

$$\operatorname{Ker} f = \{ \underline{x} \in \mathbb{R}^n : f(\underline{x}) = \underline{0} \}$$

$$\operatorname{Im} f = \{ \underline{x} \in \mathbb{R}^e : \forall \underline{y} \in \mathbb{R}^n : \underline{x} = f(\underline{y}) \}$$

$$\{ \underline{y} \in \mathbb{R}^e : \exists \underline{x} \in \mathbb{R}^n : f(\underline{x}) = \underline{y} \}$$

$\operatorname{Ker} f$ altér:

$\underline{u}, \underline{v} \in \operatorname{Ker} f \qquad \alpha \in \mathbb{R}$

$f(\underline{u} + \underline{v}) = f(\underline{u}) + f(\underline{v}) = \underline{0} + \underline{0} = \underline{0} \in \operatorname{Ker} f$

$f(\alpha \cdot \underline{u}) = \alpha \cdot f(\underline{u}) = \alpha \cdot \underline{0} = \underline{0} \in \operatorname{Ker} f$

$\operatorname{Im} f$ altér: $A := [f]$ a_1 az A iedik oszlopa

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

$$\left(a_1 \middle| a_2 \middle| \cdots \middle| a_n \right) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \underline{y}$$

$y = x_1 \cdot a_1 + x_2 \cdot a_2 + \ldots + x_n \cdot a_n$

A oszlopainak lineáris kombinációja

$\Downarrow$

$\operatorname{Im} f$ altér

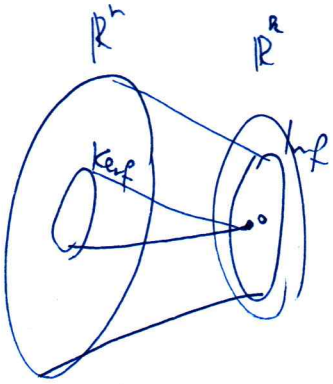
$\dim \operatorname{Im} f = \dim \langle a_1, a_2, \ldots, a_n \rangle = r(A)$

Dimenziótétel

$f: \mathbb{R}^n \to \mathbb{R}^e$ lin. lek.

$\dim \operatorname{Ker} f + \dim \operatorname{Im} f = n$

Bir



Legyen $b_1, b_2, .., b_k$ bázis $Ker f$-ben

Ez kiegészíthető $c_1, c_2, \ldots, c_m$ vektorokkal bázissá $\mathbb{R}^n$-ben

$$\dim Ker f + \dim Im f = n$$

$$\underbrace{\dim Ker f}_{k} + \underbrace{\dim Im f}_{m} = n$$

$w \in Im f$ tetszőleges vektor: $\exists v \in \mathbb{R}^n : f(v) = w$

$$v = \beta_1 b_1 + \beta_2 b_2 + \ldots + \beta_k b_k + \gamma_1 c_1 + \gamma_2 c_2 + \ldots + \gamma_m c_m$$

$$f(v) = f(\beta_1 b_1 + \beta_2 b_2 + \ldots + \beta_k b_k + \gamma_1 c_1 + \gamma_2 c_2 + \ldots + \gamma_m c_m) =$$

$$= \underbrace{\beta_1 f(b_1) + \beta_2 f(b_2) + \ldots + \beta_k f(b_k)}_{0} + \gamma_1 f(c_1) + \gamma_2 f(c_2) + \ldots + \gamma_m f(c_m)$$

$f(c_1), f(c_2), \ldots, f(c_m)$ gen. rendsz. $Im f$-ben

$f(c_1), f(c_2), \ldots, f(c_m)$ lin. független csak triv. lin. komb. 1.

$$\gamma_1 f(c_1) + \gamma_2 f(c_2) + \ldots + \gamma_m f(c_m) = 0$$

$$f(\underbrace{\gamma_1 c_1 + \gamma_2 c_2 + \ldots + \gamma_m c_m}_{\in Ker f}) = 0 \Rightarrow \gamma_1 c_1 + \gamma_2 c_2 + \ldots + \gamma_m c_m = \beta_1 b_1 + \beta_2 b_2 + \ldots + \beta_k b_k$$

$$\Leftarrow$$

$$-\beta_1 b_1 - \beta_2 b_2 - \ldots - \beta_k b_k + \gamma_1 c_1 + \gamma_2 c_2 + \ldots + \gamma_m c_m = 0 \leftarrow \text{gen. rendsz. (def szerint)}$$

$$\Leftarrow$$

$$\beta_1 = \beta_2 = \ldots = \beta_k = \gamma_1 = \gamma_2 = \ldots = \gamma_m = 0 \quad \checkmark$$

16) $f: \mathbb{R}^n \to \mathbb{R}^n$ lin. tr. $\quad B = \{b_1, b_2, \dots, b_n\}$ baza $\mathbb{R}^n$-ben

$$\begin{array}{ccc} \underline{x} & \xrightarrow{f} & f(\underline{x}) \\ h \uparrow & & \downarrow h^{-1} \\ [\underline{x}]_B & \xrightarrow{g} & [f(\underline{x})]_B \end{array}$$

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = [\underline{x}]_B$$

$$B = \left(b_1 \middle| b_2 \middle| \quad \middle| b_n \right) \begin{pmatrix} \quad \\ \quad \\ \quad \end{pmatrix} = B[\underline{x}]_B = \underline{x}$$

$\Big\} \to [h] = B$

$\exists h^{-1}$, ninel $\det B \neq 0$

(B obstoji lin. preh.)

$$[f(\underline{x})]_B = h^{-1}\left(f\left(h\left([\underline{x}]_B\right)\right)\right) = g\left([\underline{x}]_B\right)$$

$g = h^{-1} \circ f \circ h$

$[g] = B^{-1} \cdot [f] \cdot B$

(17) Def

- $A \in \mathbb{R}^{n \times n}$

① $\underline{v} \in \mathbb{R}^n$ sajátvektora A-nak, ha $\underline{v} \neq \underline{0}$ és $\exists \lambda \in \mathbb{R}$: $A \cdot \underline{v} = \lambda \cdot \underline{v}$

② $\lambda \in \mathbb{R}$ sajátértéke A-nak, ha $\exists \underline{v} \in \mathbb{R}^n$, $\underline{v} \neq \underline{0}$: $A\underline{v} = \lambda \cdot \underline{v}$

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \underline{v}$$

- $A \begin{pmatrix} a_{11} & a_{12} & \cdots \\ a_{21} & \cdots & a_{2n} \\ \vdots & & a_{nn} \end{pmatrix} \begin{pmatrix} \\ \\ \\ \\ \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ a_{21}x_1 + \ldots \\ \\ \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{pmatrix}$

$$\begin{pmatrix} (a_{11}-\lambda)x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ a_{21}x_1 + (a_{22}-\lambda)x_2 + \ldots + a_{2n}x_n \\ \ldots \\ (a_{nn}-\lambda)x_n \end{pmatrix} = \underline{0}$$

- $\left(\begin{array}{cccc|c} a_{11}-\lambda & a_{12} & \cdots & & \\ a_{21} & a_{22}-\lambda & & a_{2n} & \\ & & a_{n-1\,n} & & \\ a_{n1} & & a_{n-1\,n} & a_{nn}-\lambda & 0 \end{array}\right)$ $\rightarrow$ $\underline{v}$ ennek megoldása

$\Vert$

$(A - \lambda E \mid \underline{0})$

$\rightarrow \underline{v} = \underline{0}$ mindig megoldás $\Rightarrow \exists \underline{v} \neq \underline{0}$, ha a megoldás nem egyértelmű

$\Downarrow$

$\exists \lambda \in \mathbb{R} \iff \det(A - \lambda E) = 0$

- $\begin{vmatrix} 1-\lambda & 3 \\ 3 & 9-\lambda \end{vmatrix} = (1-\lambda)(9-\lambda) - 9 = 9 - \lambda - 9\lambda + \lambda^2 - 9 = -10\lambda + \lambda^2$

$\lambda_1 = 0 \quad \lambda_2 = 10$

$$\left(\begin{array}{cc|c} 1 & 3 & 0 \\ 3 & 9 & 0 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 3 & 0 \\ 0 & 0 & 0 \end{array}\right) \qquad x_1 + 3x_2 = 0 \ \checkmark$$

$f: \mathbb{R}^n \to \mathbb{R}^n$ lin. fv.

$\mathcal{B}$ bázis $\mathbb{R}^n$-ben

$\mathcal{B} = \{b_1, b_2, \ldots, b_n\}$

$[f]_{\mathcal{B}}$ diagonális $\Leftrightarrow$ $\mathcal{B}$ elemei $[f]$ sajátvektorai

9

$A \in \mathbb{R}^{n\times n}$ mátrix determinánsa az összes lehető bástyaelrendezésben szereplő elemek szorzatának összege az ~~bást~~ elrendezés inverziószámának megfelelően előjelezve

π egy bástyaelrendezés ~~permutációja~~, minden sorból és oszlopból csak egy elem lehet kiválasztva.

$I(\pi)$ a permutáció inverziószáma, az inverzióban (csökkenő sorrendben) álló elemek száma. Ha $I(\pi)$ ps, akkor ⊕ előjel, különben ⊖.

Jele $\det A$

1. sor szorzása skalárral
   oszlop —— " ——

$$\det A = \frac{1}{\alpha} \det A' \qquad \alpha \in \mathbb{R}$$

Minden permutációban egy elem α-szorosára nő

2. sorcsere
   oszlopcsere

$$\det A = -\det A$$

~~mindegyik permutáció inv~~

azonos elemek pont ellentétes előjellel lesznek

3. i. sor += α · j. sor
   ..oszlop..

$$\det A = \det A$$

⊛ Kiszámítása: Gauss elimináció, sorekvivalens lépések

⋮

4. csupa nulla sor/oszlop → $\det A = 0$

5. felső / alsó háromszög $n\times$ → $\det A$ = főátlóban lévő elemek szorzata