



2017/2018.

Bevezetés a számításelméletbe 1

Kidolgozott vizsgatételek

Összeállította: Csia Kitti



Tartalomjegyzék

1. tétel: Számelmélet, kongruencia.....	2
2. tétel: Lineáris kongruencia	7
3. tétel: Euler-Fermat tétel.....	10
4. tétel: Algoritmusok, nyilvános kulcsú titkosítás, RSA.....	13
5. tétel: Térbeli koordinátagéometria.....	21
6. tétel: Alterek, lineáris függetlenség	25
7. tétel: Bázis, dimenzió	31
8. tétel: Gauss-elimináció, RLA.....	35
9. tétel: Determináns	39
10. tétel: Kifejtési tétel, mátrix.....	44
11. tétel: Lineáris egyenletrendszer megoldhatósága	48
12. tétel: Mátrix inverze, rangja	52
13. tétel: Lineáris leképezés, transzformáció.....	59
14. tétel: Magtér, képtér	63
15. tétel: Bázistranszformáció.....	66
16. tétel: Sajátvektor, karakterisztikus polinom	69

Felhasznált irodalom:

Szeszlér Dávid - Bevezetés a számításelméletbe 1

Fleiner Tamás - A számítástudomány alapjai

Talált **HIBA** esetén jelzés: nospatium@gmail.com



1. tétel: Számelmélet, kongruencia

Tételcím

Oszthatóság, prímszámok, a számelmélet alaptétele (csak a felbonthatóság bizonyításával). Prímek száma, $\pi(n)$ nagyságrendje (bizonyítás nélkül). Kongruencia fogalma, alapműveletek kongruenciákkal.

1. Oszthatóság

- Definíció
 - $a \in \mathbb{Z}$ osztója $b \in \mathbb{Z}$, ha létezik olyan $c \in \mathbb{Z}$, melyre $a \cdot c = b$
 - ugyanezt fejezzük ki, ha b -t az a **többszörös**ének mondjuk
- Jelölés
 - ha a osztója b -nek: $a|b$
 - ha a nem osztója b -nek: $a \nmid b$
 - **valódi osztója**, ha fennáll $a|b$ és $1 < |a| < |b|$
- Példa
 - **igaz:** $13|91$, $-7|63$, $2|0$, $-8 \nmid -36$, még $0|0$ hiszen $0 \cdot c = 0$ bármilyen c -re igaz

[K1] megjegyzést írt: A lilával szedett, dőlt szövegek általában egy addig elő nem fordult fontos szó, definíció vagy tétel neve, melynek ismerete fontos.

2. Prímszám

- Definíció
 - $p \in \mathbb{Z}$ prímszámnak nevezzük, ha $|p| > 1$ és p -nek nincs valódi osztója
 - $|p| > 1$ kikötés a $-1, 0, 1$ számok miatt kell, ugyanis ezek se nem prímek, se nem összetettek
 - tehát $p = a \cdot b$ csak akkor lehetséges, ha $a = \pm 1$ vagy $b = \pm 1$
 - ha $|p| > 1$ és p nem prím, akkor **összetett szám**



3. Számelmélet alaptétele

o Tétel

- (1) minden 1-től, 0-tól, (-1) -től különböző \mathbb{Z} szám felbontható prímek szorzatára
- (2) ez a felbontás tényezők sorrendjétől, előjelétől eltekintve egyértelmű
 - pl. 100 felbontása lehet $2 \cdot 2 \cdot 5 \cdot 5$ vagy $(-5) \cdot 2 \cdot 5 \cdot (-2)$

o Bizonyítás (1)

- (felbonthatóság bizonyítása)
- tetszőleges $n \in \mathbb{Z}$ felbontása $|n| > 1$ *prímtényezők* szorzatára
- eljárás végig fenntartja az n egy (± 1) -től különböző egészek szorzatára való bontását
- ha $n = a_1 \cdot \dots \cdot a_k$, ahol a_i mind prím \rightarrow eljárás megáll
- ha tényezők között van összetett szám pl. $a_i \rightarrow$ van valódi osztója, így felírható: $a_i = b \cdot c$, ahol $|b|, |c| > 1$, a_i helyettesíthető $b \cdot c$ -vel \rightarrow eljárás folytatódik
- felbontáskor tényezők száma mindig 1-gyel nő, tényező $||$ legalább 2 \rightarrow eljárás véges sok lépésben elvégezhető (max. $\log_2 |n|$ tényezőszorzattal)

[K2] megjegyzést írt: Szintén egészek.

4. Prímek számossága

o Tétel

- prímek száma végtelen

o Bizonyítás

- **TFI**, prímek száma véges
- p_1, \dots, p_k az összes **+p**
- **!** $N = p_1 \cdot \dots \cdot p_k + 1 \rightarrow N$ **prímtényezők szorzatára bomlik** vagy maga is prím
- N nem osztható egyik p -vel sem, mert +1 maradékot ad mindig, így N minden prímtényezője hiányzik p_k felsorolásból \rightarrow ellentmondás

[K3] megjegyzést írt: Tegyük fel indirekten, hogy...

[K4] megjegyzést írt: Pozitív prím.

[K5] megjegyzést írt: Legyen

[K6] megjegyzést írt: Előző tételnek megfelelően.



5. Szomszédos prímek

o Tétel

- minden $N > 1 \in \mathbb{Z}$ találhatóak olyan $p < q$ prímek, hogy p és q között nincs további prím és $q - p > N$

o Bizonyítás

- be kell látni, hogy létezik N db szomszédos összetett szám
 - ezeknél kisebb prímek közül a legnagyobb p
 - ezeknél nagyobb prímek közül legkisebb q
- $a_i = (N + 1)! + i$
 - $i = 2, 3, \dots, (N + 1)$
 - N db a_2, a_3, \dots, a_{N+1}
 - összetettek, mert minden $2 \leq i \leq N + 1$ esetén a_i -nek valódi osztója $i \rightarrow (N + 1)!$ nyilván osztható $\rightarrow i$ -t adva ismét i -vel osztható számot kapunk

6. Nagy prímszámítétel

o Tétel

$$\pi(n) \approx \frac{n}{\ln n} \text{ vagyis } \lim_{n \rightarrow \infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$$

- $\pi(n)$ értékére jó becslés $\frac{n}{\ln n}$ abban az értelemben, hogy a becslés relatív hibája n növekedtével 0-hoz konvergál

[K7] megjegyzést írt: Aszimptotikus egyenlőség: $a_n \approx b_n \rightarrow$ tehát a_n sorozat akkor aszimptotikusan egyenlő b_n -nel, ha a 2 sorozat hányadosa 1-hez konvergál.

7. Kongruencia

o Definíció

- $a, b, m \neq 0, \in \mathbb{Z}$ **kongruens** b modulo m , ha a -t és b -t m -mel maradékosan osztva azonos maradékot kapunk

o Jelölés

- $a \equiv b \pmod{m}$

o Állítás

- fenti akkor és csak akkor igaz, ha $m | a - b$

o Bizonyítás

- a maradéka r_1 és b maradéka r_2 , m -mel osztva
- valamely $k_1, k_2 \in \mathbb{Z}$, ahol $0 \leq r_1, r_2 \leq m - 1$

[K8] megjegyzést írt: Legyen...



- $a = k_1 \cdot m + r_1$
- $b = k_2 \cdot m + r_2$
- a és b szerep szimmetrikus $\rightarrow r_1 \geq r_2$:
$$a - b = (k_1 - k_2) \cdot m + (r_1 - r_2) \quad /: m$$
 - maradék $r_1 - r_2$
- $m|a - b$ akkor teljesül, ha $r_1 = r_2$,
- definíció szerint ez *ekvivalens* ezzel: $a \equiv b (m)$

8. Alpműveletek kongruenciákkal

○ Tétel

- TFH. $a \equiv b (m)$ és $c \equiv d (m)$ fennállnak $a, b, c, d, m \in \mathbb{Z}, k \geq 1$ tetszőleges

$$(1) a + c \equiv b + d (m)$$

$$(1) a - c \equiv b - d (m)$$

$$(2) a \cdot c \equiv b \cdot d (m)$$

$$(3) a^k \equiv b^k (m)$$

○ Bizonyítás (1)

- előző definícióra alapozva
- m -mel osztható számok (+) és (-) is m -mel osztható \rightarrow
$$m|(a - b) + (c - d) = (a + c) - (b + d)$$
$$m|(a - b) - (c - d) = (a - c) - (b - d)$$
 - definíció miatt ismét igaz

○ Bizonyítás (2)

- mivel egy m -mel osztható szám bármely többszöröse is m -mel osztható, így

$$m|a - b$$

$$m|c \cdot (a - b)$$

$$m|a \cdot c - b \cdot c$$

- (hasonló $b(c - d)$), tehát:

$$m|(ac - bc) + (bc - bd) = ac - bd$$



○ **Bizonyítás (3)**

- Bizonyítás (2)-re alapozva, de itt most $c = a$ és $d = b$
- ekkora kapjuk: $a^2 \equiv b^2 (m)$
- újra alkalmazva előző bizonyítást kapjuk: $a^3 \equiv b^3 (m)$
- és ezt folytatva jutunk el: $a^k \equiv b^k (m)$

9. A kongruencia tétel

○ **Tétel**

- a, b, c, m tetszőlegesek és $d = \text{KÖZÖS}(c, m)$
- $a \cdot c \equiv b \cdot c (m)$
- akkor, és csak akkor igaz, ha $a \equiv b \left(\frac{m}{d}\right)$

[K9] megjegyzést írt: $d = \text{KÖZÖS}(c, m)$, tehát $d = c$ és m legnagyobb közös osztójaival.

○ **Bizonyítás**

- $c' = \frac{c}{d}$ és $m' = \frac{m}{d}$ ($c', m' \in \mathbb{Z}$, mert d közös osztójuk)
- $(c', m') = 1$, ellenkező esetben d egy d -nél nagyobb közös osztó volna
- kongruencia állítás:
 $a \cdot c \equiv b \cdot c (m) \rightarrow m | ac - bc = c(a - b)$
 - ez ekvivalens azzal, hogy:
 - $m' | c'(a - b) \rightarrow$ tovább ekvivalens $m' | a - b$

[K10] megjegyzést írt: Mert az $m \cdot k = c(a - b)$ egyenlet is ekvivalens az $m' \cdot k = c'(a - b)$



2. tétel: Lineáris kongruencia

Tételcím

Lineáris kongruenciák: a megoldhatóság szükséges és elégséges feltétele, a megoldások száma. Euklideszi algoritmus, annak lépésszáma, alkalmazása lineáris kongruenciák megoldására is (konkrét, megadott példán).

1. Eukleideszi algoritmus

o Definíció

▪ input: a, m ($0 < a < m$)

▪ output: (a, m)

▪ 1. lépés:

- m -et maradékosan osztjuk a -val, megkapva a maradékot, felírjuk őket a következő módon:

$$a = b \cdot q_1 + r_1$$

▪ 2. lépés:

- a -t elosztjuk a kapott maradékkal:

$$b = r_1 \cdot q_2 + r_2$$

▪ ... i . lépés:

- $(i - 2)$ lépésben kapott maradékot elosztjuk $(i - 1)$ -ben kapottal:

$$r_{i-2} = r_{i-1} \cdot q_i + r_i$$

▪ utolsó lépés:

- akkor érünk el ide, ha $r_i = 0$, ekkor r_{i-1} lesz az Inko

2. Eukleideszi algoritmus

o Állítás

- Eukleideszi algoritmus végrehajtása után $r_k = (a, m)$

[K11] megjegyzést írt: Példa:
(121, 39) legnagyobb közös osztója:
 $121 = 39 \cdot 3 + 4$
 $39 = 4 \cdot 9 + 3$
 $4 = 3 \cdot 1 + 1 \rightarrow$ maradék 1, megoldások száma tehát: 1

[K12] megjegyzést írt: a, m legnagyobb közös osztóját kapjuk meg.



o Bizonyítás

- $m \equiv r_1 \pmod{a}$
- ha $a \equiv b \pmod{m}$ teljesül, akkor $(a, m) = (b, m)$
 - ezt alkalmazva: $(a, m) = (a, r_1)$
$$a \equiv r_2 \pmod{r_1}$$
$$(a, r_1) = (r_1, r_2) \rightarrow$$
$$(a, m) = (a, r_1) = (r_1, r_2) = \dots = (r_{k-1}, r_k)$$
- legutolsó $(k + 1)$ lépés szerint
$$r_k | r_{k-1} \rightarrow (r_{k-1}, r_k) = r_k$$

3. Eukleideszi algoritmus lépésszáma

o Állítás

- Eukleideszi algoritmus *polinomiális időben* lefut
- legfeljebb $2 \cdot \lceil \log_2 a \rceil$ maradékos osztás után áll meg

o Bizonyítás

- vizsgáljuk meg az eljárás egy tetszőleges lépést:
 - $r_{i-2} = t_i \cdot r_{i-1} + r_i$, ahol a fentiek szerint
$$r_{i-2} > r_{i-1} > r_i$$
- tehát:
 - $t_i \geq 1$ ($r_{i-2} > r_{i-1}$ miatt) következik:
 - $r_{i-2} \geq r_{i-1} + r_i$, ebből viszont
 - $r_{i-1} > r_i$ miatt $\rightarrow r_{i-2} > 2r_i$
- így az eljárás páros számú soraiból ezt kapjuk:
$$a = r_0 > 2r_2 > 4r_4 > \dots > 2^k \cdot r_{2k}$$
- a $k = \lceil \log_2 a \rceil$ választással $2^k \geq a$
- (TFI r_{2k} maradékkal még nem ért véget)
 - $0 < r_{2k} < \frac{a}{2^k} \leq 1 \rightarrow$ ellentmondást kapnánk

[K13] megjegyzést írt: Ebből következik, hogy az Eukleideszi algoritmus polinomiális futásiidejű (de még ezen belül is nagyon hatékony), hiszen $\log_2 a$ az a jegyei számának konstanszorosa.



4. Lineáris kongruenciák megoldhatósága

o **Tétel**

- $a \cdot x \equiv b \pmod{m}$ lineáris kongruencia akkor és csak akkor megoldható, ha $(a, m) | b$
- ha teljesül, akkor megoldásainak száma modulo m egyenlő (a, m) -val

o **Bizonyítás**

- (szükségesség igazolása)

- $d = (a, m)$, $a = a'd$, $m = m'd$
- ha az $a \cdot x \equiv b \pmod{m}$ megoldható, akkor

$$d \mid m \mid ax - b \rightarrow$$

$$d \mid a \mid ax \rightarrow$$

$$d \mid ax - (ax - b) = b$$

- TFH. $d \mid b$, azaz $b = db'$ $\wedge d$ (modulust is)

- $a'x \equiv b' \pmod{m'}$

- mivel $d = (m, a)$, így leosztás után $(a', m') = 1$

- Eukleideszi algoritmus segítségével **in**ko előáll \rightarrow kiszámíthatunk olyan $k, l \in \mathbb{Z}$, amire $ka' + lm' = 1$

- k, l nem lehet közös prímosztója \rightarrow relatív prímek

$$a'x \equiv b' \pmod{m'} \quad / \cdot k$$

$$ka'x \equiv kb' \pmod{m'}$$

$$(1 - lm')x \equiv kb' \pmod{m'} \quad / + lm'x \equiv 0 \pmod{m'}$$

$$x \equiv kb' \pmod{m'}$$

- megoldások modulo m megadása

- mivel $m = m'd$, ezért minden m' szerinti **maradékosztály** pontosan d db m szerinti maradékosztály uniója

- konkrét esetben:

$$x \equiv kb' \pmod{m} \text{ vagy } \dots$$

$$x \equiv kb' + m' \pmod{m} \text{ vagy } \dots$$

$$x \equiv kb' + 2m' \pmod{m} \dots$$

[K14] megjegyzést írt: Ebből következik, hogy...

[K15] megjegyzést írt: Legnagyobb közös osztó.

[K16] megjegyzést írt: Az elvégzett átalakítások ekvivalens volta miatt az $a \cdot x = b$ kongruencia megoldásai pontosan azok az $x \in \mathbb{Z}$, amelyek modulo m' a kb' -vel egy maradékosztályba tartoznak.



3. tétel: Euler-Fermat tétel

Tételcím

Euler-féle φ -függvény, képlet a meghatározására (csak prímszámra esetre bizonyítva). Redukált maradékrendszer, Euler-Fermat-tétel, kis Fermat-tétel. Két kongruenciából álló kongruenciarendszer megoldása (konkrét, megadott példán).

1. Euler-féle φ -függvény

○ Definíció:

- ha $n \geq 2, \in \mathbb{Z}$, akkor az $1, \dots, n - 1$ számok között n -hez relatív prímszámok számát $\varphi(n)$ -nel jelöljük

[K17] megjegyzést írt: $n \rightarrow \varphi(n)$

2. Euler-féle φ -függvény képlet

○ Tétel

- ! az $n \geq 2, \in \mathbb{Z}$ kanonikus alakja $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$, ekkor:

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdot \dots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k-1})$$

○ Bizonyítás

- TFH. $n \in \mathbb{Z}$ prímtényezős felbontásban csak 1 prímszám (p) van
- $n = p^\alpha$ ($\alpha \geq 1$)
- ekkor $(n, a) > 1$, akkor és csak akkor igaz, ha $p|a$
- $1, \dots, n$ számok közül $\frac{n}{p} = p^{\alpha-1}$ db nem relatív prímszám n -hez
- definíció szerint: $\varphi(n) = n - p^{\alpha-1} = p^\alpha - p^{\alpha-1}$
- \rightarrow tehát igaz minden prímszámra

[K18] megjegyzést írt: Különböző a és n prímtényezős felbontásában nem lehet közös prímszám.

[K19] megjegyzést írt: Ugyanis nyilván ennyi a p -vel osztható számok száma.

3. Redukált maradékrendszer

○ Definíció

- $R = \{c_1, \dots, c_k\}$ számhalmaz *redukált maradékrendszer* modulo m , ha a következő feltételek teljesülnek:



- **(1)** $(c_i, m) = 1$ minden $i = 1, \dots, k$ esetén
- **(2)** $(c_i \neq c_j) (m)$ bármely $i \neq j, 1 \leq i, j \leq k$ esetén
- **(3)** $k = \varphi(m)$

o Példa

- modulo 10 redmar. az $\{1, 3, 7, 9\}, \{21, 43, 67, 89\}, \{1, -1, 3, -3\}$

[K20] megjegyzést írt: Redukált maradékrendszer.

4. Redukált maradékrendszer állítás

o Állítás

- $R = \{c_1, \dots, c_k\}$ redmar. modulo $m \in \mathbb{Z}$, amely $(a, m) = 1$
- $\rightarrow R' = \{a \cdot c_1, \dots, a \cdot c_k\}$ szintén redmar. modulo m

o Bizonyítás

- megmutatni, hogy R' -re is igaz, ami R -re is
- **(1)** (1. tétel, Számelmélet alaptétel szerint) $a \cdot c_i$ és m prímtényezősz felbontásában nem lehet közös prím, ha külön a -ban és m -ben vagy c -ben és m -ben
- **(2)** bizonyításához TFH.:

$$a \cdot c_i \equiv a \cdot c_j \pmod{m} \quad /: a$$

$$c_i \equiv c_j \pmod{m}$$

[K21] megjegyzést írt: Nincs.

[K22] megjegyzést írt: Valamely $1 \leq i, j \leq k$

[K23] megjegyzést írt: $(a, m) = 1$ miatt modulus nem változik.

- mivel R -re teljesül **(2)**, amely csak $i = j$ esetben fordulhat elő
- mivel R és R' elemszáma =, így **(3)** teljesül R' -re

5. Euler-Fermat-tétel

o Tétel

- ha az $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$

[K24] megjegyzést írt: $a, m \geq 2, \in \mathbb{Z}$

o Bizonyítás

- $R = \{c_1, \dots, c_k\}$ tetszőleges redmar. modulo m
- mivel $(a, m) = 1$ redmar. def. miatt $R' = \{a \cdot c_1, \dots, a \cdot c_k\} \pmod{m}$
- R és R' elemei párba állíthatók, párok kongruensek modulo m
- (1. tétel, Alapműveletek kongruenciákkal (3) tulajdonságot használva) $\rightarrow R$ és R' elemeit összeszorozva modulo m kongruens eredményeket kapunk:

[K25] megjegyzést írt: Redukált maradékrendszer definíciója.



$$c_1 \cdot \dots \cdot c_k \equiv (a \cdot c_1) \cdot \dots \cdot (a \cdot c_k) \pmod{m}$$

$$c_1 \cdot \dots \cdot c_k \equiv a^{\varphi(m)} \cdot c_1 \cdot \dots \cdot c_k \pmod{m} \quad /: c_1 \cdot \dots \cdot c_k$$

- mivel $(c_i, m) = 1$, ezért (1. tétel, Számelmélet alaptétel következtében) $(c_1 \cdot \dots \cdot c_k, m) = 1$ is igaz
- osztással a modulus nem változik, így megkaptuk a tételt

6. „Kis” Fermat-tétel

o Tétel

- ha p prím és $a \in \mathbb{Z}$, akkor $a^p \equiv a \pmod{p}$

o Bizonyítás

- tétel állítása magától értetődő, ha $p|a$
 - ekkor $p|a^p$ is igaz $p|a \rightarrow a^p \equiv 0 \equiv a \pmod{p}$
- ha $p \nmid a \rightarrow (a, p) = 1$ is igaz
 - Euler-Fermat-tétel a -ra és p -re
 - $\varphi(p) = p - 1$ miatt
$$a^{p-1} \equiv 1 \pmod{p} \quad / \cdot a$$
$$a^p \equiv a \pmod{p}$$

[K26] megjegyzést írt: Mert p prím.



4. tétel: Algoritmusok, nyilvános kulcsú titkosítás, RSA

Tételcím

Polinomiális futásidejű algoritmus (vázlatos) fogalma. Számelmélet és algoritmusok: alpműveletek, hatványozás az egészek körében és modulo m (ez utóbbi konkrét, megadott példán), ezek lépésszáma. Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosítás, megvalósítása RSA-kóddal.

1. Polinomiális futásidejű algoritmus

- Definíció
 - az algoritmust *polinomiális futásidejűnek* tekintjük, ha n méretű bemenethez tartozó $f(n)$ függvényre, mely az *algoritmus lépésszámát* határozza meg
 - minden n esetén fennáll:

$$f(n) \leq c \cdot n^k$$

[K27] megjegyzést írt: c és k rögzített konstansok.

2. Számelméleti algoritmusok

- Összefoglaló (számelméleti algoritmusok hatékonysága)
 - bemenet méretét mindig a bemenetet adó számok összes számjegyének számával *mérjük*
 - algoritmus *hatékony*, ha:
 - n jegyű számokon $\max c \cdot n$ vagy $c \cdot n^2$ vagy $c \cdot n^k$ lépést tesz meg
- Alpműveletek
 - összeadás feladata:
 - bemenet: $a, b \in \mathbb{Z}$
 - kimenet: $a + b$
 - ezzel analóg a kivonás, szorzás

[K28] megjegyzést írt: Azonosítható a számok (pl. 10-es alapú) logaritmusával.

[K29] megjegyzést írt: Elméletben és többnyire gyakorlatban, gyakorlatban ezek többszáz jegyű számok, melyeket a példák kedvéért 2-3 jegyű számokon illusztrálják.

[K30] megjegyzést írt: Valamely fix k -ra.



- maradékos osztás feladata:
 - $\frac{a}{b}$ alsó egészrésze, jelölés: $\left\lfloor \frac{a}{b} \right\rfloor$
 - a -nak b szerint vett osztási maradéka, jelölése: $a \bmod b$
- már alsó tagozatból ismert „írásbeli” algoritmusok megfelelők erre
- viszont, ha a és b jegyeinek száma k és l , akkor az algoritmusok lépésszáma $a(z)$...
 - írásbeli összeadás, kivonásnak: $c \cdot (k + l)$
 - szorzás, osztásnak: $c \cdot k \cdot l$
- $n = k + l$
 - összeadás, kivonás: $c \cdot n$
 - szorzás, osztás: $c \cdot n^2$
- tehát: polinomiális futásidejű \rightarrow hatékony algoritmusok
- hatványozás feladat:
 - bemenet: $a, b \in \mathbb{Z}$
 - kimenet: a^b
- ennek már nem adható hatékony algoritmus, mert a kimenet kiírása is túl sok ideig tart
 - pl. $a = 2$ esetében 2^b jegyeinek száma $\log_{10} 2^b = b \cdot \log_{10} 2 \geq \log_{10} 2 \cdot 10^{n-1} > 0,03 \cdot 10^n$
 - vagyis 2^b jegyeinek száma exponenciális függvénye b
- Hatványozás modulo m
 - nyilvános kulcsú titkosításhoz alapvető
 - kimenetet nem tudjuk kiszámítani a fentiek szerint, de annak adott m szerinti maradékát meg tudjuk határozni
 - hatványozás feladat:
 - bemenet: $a, b, m \in \mathbb{Z}$
 - kimenet: $a^b \bmod m$ vagyis a^b osztási maradéka m szerint
 - kiírási probléma megoldva, mert a kimenet $< m$
 - a^b még mindig nem kiszámítható \rightarrow
 - a, a^2, \dots, a^b m szerinti maradékokat sorra kiszámoljuk

[K31] megjegyzést írt: Maradékos osztásnál az alsó egészrész igazából egy lekerekítés, felső egészrésznél meg fel.

pl.:

$12:5 = 2,4$

ennek alsó egészrésze: 2, felső: 3

FunFact:

Jelölést Gauss vezette be az alsó egészrésze; a $\lfloor x \rfloor$ és a $\lceil x \rceil$ jelek Kenneth E. Iversontól származnak. A német nyelvben ma is használják a Gauß-Klammer nevet az alsó egészrésze.

[K32] megjegyzést írt: Valamilyen c konstansra

[K33] megjegyzést írt: Létezik ennél gyorsabb futásidejű algoritmus is, de ezeknél csak jóval nagyobb számok esetén sikerül futásidőt megtakarítani

[K34] megjegyzést írt: Ha b például 100 jegyű, akkor 2^b jegyeinek száma $3 \cdot 10^{98}$ -nál több, így a kiírás még akkor is lehetetlen volna, ha a világegyetemben található minden protonra ráírhatnánk egy kimenet egy számjegyét.

[K35] megjegyzést írt: Előző maradék a -szorosának m szerinti maradékát vesszük.



- ez az eljárás szintén használhatatlanul lassú: $b - 1$ db ilyen lépést kell tenni, ez exponenciális lépésszámú algoritmus
- erre hatékony algoritmus: **ismételt négyzetre emelések módszere**
- példa: 13^{53} maradéka 97-tel osztva

$$13^1 \equiv 13 \pmod{97}$$

$$13^2 = 169 \equiv 72 \pmod{97}$$

$$13^4 = (13^2)^2 \equiv 72^2 = 5184 \equiv 43 \pmod{97}$$

⋮

$$13^{32} = (13^{16})^2 \equiv 36^2 = 1296 \equiv 35 \pmod{97}$$

- ezzel a módszerrel 13-nak a 2-hatvány kitevőjű hatványait tudjuk meghatározni
- a sort nem tudjuk tovább négyzetre emelni, így
- $13^{53} = 13^{1+4+16+32} = 13^1 \cdot 13^4 \cdot 13^{16} \cdot 13^{32}$
- részekre bontva:

$$13^5 = 13^1 \cdot 13^4 = 13 \cdot 43 = 559 \equiv 74 \pmod{97}$$

$$13^{21} = 13^5 \cdot 13^{16} = 74 \cdot 36 = 2664 \equiv 45 \pmod{97}$$

$$13^{53} = 13^{21} \cdot 13^{32} = 45 \cdot 35 = 1575 \equiv 23 \pmod{97}$$

- végeredmény: $13^{53} \equiv 23 \pmod{97}$
 - az algoritmus tehát meghatározza a^t maradékát m szerint minden $t \leq b$ 2-hatványra, vagyis $t = 2^k$ kitevőkre, ahol $k = 0, 1, \dots, \lceil \log_2 b \rceil$
 - az így kapott maradékokból áll elő a^b maradéka is
 - tehát a maradékok kiszámítását érdemes párhuzamosan végezni a négyzetre emelésekkel, teljes leírása:
- **ismételt négyzetre emelések módszere ($a^b \bmod m$ kiszámítására)**

- bemenet: a, b, m , (amelyekre teljesül, hogy $0 < a < m, b \geq 1$)

▪ **0. lépés**

- $c \leftarrow 1$

▪ **1. lépés**

- ha b páratlan, akkor: $c \leftarrow c \cdot a \bmod m$
- ha páros, akkor b változatlan marad

[K36] megjegyzést írt: Mindegyik sor az előző sor négyzetre emelésével keletkezik.



- **2. lépés**
 - $b \leftarrow \lfloor \frac{b}{2} \rfloor$
- **3. lépés**
 - ha $b = 0$, akkor: PRINT „ $a^b \bmod m =$ ”, c ; STOP
- **4. lépés**
 - $a \leftarrow a^2 \bmod m$
 - folytassuk az **1. lépésnél**
- feladat újonnan végrehajtása ennek a módszernek a segítségével
- $a = 13, b = 53, m = 97, k =$ ciklus hányadszorra hajtódott végre, $c =$ végeredmény

k	a	b	c
0	13	53	1
1	72	26	13
2	43	13	13
3	6	6	74
4	36	3	74
5	35	1	45
6	–	0	23

- sorra ugyanazok az értékek keletkeztek, mint amelyeket a korábbi számításban kaptunk

3. Prímtesztelés, Fermat-teszt

- bemenet: $m \in \mathbb{Z}$
- **0. lépés**
 - $k \leftarrow 1$
- **1. lépés**
 - generáljunk véletlen számot 1 és $m - 1$ között
- **2. lépés**
 - Euklideszi-algoritmussal számoljuk ki (a, m) értékét
 - ha $(a, m) \neq 1, m$ nem prím, STOP



3. lépés

- számítsuk ki $a^{m-1} \pmod{m}$ értékét Ismételt négyzetre emelések módszerével
- ha $a \neq 1$, m nem prím, STOP

4. lépés

- ha $k = 100$, m valószínűleg prím

5. lépés

- $k \leftarrow k + 1$, vissza az **1. lépéshez**

o fenti eljárás más szavakkal, krimis stílusban:

- a véletlen számokat sorban a tanúk padjára idézzük
- a vallomása az $a^{m-1} \pmod{m}$ értéke
 - ha ez 1, akkor a nem közöl információt m prímiségét illetően, ekkor a **cinkosa**
 - ha $a \neq 1$, akkor a leleplezi m összetettségét, tehát a **árulója**
 - ♦ nem szokás árulónak nevezni a -t, ha $(a, m) > 1$
 - ha találunk olyan $0 < a < m$ számot, melyre $(a, m) \neq 1$
 - ♦ ekkor az Eukleideszi algoritmus az m egy valódi osztóját megtalálja
 - így a további információkat ad ki m -ről, tehát a **leleplezője**

[K37] megjegyzést írt: $(a, m) = 1$ esetben, a vallomás csak is 1 és m közötti, m -hez relatív prím a -kra vonatkozik.

[K38] megjegyzést írt: $a^{m-1} \pmod{m} \equiv 1$

4. Fermat-teszt árulók száma

o Tétel

- ha $m > 1$ összetett szám és m -nek van árulója, akkor az 1 és m közötti, m -hez relatív prímszámoknak legalább a fele áruló

o Bizonyítás

- a tetszőleges árulója m -nek, $c_1 \cdot \dots \cdot c_k$ az m összes cinkosa
- mutassuk meg, hogy $a_i = (a \cdot c_i \pmod{m})$, $i = 1, \dots, k$ számok páronként különböző árulói m -nek
- ebből következni fog, hogy az árulók száma legalább akkora, mint a cinkosok száma, amely ekvivalens a tétellel
- mivel $(a, m) = 1$ és $(c_i, m) = 1$ miatt $(a \cdot c_i, m) = 1$

[K39] megjegyzést írt: és 1. tétel, Számelmélet alaptétel miatt. alt



- így (a 3. tétel, Euler-féle φ -függvény állítása szerint) $(a_i, m) = 1$ is igaz, mert $a_i \equiv a \cdot c_i \pmod{m}$

- továbbá: $a_i \equiv a \cdot c_i \pmod{m}$ $(m - 1)$ -edik hatványra emelve:

$$a^{m-1} \equiv (a \cdot c_i)^{m-1} = a^{m-1} \cdot c_i^{m-1} \equiv a^{m-1} \cdot 1 \not\equiv 1 \pmod{m}$$

- ebből következik, hogy a_i is áruelő
- végül megmutatjuk, hogy az $a_1 \cdot a_2 \cdot \dots \cdot a_k$ áruelő páronként különbözök
- TFI $a_i = a_j$ valamely $1 \leq i, j \leq k, i \neq j$ esetén \rightarrow

$$a \cdot c_i \equiv a \cdot c_j \pmod{m} \quad /: a$$

$$c_i \equiv c_j \pmod{m}$$

- ez azonban $1 \leq i, j \leq k, i \neq j$ miatt ellentmondás, így beláttuk

5. Carmichael-számok

o Definíció

- az $m > 1$ összetett számot *univerzális álprímnek* más néven *Carmichael-szám*nak nevezzük, ha nincs áruelőja
- vagyis minden $1 < a < m, (a, m) = 1$ esetén $a^{m-1} \equiv 1 \pmod{m}$

6. A nyilvános kulcsú titkosítás

- o generálunk 2 db 300 jegyű prímszámot: p, q
- o $N = p \cdot q \rightarrow$ ha csak N -et ismerjük, nem fogjuk tudni megadni egy valódi osztóját
- o nyilvános kulcsú titkosítás alapfeladatát megoldó módszer
 - olyan $C, D: \{0, 1, \dots, N - 1\} \rightarrow \{0, 1, \dots, N - 1\}$ kölcsönösen egyértelmű függvényeket keresünk, melyek
 - minden $x \in \{0, 1, \dots, N - 1\}$ esetén $D(C(x)) = x$, vagyis $C - D$, egymás inverze
 - kód „tulajdonosa” $C(x), D(x)$ értékét ki tudja számítani
 - $C(x)$ kiszámítására vonatkozó eljárás nyilvánosságra hozható, $D(x)$ -t nem lehet kiszámolni vele
- o tehát N biztos sok számjegyű
- o függvénytár birtokában a kód tulajdonosa biztonságosan tud üzenetet fogadni kódgejeztetés nélkül

[K40] megjegyzést írt: Felhasználtuk, hogy $c_i^{m-1} \equiv 1 \pmod{m}$, $a^{m-1} \not\equiv 1 \pmod{m}$, mert c_i cinkos és a áruelő.

[K41] megjegyzést írt: Hiszen $(a, m) = 1$ miatt modulus nem változik.

[K42] megjegyzést írt: Ha kevés lenne, akkor $x = 0, 1, \dots, N - 1$ próbálgatással $C(x)$ -ből megkapható x



- elküldi C függvényt kiszámító eljárást, partner pedig x üzenet helyett annak $y = C(x)$ kódját küldi
- tulajdonos D -t ($D(y) = D(C(x)) = x$ -el ki tudja számolni)
- ha a két fél rendelkezik C, D függvénytípárral, akkor a kommunikáció teljesen biztonságos
- RSA (Rivest-Shamir-Adleman) algoritmussal való megoldás a legszélesebb körű
- (ehhez szükséges állítás:)

○ **Állítás**

- p, q különböző prímek és $N = p \cdot q$
- ekkor tetszőleges x és $k \geq 1$ egészekre

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

○ **Bizonyítás**

- ha $(x, N) = 1$, akkor az állítás következménye (a 3. tétel, Euler-Fermat tételnek): $x^{\varphi(N)} \equiv 1 \pmod{N}$, $\cdot x \rightarrow$ állítást kapjuk
- ha $(x, N) \neq 1$, akkor $p|x$ vagy $q|x$
- ha mindkettő teljesül, akkor $N|x$, így a bizonyítandó állítás $0 \equiv 0 \pmod{N}$, magától értetődő
- TFH $p \nmid x$ vagy $q \nmid x$
- mivel p prím és $q \nmid x$, ezért $(x, p) = 1$, $\varphi(p) = p - 1$, Euler-Fermat tétel miatt

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

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

- ugyanez a kongruencia modulo q és N is fennáll
- $p|x^{k \cdot \varphi(N)+1} - x$ és $q|x^{k \cdot \varphi(N)+1} - x \rightarrow p \cdot q|x^{k \cdot \varphi(N)+1} - x$

7. RSA algoritmus

- előző $N = p \cdot q$ dolgozva, és legyen $c \in \mathbb{Z}$, amelyre: $(c, \varphi(N)) = 1$
- tegyük közzé a C kódoló függvényünk

$$C: x \rightarrow x^c \pmod{N}$$

- kiszámolható ismételt négyzetre emelések módszerével
- D keresése hasonló módon:

[K43] megjegyzést írt: Ezen alapszik a https protokoll is.

[K44] megjegyzést írt: $p|x$ vagy $q|x$ bizonyítás ezzel analóg.

[K45] megjegyzést írt: $\varphi(N) = (p-1)(q-1)$

[K46] megjegyzést írt: $N =$ csupa különböző prím szorzatára is megfelel ez a bizonyítás.



$$D: y \rightarrow y^d \pmod N$$

- o d -t úgy választjuk, hogy D C inverze legyen
- o ez akkor teljesül, ha $D(C(x)) = x$ minden $0 \leq x \leq N - 1$ esetén, ami

$$C(x) \equiv x^c \pmod N \rightarrow x^{c \cdot d} \equiv x \pmod N$$

- o a fent említett állítás miatt
 - D inverze lesz C -nek, ha d értékét sikerül úgy megválasztanunk, hogy $c \cdot d = k \cdot \varphi(N) + 1$ teljesül valamely $k \geq 1$ egészre
 - tehát a cél ezen kongruencia kielégítése
 - $c \cdot d \equiv 1 \pmod{\varphi(N)}$
 - itt $c, \varphi(N)$ adottak, d -re egy lineáris kongruencia feladat, amely megoldható, de d kiszámítható Euklideszi algoritmussal is

[K47] megjegyzést írt: $D(C(x)) \equiv x^{c \cdot d} \pmod N$ miatt ekvivalens a második feltétellel.

[K48] megjegyzést írt: c választáskor előrelátóan teljesített és $(c, \varphi(N)) = 1$ feltétel miatt.



5. tétel: Térbeli koordinátageometria

Tétalcím

Térbeli koordinátageometria: sík egyenlete, egyenes egyenletrendszerei. Skaláris szorzat fogalma és kiszámítása (bizonyítás nélkül); vektoriális szorzat fogalma és kiszámítása (bizonyítás nélkül). Adott térbeli vektorok lineáris függetlenségének, \mathbb{R}^3 -beli generátorrendszer voltának, illetve bázis voltának geometriai feltétele.

1. Térvektor tulajdonságok

o Tétel

- $\underline{u} = (u_1, u_2, u_3) \in \mathbb{R}^3$ és $\underline{v} = (v_1, v_2, v_3) \in \mathbb{R}^3$ térvektorok, $\lambda \in \mathbb{R}$
 - $\underline{u} + \underline{v} = (u_1 + v_1, u_2 + v_2, u_3 + v_3)$
 - $\underline{u} - \underline{v} = (u_1 - v_1, u_2 - v_2, u_3 - v_3)$
 - $\lambda \cdot \underline{u} = (\lambda \cdot u_1, \lambda \cdot u_2, \lambda \cdot u_3)$

2. Skaláris szorzat

o Definíció

- \underline{u} és \underline{v} *skaláris szorzatán* az alábbiértjük:
 - $\underline{u} \cdot \underline{v} = |\underline{u}| \cdot |\underline{v}| \cdot \cos \gamma$
- ha $\gamma = k \cdot 90^\circ$, $k \in \mathbb{Z}$, akkor a szorzatösszeg 0

[K49] megjegyzést írt: $0^\circ \leq \gamma \leq 180^\circ$

3. Skaláris szorzat tétele

o Tétel

- $\underline{u} = (u_1, u_2, u_3) \in \mathbb{R}^3$ és $\underline{v} = (v_1, v_2, v_3) \in \mathbb{R}^3$ térvektorok, ekkor:

$$\underline{u} \cdot \underline{v} = u_1 \cdot v_1 + u_2 \cdot v_2 + u_3 \cdot v_3$$



4. Egyenes

○ Definíció

- az e egyenes paraméteres egyenletrendszerére (*fenti Térvektor tulajdonságok tétele miatt*)
- $P_0(x_0, y_0, z_0)$ pont rajta van az egyenesen
- $\underline{v} = (a, b, c) \neq 0$ *irányvektora*

$$x = x_0 + \lambda \cdot a$$

$$y = y_0 + \lambda \cdot b$$

$$z = z_0 + \lambda \cdot c$$

$$\lambda \in \mathbb{R}$$

5. Egyenes tétele

○ Tétel

- ! az e egyenesnek $P_0(x_0, y_0, z_0)$ pontja
- $\underline{v} = (a, b, c) \neq 0$ irányvektora
- tetszőleges pontjának nem paraméteres alakja:

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

$$\frac{x - x_0}{a} = \frac{y - y_0}{b} \quad \text{és} \quad z = z_0 \quad c = 0$$

$$x = x_0 \quad y = y_0 \quad a, b = 0$$

○ Bizonyítás

- $P \in e$, akkor igaz, ha e paraméteres egyenletrendszerére $\lambda \in \mathbb{R}$ értékére P -t adja
- ha $a, b, c \neq 0$, akkor a 3 egyenletből egy közös λ -ra kell jutnunk
- ha $c = 0$, akkor megfelelő λ létezése azt jelenti, hogy $z = z_0$ és az első 2 egyenletből közös λ értéket kell kapnunk
- ha csak $c \neq 0$, akkor az első két egyenlet egyértelmű, míg a 3. egyenlet mindig kielégíthető a $\lambda = \frac{z - z_0}{c}$ választással



6. Sík tétele

o Tétel

- ! az adott S síknek $P_0(x_0, y_0, z_0)$
- $n = (a, b, c) \neq 0$ normálvektora
- ekkor $P(x, y, z) \in S$ akkor igaz, ha

$$a \cdot x + b \cdot y + c \cdot z = a \cdot x_0 + b \cdot y_0 + c \cdot z_0$$

o Bizonyítás

- $P \in e$, akkor igaz, ha $\overrightarrow{P_0P} \parallel S$ -el
- $\overrightarrow{P_0P}$ pedig akkor $\parallel S$ -el, ha merőleges \underline{n} -el \rightarrow ez akkor teljesül, ha skaláris szorzatuk 0
- tétel szerint:
- $\overrightarrow{P_0P} \cdot \underline{n} = a(x - x_0) + b(y - y_0) + c(z - z_0) \quad / \overrightarrow{P_0P} \cdot \underline{n} = 0$
beszorzás és átrendezés után megkapjuk a tételben kimondott egyenletet

7. Vektoriális szorzat

o Definíció

- \underline{u} és \underline{v} vektorok **vektoriális szorzata** az az $\underline{u} \times \underline{v}$ -vel jelölt vektor, amelyre az alábbi feltételek fennállnak:
 - $\underline{u} \times \underline{v}$ hossza: $|\underline{u} \times \underline{v}| = |\underline{u}| \cdot |\underline{v}| \cdot \sin \gamma$
 - $\underline{u} \times \underline{v}$ merőleges \underline{u} és \underline{v} -re
- **jobbsodrású rendszert** alkotnak
- ha valamelyik vektor $\underline{0}$, akkor az eredmény is $\underline{0}$

8. Vektoriális szorzat tétele

o Tétel

- ! $\underline{u} = (u_1, u_2, u_3)$ és $\underline{v} = (v_1, v_2, v_3)$ vektorok, ekkor

$$\underline{u} \times \underline{v} = \left(\begin{vmatrix} u_2 & u_3 \\ v_2 & v_3 \end{vmatrix}, - \begin{vmatrix} u_1 & u_3 \\ v_1 & v_3 \end{vmatrix}, \begin{vmatrix} u_1 & u_2 \\ v_1 & v_2 \end{vmatrix} \right)$$

9. Vegyesszorzat

o Definíció

- $\underline{u}, \underline{v}, \underline{w}$ jelölt vektorok **vegyesszorzata** $\underline{w} \cdot (\underline{u} \times \underline{v})$



10. Vegyesszorzat tétele

o Tétel

- a vegyesszorzat kapcsolata a térfogattal az \underline{u} , \underline{v} , \underline{w} által kifeszített paralelepipedon térfogata:

$$V = |\underline{u} \ \underline{v} \ \underline{w}|$$

o Bizonyítás

- térfogatot a paralelogramma T területének és m magasságának szorzatából kapjuk
- T terület egyenlő az $|\underline{u} \times \underline{v}|$ -vel
- m magasságot meg úgy kapjuk, hogy meghatározunk egy (tetszőlegesen megbetűzött) **OMW** háromszöget
 - **O**: origó
 - **M**: a W -ből az $\underline{u} \times \underline{v}$ -re állított merőleges talppontja
 - **W**: \underline{w} végpontja
- Pitagorasz tétel $\rightarrow OM = m = \underline{w} \cdot \cos \gamma$



6. tétel: Alterek, lineáris függetlenség

Tétalcím

\mathbb{R}^n és \mathbb{R}^n alterének a fogalma. Lineáris kombináció, generált altér (és ennek altér volta), generátorrendszer. Lineáris függetlenség (ennek kétféle definíciója és ezek ekvivalenciája). Az „újonnan érkező vektor” lemmája. F-G egyenlőtlenség.

1. \mathbb{R}^n

o Definíció

- $n \geq 1$ esetén az n db valós számból álló *számszlopok* halmazát \mathbb{R}^n jelöli
- ezen értelmezett összeadás "+" és tetszőleges $\lambda \in \mathbb{R}$ "·" *skalárszorosát* az alábbi alapján értelmezzük:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix} \text{ és } \lambda \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{pmatrix}$$

2. \mathbb{R}^n tulajdonságok

o Tétel

- ! $\underline{u}, \underline{v}, \underline{w} \in \mathbb{R}^n$ és $\lambda, \mu \in \mathbb{R}$, ekkor igazak az alábbiak:

- $\underline{u} + \underline{v} = \underline{v} + \underline{u}$
- $(\underline{u} + \underline{v}) + \underline{w} = \underline{u} + (\underline{v} + \underline{w})$
- $\lambda \cdot (\underline{u} + \underline{v}) = \lambda \cdot \underline{u} + \lambda \cdot \underline{v}$
- $\underline{v} \cdot (\lambda + \mu) = \underline{v} \cdot \lambda + \underline{v} \cdot \mu$
- $\lambda \cdot (\mu \cdot \underline{v}) = (\lambda \cdot \mu) \cdot \underline{v}$

[K50] megjegyzést írt: Kommutatív – felcserélhetőség.

[K51] megjegyzést írt: Asszociatív – felbonthatóság/csoportosíthatóság.

[K52] megjegyzést írt: Disztributív a vektorokra.

[K53] megjegyzést írt: Disztributív a skalárokra.

[K54] megjegyzést írt: Skalárszoros asszociatív.

o Bizonyítás

- *triviális, mert mindegyike azonnal következik a valós számok műveleti tulajdonságaiból*



3. \mathbb{R}^n altere

- Definíció
 - $V \subseteq \mathbb{R}^n \neq \emptyset$, tehát az \mathbb{R}^n tér egy nemüres *részhalmlaza*
 - V -t az *alterének* nevezzük, ha az alábbi két feltétel teljesül:
 - bármely $\underline{u}, \underline{v} \in V$ esetén $\underline{u} + \underline{v} \in V$ is igaz
 - bármely $\underline{u} \in V, \lambda \in \mathbb{R}$ esetén $\lambda \cdot \underline{u} \in V$ is igaz
- Jelölés
 - $V \leq \mathbb{R}^n$

3. Lineáris kombináció

- Definíció
 - $\underline{v}_1, \dots, \underline{v}_k \in \mathbb{R}^n$ vektorok és $\lambda_1, \dots, \lambda_k \in \mathbb{R}$ skalárok
 - $\lambda_1 \cdot \underline{v}_1 + \dots + \lambda_k \cdot \underline{v}_k$ vektort a $\underline{v}_1, \dots, \underline{v}_k$ vektorok $\lambda_1, \dots, \lambda_k$ skalárokkal vett *lineáris kombinációja*

4. Generált altér

- Definíció
 - $\underline{v}_1, \dots, \underline{v}_k \in \mathbb{R}^n$ vektorok, ezeknek a lineáris kombinációival kifejezhető \mathbb{R}^n -beli vektorok halmazát $\underline{v}_1, \dots, \underline{v}_k$ *generált altérnek* nevezzük
- Jelölés
 - $\langle \underline{v}_1, \dots, \underline{v}_k \rangle$

5. Generátorrendszer

- Definíció
 - $\underline{v}_1, \dots, \underline{v}_k \in \mathbb{R}^n$ vektorok, ha $W = \langle \underline{v}_1, \dots, \underline{v}_k \rangle$, akkor a $\underline{v}_1, \dots, \underline{v}_k$ vektorhalmazt a W altér *generátorrendszerének* nevezzük

6. Lineáris függetlenség, összefüggőség

- Definíció
 - a $\underline{v}_1, \dots, \underline{v}_k \in \mathbb{R}^n$ vektorrendszert akkor nevezzük *lineárisan függetlennek*, ha $\underline{v}_1, \dots, \underline{v}_k$ vektorok közül semelyik sem fejezhető ki a többi lineáris kombinációjaként



- ha ez nem teljesül (vagyis a $\underline{v}_1, \dots, \underline{v}_k$ vektorok között legalább egy olyan, amely kifejezhető a többi lineáris kombinációjaként), akkor a $\underline{v}_1, \dots, \underline{v}_k$ vektorrendszer *lineárisan összefüggőnek* nevezzük

7. Triviális lineáris kombináció

o Tétel

- a $\underline{v}_1, \dots, \underline{v}_k \in \mathbb{R}^n$ vektorrendszer akkor és csak akkor lineárisan független, ha $\lambda_1 \cdot \underline{v}_1, \dots, \lambda_k \cdot \underline{v}_k = \underline{0}$ egyenlőség kizárólag abban az esetben teljesül, ha $\lambda_1 = \dots = \lambda_k = 0 \rightarrow$ ezt nevezzük a triviális lineáris kombinációnak

o Bizonyítás

- („akkor lineárisan független, ha...”)
- TFH. $\lambda_1 \cdot \underline{v}_1, \dots, \lambda_k \cdot \underline{v}_k = \underline{0}$ csak a triviális lineáris kombináció esetén teljesül
- belátjuk, hogy $\underline{v}_1, \dots, \underline{v}_k$ lineárisan független
- TFI.:
 - feltesszük, hogy ez mégsem lineárisan független
 - ha $\underline{v}_1, \dots, \underline{v}_k$ nem lineárisan független, akkor valamelyikük kifejezhető a többi lineáris kombinációjából: $! \underline{v}_1$, ekkor

$$\underline{v}_1 = \alpha_2 \cdot \underline{v}_2 + \dots + \alpha_k \cdot \underline{v}_k \quad \alpha_1, \dots, \alpha_k \in \mathbb{R} \quad / \text{átrendezve}$$

$$1 \cdot \underline{v}_1 - \alpha_2 \cdot \underline{v}_2 - \dots - \alpha_k \cdot \underline{v}_k = \underline{0}$$

- ez ellentmondás \rightarrow nemtriviális lineáris kombináció esetén is teljesül ($\lambda_1 = 1, \lambda_2 = -\alpha_2, \dots, \lambda_k = -\alpha_k$) \rightarrow igazolva
- („csak akkor...”)
- feltesszük, hogy $\underline{v}_1, \dots, \underline{v}_k$ lineárisan független és megmutatjuk, hogy ekkor $\lambda_1 \cdot \underline{v}_1, \dots, \lambda_k \cdot \underline{v}_k = \underline{0}$ csak a $\lambda_1 = \dots = \lambda_k = 0$ esetben teljesül
- TFI.:
 - TFH. $\lambda_1 \cdot \underline{v}_1, \dots, \lambda_k \cdot \underline{v}_k = \underline{0}$, de a lambdák között van nemnulla
 - ♦ pl.: $\lambda_1 \neq 0$



- ekkor átrendezés és $\lambda_1 \neq 0$ -val való osztás után a következő alakot kapjuk:

$$\underline{v}_1 = -\frac{\lambda_2}{\lambda_1} \cdot \underline{v}_2 - \dots - \frac{\lambda_k}{\lambda_1} \cdot \underline{v}_k$$

- ellentmondás, $\underline{v}_1, \dots, \underline{v}_k$ mégsem lineárisan független, mert \underline{v}_1 kifejezhető a többiből lineáris kombinációval

8. Újonnan érkező vektor lemmája (ÚÉVL)

[K55] megjegyzést írt: Segédttétel.

o Tétel

- TFH. az f_1, \dots, f_k rendszer lineárisan független, de $f_1, f_2, \dots, f_k, f_{k+1}$ lineárisan összefüggő
- ekkora $f_{k+1} \in \langle f_1, \dots, f_k \rangle$, tehát f_{k+1} kifejezhető f_1, \dots, f_k lineáris kombinációjaként

o Bizonyítás

- mivel f_1, \dots, f_k, f_{k+1} lineárisan összefüggő, ezért lineáris függetlenség tétele alapján létezik nemtriviális lineáris kombináció, mely nullvektort adja végeredményül
- ha a $\lambda_1 \cdot f_1, \dots, \lambda_k \cdot f_k, \lambda_{k+1} = \underline{0}$ egyenletben $\lambda_{k+1} = 0$ azt jelenti, hogy a maradék egyenlet így néz ki $\lambda_1 \cdot f_1 + \dots + \lambda_k \cdot f_k = \underline{0}$ ÉS a $\lambda_1, \dots, \lambda_k$ skalárok között van egy (vagy több) nemnulla tag
- emiatt az eredeti f_1, \dots, f_k rendszer lineárisan összefüggő \rightarrow ellentmondás
- $\rightarrow \lambda_{k+1} \neq 0$, és az ezzel való osztás után kapott egyenletből következik, hogy f_{k+1} előállítható az f_1, \dots, f_k rendszer lineáris kombinációjaként
- $\rightarrow f_{k+1} \in \langle f_1, \dots, f_k \rangle$

9. F-G egyenlőtlenség

o Tétel

- $V \leq \mathbb{R}^n$ altér, f_1, \dots, f_k V -beli vektorokból álló lineárisan független rendszer
- g_1, \dots, g_m pedig generátorrendszer V -ben $\rightarrow k \leq m$



o **Bizonyítás**

- ha $k = 1$, akkor V -ben van a nullvektortól különb vektor (mert $\underline{f}_1 \neq 0$) \rightarrow minden generátorrendszer legalább 1 elemű (üres halmaz esetén $\underline{0}$ alteret generálja csak)
- tétel $k = 1$ esetén igaz
- TFH. $k \geq 2$ és már igaz $k - 1$ -re igaz \rightarrow belátni k -ra is
- mivel $\underline{g}_1, \dots, \underline{g}_k$ generátorrendszer V -ben, ezért minden V -beli vektor $\rightarrow \underline{f}_k$ is előáll ennek lineáris kombinációjaként:

- $\underline{f}_k = \lambda_1 \cdot \underline{g}_1, \dots, \lambda_m \cdot \underline{g}_m$
- λ lambdák között nemnulla, mert $\underline{f}_k \neq 0$
- $\lambda_m \neq 0, W = \langle \underline{g}_1, \dots, \underline{g}_k \rangle$
- megmutatjuk, hogy minden $1 \leq j \leq k - 1$ esetén az \underline{f}_j -hez található olyan α_j skalár, hogy $\underline{f}_j + \alpha_j \cdot \underline{f}_k \in W$
- \underline{f}_j felírható $\underline{g}_1, \dots, \underline{g}_k$ lineáris kombinációjaként:

$$\underline{f}_j = \beta_1 \underline{g}_1, \dots, \beta_m \underline{g}_m$$

- ekkor $\alpha_j = -\frac{\beta_m}{\lambda_m}$ megfelel:

$$\underline{f}_j + \alpha_j \cdot \underline{f}_k = \underline{g}_1 \cdot \left(\beta_1 - \frac{\beta_m}{\lambda_m} \cdot \gamma_1 \right) + \underline{g}_2 \cdot \left(\beta_2 - \frac{\beta_m}{\lambda_m} \cdot \gamma_2 \right) + \dots + \underline{g}_m \cdot \left(\beta_m - \frac{\beta_m}{\lambda_m} \cdot \gamma_m \right)$$

- \underline{g}_m együtthatója $\beta_m - \frac{\beta_m}{\lambda_m} \cdot \gamma_m = 0$, így $\underline{f}_j + \alpha_j \cdot \underline{f}_k$ **W-beli**

- megmutatjuk, hogy $\underline{f}_j + \alpha_j \cdot \underline{f}_k, j = 1, 2, \dots, k - 1$ vektorok lineárisan függetlenek
- vegyük egy $\underline{0}$ -t adó lineáris kombinációjukat a $\lambda_1, \lambda_2, \dots, \lambda_{k-1}$ skalárokkal

$$\lambda_1 \cdot (\underline{f}_1 + \alpha_1 \cdot \underline{f}_k) + \lambda_2 \cdot (\underline{f}_2 + \alpha_2 \cdot \underline{f}_k) + \dots + \lambda_{k-1} \cdot (\underline{f}_{k-1} + \alpha_{k-1} \cdot \underline{f}_k) = \underline{0}$$

$$\lambda_1 \cdot \underline{f}_1 + \lambda_2 \cdot \underline{f}_2 + \dots + \lambda_{k-1} \cdot \underline{f}_{k-1} + \underline{f}_k \cdot (\lambda_1 \cdot \alpha_1 + \lambda_2 \cdot \alpha_2 + \dots + \lambda_{k-1} \cdot \alpha_{k-1}) = \underline{0}$$

- ezzel az $\underline{f}_1, \dots, \underline{f}_k$ egy $\underline{0}$ -t adó lineáris kombinációját kaptuk
- tudjuk, hogy ezek lineárisan független \rightarrow lineáris kombináció minden együtthatója 0 kell legyen

[K56] megjegyzést írt: Legyen.

[K57] megjegyzést írt: Mert felírható $\underline{g}_1, \dots, \underline{g}_{m-1}$ lineáris kombinációjaként.



- vagyis $\lambda_1 = \lambda_2 = \dots = \lambda_{k-1} = 0 \rightarrow \underline{f}_j + \alpha_j \cdot \underline{f}_k$ vektorok valóban lineárisan független



7. tétel: Bázis, dimenzió

Tételcím

Bázis és dimenzió fogalma, a dimenzió egyértelműsége. Standard bázis, \mathbb{R}^n dimenziója. Koordinátavektor fogalma és annak egyértelműsége. Bázis létezése \mathbb{R}^n tetszőleges altérben.

1. Bázis

- Definíció
 - $V \leq \mathbb{R}^n$ altér
 - V -beli vektorokból álló $\underline{b}_1, \dots, \underline{b}_k$ rendszert *bázis*nak nevezzük V -ben, ha
 - a rendszer *lineárisan független*
 - *generátorrendszer*t alkot

2. Bázis egyértelműsége

- Tétel
 - TFH. a $V \leq \mathbb{R}^n$ altérben a $\underline{b}_1, \dots, \underline{b}_k$ rendszer és a $\underline{c}_1, \dots, \underline{c}_m$ rendszer egyaránt bázisok $\rightarrow k = m$
- Bizonyítás
 - mindkét rendszer bázis, ezért V -ben
 - $\underline{b}_1, \dots, \underline{b}_k$ lineárisan független
 - $\underline{c}_1, \dots, \underline{c}_m$ generátorrendszer
 - (6. tétel, F-G egyenlőtlenséget tétel miatt)
 $k \leq m$
 - ennek fordítottját is kimondhatjuk, így V -ben
 - $\underline{b}_1, \dots, \underline{b}_k$ generátorrendszer
 - $\underline{c}_1, \dots, \underline{c}_m$ lineárisan független
 - (ismét F-G miatt) $m \leq k$

Mivel egyszerre igazak, így $k = m$



3. Dimenzió

- Definíció
 - $V \leq \mathbb{R}^n$ *altér*ben $\underline{b}_1, \dots, \underline{b}_k$ rendszer bázis
 - ekkor V *dimenziója* k
- Jelölés
 - $\dim V = k$

4. Standard bázis

- Definíció
 - jelölje minden $1 \leq i \leq n$ esetén e_i azt az \mathbb{R}^n -beli vektort, melynek (felülről) az i -edik koordinátája 0
 - ekkor $\underline{e}_1, \dots, \underline{e}_n$ bázis az \mathbb{R}^n -ben \rightarrow ez a *standard bázis*

- Jelölés

- E_n

- Bizonyítás

- $\underline{e}_1, \dots, \underline{e}_n$ *lineáris kombinációja* $\underline{\lambda}_1, \dots, \underline{\lambda}_n$ skalárokkal

$$\lambda_1 \cdot \underline{e}_1 + \dots + \lambda_n \cdot \underline{e}_n = \lambda_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \dots + \lambda_n \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix}$$

- látszik, hogy $\underline{e}_1, \dots, \underline{e}_n$ generátorrendszer \mathbb{R}^n -ben, hiszen lineáris kombinációjukként tetszőleges vektor előállhat
- ha *nullvektor* akarjuk kifejezni, akkor csak a triviális lineáris kombináció esetén fog az előállni
- tehát a rendszer lineárisan független $\rightarrow \underline{e}_1, \dots, \underline{e}_n$ tényleg bázist alkot az \mathbb{R}^n -ben
- fenti állításból következik, hogy $\dim \mathbb{R}^n = n$
- viszont \mathbb{R}^n csak az egyike az „ n dimenziós tereknek” és minden ($n \leq m$) \mathbb{R}^m -nek van n -dimenziós altere



5. Bázis tétele

o Tétel

- $V \leq \mathbb{R}^n$ altérben a $\underline{b}_1, \dots, \underline{b}_k$ vektorok akkor és csak akkor alkotnak bázist, ha minden $\underline{v} \in V$ egyértelműen, azaz pontosan egyféleképpen fejezhető ki lineáris kombinációjukként

o Bizonyítás

- („csak akkor” alkotnak bázist... kifejtése)
- akkor bázis, ha V -ben generátorrendszer és lineárisan független (bázis tételből)
- („akkor” ... kifejtése)
- minden $\underline{v} \in \mathbb{R}^n$ kifejezhető $\underline{b}_1, \dots, \underline{b}_k$ lineáris kombinációjaként
- **TFI.** valamely $\underline{v} \in V$ kétféleképpen kifejezhető:

$$\underline{v} = \lambda_1 \underline{b}_1 + \dots + \lambda_k \underline{b}_k = \mu_1 \underline{b}_1 + \dots + \mu_k \underline{b}_k \text{ és } \lambda_j \neq \mu_j$$

- kettő különbségét véve:

$$\underline{0} = \underline{b}_1(\lambda_1 - \mu_1) + \dots + \underline{b}_k(\lambda_k - \mu_k)$$

tehát $\underline{0}$ kifejezhető a $\underline{b}_1, \dots, \underline{b}_k$ nemtriviális lineáris kombinációjaként, hiszen $(\lambda_j - \mu_j) \neq 0$, ez ellentmondás

[K58] megjegyzést írt: Tegyük Fel Indirekten, hogy...

6. Koordinátavektor

o Definíció

- $V \leq \mathbb{R}^n$, $B = \{\underline{b}_1, \dots, \underline{b}_k\}$ bázis V -ben, $\underline{v} \in V$ tetszőleges vektor

- azt mondjuk, hogy $\underline{k} = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_k \end{pmatrix} \in \mathbb{R}^k$ vektor a \underline{v} vektor B szerinti

koordinátavektora, ha $\underline{v} = \lambda_1 \cdot \underline{b}_1 + \dots + \lambda_k \cdot \underline{b}_k$

o Jelölés

- $\underline{k} = [\underline{v}]_B$

- $[\underline{v}]_B$ nem csak \underline{v} -től függ:

- ugyanannak a vektornak más-más bázis esetén más-más koordinátavektorok felelnek meg



7. Bázis létezése tétele

o **Tétel**

- $! V \leq \mathbb{R}^n$ altér, f_1, \dots, f_k V -beli vektorokból álló lineárisan független rendszer
- f_1, \dots, f_k kiegészíthető véges sok további vektorral úgy, hogy a kapott rendszer bázis legyen

o **Bizonyítás**

- $! W = \langle f_1, \dots, f_k \rangle$
- igaz, hogy $W \subseteq V$, mivel V altér
 - ha $V = W$, akkor f_1, \dots, f_k generátorrendszer, így bázis V -ben \rightarrow tétel belátva
 - ha $V \neq W$, akkor létezik egy $\underline{v} \in V$, $\underline{v} \notin W$ vektor
 - ♦ **újonnan érkező vektor lemmája** szerint ekkor $f_1, \dots, f_k, \underline{v}$ lineárisan független
 - ♦ ha ez már generátorrendszer V -ben, akkor **kész**
 - ♦ különben be kell látni, hogy ez a folyamat leáll egy idő után \rightarrow F-G egyenlőtlenség igénybevétele
 - ♦ ez alapján n -nél nagyobb elemszámú lineárisan független rendszer \mathfrak{R}^n -ben, de létezik n elemű generátorrendszer ebben a térben
 - ♦ az eljárás tehát $n - k$ lépés után biztos megáll
 - \rightarrow minden $V \leq \mathbb{R}^n$ altérben van bázis \rightarrow $\dim V$ létezik
- ha $V = \underline{0}$, akkor az üres halmaz bázis V -ben
- ha V tartalmaz egy $\underline{v} \neq \underline{0}$, akkor \underline{v} -re alkalmazva a fenti tételt kapunk egy V -beli bázist

[K59] megjegyzést írt: Ugyanis ezt már beláttuk egyszer



8. tétel: Gauss-elimináció, RLA

Tételcím

Lineáris egyenletrendszer megoldása Gauss-eliminációval. Megoldhatóság, a megoldás egyértelműségének feltétele. Lépcsős alak és redukált lépcsős alak fogalma. Kapcsolat az egyenletek és ismeretlenek száma, illetve a megoldás egyértelműsége között.

1. Lineáris egyenletrendszer

o Definíció

- egy k egyenletből álló n változós röviden: $(k \times n)$ -es *lineáris egyenletrendszer*
- *kettős indexelésű együtthatók* bevezetése: $a_{i,j}$
 - i -edik egyenletben a j -edik változó együtthatója minden:
 - ♦ $1 \leq i \leq k$
 - ♦ $1 \leq j \leq n$ esetén
 - b_i konstans tag
- lineáris egyenletrendszer „hagyományos” alakja:

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + \dots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \dots + a_{2,n}x_n &= b_2 \\ &\vdots \\ a_{k,1}x_1 + a_{k,2}x_2 + \dots + a_{k,n}x_n &= b_k \end{aligned}$$

- *kibővített együtthatómátrixos* alakja

$$\left(\begin{array}{cccc|c} a_{1,1} & a_{1,2} & \dots & a_{1,n} & b_1 \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{k,1} & a_{k,2} & \dots & a_{k,n} & b_k \end{array} \right)$$



- (fontos elméleti következmény:)
- TFH. adott egy k egyenletből álló, n ismeretlenes lineáris egyenletrendszer
- megoldhatóságával kapcsolatos következmények, ha csak k és n relációját ismerjük
 - *nem igaz*, hogy ha $k = n$, akkor biztosan van megoldás
 - *nem igaz*, hogy ha $k < n$, akkor biztosan végtelen sok megoldás van
 - *nem igaz*, hogy ha $k > n$, akkor biztosan nincs megoldás
→ ellenpélda lásd (lentebb): **Lineáris rendszer megoldhatóság tétele**

2. Elemi sorkvivalens lépések

- **Definíció**
 - kibővített együtthatómátrixával adott lineáris egyenletrendszer esetén **elemi sorkvivalens** lépésnek nevezzük alábbiakat
 - ($1 \leq i, j \leq k, i \neq j$ és $\lambda \in \mathbb{R}, \lambda \neq 0$ skalár esetén):
 - **(1)** a mátrix i -edik sorának (tagonként való) megszorozása λ -val
 - **(2)** a mátrix i -edik sorának helyettesítése sajátmagának és a j -edik sor λ -szorosának (tagonként vett) összegével
 - **(3)** az i -edik és j -edik sor felcserélése
 - **(4)** egy csupa nulla elemeket tartalmazó sor elhagyása

3. Gauss elimináció

- **Állítás**
 - előző definícióban felsorolt lépések ekvivalens átalakítások
 - → egyenletrendszer megoldásait nem változtatják meg
 - (részletesebben: ha az x_1, \dots, x_n számok kielégítik az egyenletrendszert egy lépés megtétele előtt, akkor annak megtétele után is, és fordítva is)
- **Bizonyítás**
 - (csak a (2) lépésre bizonyítva...)
 - ha x_1, \dots, x_n kielégítik az egyenletrendszert, akkor:

$$a_{i,1} \cdot x_1 + \dots + a_{i,n} \cdot x_n = b_i$$



$$a_{j,1} \cdot x_1 + \dots + a_{j,n} \cdot x_n = b_j \quad / \cdot \lambda, + \uparrow \text{ fentihez adva}$$
$$x_1 \cdot (a_{i,1} + \lambda \cdot a_{j,1}) + \dots + x_n \cdot (a_{i,n} + \lambda \cdot a_{j,n}) = b_i + \lambda \cdot b_j$$

- tehát az új i -edik egyenlet teljesül
- megfordítva: ha x_1, \dots, x_n megoldása a rendszernek a (2 lépés megtétele után, akkor a $b_i + \lambda \cdot b_j$ és b_j egyenletek igazak
- $b_i + \lambda \cdot b_j$ ebből kivonva λ -szorosát b_i egyenletét kapjuk
- tehát lépés megtétel előtt is teljesül

4. Lépcsős alak, redukált lépcsős alak

- Definíció
 - egy kibővített együtthatómátrixával adott lineáris egyenletrendszert **lépcsős alakúnak (LA)** mondunk, ha az alábbiak teljesülnek:
 - a mátrix minden sorában van nemnulla elem és (balról) az első nemnulla elem egy 1-es, úgynevezett **vezéregyes**
 - ♦ (Vezéregyeseket nem tartalmazó oszlopok szabad paramétereknek felelnek meg. A sorok adják meg átrendezés után, hogy a többi változó hogyan fejezhető ki a szabad paraméterekből.)
 - ha $1 \leq i, j \leq k$, akkor az i -edik sorban álló vezéregyes kisebb sorszámú oszlopban van, mint a j -edik sor vezéregyese
 - a vezéregyesekkel egy oszlopban, azok alatt álló minden elem 0
 - **redukált lépcsős alakúnak (RLA)** mondjuk a mátrixot, ha még az alábbi is teljesül:
 - vezéregyesekkel egy oszlopban, azok fölött álló minden elem 0

5. Gauss elimináció tétele

- Tétel
 - tetszőleges, kibővített együtthatómátrixával adott lineáris egyenletrendszer esetén a Gauss-eliminációt futtatva az alábbi esetek közül pontosan az egyik valósul meg
 - az első fázis 3. lépésének végrehajtásakor az eljárás „tilos sort” talál \rightarrow az egyenletrendszer nem megoldható



- az algoritmus RLA-ra hozza a kibővített együtthatómátrixot, amelynek minden oszlopában van vezéregyes \rightarrow az egyenletrendszer egyértelműen megoldható
- az algoritmus RLA-ra hozza a kibővített együtthatómátrixot, de annak nem minden oszlopában van vezéregyes \rightarrow az egyenletrendszernek végtelensok megoldása van
 - a második és harmadik esetben a megoldások a RLA-ból közvetlenül kiolvashatóak

6. Lineáris egyenletrendszer megoldhatóság

- **Tétel**
 - ha egy k egyenletből álló, n ismeretlenes lineáris egyenletrendszer egyértelműen megoldható, akkor $k \geq n$
- **Bizonyítás**
 - lefuttatjuk a Gauss-eliminációt az egyenletrendszerre
 - megoldható (tehát nincs *tilos sor*), az algoritmus egy RLA-t hoz létre
 - ! ebben a sorok száma: k'
 - nyilván $k' \leq k$, mert az algoritmus csökkentheti a sorok számát (első fázis 3. lépésben), de nem növelheti
 - mivel az egyenletrendszer egyértelműen megoldható, ezért RLA minden oszlopa tartalmaz vezéregyest $\Rightarrow k' = n$
 - ezeket összevetve: $k \geq k' = n$, ezzel a tétel belátva

[K60] megjegyzést írt: Ebből következik, hogy...



9. tétel: Determináns

Tételcím

Determináns definíciója, alaptulajdonságai, kiszámítása.

1. Determináns

- Definíció
 - ! egy adott $(n \times n)$ A mátrix
 - minden *bástyaelhelyezés*re szorozzuk össze az azt alkotó n elemet
 - szorzathoz adjunk előjelet következő szabály szerint:
 - ha a bástyaelhelyezésnek megfelelő *permutáció* inverziószáma páros, akkor az előjel pozitív (+)
 - ha páratlan, akkor az előjel negatív (-)
 - az így kapott $n!$ db, n tényezős szorzat összegét az A *determináns*ának nevezzük
- Jelölés
 - $|A|$ vagy $\det A$

2. Determináns alaptulajdonságai (1)

- Tétel
 - ! A $(n \times n)$ -es mátrix
 - ha annak van csupa 0 elemet tartalmazó sora vagy oszlopa, akkor $\det A = 0$
 - ha A felsőháromszög mátrix vagy alsóháromszög mátrix, akkor a determinánsa a főátlóbeli elemek szorzata:

$$\det A = a_{1,1} \cdot a_{2,2} \cdot \dots \cdot a_{n,n}$$

- Bizonyítás

- csupa 0 állítás azonnal következik a determináns definíciójából:
 - mivel mind az $n!$ db szorzat tartalmaz elemet abból a sorból/oszlopból, amelyeknek minden tagja 0, ezért minden szorzat értéke és ezek összege is 0 lesz

[K61] megjegyzést írt: Akkor is $\det A = 0$, ha van két azonos sora:

$$\det \begin{pmatrix} 1 & 3 & 2 & 1 \\ 4 & 6 & 9 & 2 \\ 1 & 3 & 2 & 1 \\ 6 & 5 & 5 & 8 \end{pmatrix} = 0$$

• vagy egyik sor a másik sor számszorosa:

$$\det \begin{pmatrix} 1 & 3 & 2 & 1 \\ 4 & 6 & 9 & 2 \\ 2 & 6 & 4 & 2 \\ 6 & 5 & 5 & 8 \end{pmatrix} = 0$$

• egyik sor a másik sorok lineáris kombinációja:

$$-2 \cdot (1 \ 3 \ 2 \ 1) + 1 \cdot (4 \ 6 \ 9 \ 2) = (2 \ 0$$

$$\det \begin{pmatrix} 1 & 3 & 2 & 1 \\ 1 & 1 & 3 & 2 \\ 4 & 6 & 9 & 2 \\ 2 & 0 & 5 & 0 \end{pmatrix} = 0$$

Oszlopokra is igazak.



- (második állítás bizonyítása)
- vegyük A **felsőháromszög-mátrix**ot
- a bástyaelhelyezések akkor nem tartalmaznak 0 elemet, ha az első oszlopból az első elemet, a második oszlopból a második elemet, választjuk ki (többet nem lehetne) és így tovább...
- a kapott permutáció **inverziószáma** 0, így pozitív előjelű ez a tag, és mivel ez az egyetlen tag, amiben nem szerepel 0, ezért ez lesz az előjeles összeg eredménye
- ezt megismételve (**felt az oszlop és a sor szavak megcserélésével**) megkapjuk ugyanezt a bizonyítást **alsóháromszög-mátrix**ra is

3. Determináns alaptulajdonságai (2)

o Tétel

- A ($n \times n$)-es mátrix, $\lambda \in \mathbb{R}$ skalár, $1 \leq i, j \leq n, i \neq j \in \mathbb{Z}$
- (1) ha A egy sorát megszorozzuk λ -val, akkor a kapott A' mátrix determinánisa λ -szorososa A -énak:

$$\det A' = \lambda \cdot \det A$$

- (2) ha A két sorát felcseréljük, akkor a kapott A' mátrix determinánisa ellentétje A -énak:

$$\det A' = (-1) \cdot \det A$$

- (3) ha A i -edik sorát helyettesítjük sajátmagának és a j -edik sor λ -szorosának összegével, akkor a kapott A' mátrix determinánisa megegyezik A -ével:

$$\det A' = \det A$$

- oszlopokra igaz ugyanez

o Bizonyítás (egy hosszú bizonyítás következik... készüli fel rá lelkiileg)

- (1) TFH. A' -t az i -edik sor λ szorzásával kaptuk
- hasonlítsuk össze A és A' determinánának definíció szerinti kiszámítását:
- mivel minden bástyaelhelyezés pontosan egy elemet tartalmaz az i -edik sorból, ezért az A kiszámítása közben keletkező szorzatok mindegyikében egy tényező a λ -szorosára változik, amikor $\det A'$ -t számítjuk
- maga a szorzat értéke is a λ -szoros lesz, **előjel nem változik**

$$B = \begin{pmatrix} 3 & 1 & 2 & 0 \\ 0 & 2 & 4 & 8 \\ 0 & 0 & 5 & 4 \\ 0 & 0 & 0 & \end{pmatrix}$$

[K62] megjegyzést írt:

$$A = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 5 & 2 & 0 & 0 \\ 4 & 7 & 5 & 0 \\ 6 & 2 & \end{pmatrix}$$

[K63] megjegyzést írt:

$$\det \begin{pmatrix} 4 & 3 & 0 & 7 \\ 1 & 0 & 2 & 4 \\ 2 & 6 & 4 & 2 \\ 6 & 5 & 5 & 8 \end{pmatrix} = 2 \cdot \det \begin{pmatrix} 4 & 3 & 0 & 7 \\ 1 & 0 & 2 & 4 \\ 2 & 6 & 4 & 2 \\ 6 & 5 & 5 & 8 \end{pmatrix} \leftarrow \begin{matrix} \times 2 \\ \times 2 \end{matrix}$$

[K64] megjegyzést írt:

$$\det \begin{pmatrix} 1 & 3 & 2 & 1 \\ 1 & 0 & 2 & 4 \\ 4 & 3 & 0 & 7 \\ 6 & 5 & 5 & 8 \end{pmatrix} = -\det \begin{pmatrix} 1 & 3 & 2 & 1 \\ 1 & 0 & 2 & 4 \\ 4 & 3 & 0 & 7 \\ 6 & 5 & 5 & 8 \end{pmatrix}$$

[K65] megjegyzést írt:

$$\det \begin{pmatrix} 7 & 9 & 6 & 1 \\ \end{pmatrix}$$

[K66] megjegyzést írt:

$$1 \cdot (4 \ 3 \ 0 \ 7) + 2 \cdot (1 \ 3 \ 2 \ 1) = (6 \ 9 \ 2 \ 15)$$

$$1 \cdot (4 \ 3 \ 0 \ 7) + 2 \cdot (1 \ 3 \ 2 \ 1) = (6 \ 9 \ 2 \ 15)$$

[K67] megjegyzést írt: Az azt meghatározó bástyaelhelyezés ugyanaz



- mindegyik összeadandó a λ -szorosára változik, ezért ezek (előjeles) összege, vagyis a determináns értéke is
- bizonyítás érvényes a j -edik oszlopra is
- **(2)** példán keresztüli bemutatása:

$$A = \begin{pmatrix} 2 & 3 & 4 & \boxed{5} & 6 \\ 7 & \boxed{8} & 9 & 10 & 11 \\ \boxed{12} & 13 & 14 & 15 & 16 \\ 17 & 18 & 19 & 20 & \boxed{21} \\ 22 & 23 & \boxed{24} & 25 & 26 \end{pmatrix} \quad A' = \begin{pmatrix} 2 & 3 & 4 & \boxed{5} & 6 \\ 7 & \boxed{8} & 9 & 10 & 11 \\ 22 & 23 & \boxed{24} & 25 & 26 \\ 17 & 18 & 19 & 20 & \boxed{21} \\ \boxed{12} & 13 & 14 & 15 & 16 \end{pmatrix}$$

- a 3. és az 5. sor felcserélésével kaptuk A' -t
- A -ban bekeretezett rész a bástyaelhelyezés
- ennek megfelelő permutáció $\pi = (4, 2, 1, 5, 3)$, ennek inverziószáma 5 \rightarrow keletkező szorzat negatív előjelet kap
- A' kiszámításánál ugyanez, különbség a tényezők sorrendjében, és a bástyaelhelyezésben
- $\pi' = (4, 2, 3, 5, 1)$, ekkor inverziószám már 6, előjel pozitív
- π -ből $\pi_3 = 1$ és $\pi_5 = 3$ felcserélésével kapjuk π'
- ugyanígy A és A'
- tehát: bástyaelhelyezés szorzatok sorrendtől eltekintve azonosak, előjelük ellentétes
- oszlopcserénél **lényegében azonos**
- **(3)** lemmával/segédttétellel bizonyítjuk:

[K68] megjegyzést írt: π -ből nem π_i és π_j , hanem i és j felcserélésével kapjuk π'

Determináns alaptulajdonságai lemma

o Tétel

- TFH. az $(n \times n)$ -es X, Y, Z mátrixok az i -edik soraiktól eltekintve elemről elemre megegyeznek
- i -edik soraikra viszont fennáll, hogy $z_{i,j} = x_{i,j} + y_{i,j}$ minden $1 \leq j \leq n$ esetén
- a Z i -edik sora épp az X és az Y i -edik sorának (tagonkénti) összege
- ekkor $\det Z = \det X + \det Y$
- az állítás érvényes oszlopokra is



o Lemma bizonyítása

- vegyünk egy tetszőleges *bástyaelhelyezést* Z -ben
- feleljen meg a π permutációinak, ebből keletkező szorzat tehát:

$$(-1)^{l(\pi)} \cdot z_{1,\pi_1} \cdot \dots \cdot z_{i,\pi_i} \cdot \dots \cdot z_{n,\pi_n}$$

- a $z_{i,\pi_i} = x_{i,\pi_i} + y_{i,\pi_i}$ behelyettesítéssel:

$$(-1)^{l(\pi)} \cdot z_{1,\pi_1} \cdot \dots \cdot (x_{i,\pi_i} + y_{i,\pi_i}) \cdot \dots \cdot z_{n,\pi_n}$$

- felbontva a zárójelet, és felhasználva, hogy minden $k \neq i$ esetén $z_{k,\pi_k} = x_{k,\pi_k} = y_{k,\pi_k}$:

$$(-1)^{l(\pi)} \cdot x_{1,\pi_1} \cdot \dots \cdot x_{i,\pi_i} \cdot \dots \cdot x_{n,\pi_n} + (-1)^{l(\pi)} \cdot y_{1,\pi_1} \cdot \dots \cdot y_{i,\pi_i} \cdot \dots \cdot y_{n,\pi_n} \\ + (-1)^{l(\pi)} \cdot z_{1,\pi_1} \cdot \dots \cdot z_{i,\pi_i} \cdot \dots \cdot z_{n,\pi_n}$$

- mivel minden *bástyaelhelyezésre* összegezve definíció szerint $\det Z$ és $(\det X + \det Y)$ -t kapjuk, a lemmát belátva
- (oszlopok esetén bizonyítás lényegében azonos)

o Bizonyítás

- **(3) folytatás...**

- lemma alkalmazható az A' mátrixra, hiszen abban az i -edik sor minden eleme egy kéttagú összeg:
- $a'_{i,k} = a_{i,k} + \lambda \cdot a_{j,k}$ minden k -ra
- lemmát alkalmazva: $Z = A'$, $X = A$, és Y pedig az a mátrix, amely az i -edik sorától eltekintve azonos A -val
- az i -edik sorában pedig az A j -edik sorának λ -szorososa áll: $y_{i,k} = \lambda \cdot a_{j,k}$
- lemmát ezekre alkalmazva: $\det A' = \det A + \det Y$
- **már csak** $\det Y = 0$ bizonyítása kell
- Y i -edik sorára alkalmazható a tétel (már bebizonyított) **(1)** állítás:
- ha Y' jelöli azt a mátrixot, amely az i -edik sorától eltekintve azonos Y -nal (és így A -val), az i -edik sorában pedig az A j -edik sorának másolata áll
 - vagyis $y'_{i,k} = a_{j,k}$ minden k -ra, akkor **(1-ből)** $\det Y = \lambda \cdot \det Y$ következik

[K69] megjegyzést írt: Mindjárt vége, mély levegő...



- Y' -re pedig a tétel (2 állítását alkalmazzuk:
- ha Y' -ben felcseréljük az i -edik és j -edik sort, akkor a determináns az ellentéjtéjére változik, és változatlan is marad (hiszen Y' -n a sorcsere „nem látszik”, annak i -edik és j -edik sora azonos)
- $\rightarrow \det Y' = -(\det Y) \rightarrow \det Y = 0$, tétel bizonyítva
- $\det Y = \lambda \cdot \det Y' \rightarrow \det Y = 0 \rightarrow \det A' = \det A + \det Y \rightarrow \det A' = \det A$
- oszlopokra ismét változtatás nélkül elmondható

4. Determináns kiszámolása – Gauss eliminációval

- Bemenet: $(n \times n)$ - es A mátrix
- **0. lépés**
 - $i \leftarrow 1, D \leftarrow 1$
- **1. lépés**
 - ha $a_{i,j} = 0$, akkor folytassuk a **2. lépés**nél
 - szorozzuk meg i -edik sort $\frac{1}{a_{i,j}}$ -vel
 - $D \leftarrow D \cdot a_{i,j}$
 - ha $i = n$, akkor PRINT " detA = ", D; STOP
 - minden $i < t \leq n$ esetén adjuk a t -edik sorhoz az i -edik sor $(-a_{t,i})$ -szeresét
 - $i \leftarrow i + 1$
- **2. lépés**
 - ha $i < n$, és van olyan $i < t \leq k$, melyre $a_{t,i} \neq 0$, akkor:
 - cseréljük fel az i -edik sort a t -edikkel
 - $D \leftarrow (-1) \cdot D$
 - folytassuk az **1. lépés**nél
 - PRINT " detA = 0"; STOP

6. Sarrus-szabály, speciális

- csak (3×3) - as mátrixoknál működik

[K70] megjegyzést írt: Többi állításban is az oszlopos verziókat kell használni.

Hozzuk felső háromszög alá!

$$\begin{array}{c} \left. \begin{array}{cccc|l} 1 & -1 & -2 & 1 & \text{II.}+I.(-2) \\ 2 & 1 & 1 & 0 & \text{III.}+I. \\ -1 & -2 & 0 & 1 & \text{IV.}+I.(-3) \\ 3 & -2 & 2 & -1 & \end{array} \right\} \\ \xrightarrow{\text{III.}+II.(3)} \quad \xrightarrow{\text{IV.}+II.(-3)} \quad \left. \begin{array}{ccc|l} 1 & -1 & - & \\ 0 & 1 & \xi & \\ 0 & 0 & 2\xi & \\ 0 & 0 & -1 & \end{array} \right\} \end{array}$$

Végül a determináns értéke – |

[K711] megjegyzést írt:

A szabály lényege, hogy fogjuk és leírjuk saját maga mögé még majd vesszük a főátlókat és a n

$$\det(A) = -a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32}$$

[K721] megjegyzést írt:



10. tétel: Kifejtési tétel, mátrix

Tételcím

A determinánsok kifejtési tétele (bizonyítás nélkül). Műveletek mátrixokkal (összeadás, skalárral szorzás, transzponálás), ezek tulajdonságai. A transzponált determinánsa. Determinánsok szorzástétele (bizonyítás nélkül).

1. Kifejtési tétel

o Tétel

- az $(n \times n)$ -es A mátrix valamelyik sorának vagy oszlopának minden elemét megszorozzuk a hozzá tartozó előjeles al-determináns értékével
- a kapott n db kéttényezős szorzatot összeadjuk $\rightarrow A$ determináns értékét kapjuk

2. Mátrix

o Definíció

- adott egy $k, n \geq 1$ -es egészek esetén $(k \times n)$ -es mátrixnak nevezzük egy k sorból, és n oszlopból álló táblázatot
- minden cellájában valós szám áll
- $(k \times n)$ -es mátrixok halmazát $\mathbb{R}^{k \times n}$ jelöli
- A mátrix i -edik sorának és j -edik oszlopának kereszteződésében álló elemet $a_{i,j}$ jelöli
- $\mathbb{R}^{k \times n}$ -en értelmezett, " + "-al jelölt összeadást és tetszőleges $\lambda \in \mathbb{R}$ esetén " \cdot "-tal jelölt skalárral való szorzást tudjuk értelmezni



$$\begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k,1} & a_{k,2} & \dots & a_{k,n} \end{pmatrix} + \begin{pmatrix} b_{1,1} & b_{1,2} & \dots & b_{1,n} \\ b_{2,1} & b_{2,2} & \dots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{k,1} & b_{k,2} & \dots & b_{k,n} \end{pmatrix} = \begin{pmatrix} a_{1,1}+b_{1,1} & a_{1,2}+b_{1,2} & \dots & a_{1,n}+b_{1,n} \\ a_{2,1}+b_{2,1} & a_{2,2}+b_{2,2} & \dots & a_{2,n}+b_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k,1}+b_{k,1} & a_{k,2}+b_{k,2} & \dots & a_{k,n}+b_{k,n} \end{pmatrix}$$

$$\lambda \cdot \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k,1} & a_{k,2} & \dots & a_{k,n} \end{pmatrix} = \begin{pmatrix} \lambda a_{1,1} & \lambda a_{1,2} & \dots & \lambda a_{1,n} \\ \lambda a_{2,1} & \lambda a_{2,2} & \dots & \lambda a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda a_{k,1} & \lambda a_{k,2} & \dots & \lambda a_{k,n} \end{pmatrix}$$

3. Mátrixműveletek

o **Tétel**

- $A, B, C \in \mathbb{R}^{k \times n}$ és $\lambda, \mu \in \mathbb{R}$
- ekkor igazak az alábbiak:

- (1) $A + B = B + A$
- (2) $(A + B) + C = A + (B + C)$
- (3) $\lambda \cdot (A + B) = \lambda \cdot A + \lambda \cdot B$
- (4) $A \cdot (\lambda + \mu) = A \cdot \lambda + A \cdot \mu$
- (5) $\lambda \cdot (\mu \cdot A) = (\lambda \cdot \mu) \cdot A$

[K73] megjegyzést írt: Kommutatív - felcserélhetőség

[K74] megjegyzést írt: Asszociatív – felbonthatóság/csoportosíthatóság

[K75] megjegyzést írt: Szorzásra nem kommutatív!!

[K76] megjegyzést írt: Hasonló igazak: Mátrixszorzás az összeadásra nézve disztributív
 $A \cdot (B + C) = A \cdot B + A \cdot C$
 $(B + C) \cdot A = B \cdot A + C \cdot A$
 Mátrixszorzás asszociatív
 $A \cdot (B \cdot C) = (A \cdot B) \cdot C$

4. Transzponált

o **Definíció**

- egy $(k \times n)$ -es A mátrixának nevezzük az $(n \times k)$ -es B mátrixot, ha $b_{i,j} = a_{j,i}$ teljesül minden $1 \leq i \leq n$ és $1 \leq j \leq k$ esetén

o **Jelölés**

- $B = A^T$

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 7 \\ 4 & 9 & 2 \\ 6 & 0 & 5 \end{bmatrix}, A^T = \begin{bmatrix} 1 \\ 1 \\ 4 \\ 6 \end{bmatrix} \begin{bmatrix} 2 & 2 & 9 & 0 \\ 3 & 7 & 2 & 5 \end{bmatrix}$$

[K77] megjegyzést írt:

5. Mátrixszorzás

o **Definíció**

- a $(k \times n)$ -es A $(n \times m)$ -es B mátrixok szorzatának nevezzük



- $A \cdot B$ -vel jelöljük azt a $(k \times m)$ -es C mátrixot, melyre minden $1 \leq i \leq k$ és $1 \leq j \leq m$ esetén

$$c_{i,j} = a_{i,1} \cdot b_{1,j} + \dots + a_{i,n} \cdot b_{n,j}$$

- **Állítás**

- ha az A és B mátrixokra $A \cdot B$ szorzat létezik, akkor $A^T \cdot B^T$ is létezik és $(A \cdot B)^T = A^T \cdot B^T$

6. Transzponált determinánsa

- **Tétel**

- minden négyzetes mátrixra $\det A^T = \det A$

- **Bizonyítás**

- (példán mutatjuk be, felhasználva a 9. tételben látott mátrixokat:)

$$A = \begin{pmatrix} 2 & 3 & 4 & \boxed{5} & 6 \\ 7 & \boxed{8} & 9 & 10 & 11 \\ \boxed{12} & 13 & 14 & 15 & 16 \\ 17 & 18 & 19 & 20 & \boxed{21} \\ 22 & 23 & \boxed{24} & 25 & 26 \end{pmatrix}, \quad A^T = B = \begin{pmatrix} 2 & 7 & \boxed{12} & 17 & 22 \\ 3 & \boxed{8} & 13 & 18 & 23 \\ 4 & 9 & 14 & 19 & \boxed{24} \\ \boxed{5} & 10 & 15 & 20 & 25 \\ 6 & 11 & 16 & \boxed{21} & 26 \end{pmatrix}$$

- A^T determinánsának definíció szerinti kiszámításakor is megjelenik ez a szorzat
- itt a megfelelő permutáció $\pi' = (3, 2, 5, 1, 4)$, amelynek az inverziószáma „véletlenül” szintén 5, előjel marad negatív
- A tetszőleges $(n \times n)$ -es mátrix és $B = A^T$
- bizonyítjuk, hogy $\det A$ és $\det B$ kiszámításakor ugyanazok a szorzatok keletkeznek, ugyanolyan előjellel
- $\pi = (\pi_1, \pi_2, \dots, \pi_n)$ tetszőleges permutáció
- ennek $\det A$ kiszámításakor $(-1)^{l(\pi)} \cdot a_{1,\pi_1} \cdot a_{2,\pi_2} \cdot \dots \cdot a_{n,\pi_n}$ előjelezett szorzat felel meg
- mivel $a_{i,j} = b_{j,i}$ minden $1 \leq i$ és $j \leq n$ esetén, ezért ugyanez a szorzat (egyelőre előjeltől eltekintve) megjelenik B -ben is $b_{\pi_1,1} \cdot b_{\pi_2,2} \cdot \dots \cdot b_{\pi_n,n}$ alakban
- ezért π' permutáció, amiben az 1 és a π_1 -edik helyen, a 2 és a π_2 -edik helyen stb. az n és a π_n -edik helyen áll
- ekkor π' -t π inverzének hívjuk

[K78] megjegyzést írt: Melyekről tudjuk, hogy permutáció $\pi = (4, 2, 1, 5, 3)$, inverziószám 5, szorzat negatív előjelet kap.



- ugyanis π permutációt olyan kölcsönösen egyértelmű függvénynek fogjuk fel, amely az $1, 2, \dots, n$ számokhoz rendre $\pi_1, \pi_2, \dots, \pi_n$ értékeket rendel
- függvénytanban π inverze, és π' is permutáció
- B elemeiből készített szorzat $b_{1,\pi'_1} \cdot b_{2,\pi'_2} \cdot \dots \cdot b_{n,\pi'_n}$ alakban írható fel, így $I(\pi')$ előjelet kapja
- meg kell mutatni, hogy $I(\pi) = I(\pi')$ igaz minden π permutációra és annak a π' inverzére
- π permutációban $\pi_i = k, \pi_j = m$, ekkor a π' inverz permutációban $\pi'_k = i$ és $\pi'_m = j$
- k és m tagok π -ben definíció szerint akkor állnak inverzióban, ha $i < j$, de $m < k$
- definíció szerint ez azt jelenti, hogy π' -ben az i, j tagok állnak inverzióban, hiszen $m < k$, de $\pi'_m = j > i = \pi'_k$
- összefoglalva:
 - π -ben π_i, π_j , akkor és csak akkor állnak inverzióban, ha π' -ben i, j állnak inverzióban
- így π -ben inverzióban álló elempárok kölcsönösen egyértelműen megfeleltethetők a π' -ben inverzióban álló elempároknak
- $\rightarrow I(\pi) = I(\pi')$ valóban következik

[K79] megjegyzést írt: És hogy minden permutáció inverze egyértelműen létezik, valamint π' inverze π Vica versa dolog...

[K80] megjegyzést írt: ezt a fenti példán illusztrálva: π -ben a $\pi_1 = 4, \pi_3 = 1$ tagok inverzióban állnak, ennek megfelelően π' -ben az 1 és 3 állnak inverzióban.

7. Determinánsok szorzástétele

o Tétel

- bármely A és B ($n \times n$)-es mátrixokra:

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



11. tétel:

Lineáris egyenletrendszer megoldhatósága

Tételcím

$(n \times n)$ -es lineáris egyenletrendszer egyértelmű megoldhatóságának jellemzése a determináns segítségével. Kapcsolat a lineáris egyenletrendszerek, az \mathbb{R}^n -beli generált altérhez tartozás kérdése, illetve a mátrixszorzáson alapuló mátrixegyenletek között. Kapcsolat négyzetes mátrix determinánsa, illetve a sorok és az oszlopok lineáris függetlensége között.

1. Lineáris egyenletrendszer megoldhatósága

o Tétel

- $!(A|b)$ egy n változós, n egyenletről álló lineáris egyenletrendszer kibővített együtthatómátrixa
- az egyenletrendszer akkor és csak akkor egyértelműen megoldható, ha $\det A \neq 0$

o Bizonyítás

- futtassuk $(A|b)$ -re Gauss-eliminációt
- az algoritmus által megtett sorokvivalens lépések az együtthatómátrix determinánsát megváltoztatják ugyan, de annak nulla/ nemnulla mivoltán nem változtatnak
- Gauss-elimináció az alábbi három lehetőség valamelyikével ér véget:
 - tilos sor: egyenletrendszer nem megoldható
 - egyenletrendszernek végtelen sok megoldása van:
 - ♦ kevesebb sor, mint oszlop (és fordítva), mivel eredetileg A $(n \times n)$ -es volt
 - ♦ \rightarrow az első fázis 3. lépésében keletkeznie kellett csupa 0 sornak, emiatt $\det A$ eredetileg is 0
 - egyenletrendszer megoldása egyértelmű:
 - ♦ RLA, determinánsa 1
 - ♦ főátlóban csupa 1

[K81] megjegyzést írt: A tehát csak a változók együtthatóit tartalmazza, b az egyenletek jobb oldalából áll.



- mindenhol máshol 0
- \rightarrow mivel determináns végül nem 0, ezért eredetileg sem volt 0

2. \mathbb{R}^k -n ekvivalens állítások

o Tétel

- $\underline{a}_1, \dots, \underline{a}_n, \underline{b} \in \mathbb{R}^k$ vektorok és A az \underline{a}_i -k egyesítésével keletkező $(k \times n)$ -es A mátrix
- az alábbi állítások ekvivalensek:
 - (1) megoldható $A \cdot \underline{x} = \underline{b}$ „mátrixegyenlet”
 - (2) megoldható az $(A|\underline{b})$ kibővített együtthatómátrixú lineáris egyenletrendszer
 - (3) $\underline{b} \in \langle \underline{a}_1, \dots, \underline{a}_n \rangle$

o Bizonyítás

- (2) és (3) állítás ekvivalens
- (3) állítás teljesülése azt jelenti, hogy létezik a $\lambda_1 \underline{a}_1 + \dots + \lambda_n \underline{a}_n = \underline{b}$ lineáris kombináció
- vektor i -edik koordinátája minden $1 \leq i \leq k$ esetén $a_{i,1}\lambda_1 + \dots + a_{i,n}\lambda_n = b_i$
- tehát az alsó és a felső egyenlet ekvivalens, és ezzel $(A|\underline{b})$ lineáris egyenletrendszert kapjuk
- (1) és (2) ekvivalenciájához azt kell észrevennünk, hogy \underline{x} csak \mathbb{R}^n -beli oszlopvektor lehet
- \underline{x} j -edik koordinátája minden $1 \leq j \leq n$ esetén x_j -vel jelölve az $A \cdot \underline{x}$ szorzat i -edik koordinátája a mátrixszorzás definíciója szerint $a_{i,1}x_1 + \dots + a_{i,n}x_n$
- ezért $A \cdot \underline{x} = \underline{b}$ azzal ekvivalens, hogy $a_{i,1}x_1 + \dots + a_{i,n}x_n = b_i$ teljesül minden $1 \leq i \leq k$ esetén \rightarrow ismét $(A|\underline{b})$ lineáris egyenletrendszert kapjuk

[K82] megjegyzést írt: A tehát csak a változók együtthatóit tartalmazza, \underline{b} az egyenletek jobb oldalából áll.

[K83] megjegyzést írt: A tehát csak a változók együtthatóit tartalmazza, \underline{b} az egyenletek jobb oldalából áll.

[K84] megjegyzést írt: A tehát csak a változók együtthatóit tartalmazza, \underline{b} az egyenletek jobb oldalából áll.

[K85] megjegyzést írt: A tehát csak a változók együtthatóit tartalmazza, \underline{b} az egyenletek jobb oldalából áll.

[K86] megjegyzést írt: Mert n sora van, ha $A \cdot \underline{x}$, másrészt 1 oszlopa van, ha $A \cdot \underline{x}$ 1 oszlopú

[K87] megjegyzést írt: A tehát csak a változók együtthatóit tartalmazza, \underline{b} az egyenletek jobb oldalából áll.



○ **Következmény:**

- $\underline{a}_1, \dots, \underline{a}_n \in \mathbb{R}^k$ vektorok és A az \underline{a}_i -k egyesítésével keletkező $(k \times n)$ -es A mátrix
- az alábbi állítások ekvivalensek:
 - $A \cdot \underline{x} = \underline{0}$ lineáris egyenletrendszernek az egyetlen megoldása $\underline{x} = \underline{0}$
 - $\underline{a}_1, \dots, \underline{a}_n$ vektorok lineárisan függetlenek

[K88] megjegyzést írt: A tehát csak a változók együtthatóit tartalmazza, \underline{b} az egyenletek jobb oldalából áll.

○ **Bizonyítás.**

- $\underline{a}_1, \dots, \underline{a}_n$ akkor és csak akkor lineárisan független, ha $\lambda_1 \underline{a}_1, \dots, \lambda_n \underline{a}_n = \underline{0}$, triviális lineáris kombináció esetén
 - vagyis: $\lambda_1 = \dots = \lambda_n = 0$
- ez ekvivalens azzal, hogy $A \cdot \underline{x} = \underline{0}$ lineáris egyenletnek egyetlen megoldása az, hogy minden változó értéke 0

[K89] megjegyzést írt: A tehát csak a változók együtthatóit tartalmazza, \underline{b} az egyenletek jobb oldalából áll.

[K90] megjegyzést írt: A tehát csak a változók együtthatóit tartalmazza, \underline{b} az egyenletek jobb oldalából áll.

3. Sor/oszlopvektor lineáris függetlenség

○ **Tétel**

- \underline{A} $(n \times n)$ -es mátrix
- az alábbi állítások ekvivalensek:
 - **(1)** A oszlopai, mint \mathbb{R}^n -beli vektorok, lineárisan függetlenek
 - **(2)** $\det A \neq 0$
 - **(3)** A sorai, mint n hosszú sorvektorok lineárisan függetlenek

[K91] megjegyzést írt: A tehát csak a változók együtthatóit tartalmazza, \underline{b} az egyenletek jobb oldalából áll.

○ **Bizonyítás.**

- **(1)** állítás az előző következmény miatt azzal ekvivalens, hogy az $(A|\underline{b})$ kibővített együtthatómátrixú lineáris egyenletrendszer egyértelműen megoldható
- mivel A négyzetes mátrix, ezért a lineáris egyenletrendszer megoldhatósága tétel szerint, akkor és csak akkor teljesül, ha $\det A \neq 0$ (**(1)** és **(2)** állítás bizonyítva)
- **(2)** és **(3)** állítás közötti ekvivalenciához A transzponáltjára alkalmazzuk az **(1)** és **(2)** állítás közötti, már bizonyított ekvivalenciát



- mivel A^T oszlopai megegyeznek A soraival, és fordítva, ezért A sorai akkor és csak akkor lineárisan függetlenek, ha $\det A^T \neq 0$
- azonban transzponált-determináns tétel miatt $\det A = \det A^T$, ezért ez valóban ekvivalens $\det A \neq 0$ feltétellel



12. tétel: Mátrix inverze, rangja

Tételcím

Mátrix inverze, létezésének szükséges és elégséges feltétele, az inverz kiszámítása. Mátrix rangja, rangfogalmak egyenlősége, rang meghatározása.

1. Inverz mátrix

- Definíció
 - egy $(n \times n)$ -es A *mátrix inverzének* nevezzük az $(n \times n)$ -es X mátrixot, ha teljesül:

$$A \cdot X = E = X \cdot A$$

- Jelölés
 - $X = A^{-1}$

2. Inverz mátrix létezése

- Tétel
 - A $(n \times n)$ -es mátrixnak akkor és csak akkor létezik inverze, ha $\det A \neq 0$
 - ha A^{-1} létezik, akkor az egyértelmű
- Bizonyítás
 - TFH. $X = A^{-1}$ létezik
 - megmutatjuk, hogy $\det A \neq 0$
 - definíció szerint $A \cdot X = E$ egyenlet mindkét oldalának determinánsát véve: $\det(A \cdot X) = \det E$, ahol
 - $\det E = 1$
 - alkalmazzuk szorzástételt: $\det A \cdot \det X = 1 \rightarrow \det A \neq 0$

[K92] megjegyzést írt: A mátrix inverzének a kiszámításánál nem számít a szorzatok sorrendje, mindkét esetben, tehát $A \cdot A^{-1} = A^{-1} \cdot A = 1$. Ez kizárólag csak négyzetes, azaz $(n \times n)$ -es mátrixokra igaz.

3. Inverz mátrix létezés lemmája

o **Tétel**

- ha $A \in \mathbb{R}^{n \times n}$ és $\det A \neq 0$, akkor egyértelműen létezik $X \in \mathbb{R}^{n \times n}$ mátrix, hogy $A \cdot X = E$

o **Bizonyítás**

- fenti szorzás ekvivalens, mátrixszorzás szerint a következővel:

$$A \cdot \underline{x}_1 = \underline{e}_1$$

$$A \cdot \underline{x}_2 = \underline{e}_2$$

⋮

$$A \cdot \underline{x}_n = \underline{e}_n$$

- az $A \cdot \underline{x}_i = \underline{e}_i$ lineáris egyenletrendszer, amely úgy jelölhető, hogy $(A|\underline{e}_i)$
- mivel $\det A \neq 0$, ezért ez az egyenletrendszer egyértelműen megoldható
- beláttuk a lemmát: a keresett X i -edik oszlopa a $A \cdot \underline{x}_i = \underline{e}_i$ rendszer egyértelmű megoldása minden $1 \leq i \leq n$ esetén

o **Inverz kiszámítása Gauss-eliminációval**

- egymás mellé felírjuk az $(n \times n)$ -es A mátrixot, valamint az $(n \times n)$ -es egységmátrixot
- lefuttatjuk a Gauss-eliminációt az A -n, úgy, hogy sorokvivalens lépéseket megismételjük, az E -n is
- addig folytatjuk a Gauss-eliminációt, amíg az A RLA-ban nem lesz
- ekkor az $E' = A^{-1}$

4. Négyzetes részmátrix

o **Definíció**

- ! A $(n \times n)$ -es mátrix és $r \leq n, n \in \mathbb{Z}$
- válasszuk ki tetszőlegesen A sorai és oszlopai közül r - r db
- ekkor kiválasztott sorok és oszlopok kereszteződéseiben kialakuló $(r \times r)$ -es mátrixot A egy négyzetes **részmátrix**ának nevezzük

Példa

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 6 \end{pmatrix} \quad A$$

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 3 & 0 & 1 & 0 \\ 1 & 3 & 6 & 0 & 0 & 1 \end{array} \right) \Rightarrow$$

IK931 megajegyzést írt:



5. Rang (1)

○ Definíció

- ! A tetszőleges mátrix, azt mondjuk, hogy
 - A **oszlorangja** r , ha A oszlopai közül kiválasztható r db úgy, hogy a kiválasztott oszlopok lineárisan függetlenek, de $r + 1$ már nem választható ki így
 - A **sorrangja** r , ha A sorai közül kiválasztható r db úgy, hogy a kiválasztott sorok lineárisan függetlenek, de $r + 1$ már nem választható ki így
 - A **determinánsrangja** r , ha A -nak van nemnulla determinánsú $(r \times r)$ -es részmátrixa, de $(r + 1 \times r + 1)$ -es nemnulla determinánsú már nincs

6. Rangfogalmak egyenlősége

○ Tétel

- minden A mátrixra $o(A) = s(A) = d(A)$

○ Bizonyítás

- elég belátni, hogy $o(A) = d(A)$ igaz minden A mátrixra
- mivel A^T oszlopai megegyeznek A soraival, ezért $s(A) = o(A^T)$, valamint $d(A) = d(A^T)$
- mivel az A^T -ből választható négyzetes részmátrixok az A -ból választhatók transzponáltjai
- legnagyobb nemnulla determinánsú is ugyanazon méretű
- ha az $o(A) = d(A)$ állítást minden mátrixra, így A^T -ra is igaznak feltételezzük, akkor összesítve az $s(A) = o(A^T) = d(A^T) = d(A) = o(A)$ egyenlőséget kapjuk
- csak $o(A) = d(A)$ -t kell bizonyítani:
- először megmutatjuk, hogy **1: $o(A) \geq d(A)$** , majd, hogy **2: $o(A) \leq d(A)$**
- **1:TFH.** $d(A) = r$
- meg kell mutatnunk, hogy $o(A) \geq r$, vagyis, hogy A oszlopai közül kiválasztható r db lineárisan független
- A -ból $d(A) = r$ miatt kiválasztható egy $(r \times r)$ -es nemnulla determinánsú M részmátrix



- A_M A -nak abból az r oszlopából álló mátrixa, amelyeket az M készítésekor választunk ki
- ekkor tehát M sorai A_M sorainak részhalmaza, és A_M oszlopairól állítjuk, hogy lineárisan függetlenek
 - ha nem így volna, akkor (a 11-es tételben levő következmény miatt) $A_M \cdot \underline{x} = \underline{0}$ lineáris egyenletrendszernek volna egy $\underline{x} \neq \underline{0}$ megoldása
 - ekkor azonban \underline{x} megoldása volna az $M \cdot \underline{x} = \underline{0}$ lineáris egyenletrendszernek is, hiszen az utóbbi rendszert az előbbiből kapjuk
 - tehát M oszlopai lineárisan összefüggők volnának, ami a sorvektor lineáris függetlenség tétele miatt (előző tétel) ellentmondana annak, hogy $\det M \neq 0$
 - így $o(A) \geq d(A)$ valóban igaz
- 2: ezt lemmával bizonyítjuk

[K94] megjegyzést írt: M -hez nem tartozó A_M -beli soroknak megfelelő egyenleteket elhagyjuk

Mátrix oszlopok lineáris függetlenség lemmája

- **Tétel**
 - C ($k \times n$)-es mátrix, amelynek az oszlopai (mint \mathbb{R}^k -beli vektorok) lineárisan függetlenek
 - ha $k > n$, akkor C sorai közül kiválasztható egy úgy, hogy ezt a sort elhagyva a kapott $(k-1) \times n$ -es C' mátrix oszlopai szintén lineárisan függetlenek
- **Bizonyítás**
 - C oszlopai $\underline{c}_1, \dots, \underline{c}_n$, az ezek által generált \mathbb{R}^k -beli altért $W = \langle \underline{c}_1, \dots, \underline{c}_n \rangle$
 - mivel W -ben van n elemű generátorrendszer, és $k > n$ F-G egyenlőtlenség miatt nem lehet benne k elemű lineárisan független rendszer
 - \mathbb{R}^k -beli standard bázis vektorai között van olyan, amelyik nem tartozik W -hez
 - \underline{e}_j ilyen, állítjuk, hogy C j -edik sora teljesíti a lemma feltételeit:
 - az elhagyásával a kapott C' mátrix oszlopai lineárisan függetlenek
 - TFI nem így van

[K95] megjegyzést írt: Amelyben tehát az 1-es a j -edik helyen áll



- $C' \cdot \underline{x} = \underline{0}$ lineáris egyenletrendszernek van egy $\underline{x} \neq \underline{0}$ megoldása
 - ekkor $C' \cdot \underline{x} \neq \underline{0}$, mert C oszlopai lineárisan függetlenek
 - mivel $C \cdot \underline{x} *$ szorzat abban különbözik $C' \cdot \underline{x} *$ -tól, hogy az utóbbiba a j -edik helyre „beszűrődik” a C j -edik sorának és a $\underline{x} *$ -nak a skaláris szorzata
 - ezért $C \cdot \underline{x} *$ oszlopvektor j -edik koordinátája egy $\alpha \neq 0$ szám, többi 0
 - következnek, hogy $C \cdot \left(\frac{1}{\alpha} \cdot \underline{x} *\right) = \frac{1}{\alpha} \cdot (C \cdot \underline{x} *) = \underline{e}_j$
 - ez ellentmond annak, hogy $\underline{e}_j \notin W$
 - viszont ez ellentmond a 11.tétel Mátrixszorzás tételének
 - mely szerint a C oszlopainak az $\left(\frac{1}{\alpha} \cdot \underline{x} *\right)$ kombinációja épp \underline{e}_j -t adja vissza, lemma bizonyítva
- 2: bizonyítás folytatása:
- $o(A) = r$ és válasszunk A oszlopai közül r lineárisan függetlent \rightarrow alkossák ezek C mátrixot
 - mutassuk meg, hogy $d(A) \geq r$
 - C, A sorainak számát k -val jelölve C oszlopai \mathbb{R}^k -beli vektorok, így az F-G egyenlőtlenség miatt $k \geq n$
 - $k > r$, akkor a fenti lemmát C -re alkalmazva kapjuk a $(k - 1) \times r$ -es C' mátrixot, amelynek az oszlopai továbbra is lineárisan függetlenek
 - ha $k - 1 > r$, akkor ismét alkalmazhatjuk a lemmát C' -re és ezt folytathatjuk egészen amíg $k - r$ lépés után egy $(r \times r)$ -es $C *$ mátrixot kapunk
 - (11. tétel Sorvektor lineáris függetlenség tétel miatt) $\det C * \neq 0$
 - mivel $C *$ az A -nak $(r \times r)$ -es részmatrice, ezért ez bizonyítja $d(A) \geq r$, és a tételt is

7. Rang (2)

o Definíció

- az A mátrix rangjának nevezzük az $o(A), s(A), d(A)$ közös értékét

[K96] megjegyzést írt: Hiszen \mathbb{R}^k -ban van k elemű generátorrendszer: bármely bázis ilyen

[K97] megjegyzést írt: Mert $C *$ oszlopai lineárisan függetlenek



- Jelölés
 - $r(A)$

8. Rang kiszámolása (1)

- Tétel
 - $A (k \times n)$ -es mátrix és az oszlopai legyenek $\underline{a}_1, \dots, \underline{a}_n$
 - ekkor $r(A) = \dim\langle \underline{a}_1, \dots, \underline{a}_n \rangle$
- Bizonyítás
 - válasszuk ki A oszlopai közül a legtöbbet úgy, hogy ezek lineárisan függetlenek legyenek
 - oszloprang definíció szerint ekkor $r = r(A)$
 - állítjuk, hogy $\underline{a}_1, \dots, \underline{a}_r$ bázist alkot a $W = \dim\langle \underline{a}_1, \dots, \underline{a}_r \rangle$ altérben
 - be kell látni, hogy $\underline{a}_1, \dots, \underline{a}_r$ generátorrendszer W -ben
 - $U = \langle \underline{a}_1, \dots, \underline{a}_r \rangle$, lássuk be, hogy $U = W$
 - $r < i \leq n$ esetén $\underline{a}_1, \dots, \underline{a}_i$ lineárisan összefüggő, mivel A -ból $r + 1$ lineárisan független oszlopot nem lehet kiválasztani
 - az Újonnan érkező vektor lemmája szerint ekkor $\underline{a}_i \in \langle \underline{a}_1, \dots, \underline{a}_r \rangle = U$, tehát $\underline{a}_1, \dots, \underline{a}_n$ mind U -beli
 - mivel U altér, ezért minden W -beli, tehát $\underline{a}_1, \dots, \underline{a}_n$ vektorokból lineáris kombinációval kifejezhető vektor is U -beli kell, hogy legyen
 - bizonyítottuk, hogy $W \subseteq U$

9. Rang kiszámolása (2)

- Tétel
 - az elemi sorkvivalens lépések a mátrix rangját nem változtatják meg
 - a LA mátrix sorainak a száma egyenlő a mátrix rangjával
- Bizonyítás
 - (elemi sorkvivalens lépések bizonyítása)
 - válasszunk ki A oszlopai közül tetszőleges néhányat, ezek együtt az A'
 - A' oszlopai az előző tétel Következménye miatt akkor és csak akkor lineárisan független, ha az $A' \cdot \underline{x} = \underline{0}$ lineáris egyenletrendszernek az egyetlen megoldása $\underline{x} = \underline{0}$



- amikor A -ra alkalmazzuk valamelyik elemi sorkvivalens lépést, akkor ugyanezt alkalmazzuk az $(A' | 0)$ kibővített együtthatómátrixra is
- egyrészt A' sorai az A sorainak részei, másrészt, ha a jobb oldalakon csupa 0 áll, akkor ezt a tulajdonságot mindegyik elemi sorkvivalens lépés fenntartja
- azonban $(A' | 0)$ -n végzett lépések az $A' \cdot \underline{x} = \underline{0}$ lineáris egyenletrendszer megoldásait **nem változtatják meg**
- \rightarrow A -n végzett elemi sorkvivalens lépések nem változtatnak azon, hogy A' oszlopai lineárisan függetlenek-e
- így A oszlopai közül kiválasztható legnagyobb lineárisan független rendszer mérete, vagyis az oszloprang se változik
- (LA mátrix sorainak száma egyenlő a... bizonyítás)
- ha a LA mátrix sorainak száma k , akkor A -ból az összes sor és a vezéregyeseket tartalmazó oszlopok kiválasztásával keletkező M négyzetes részmátrix egy felsőháromszög-mátrix
- ennek főátlójában minden elem 1 (vezéregyesek)
- így $\det M = 1 \neq 0$ vagyis A -nak van $(k \times k)$ -as, nemnulla determinánsú négyzetes részmátrixa
- ennél nagyobb nyilván nincs, mert A -nak csak k sora van
- tehát determináns rangja valóban k

[K98] megjegyzést írt: Így az A teljes sorain végzett lépés A' -re is azonos hatással van

[K99] megjegyzést írt: Ezt mondja ki a Gauss-eliminációs állítás a 8. tételben, és épp ezért lettek ezek a Gauss-elimináció megengedett lépései

[K100] megjegyzést írt: A' -n is



13. tétel: Lineáris leképezés, transzformáció

Tételcím

Lineáris leképezés fogalma, mátrixa. Szükséges és elégséges feltétel egy függvény lineáris leképezés voltára. Lineáris leképezések szorzata, szorzat mátrixa. Következmény: addíciós tételek a sinus és cosinus függvényekre. Lineáris transzformáció invertálhatósága.

1. Lineáris leképezés

○ Definíció

- $f: \mathbb{R}^n \rightarrow \mathbb{R}^k$ *lineáris leképezés*nek hívjuk, ha
 - létezik olyan $(k \times n)$ -es mátrix, melyre $f(\underline{x}) = A \cdot \underline{x}$ minden $\underline{x} \in \mathbb{R}^n$
 - $n = k$ esetben f -et *lineáris transzformáció*nak is nevezzük
 - ha $f: \mathbb{R}^n \rightarrow \mathbb{R}^k$ leképezésnek és $f(\underline{x}) = A \cdot \underline{x}$ minden $\underline{x} \in \mathbb{R}^n$ -re, akkor mátrixa A

○ Jelölés

- $A = [f]$ (3. állítás jelölése)

2. Lineáris leképezés feltétele

○ Tétel

- $f: \mathbb{R}^n \rightarrow \mathbb{R}^k$ függvény akkor és csak akkor lineáris leképezés, ha:
 - **(1)** $f(\underline{x} + \underline{y}) = f(\underline{x}) + f(\underline{y})$ igaz minden $x, y \in \mathbb{R}^n$
 - **(2)** $f(\lambda \cdot \underline{x}) = \lambda \cdot f(\underline{x})$ igaz minden $x \in \mathbb{R}^n$ és $\lambda \in \mathbb{R}$ esetén
- ha f teljesíti ezt a 2 tulajdonságot, akkor:
 - $[f]$ egyértelmű
 - és azonos azzal a $(k \times n)$ -es mátrixszal, melynek minden $1 \leq i \leq n$ esetén az i -edik oszlopa $f(\underline{e}_i)$

[K101] megjegyzést írt: Itt \underline{e}_i az \mathbb{R}^n -beli standard bázis vektora.



o Bizonyítás

- (szükségesség belátása)
- TFH. f lineáris leképezés és $A = [f]$
- (10. tétel, Mátrixműveletek tétel, Megjegyzések: mátrixszorzás összeadásra nézve disztributivitás miatt:)

$$f(\underline{x} + \underline{y}) = A(\underline{x} + \underline{y}) = A\underline{x} + A\underline{y} = f(\underline{x}) + f(\underline{y})$$

- (10. tétel, Mátrixműveletek tétel, Megjegyzések: mátrixszorzás asszociativitás miatt:)

$$f(\lambda \cdot \underline{x}) = A(\lambda \cdot \underline{x}) = \lambda(A \cdot \underline{x}) = \lambda \cdot f(\underline{x})$$

- (egyértelműség belátása)
- ! f -nek A egyik mátrixa, \underline{a}_i : A -nak i -edik oszlopa minden i -re
- (10. tétel, Mátrixszorzás definíció miatt:)

$$A \cdot \underline{e}_i = \underline{a}_i$$

- ebből $A = [f]$ miatt: $f(\underline{e}_i) = A \cdot \underline{e}_i = \underline{a}_i$, amely bizonyítja $[f]$ egyértelműségét
 - $[f]$ csak az a mátrix lehet, amelynek i -edik oszlopa $f(\underline{e}_i)$, vagyis csak A

- (elégesség bizonyítása)
- ha az első 2 tulajdonság teljesül, akkor f lineáris leképezés
- mutassunk olyan mátrixot, amelyre: $f(\underline{x}) = A \cdot \underline{x}$ minden $\underline{x} \in \mathbb{R}^n$
- A mátrix i -edik oszlopa $f(\underline{e}_i)$ minden i -re, jelölje \underline{a}_i

- ekkor: $f(\underline{x}) = A \cdot \underline{x}$ teljesül $\underline{x} = \underline{e}_i$ vektorokra
- belátjuk, hogy (1) n tagú összegekre is teljesül

$$\begin{aligned} f(\underline{v}_1 + \dots + \underline{v}_n) &= f(\underline{v}_1) + f(\underline{v}_2 + \dots + \underline{v}_n) = f(\underline{v}_1) + f(\underline{v}_2) + f(\underline{v}_3 + \dots + \underline{v}_n) \\ &= f(\underline{v}_1) + f(\underline{v}_2) + \dots + f(\underline{v}_n) \end{aligned}$$

- vagyis $(n - 1)x$ egymás után alkalmazva az (1)
- ! $\underline{x} \in \mathbb{R}^n$ tetszőleges i -edik koordinátáját jelölje: x_i , ekkor:

$$\underline{x} = x_1 \cdot \underline{e}_1 + \dots + x_n \cdot \underline{e}_n$$

$$\begin{aligned} f(\underline{x}) &= f(x_1 \cdot \underline{e}_1 + \dots + x_n \cdot \underline{e}_n) = \\ &= f(x_1 \cdot \underline{e}_1) + \dots + f(x_n \cdot \underline{e}_n) = \\ &= x_1 \cdot f(\underline{e}_1) + \dots + x_n \cdot f(\underline{e}_n) = \end{aligned}$$

[K102] megjegyzést írt: Fenti bekezdés segít.

[K103] megjegyzést írt: Be kell látni, hogy minden más \underline{x} -re is.

[K104] megjegyzést írt: Lásd 7. tétel, Standard bázis definíció bizonyítás.



$$= f(\underline{e}_n) = (x_1 \cdot \underline{a}_1 + \dots + x_n \cdot \underline{a}_n)$$

$$= A \cdot \underline{x}$$

3. Lineáris leképezés szorzata

o Tétel

- ! $f: \mathbb{R}^n \rightarrow \mathbb{R}^k$ és $g: \mathbb{R}^k \rightarrow \mathbb{R}^m$ lineáris leképezések
- ezeknek a $g \circ f$ szorzata is lineáris leképezés, melyre $[g \circ f] = [g] \cdot [f]$

o Bizonyítás

- ! $[f] = A$, minden $\underline{x} \in \mathbb{R}^n$ -re, $f(\underline{x}) = A \cdot \underline{x}$
- ! $[g] = B$, minden $\underline{y} \in \mathbb{R}^k$ -re, $g(\underline{y}) = B \cdot \underline{y}$
- alkalmazzuk a $g \circ f$ függvényt tetszőleges $\underline{x} \in \mathbb{R}^n$ -re

$$(g \circ f) \cdot (\underline{x}) = g \cdot (f(\underline{x})) = g \cdot (A \cdot \underline{x}) = B \cdot (A \cdot \underline{x}) = (B \cdot A) \cdot \underline{x}$$

- tehát $B \cdot A = [g] \cdot [f]$

4. Addíciós tételek

o Tétel

- tetszőleges α és β szögekre teljesülnek az alábbi összefüggések
 - $\sin(\alpha + \beta) = \sin \alpha \cdot \cos \beta + \cos \alpha \cdot \sin \beta$
 - $\cos(\alpha + \beta) = \cos \alpha \cdot \cos \beta - \sin \alpha \cdot \sin \beta$

o Bizonyítás

- ! $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ a síkban az origó körüli α, β szöggel való elforgatás
- ezek lineáris leképezések
- alkalmazzuk a fenti *Lineáris leképezés szorzata tétel*t
- igaz, hogy $f_\alpha \circ f_\beta = f_{\alpha+\beta}$ az origó körüli $\alpha + \beta$ szögű elforgatással
 - hiszen egy tetszőleges \underline{v} -t először β , majd α szöggel elforgatva ugyanazt kapjuk, mintha $\alpha + \beta$ szöggel forgattuk volna
- f_α, f_β és $f_{\alpha+\beta}$ lineáris transzformációk mátrixa kiolvasható az állításból, ezekre lineáris leképezés szorzata fennáll:

$$[f_{\alpha+\beta}] = [f_\alpha] \cdot [f_\beta]$$

[K105] megjegyzést írt: Egy állításból tudjuk, hogy! $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ az a függvény, minden $\underline{v} \in \mathbb{R}^2$ síkvektorban annak az origó körüli α szöggel való elforgatottját rendeli, ekkor f lineáris transzformáció, melynek mátrixa

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

[K106] megjegyzést írt: Előbbi megjegyzésben leírva.



$$\begin{aligned} [f_\alpha] &= \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \begin{pmatrix} \cos(\alpha + \beta) & -\sin(\alpha + \beta) \\ \sin(\alpha + \beta) & \cos(\alpha + \beta) \end{pmatrix} = [f_{\alpha+\beta}] \\ & \begin{pmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{pmatrix} = [f_\beta] \end{aligned}$$

5. Lineáris transzformáció invertálhatósága

o Tétel

- $f: \mathbb{R}^n \rightarrow \mathbb{R}^k$ lineáris transzformáció akkor és csak akkor invertálható, ha $\det[f] \neq 0$
- ha ez a feltétel fennáll, akkor $[f^{-1}] = [f]^{-1}$, vagyis az f^{-1} inverz transzformáció mátrixa az f mátrixnak az inverze

o Bizonyítás

- $[f] = A$, vagyis $f(\underline{x}) = A \cdot \underline{x}$ minden $\underline{x} \in \mathbb{R}^n$
- (szükségesség bizonyítása)
- ha f invertálható, akkor $\det A \neq 0$
- TFI $\det A = 0$, ekkor (8. tétel, Lineáris egyenletrendszer megoldhatósága tétel miatt) A oszlopai lineárisan összefüggők, ellentmond annak, hogy f invertálható
- (elégesség bizonyítása)
- ha $\det A \neq 0$, akkor f invertálható
- mivel $\det A \neq 0$, ezért (12. tétel, Inverz mátrix tétel miatt) létezik A^{-1} inverz mátrix
- tetszőleges $\underline{x} \in \mathbb{R}^n$ esetén $f(\underline{x}) = \underline{y}$ azt jelenti, hogy

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

$$A^{-1} \cdot \underline{y} = A^{-1} \cdot (A \cdot \underline{x}) = (A^{-1} \cdot A) \cdot \underline{x} = E \cdot \underline{x} = \underline{x}$$

- tehát $\underline{y} \rightarrow A^{-1} \cdot \underline{y}$ függvény azonos az f inverzével

[K107] megjegyzést írt: $(n \times n)$ -es egységmátrix.

[K108] megjegyzést írt: Beláttuk tehát, hogy létezik f^{-1} , másrészt, hogy $[f^{-1}] = A = [f]^{-1}$.



14. tétel: Magtér, képtér

Tételcím

Lineáris leképezések magtere, képtere, ezek altér volta. Dimenziótétel.

1. Magtér, képtér

o Definíció

- $f: \mathbb{R}^n \rightarrow \mathbb{R}^k$ lineáris leképezés
- f *magtere*:
 - jelölés: $\text{Ker } f$
 - azon \mathbb{R}^n -beli vektorok halmazát (V_1), melyeknek a képe az \mathbb{R}^k -beli $\underline{0}$

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

▪ f *képtere*:

- jelölés: $\text{Im } f$
- azon \mathbb{R}^k -beli vektorok halmazát (V_2), melyek megkaphatók (legalább) 1 alkalmas \mathbb{R}^n -beli vektor f -fel vett képeként

$$\text{Im } f = \{\underline{y} \in \mathbb{R}^k: \exists \underline{x} \in \mathbb{R}^n, f(\underline{x}) = \underline{y}\}$$

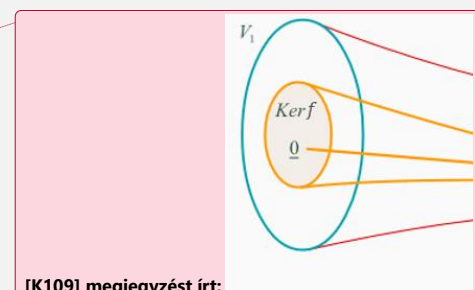
2. Mag - és képtér altér volta

o Tétel

- $f: \mathbb{R}^n \rightarrow \mathbb{R}^k$ lineáris leképezés, ekkor
 - $\text{Ker } f \leq \mathbb{R}^n$, vagyis $\text{Ker } f$ altér \mathbb{R}^n -ben
 - $\text{Im } f \leq \mathbb{R}^k$, vagyis $\text{Im } f$ altér \mathbb{R}^k -ban

o Bizonyítás

- ($\text{Ker } f$ bizonyítása)
- (6. tétel, \mathbb{R}^n alterei definíció miatt) meg kell mutatnunk, hogy bármely $\underline{x}_1, \underline{x}_2 \in \text{Ker } f$ és $\lambda \in \mathbb{R}$ esetén



[K1091 megieavzést írt:



- $\underline{x}_1 + \underline{x}_2, \lambda \cdot \underline{x}_1 \in \text{Ker } f$ teljesülnek
- ha $\underline{x}_1, \underline{x}_2 \in \text{Ker } f$, akkor $f(\underline{x}_1) = \underline{0}$ és $f(\underline{x}_2) = \underline{0}$
- (13. tétel, Lineáris leképezés feltétele tétel tulajdonság (1) miatt)
 $f(\underline{x}_1 + \underline{x}_2) = f(\underline{x}_1) + f(\underline{x}_2) = \underline{0} + \underline{0} = \underline{0} \rightarrow \underline{x}_1 + \underline{x}_2 \in \text{Ker } f$
- (13. tétel, Lineáris leképezés feltétele tétel tulajdonság (2) miatt)
 $f(\lambda \cdot \underline{x}_1) = \lambda \cdot \underline{0} = \underline{0} \rightarrow \lambda \in \text{Ker } f$
- $\text{Ker } f$ nem lehet üres, hiszen $\underline{0} \in \text{Ker } f$ definíció szerint mindig igaz
- ($\text{Im } f$ bizonyítása)
- ha $[f] = A$, akkor $\text{Im } f$ definíció szerint azokból az $\underline{y} \in \mathbb{R}^k$ vektorokból áll, melyek kifejezhetők $A \cdot \underline{x} = \underline{y}$ alakban
- (11. tétel, Mátrixszorzás tétel szerint) ez ekvivalens $\underline{y} \in \langle \underline{a}_1, \dots, \underline{a}_n \rangle$, ahol A oszlopait \underline{a}_i -k jelölik
- $\text{Im } f \langle \underline{a}_1, \dots, \underline{a}_n \rangle$ generált altér

3. Dimenziótétel

o Tétel

- ha $f: \mathbb{R}^n \rightarrow \mathbb{R}^k$ lineáris leképezés, akkor $\dim \text{Ker } f + \dim \text{Im } f = \dim V_1$

o Bizonyítás

- $\dim \text{Ker } f = m$, válasszunk egy tetszőleges bázist $\text{Ker } f$ -ben, $\underline{b}_1, \dots, \underline{b}_m$, amely lineárisan független
- (7. tétel, Bázis létezése tétel szerint) ez a rendszer kiegészíthető \mathbb{R}^n egy bázisává
- mivel $\dim \mathbb{R}^n = n$, kellene további $n - m$ vektor szükséges: $\underline{c}_1, \dots, \underline{c}_{n-m}$
- megmutatjuk, hogy $f(\underline{c}_1), \dots, f(\underline{c}_{n-m})$ rendszer bázis $\text{Im } f$ -ben $\rightarrow \dim \text{Im } f = n - m$
- lássuk be: $f(\underline{c}_1), \dots, f(\underline{c}_{n-m})$ generátorrendszer $\text{Im } f$ -ben
- $\underline{y} \in \text{Im } f$ tetszőleges, ekkor $\underline{y} = f(\underline{x})$ valamely $\underline{x} \in \mathbb{R}^n$
- mivel $\underline{b}_1, \dots, \underline{b}_m, \underline{c}_1, \dots, \underline{c}_{n-m}$ generátorrendszer \mathbb{R}^n -ben, ezért \underline{x} kifejezhető lineáris kombinációjuként

[K110] megjegyzést írt: A képtér és a magtér dimenziója összesen éppen kiadja a V_1 dimenzióját.

[K111] megjegyzést írt: 7. tétel, Bázis létezése következmény miatt.



$$\begin{aligned}\underline{x} &= \beta_1 \underline{b}_1 + \dots + \beta_m \underline{b}_m + \gamma_1 \underline{c}_1 + \dots + \gamma_{n-m} \underline{c}_{n-m} \quad / \cdot f \\ \underline{y} &= f(\underline{x}) = f(\beta_1 \underline{b}_1 + \dots + \beta_m \underline{b}_m + \gamma_1 \underline{c}_1 + \dots + \gamma_{n-m} \underline{c}_{n-m}) \\ &= f(\beta_1 \underline{b}_1) + \dots + f(\beta_m \underline{b}_m) + f(\gamma_1 \underline{c}_1) + \dots + f(\gamma_{n-m} \underline{c}_{n-m}) \\ &= \beta_1 f(\underline{b}_1) + \dots + \beta_m f(\underline{b}_m) + \gamma_1 f(\underline{c}_1) + \dots + \gamma_{n-m} f(\underline{c}_{n-m}) \\ &= \beta_1 \underline{0} + \dots + \beta_m \underline{0} + \gamma_1 f(\underline{c}_1) + \dots + \gamma_{n-m} f(\underline{c}_{n-m}) \\ &= \gamma_1 f(\underline{c}_1) + \dots + \gamma_{n-m} f(\underline{c}_{n-m})\end{aligned}$$

- utolsó lépésben felhasználjuk, hogy
$$f(\underline{b}_1) = \dots = f(\underline{b}_m) = \underline{0}$$
- tetszőlegesen választott $\underline{y} \in \text{Im} f$ kifejezhető $f(\underline{c}_1), \dots, f(\underline{c}_{n-m})$ lineáris kombinációja

- most belátjuk, hogy $f(\underline{c}_1), \dots, f(\underline{c}_{n-m})$ lineárisan független
- TFH. $\gamma_1 f(\underline{c}_1) + \dots + \gamma_{n-m} f(\underline{c}_{n-m}) = \underline{0}$
- meg kell mutatnunk, hogy (7. tétel, Standard bázis tétele miatt) ekkor $\gamma_1 = \gamma_2 = \dots = \gamma_{n-m} = 0$

$$\begin{aligned}\underline{0} &= \gamma_1 f(\underline{c}_1) + \dots + \gamma_{n-m} f(\underline{c}_{n-m}) \\ &= f(\gamma_1 \underline{c}_1) + \dots + f(\gamma_{n-m} \underline{c}_{n-m}) \\ &= f(\gamma_1 \underline{c}_1 + \dots + \gamma_{n-m} \underline{c}_{n-m})\end{aligned}$$

- ebből $\text{Ker} f$ definíció szerint $\in \text{Ker} f \rightarrow$ kifejezhető $\underline{b}_1, \dots, \underline{b}_m$ lineáris kombinációjaként

$$\begin{aligned}\gamma_1 \underline{c}_1 + \dots + \gamma_{n-m} \underline{c}_{n-m} &= \beta_1 \underline{b}_1 + \dots + \beta_m \underline{b}_m \quad / \text{átrendezve} \\ -\beta_1 \underline{b}_1 - \dots - \beta_m \underline{b}_m + \gamma_1 \underline{c}_1 + \dots + \gamma_{n-m} \underline{c}_{n-m} &= \underline{0}\end{aligned}$$

- azonban $\underline{b}_1, \dots, \underline{b}_m, \underline{c}_1, \dots, \underline{c}_{n-m}$ lineárisan független
- triviális lineáris kombinációja adhatja $\underline{0} \rightarrow \gamma_1 = \gamma_2 = \dots = \gamma_{n-m} = 0$
- megmutattuk, hogy $f(\underline{c}_1) + \dots + f(\underline{c}_{n-m})$ lineárisan független, így **bázis** is

[K112] megjegyzést írt: Kihaználjuk f lineáris leképezés tételbeli tulajdonságát.

[K113] megjegyzést írt: $\underline{b}_1, \dots, \underline{b}_m \in \text{Ker} f$ miatt igaz.

[K114] megjegyzést írt: 13. tétel, Lineáris leképezés feltétele tétel tulajdonság használata.

[K115] megjegyzést írt: $\underline{b}_1, \dots, \underline{b}_m \in \text{Ker} f$ miatt igaz

[K116] megjegyzést írt: β is.

[K117] megjegyzést írt: Mert már beláttuk, hogy generátorrendszer.



15. tétel: Bázistranszformáció

Tételcím

Bázistranszformáció fogalma, lineáris transzformáció mátrixa adott bázis szerint, annak kiszámítása.

1. Bázistranszformáció

o Tétel

- $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ lineáris transzformáció és B egy $f(n \times n)$ -es mátrix, melynek oszlopai bázist alkotnak \mathbb{R}^n -ben
- $g: \mathbb{R}^n \rightarrow \mathbb{R}^n$ az a függvény, mely minden $\underline{x} \in \mathbb{R}^n$ esetén $[\underline{x}]_B$ -hez $[f(\underline{x})]_B$ -t rendel
- ekkor g is lineáris transzformáció, melynek mátrixa $[g] = B^{-1} \cdot [f] \cdot B$

o Bizonyítás

- B oszlopai akkor és csak akkor alkotnak bázist, ha $\det B \neq 0$
- **altér következmény** szerint \mathbb{R}^n bázisai az n tagú lineárisan független rendszerek
- (11. tétel, Sorvektor lineáris függetlenség tétele miatt) B oszlopainak lineáris függetlensége ekvivalens $\det B \neq 0$
- (12. tétel, Inverz mátrix létezése tétele miatt) B^{-1} inverz mátrix valóban létezik
- folytatáshoz lemmát használunk
- ⋮
- folytatva a tételt a lenti lemma segítségével:
- $g: [\underline{x}]_B \rightarrow [f(\underline{x})]_B$ függvény azonos $h^{-1} \circ f \circ h$ függvénnyel
- ha $[\underline{x}]_B$ -re alkalmazzuk h -t, akkor \underline{x} -et kapjuk, erre f -et alkalmazva $f(\underline{x})$ -et kapjuk, végül erre h^{-1} -et alkalmazva $[f(\underline{x})]_B$ -t kapjuk

[K118] megjegyzést írt: $V \leq \mathbb{R}^n$ altér $\underline{f}_1, \dots, \underline{f}_k$ V -beli vektorokból álló lineárisan független rendszer. Ha $\dim V = k$, akkor $\underline{f}_1, \dots, \underline{f}_k$ bázis V -ben.

[K119] megjegyzést írt: Az itt bevezetett g lineáris transzformáció mátrixnak a lemmát követő definíció ad nevet.

[K120] megjegyzést írt: Kompozíció.



- (13. tétel, Lineáris leképezés szorzata tétel miatt) $g = h^{-1} \circ f \circ h$ valóban lineáris transzformáció, mátrixa:

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

2. Bázistranszformáció lemmája

o Tétel

- ! $h: \mathbb{R}^n \rightarrow \mathbb{R}^n$ az a függvény, mely minden $\underline{x} \in \mathbb{R}^n$ esetén $[\underline{x}]_B$ -hez \underline{x} -et rendel
- ekkor h lineáris transzformáció, melynek mátrixa $[h] = B$

o Bizonyítás

- ! $\underline{x} \in \mathbb{R}^n$ -re $[\underline{x}]_B$ koordinátavektor i -edik koordinátája α_i minden $1 \leq i \leq n$ esetén
- ekkor $\underline{x} = \alpha_1 \underline{b}_1 + \dots + \alpha_n \underline{b}_n$
- (10. tétel, Mátrixszorzás definíciója szerint) $B \cdot [\underline{x}]_B$ azonos B oszlopaiból $[\underline{x}]_B$ koordinátaival, mint együtthatókkal képzett lineáris kombinációval
- így $\underline{x} = B \cdot [\underline{x}]_B$, amely mutatja, hogy a $h: [\underline{x}]_B \rightarrow \underline{x}$ függvény lineáris transzformáció, melynek mátrixa B
- mivel $\det B \neq 0$, ezért (13. tétel, Lineáris transzformációk invertálhatósága tétel szerint) h^{-1} inverz transzformáció is létezik, mátrixa: $[h^{-1}] = [h]^{-1} = B^{-1}$
- ez minden $\underline{x} \in \mathbb{R}^n$ esetén $[\underline{x}]_B$ -hez \underline{x} -et rendel

[K121] megjegyzést írt: \underline{b}_i -kből

[K122] megjegyzést írt: \underline{a}_i -kkel

3. Lineáris transzformáció adott bázis szerint

o Definíció

- ! $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ lineáris transzformáció és B bázis \mathbb{R}^n -ben
- ekkor $g: [\underline{x}]_B \rightarrow [f(\underline{x})]_B$ lineáris transzformáció mátrixát az f transzformáció B bázis szerinti mátrixának nevezzük

o Jelölés

- $[f]_B$

[K123] megjegyzést írt: Az itt bevezetett g lineáris transzformáció mátrixnak a lemmát követő definíció ad nevet



4. Lineáris transzformáció kiszámítása adott bázis szerint

o **Tétel**

- $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ lineáris transzformáció
- B egy $(n \times n)$ -es mátrix, melynek oszlopai bázist alkotnak \mathbb{R}^n -ben
- ekkor $[f]_B$ mátrixra alábbiak teljesülnek:
 - (1) $[f(\underline{x})]_B = [f]_B \cdot [\underline{x}]_B$ minden $\underline{x} \in \mathbb{R}^n$ -re
 - (2) $[f]_B = B^{-1} \cdot [f] \cdot B$
 - (3) $[f]_B$ i -edik oszlopa egyenlő $[f(\underline{b}_i)]_B$ koordinátavektorral minden $1 \leq i \leq n$ esetén

o **Bizonyítás**

- (2) már beláttuk az előző tétel bizonyításában
- (1) közvetlenül következik a Lineáris transzformáció adott bázis szerinti definíciójából és annak tételéből
 - mivel $[f]_B$ annak a g lineáris transzformációnak a mátrixa, amely minden $\underline{x} \in \mathbb{R}^n$ -re $[f(\underline{x})]_B$ -t rendel, az állítás igaz
- (3) (13. tétel, Lineáris leképezés feltétele tétel következménye):
 - mivel $[f]_B$ a $g: [\underline{x}]_B \rightarrow [f(\underline{x})]_B$ lineáris transzformáció mátrixa, ezért i -edik oszlopa $g(\underline{e}_i)$ -vel egyenlő minden i -re
 - (7. tétel, Koordinátavektor definíciója szerint) \underline{e}_i éppen \underline{b}_i koordinátavektora
 - vagyis:
 - $\underline{e}_i = [\underline{b}_i]_B \rightarrow g(\underline{e}_i) = g([\underline{b}_i]_B) = [f(\underline{b}_i)]_B$

[K124] megjegyzést írt: + a Lineáris leképezés definíciója miatt

[K125] megjegyzést írt: Az itt bevezetett g lineáris transzformáció mátrixnak a lemmát követő definíció ad nevet

[K126] megjegyzést írt: Az itt bevezetett g lineáris transzformáció mátrixnak a lemmát követő definíció ad nevet



16. tétel: Sajátvektor, karakterisztikus polinom

Tételcím

Négyzetes mátrixok sajátértékei és sajátvektorai, ezek meghatározása. Karakterisztikus polinom. A sajátértékek és sajátvektorok kapcsolata lineáris transzformáció valamely bázis szerinti mátrixának diagonalitásával.

1. Sajátérték, sajátvektor

○ Definíció

▪ A ($n \times n$)-es mátrix

▪ sajátérték

- olyan $\lambda \in \mathbb{R}$ skalár
- ha létezik olyan $\underline{x} \in \mathbb{R}^n$, $\underline{x} \neq \underline{0}$ vektor, melyre

$$A \cdot \underline{x} = \lambda \cdot \underline{x}$$

▪ sajátvektor

- olyan $\underline{x} \in \mathbb{R}^n$ vektor
- ha $\underline{x} \neq \underline{0}$, létezik olyan $\lambda \in \mathbb{R}$ skalár, melyre

$$A \cdot \underline{x} = \lambda \cdot \underline{x}$$

▪ röviden:

- ha $A \cdot \underline{x} = \lambda \cdot \underline{x}$, $\underline{x} \neq \underline{0}$, akkor λ sajátértéke, \underline{x} sajátvektora A -nak

2. Sajátérték meghatározása

○ Tétel

▪ négyzetes A mátrixnak a $\lambda \in \mathbb{R}$ skalár akkor és csak akkor sajátértéke, ha $\det(A - \lambda \cdot E) = 0$

○ Bizonyítás

- λ definíció szerint akkor sajátérték, ha $A \cdot \underline{x} = \lambda \cdot \underline{x}$, $\underline{x} \neq \underline{0}$, van megoldása
- írhatunk $\lambda \cdot \underline{x}$ helyett $(\lambda \cdot E) \cdot \underline{x}$

[K127] megjegyzést írt: Egységmátrix.



- (10. tétel, Mátrixműveletek tétel (1) szerint)

$$(\lambda \cdot E) \cdot \underline{x} = \lambda \cdot (E \cdot \underline{x}) = \lambda \cdot \underline{x}$$
- $A \cdot \underline{x} = (\lambda \cdot E) \cdot \underline{x}$ egyenletet átrendezve, majd (Mátrixműveletek tétel (2) szerint):

$$A \cdot \underline{x} - (\lambda \cdot E) \cdot \underline{x} = \underline{0}$$

$$(A - \lambda \cdot E) \cdot \underline{x} = \underline{0}$$

- λ akkor és csak akkor sajátértéke A -nak, ha az $A \cdot \underline{x} - (\lambda \cdot E) \cdot \underline{x} = \underline{0}$ lineáris egyenletrendszernek van $\underline{x} \neq \underline{0}$ megoldása
- a következők szerint ekvivalens $A - \lambda \cdot E$ mátrix oszlopai lineárisan összefüggők
- (11. tétel, Sorvektor lineáris függetlenség tétel szerint) valóban azzal ekvivalens, hogy $\det(A - \lambda \cdot E) = 0$

[K128] megjegyzést írt: Legyenek $\underline{a}_1, \dots, \underline{a}_n \in \mathbb{R}^k$ vektorok és legyen A az ezek egyesítésével keletkező $(k \times n)$ -es mátrix. Ekkor az alábbi állítások ekvivalensek:
 $A \cdot \underline{x} = \underline{0}$ lineáris egyenletrendszer az egyetlen megoldása $\underline{x} = \underline{0}$
 $\underline{a}_1, \dots, \underline{a}_n$ vektorok lineárisan függetlenek.

3. Karakterisztikus polinom

- Definíció
 - A ($n \times n$)-es mátrix **karakterisztikus polinomjának** nevezzük a $\det(A - \lambda \cdot E)$ determináns értékét, ahol λ változó
- Jelölés
 - $k_a(\lambda)$
- (sajátérték definíciója átfogalmazva az előző tétel és definíció felhasználásával):
 - A mátrix sajátértékei a $k_a(\lambda)$ karakterisztikus polinom gyökei, tehát $k_a(\lambda) = 0$ egyenlet megoldásai
 - algebra egyik tétele szerint tehát n -edfokú polinomnak legfeljebb n gyöke lehet \rightarrow ($n \times n$)-es mátrixnak legfeljebb n sajátértéke van)

4. Diagonális mátrix

- Definíció
 - A ($n \times n$)-es mátrix akkor nevezzük **diagonális mátrixnak**, ha minden $i \neq j$ esetén $a_{i,j} = 0$ teljesül

5. Kapcsolat sajátérték és lineáris leképezések közt

- $B = \{\underline{b}_1, \dots, \underline{b}_n\}$ tetszőleges bázis
- TFH. $[f]_B$ mátrix diagonális, a főátlóban álló elemeket jelölje sorba $\underline{\lambda}_1, \dots, \underline{\lambda}_n$



- $[f]_B$ i -edik oszlopa $\lambda_i \cdot \underline{e}_i$ -vel egyenlő
- ebből kifolyólag $[f(\underline{b}_i)]_B = \lambda_i \cdot \underline{e}_i$, ez viszont azt jelenti, hogy
$$f(\underline{b}_i) = 0 \cdot \underline{b}_1 + \dots + \lambda_i \cdot \underline{b}_i + \dots + 0 \cdot \underline{b}_n, \text{ vagyis } f(\underline{b}_i) = \lambda_i \cdot \underline{b}_i$$
- összefoglalva:
 - $[f]_B$ akkor lesz diagonális, ha B minden tagjára $f(\underline{b}_i) = \lambda_i \cdot \underline{b}_i$ teljesül valamilyen λ skalárral