Bevezetés a Számításelméletbe 1.

Hegyi Zsolt

2017. január 13.

A jegyzet és annak forrása megtalálható a `bme-notes.github.io` weboldalon.

Közreműködtek: Bálint Ádám, Bereczki Márk, Bognár Márton, Bokros Bálint, Braun Márton, Dános Péter, Hanusch Róbert, az IRC-s baráti társaságom, Koczka Tamás, Kormány Zsolt, a KSZK reszort tagjai, Müller András, Nagy "Sid" Jenő, Rostás Balázs.

Kellemes vizsgázást!

Tartalomjegyzék

Előszó

A tételsor Szeszlér Dávid fantasztikus előadásai és jegyzete alapján készült.

1. tétel

Tétel: TÉRVEKTOR TULAJDONSÁGOK
Legyenek $\underline{u} = (u_1, u_2, u_3) \in \mathbb{R}^3$ és $\underline{v} = (v_1, v_2, v_3) \in \mathbb{R}^3$ térvektorok és $\lambda \in \mathbb{R}$. Ekkor

$$\underline{u} + \underline{v} = (u_1 + v_1, u_2 + v_2, u_3 + v_3)$$
$$\underline{u} - \underline{v} = (u_1 - v_1, u_2 - v_2, u_3 - v_3)$$
$$\lambda \underline{u} = (\lambda u_1, \lambda u_2, \lambda u_3)$$

Definíció: SKALÁRIS SZORZAT
$\underline{u}$ és $\underline{v}$ skaláris szorzatán az alábbit értjük:

$$\underline{u} \cdot \underline{v} = |\underline{u}| \cdot |\underline{v}| \cdot \cos \phi$$

Ha $\phi = k \cdot 90° \quad k \in \mathbb{Z}$, akkor a szorzatösszeg 0.

Tétel: SKALÁRIS SZORZAT
Egy alternatív meghatározása a skaláris szorzatnak:
Legyenek $\underline{u} = (u_1, u_2, u_3) \in \mathbb{R}^3$ és $\underline{v} = (v_1, v_2, v_3) \in \mathbb{R}^3$ térvektorok. Ekkor

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

Tétel: EGYENES
Az e egyenes paraméteres egyenletrendszere (1. tétel miatt)

$$x = x_0 + \lambda \cdot a$$
$$y = y_0 + \lambda \cdot b$$
$$z = z_0 + \lambda \cdot c$$
$$\lambda \in \mathbb{R}$$

Ahol $P_0(x_0, y_0, z_0)$ ponton átmegy a vonal és $\underline{v} = (a,b,c)(\underline{v} \neq \underline{0})$ irányvektora. Nem paraméteres alakban ugyanez:

Tétel: EGYENES
Legyen az e egyenesnek $P_0(x_0, y_0, z_0)$ pontja és $\underline{v} = (a,b,c)(\underline{v} \neq \underline{0})$ irányvektora. Ekkor tetszőleges pontjának NEM paraméteres alakja:

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

Bizonyítás:
P $\in$ e akkor igaz, ha e param.egy.rszr-ére $\lambda \in \mathbb{R}$ értékre P-t adja. Ha $a, b, c \neq 0$, akkor a három egyenletből egy közös λ-ra kell jutnunk. Ha $c = 0$, akkor megfelelő λ létezése azt jelenti, hogy $z = z_0$

és az első két egyenletből közös λ értéket kell kapnunk. Végül ha csak $c \neq 0$, akkor az első két egyenlet egyértelmű míg a harmadik egyenlet mindig kielégíthető a $\lambda = \frac{z-z_0}{c}$ választással.

Tétel: SÍK

Legyen adott az S síknak $P_0(x_0, y_0, z_0)$ és $\underline{n} = (a, b, c) \quad n \neq \underline{0}$ normálvektora. Ekkor *P(x,y,z)* P $\in$ S akkor igaz, ha

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

Bizonyítás:

$P \in S$ akkor igaz, ha $\vec{P_0P}$ || S-sel, $\vec{P_0P}$ pedig akkor || S-sel, ha merőleges $\underline{\text{n}}$-nel, ez akkor igaz, ha (skaláris szorzat def!) skaláris szorzatuk 0. Az skal. szorzat alternatív formáját véve és átrendezve megkapjuk az egyenletet.

Definíció: VEKTORIÁLIS SZORZAT

Az $\underline{\text{u}}$ és $\underline{\text{v}}$ vektorok vektoriális szorzata az az $\underline{\text{u}}\times\underline{\text{v}}$-vel jelölt vektor, amelyre az alábbi feltételek fennállnak:

$$\underline{u} \times \underline{v}\; hossza: \; |\underline{u} \times \underline{v}| = |\underline{u}| \cdot |\underline{v}| \cdot \sin\phi$$

$$\underline{u} \times \underline{v}\;\; meröleges\; \underline{u}\; és\; \underline{v} - re$$

Ezek jobbsodrású rendszert alkotnak. Ha valamelyik vektor $\underline{0}$, akkor az eredmény is nulla.

Tétel: VEKTORIÁLIS SZORZAT

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

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

Definíció: VEGYESSZORZAT

Az $\underline{\text{u}}$, $\underline{\text{v}}$, $\underline{\text{w}}$ vektorok vegyesszorzata $(\underline{u} \times \underline{v}) \cdot \underline{w}$.
Jelölés: $\underline{\text{u}}\ \underline{\text{v}}\ \underline{\text{w}}$.

Tétel: VEGYESSZORZAT

A vegyesszorzat kapcsolata a térfogattal - az $\underline{\text{u}}$, $\underline{\text{v}}$ és $\underline{\text{w}}$ által kifeszített *paralelepipedon* térfogata:

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

Bizonyítás:

A térfogatot a paralelogramma T területének és m magasságának a szorzatából kapjuk meg. T terület egyenlő az $|\underline{u} \times \underline{v}|$-vel, m magasságot pedig úgy kapjuk meg, hogy meghatározunk egy OMW háromszöget, melyben O az origó, M a W-ből az $\underline{u}\times\underline{v}$-re állított merőleges talppontja és W pedig $\underline{\text{w}}$ végpontja. Pitagorasz -> $OM = m = |\underline{w}| \cdot \cos\phi$. Tehátösszvissz

2. tétel

Definíció: $\mathbb{R}^n$

$n \geq 1$ esetén az n db. valós számból álló számoszlopok halmazát $\mathbb{R}^n$ jelöli. Ezen értelmezett összeadás "+" és tetszőleges $\lambda \in \mathbb{R}$ "$\cdot$" skalárszorzást az alábbi alapján értelmezzük:

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

Tétel: $\mathbb{R}^n$ **TULAJDONSÁGOK**

Legyen $\underline{u}, \underline{v}, \underline{w} \in \mathbb{R}^n$ és λ, $\mu \in \mathbb{R}$, ekkor igazak az alábbiak:
Összeadás *asszociatív, kommutatív.*
Szorzás *asszociatív, kommutatív* és *disztributív.*

Bizonyítás:
Triviális.

Definíció: $\mathbb{R}^n$ **ALTERE**

Legyen $V \subseteq \mathbb{R}^n \neq \varnothing$ az $\mathbb{R}^n$ tér egy nemüres részhalmaza. V-t az $\mathbb{R}^n$ alterének nevezzük, ha az alábbi két feltétel teljesül:
Bármely $\underline{u}, \underline{v} \in V$ esetén $\underline{u} + \underline{v} \in V$ is igaz, és
Bármely $\underline{u} \in V, \lambda \in \mathbb{R}$ esetén $\lambda \cdot \underline{u} \in V$ is igaz.
Jelölés: V $\leq \mathbb{R}^n$.

Definíció: LINEÁRIS KOMBINÁCIÓ

Legyenek $\underline{v}_1, \ldots, \underline{v}_k \in \mathbb{R}^n$ vektorok és $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ skalárok. Ekkor $\lambda_1\underline{v}_1 + \ldots + \lambda_k\underline{v}_k$ vektort a $\underline{v}_1, \ldots, \underline{v}_k$ vektorok $\lambda_1, \ldots, \lambda_k$ skalárokkal vett lineáris kombinációjának nevezzük.

Definíció: GENERÁLT ALTÉR

Legyenek $\underline{v}_1, \ldots, \underline{v}_k \in \mathbb{R}^n$ vektorok, ezekenek a lineáris kombinációval kifejezhető $\mathbb{R}^n$-beli vektorok halmazát $\underline{v}_1, \ldots, \underline{v}_k$ generált alterének nevezzük.
Jelölés: $\langle \underline{v}_1, \ldots, \underline{v}_k \rangle$

Definíció: GENERÁTORRENDSZER

Legyenek $\underline{v}_1, \ldots, \underline{v}_k \in \mathbb{R}^n$ vektorok, ha W $= \langle \underline{v}_1, \ldots, \underline{v}_k \rangle$, akkor a $\underline{v}_1, \ldots, \underline{v}_k$ vektorhalmazt a W altér generátorrendszerének nevezzük.

Definíció: LINEÁRIS FÜGGETLENSÉG

A $\underline{v}_1, \ldots, \underline{v}_k \in \mathbb{R}^n$ vektorrendszert akkor nevezzük lineárisan függetlennek, ha $\underline{v}_1, \ldots, \underline{v}_k$ vektorok közül semelyik sem fejezhető ki a többi lineáris kombinációjaként. Ha ez nem teljesül – vagyis a $\underline{v}_1, \ldots, \underline{v}_k$ vektorok között legalább egy olyan, ami kifejezhető a többi lineáris kombinációjaként, akkor a $\underline{v}_1, \ldots, \underline{v}_k$ vektorrendszert lineárisan összefüggőnek nevezzük.

Tétel: LINEÁRIS FÜGGETLENSÉG
A $\underline{v}_1, \ldots, \underline{v}_k \in \mathbb{R}^n$ vektorrendszer akkor és csak akkor lineárisan független, ha a $\lambda_1\underline{v}_1 + \ldots + \lambda_k\underline{v}_k = \underline{0}$ egyenlőség kizárólag abban az esetben teljesül, ha $\lambda_1 = \ldots = \lambda_k = 0$ – ezt nevezzük a triviális lineáris kombinációnak.

Bizonyítás:
"akkor":
T.f.h. $\lambda_1\underline{v}_1, \ldots, \lambda_k\underline{v}_k = \underline{0}$ csak a triviális lin. kombináció esetén teljesül, belátjuk, hogy $\underline{v}_1, \ldots, \underline{v}_k$ lin.flen. INDIREKT bizonyítjuk: feltesszük, hogy ez mégsem lin.flen. Ha $\underline{v}_1, \ldots, \underline{v}_k$ nem lin. flen., akkor valamelyikük kifejezhető a többi lineáris kombinációjából: legyen ez pl. $\underline{v}_1$. Ekkor

$$\underline{v}_1 = \alpha_2\underline{v}_2 + \ldots + \alpha_k\underline{v}_k \quad \alpha_1, \ldots, \alpha_k \in \mathbb{R}$$

Átrendezve:

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

Ezzel ellentmondásra jutottunk: Az fentebbi egyenlet nemtriviális lin. kombináció esetén is teljesül ($\lambda_1 = 1$, $\lambda_2 = -\alpha_2, \ldots, \lambda_k = -\alpha_k$), tehát ezt az állítást igazoltuk.

A "csak akkor" állítás: feltesszük, hogy $\underline{v}_1, \ldots, \underline{v}_k$ lin.flen. és megmutatjuk, hogy ekkor $\lambda_1\underline{v}_1, \ldots, \lambda_k\underline{v}_k = \underline{0}$ csak a $\lambda_1 = \ldots = \lambda_k = 0$ esetben teljesül. INDIREKT bizonyítjuk: T.f.h. $\lambda_1\underline{v}_1, \ldots, \lambda_k\underline{v}_k = \underline{0}$ 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:

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

Ezzel ellentmondásra jutottunk, $\underline{v}_1, \ldots, \underline{v}_k$ mégsem lin.flen., mert $\underline{v}_1$ kifejezhető a többiből lin. kombinációval.

Tétel: ÚJONNAN ÉRKEZŐ VEKTOR LEMMÁJA
T.f.h. az $f_1, \ldots, f_k$ rendszer lin.flen., de $f_1, \ldots, f_k, f_{k+1}$ lin.öf. Ekkor $f_{k+1} \in \langle f_1, \ldots, f_k \rangle$, tehát f_{k+1} kifejezhető $f_1, \ldots, f_k$ lin. kombinációjaként.

Bizonyítás:
Mivel $f_1, \ldots, f_k, f_{k+1}$ lin.öf., ezért a lin.flen. tétele alapján létezik nemtriviális lin. kombináció, mely a nullvektort adja végeredményül. Ha a $\lambda_1 f_1 + \ldots + \lambda_k f_k, \lambda_{k+1} = \underline{0}$ egyenletben $\lambda_{k+1} = 0$, az azt jelenti, hogy a maradék egyenlet így néz ki $\lambda_1 f_1 + \ldots + \lambda_k f_k = \underline{0}$ ÉS a $\lambda_1, \ldots, \lambda_k$ skalárok között van egy (vagy több) nemnulla tag. Ez az állítás viszont azt eredményezné, hogy az eredeti $f_1, \ldots, f_k$ rendszer lin.öf., ezzel ellentmondásra jutottunk. Ebből következtetve $\lambda_{k+1} \neq 0$, és az ezzel való osztás után kapott egyenletből az következik, hogy f_{k+1} előállítható az $f_1, \ldots, f_k$ rendszer lineáris kombinációjaként, tehát $f_{k+1} \in \langle f_1, \ldots, f_k \rangle$.

Tétel: F-G EGYENLŐTLENSÉG
Legyen V $\leq \mathbb{R}^n$ altér, $\underline{f}_1, \ldots, \underline{f}_k$ V-beli vektorokból álló lineárisan független rendszer, $\underline{g}_1, \ldots, \underline{g}_m$ pedig genenátorrendszer V-ben, ekkor $k \leq m$.

Bizonyítás:
TELJES INDUKCIÓVAL:
Ha k = 1, akkor V-ben van a nullvektortól különb vektor (mert $\underline{f}_1 \neq 0$), így minden gen.rszr.-e legalább 1 elemű (üres halmaz $\{\underline{0}\}$ alteret generálja csak). Tétel k = 1 esetén igaz. Továbbiakban t.f.h. $k \geq 2$ és a tétel $(k-1)$-re már igaz, cél belátni, hogy k-ra is igaz a tétel.
Mivel $\underline{g}_1, \ldots, \underline{g}_m$ gen.rszr. V-ben, ezért minden V-beli vektor, így f_k is előáll ennek a lin. kombinációjaként: $f_k = \lambda_1\underline{g}_1 + \ldots + \lambda_m\underline{g}_m$. A lambdák között kell legyen nemnulla (mert $f_k \neq 0$). Legyen pl. $\lambda_m \neq 0$ és legyen $W = \langle \underline{g}_1, \ldots, \underline{g}_{m-1} \rangle$. Megmutatjuk, hogy minden $1 \leq j \leq k-1$ esetén az $\underline{f}_j$-hez

található olyan α_j skalár, hogy $\underline{f}_j + \alpha_j \underline{f}_k \in W$. Ugyanis $\underline{f}_j$ felírható $\underline{g}_1, \dots, \underline{g}_m$ lin. kombinációjaként: $\underline{f}_j = \beta_1 \underline{g}_1 + \ldots + \beta_m \underline{g}_m$. Ekkor $\alpha_j = -\frac{\beta_m}{\lambda_m}$ megfelel a célnak. A bizonyítás további része megtalálható a hivatalos, Szeszlér-féle BSz1 jegyzet 23. oldalán, mivel az író megunta ennek a nagyon unalmas bizonyításnak a leírását.

3. tétel

Definíció: BÁZIS

Legyen $V \leq \mathbb{R}^n$ altér. A V-beli vektorokból álló $\underline{b}_1, \ldots, \underline{b}_k$ rendszert bázisnak nevezzük V-ben, ha a rendszer lin.flen. és gen.rszr. V-ben.

Tétel: BÁZIS EGYÉRTELMŰSÉGE

T.f.h. a $V \leq \mathbb{R}^n$ altérben a $\underline{b}_1, \ldots, \underline{b}_k$ rendszer és a $\underline{c}_1, \ldots, \underline{c}_m$ rendszer egyaránt bázisok. Ekkor $k = m$.

Bizonyítás:

Mindkét rendszer bázis, ezért $\underline{b}_1, \ldots, \underline{b}_k$ lin.flen. és $\underline{c}_1, \ldots, \underline{c}_m$ gen.rszr. V-ben. F-G egyenlőtlenséget alkalmazva: $k \leq m$. Ennek a fordítottját is kimondhatjuk: $\underline{b}_1, \ldots, \underline{b}_k$ gen.rszr. V-ben és $\underline{c}_1, \ldots, \underline{c}_m$ lin.flen. Az F-G egyenlőtlenség alapján $m \leq k$. Mivel mindkét állítás egyszerre igaz, ezért $k = m$.

Definíció: DIMENZIÓ

Legyen $V \leq \mathbb{R}^n$ altérben $\underline{b}_1, \ldots, \underline{b}_k$ rendszer bázis. Ekkor azt mondjuk, hogy a V dimenziója k.
Jelölés: dim V = k.

Definíció: STANDARD BÁZIS $\mathbb{R}^n$-BEN

Jelölje minden $1 \leq i \leq n$ esetén $\underline{e}_i$ azt az $\mathbb{R}^n$-beli vektort, amelynek (felülről) az i-edik koordinátája 1, az összes többi koordinátája 0. Ekkor $\underline{e}_1, \ldots, \underline{e}_n$ bázis az $\mathbb{R}^n$-ben és ennek külön nevet is szentelünk - standard bázis.
Jelölés: E_n.

Bizonyítás:

$\underline{e}_1, \ldots, \underline{e}_n$ lineáris kombinációja $\lambda_1, \ldots, \lambda_n$ skalárokkal:

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

Látszik, hogy $\underline{e}_1, \ldots, \underline{e}_n$ gen.rszr. $\mathbb{R}^n$-ben, hiszen lin. kombinációjukként tetszőleges vektor előállhat. Ha a nullvektort akarjuk kifejezni, akkor csak a triviális lineáris kombináció esetén fog az előállni, tehát a rendszer lin.flen., és ezek alapján $\underline{e}_1, \ldots, \underline{e}_n$ tényleg bázist alkot az $\mathbb{R}^n$-ben.

A fenti állításból következik, hogy dim $\mathbb{R}^n$ = n, viszont figyeljünk arra, hogy $\mathbb{R}^n$ csak az egyike az "n-dimenziós tereknek" és minden $(n \leq m)$ $\mathbb{R}^m$-nek van n-dimenziós altere.

Tétel: BÁZIS

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

Bizonyítás:

"csak akkor": akkor bázis, ha gen.rszr V-ben és lin.flen. Előbbi következik tételből, utóbbi pedig 2. tételsor alternatív lin.flen. def.-jéből.
"akkor": Minden $\underline{v} \in \mathbb{R}^n$ kifejezhető $\underline{b}_1, \ldots, \underline{b}_k$ lin. kombinációjaként, INDIREKT t.f.h. valamely $\underline{v} \in$ V kétféleképpen kifejezhető:

$$\underline{v} = \lambda_1 \underline{b}_1 + \ldots + \lambda_k \underline{b}_k = \mu_1 \underline{b}_1 + \ldots + \mu_k \underline{b}_k \quad \textit{és} \quad \lambda_j \neq \mu_j$$

A kettő különbségét véve:

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

Azt kaptuk tehát, hogy a $\underline{0}$ kifejezhető a $\underline{b}_1, \ldots, \underline{b}_k$ nemtriviális lin. kombinációjából, hiszen $(\lambda_j - \mu_j) \neq 0$, ez ellentmondás, tehát ezt az irányt is bizonyítottuk.

Definíció: KOORDINÁTAVEKTOR

Legyen $\mathrm{V} \leq \mathbb{R}^n$, $\mathrm{B} = \{\underline{b}_1, \ldots, \underline{b}_k\}$ bázis V-ben és $\underline{\mathrm{v}} \in \mathrm{V}$ tetszőleges vektor. Azt mondjuk, hogy a $\underline{k} = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_k \end{pmatrix} \in \mathbb{R}^k$ vektor a $\underline{\mathrm{v}}$ vektor B szerinti koordinátavektora, ha $\underline{v} = \lambda_1\underline{b}_1 + \ldots + \lambda_k\underline{b}_k$.

Jelölés: $\underline{k} = [\underline{v}]_B$

Fontos még, hogy $[\underline{v}]_B$ nem csak $\underline{\mathrm{v}}$-től függ: ugyanannak a vektornak más-más bázis esetén más-más koordinátavektorok felelnek meg.

Tétel: BÁZIS LÉTEZÉSE

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

Bizonyítás:

Leqyen $\mathrm{W} = \langle f_1, \ldots, f_k \rangle$. Nyilván igaz, hogy $\mathrm{W} \subseteq \mathrm{V}$, mivel V altér. Ha $\mathrm{V} = \mathrm{W}$, akkor $f_1, \ldots, f_k$ gen.rszr. és így bázis V-ben, tehát a tételt beláttuk. Ha $\mathrm{W} \neq \mathrm{V}$, akkor létezik egy $\underline{\mathrm{v}} \in \mathrm{V}$, $\underline{\mathrm{v}} \notin \mathrm{W}$ vektor. Újonnan érkező vektor lemmája szerint ekkor $f_1, \ldots, f_k, \underline{v}$ lin.flen. Ha ez már gen.rszr. V-ben, akkor a tételt beláttuk, ellenkező esetben ismételjük meg a lépéseket. Be kell még látnunk, hogy ez a folyamat egy idő után leáll, ekkor az F-G egyenlőtlenséget vesszük igénybe, ez alapján n-nél nagyobb elemszámú lin.flen rendszer nem létezhet $\mathbb{R}^n$-ben, és létezik n elemű gen.rszr. is ebben a térben. Tehát az eljárás $n - k$ lépés után biztosan leáll.

Ebből következik, hogy minden $\mathrm{V} \leq \mathbb{R}^n$ altérben van bázis – tehát dim V is létezik.

Bizonyítás:

Ha $\mathrm{V} = \underline{0}$, akkor az üres halmaz bázis V-ben, viszont ha V tartalma egy $\underline{v} \neq \underline{0}$ vektort, akkor $\underline{\mathrm{v}}$-re alkalmazva fenti tételt kapunk egy V-beli bázist.

4. tétel

Lásd Szeszlér-féle BSz1 jegyzet 35.-40. oldalt, annál jobban nem lehet lebutítani. (lel)

5. tétel

Definíció: DETERMINÁNS
Legyen adott egy $(n \times n)$-es A mátrix. Az A minden bástyaelhelyezésére szorozzuk össze az azt alkotó n elemet, majd a szorzatot lássuk el előjellel a következő szabály szerint: ha a bástyaelhelyezésnek megfelelő permutáció inverziószáma páros, akkor az előjel legyen pozitív, ha viszont páratlan az inverziószám, akkor az előjel legyen negatív. Az így kapott n! darab, n tényezős előjelezett szorzat összegét az A determinánsának nevezzük.
Jelölés: |A| vagy detA.

Tétel: DETERMINÁNS ALAPTULAJDONSÁGAI
Legyen A egy $(n \times n)$-es mátrix,
Ha A-nak van csupa 0 elemet tartalmazó sora vagy oszlopa, akkor detA = 0.
Ha A felsőháromszög-mátrix vagy alsóháromszög-mátrix, akkor a determinánsa a főátlóbeli elemek szorzata:

$$detA = a_{1,1} \cdot a_{2,2} \cdot \ldots \cdot a_{n,n}$$

Bizonyítás:
Az első állítás bizonyítása azonnal következik a determináns definíciójából: mivel mind az n! db. szorzat tartalmaz elemet abból a sorból/oszlopból, amelyiknek minden tagja 0, ezért minden szorzat értéke és ezek összege is 0 lesz.
A második állítás bizonyításához vegyük A felsőháromszög-mátrixot. A bástyaelhelyezések akkor nem tartalmaznak 0 elemet, ha az első oszlopból az első elemet, a második oszlopból a második elemet, választjuk ki (a többit nem válaszhatnánk ki) és így tovább... Az így 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 az oszlop és a sor szavak megcserélésével megkapjuk ugyanezt a bizonyítást az alsóháromszög-mátrixra is.

Tétel: DETERMINÁNS ALAPTULAJDONSÁGAI
Legyen A $(n \times n)$-es mátrix, $\lambda \in \mathbb{R}$ skalár, $1 \leq i, j \leq n, i \neq j$ egészek.
Ha A egy sorát/oszlopát megszorozzuk λ-val, akkor a kapott A' mátrix determinánsa λ-szorosa A-ének:

$$detA' = \lambda \cdot detA$$

Ha A két sorát/oszlopát felcseréljük, akkor a kapott A' mátrix determinánsa ellentetje az A-énak:

$$detA' = (-1) \cdot detA$$

Ha A i-edik sorát helyettesítjük sajátmagának és a j-edik sor λ-szorosának összegével, akkor a kapott A' mátrix determinánsa megegyezik A-éval:

$$detA' = detA$$

Ugyanez igaz oszlopokra is.

Bizonyítás:
Lásd 48-50. oldal Szeszlér-jegyzet.

Tétel: DETERMINÁNS KISZÁMOLÁSA - GAUSS ELIMINÁCIÓVAL
Bemenet - $n \times n$ mátrix
.
0. lépés i <- 1, D <- 1
1. lépés:

- Ha $a_{i,j} = 0$, akkor folytassuk **2. lépésnél**.
- Szorozzuk meg i-edik sort $\frac{1}{a_{i,j}}$-vel.
- D <- $D \cdot a_{i,j}$
- 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 <- $i + 1$
- Folytassuk az **1. lépésnél**.

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-edik sorral.
  - D <- $(-1) \cdot D$
  - Folytassuk az **1. lépésnél**.
- PRINT "detA = 0"; STOP.

Tétel: TRANSZPONÁLT DETERMINÁNSA
Minden A négyzetes mátrixra $detA^T = detA$

Bizonyítás:
A bizonyítás megtalálható a Szeszlér-jegyzet 65-66. oldalán.

6. tétel

Tétel: KIFEJTÉSI Tétel
Ha az $(n \times n)$-es A mátrix valamelyik sorának, vagy oszlopának minden elemét megszorozzuk a hozzá tartozó előjeles aldetermináns értékével és a kapott n darab kéttényezős szorzatot összeadjuk, akkor az A determinánsának értékét kapjuk.

Bizonyítás:
A Szeszlér-jegyzet 55-58. oldalán.

Definíció: MÁTRIX
Adott $k, n \geq 1$ egészek esetén $(k \times n)$-es mátrixnak nevezünk egy k sorból és n oszlopból álló táblázatot, melynek minden cellájában egy valós szám áll. A $(k \times n)$-es mátrixok halmazát $\mathbb{R}^{k \times n}$ jelöli. Az A mátrix i-edik sorának és j-edik oszlopának kereszteződésében álló elemet $a_{i,j}$ jelöli. Az $\mathbb{R}^{k \times n}$-en értelmezett, "+"-al jelölt összeadást és tetszőleges $\lambda \in \mathbb{R}$ esetén "·"-tal jelölt skalárral való szorzást tudjuk értelmezni. Nem, nem fogom leírni, hogyan néz ki egy szorzás/összeadás $k \times n$-es mátrixon.

Tétel: MÁTRIXMŰVELETEK
Legyen A,B,C $\in \mathbb{R}^{k \times n}$ és $\lambda, \mu \in \mathbb{R}$. Ekkor igazak az alábbiak:
A mátrixösszeadás asszociatív és kommutatív.
A mátrixszorzás asszociatív és disztributív. (NEM KOMMUTATÍV)!

Definíció: TRANSZPONÁLT
A $(k \times n)$-es A mátrix transzponáltjának nevezzük az $(n \times k)$-as B mátrixot, ha $b_{i,j} = a_{j,i}$ teljesül minden $1 \leq i \leq n$ és $1 \leq j \leq k$ esetén.
Jelölés: $B = A^T$

Definíció: MÁTRIXSZORZÁS
A $(k \times n)$-es A $(n \times m)$-es B mátrixok szorzatának nevezzük és $A \cdot B$-vel jelöljük azt a $(k \times m)$-es C mátrixot, melyre minden $1 \leq i \leq k$ és $1 \leq j \leq m$ esetén

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

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

Tétel: DETERMINÁNSOK SZORZÁSTÉTELE
Bármely A és B $(n \times n)$-es mátrixokra:

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

7. tétel

Tétel:
Legyen (A|$\underline{b}$) egy n változós, n egyenletből álló lin. egyenletrendszer kibővített együtthatómátrixa. Ekkor az egyenletrendszer akkor és csak akkor egyértelműen megoldható, ha detA $\neq 0$

Bizonyítás:
Futtassuk (A|b)-re Gauss-eliminációt. Az algoritmus által megtett sorekvivalens lépések az együtthatómátrix determinánsát megváltoztatják ugyan, de annak nulla/nemnulla mivoltán nem változtatnak. A Gauss-elimináció az alábbi három lehetőség valamelyikével ér véget:

- Az egyenletrendszer nem megoldható: tilos sor.
- Az egyenletrendszernek végtelen sok megoldása van: Kevesebb sor, mint oszlop (és fordítva) – mivel A eredetileg $(n \times n)$-es volt, ezért az első fázis 3. lépésében keletkeznie kellett csupa 0 sornak, ez pedig azt jelenti, hogy detA eredetileg is 0.
- Az egyenletrendszer megoldása egyértelmű: A redukált lépcsős alak determinánsa 1, főátlóban csupa 1-es, mindenhol máshol 0 áll. Mivel det végül nem nulla, ezért eredetileg is detA $\neq 0$.

Tétel:
Legyenek $\underline{a}_1, \ldots, \underline{a}_n, \underline{b} \in \mathbb{R}^k$ vektorok és legyen A az $\underline{a}_i$-k egyesítésével keletkező $(k \times n)$-es mátrix.
Ekkor az alábbi állítások ekvaliensek:
Megoldható az $A \cdot \underline{x} = \underline{b}$ "mátrixegyenlet"
Megoldható az (A|$\underline{b}$) kibővített együtthatómátrixú lineáris egyenletrendszer.
$\underline{b} \in \langle \underline{a}_1, \ldots \underline{a}_n \rangle$

Bizonyítás:
A 2. és a 3. állítás ekvivalens. A 3. állítás teljesülése azt jelenti, hogy létezik a $\lambda_1 \underline{a}_1 + \ldots + \lambda_n \underline{a}_n = \underline{b}$ lineáris kombináció. Itt a $\lambda_1 \underline{a}_1 + \ldots + \lambda_n \underline{a}_n = \underline{b}$ vektor i-edik koordinátája minden $1 \leq i \leq k$ esetén $\lambda_1 \underline{a}_{i,1} + \ldots + \lambda_n \underline{a}_{i,n} = \underline{b}_i$. Következtetésképp azt kapjuk, hogy a felső és alsó egyenlet ekvaliens, és ezzel épp az (A|$\underline{b}$) lineáris egyenletrendszert kapjuk.
1. és 2. ekvivalenciájához azt kell észrevennünk, hogy $\underline{\mathrm{x}}$ csak $\mathbb{R}^n$-beli oszlopvektor lehet (mert egyrészt n sora van, ha $A \cdot \underline{x}$, másrészt 1 oszlopa van, ha $A \cdot \underline{x}$ 1 oszlopú). Az $\underline{\mathrm{x}}$ j-edik koordinátáját minden $1 \leq j \leq n$ esetén x_j-vel jelölve az $A \cdot \underline{x}$ szorzat i-edik koordinátája a mátrixszorzás definíciója szerint $a_{i,1}x_1 + \ldots + a_{i,n}x_n$. Ezért $A \cdot \underline{x} = \underline{b}$ azzal ekvivalens, hogy $a_{i,1}x_1 + \ldots + a_{i,n}x_n = b_i$ teljesül minden $1 \leq i \leq k$ esetén - vagyis ismét az (A|$\underline{b}$) lineáris egyenletrendszert kaptuk.

Ebből következmény: Az $A \cdot \underline{x} = \underline{0}$ lineáris egyenletrendszernek az egyetlen megoldása $\underline{\mathrm{x}} = \underline{0}$. Ez ekvivalens a következővel: Az $\underline{a}_1, \ldots, \underline{a}_n$ vektorok lineárisan függetlenek.

Bizonyítás:
$\underline{a}_1, \ldots, \underline{a}_n$ akkor és csak akkor lin.flen., ha $\lambda_1 \underline{a}_1, \ldots, \lambda_n \underline{a}_n = \underline{0}$ csak a triviális lin. kombináció esetén, vagyis $\lambda_1 = \ldots = \lambda_n = 0$. Ez ekvaliens azzal, hogy az $A \cdot \underline{x} = \underline{0}$ lineáris egyenletnek egyetlen megoldása az, hogy minden változó értéke 0.

Tétel:
Legyen A $(n \times n)$-es mátrix. Ekkor az alábbi állítások ekvivalensek:
A oszlopai, mint $\mathbb{R}^n$-beli vektorok lineárisan függetlenek;
detA $\neq 0$;
A sorai, mint n hosszú sorvektorok lineárisan függetlenek.

Bizonyítás:
1. állítás az előző következmény miatt azzal ekvivalens, hogy az (A|$\underline{0}$) kibővített együtthatómátrixú lin. egyenletrendszer egyértelműen megoldható. Mivel A négyzetes mátrix, ezért 1. tétel szerint ez akkor és csak akkor teljesül, ha detA $\neq 0$. Bizonyítottuk, hogy 1. és 2. állítás ekvivalens.
2. és 3. állítás közötti ekvivalenciához A transzponáltjára alkalmazzuk az 1. és 2. közötti, már bizonyított ekvivalenciát. Ezt megtehetjük, mivel A^T oszlopai megegyeznek A soraival, és fordítva, ezért A sorai akkor és csak akkor lin.flen.-ek, ha det$A^T \neq 0$. Azonban transzponált-determináns tétel miatt detA $=$ detA^T, ezért ez valóban ekvivalens detA $\neq 0$ feltétellel.

8. tétel

Definíció: INVERZ MÁTRIX

Egy $(n \times n)$-es A mátrix inverzének nevezzük az $(n \times n)$-es X mátrixot, ha $A \cdot X = E = X \cdot A$ teljesül. Jelölés: $X = A^{-1}$.

Tétel: INVERZ LÉTEZÉSE

Az $(n \times n)$-es A mátrixnak akkor és csak akkor létezik inverze, ha $detA \neq 0$. Ha A^{-1} létezik, akkor az egyértelmű.

Bizonyítás:

T.f.h. $X = A^{-1}$ létezik: megmutatjuk, hogy $detA \neq 0$. Def. szerint $A \cdot X = E$ egyenlet mindkét oldalának determinánását véve: $det(A \cdot X) = detE$, ahol $detE = 1$, alkalmazzuk szorzástételt: $detA \cdot detX = 1$, ebből adódik, hogy $detA \neq 0$.

Tétel: INVERZ MÁTRIX LÉTEZÉSE Lemma

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

Bizonyítás:

Fenti szorzás ekvivalens, mátrixszorzás szerint a következővel: $A \cdot \underline{x}_1 = \underline{e}_1, \ldots, A \cdot \underline{x}_n = \underline{e}_n$. Az $A \cdot \underline{x}_i = \underline{e}_i$ lin. egyenletrendszer, ami úgy jelölhető, hogy $(A|\underline{e}_i)$. Mivel $detA \neq 0$, 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.

Az inverz kiszámítása: Egymás mellé felírjuk az $(n \times n)$-es A mátrixot valamint az $(n \times n)$-es egységmátrixot. Gauss-eliminációt lefuttatjuk az A-n, úgy, hogy a sorekvivalens lépéseket megismételjük az E-n is. Addig folytatjuk a Gauss-eliminációt, amíg az A redukált lépcsős alakban nem lesz. Ekkor az $E' = A^{-1}$.

Definíció: NÉGYZETES RÉSZMÁTRIX

Legyen A $(k \times n)$-es mátrix és $r \leq k, n$ egész. Válasszuk ki tetszőlegesen A sorai és oszlopai közül r-r darabot. Ekkor a kiválasztott sorok és oszlopok kereszteződéseiben kialakuló $(r \times r)$-es mátrixot A egy négyzetes részmátrixának nevezzük.

Definíció: RANG

Legyen A tetszőleges mátrix. Azt mondjuk, hogy

- A oszloprangja r, ha A oszlopai közül kiválasztható r db. úgy, hogy a kiválasztott oszlopok lin.flen.-ek, de r+1 már nem választható ki így;
- A sorrangja r, ha A sorai közül kiválaszható r db. úgy, hogy a kiválasztott sorok lin.flen.-ek, de r+1 már nem válaszható 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.

Tétel: RANGFOGALMAK EGYENLŐSÉGE

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, és a 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 $s(A) = o(A^T) = d(A^T) = d(A) = o(A)$ egyenlőségeket kapjuk. Tehát azt kell bizonyítanunk csak, hogy $o(A) = d(A)$. Először megmutatjuk, hogy $o(A) \geq d(A)$, majd hogy $o(A) \leq d(A)$. Ezekről a Szeszlér-jegyzet 83-85. oldalán többet olvashat.

Definíció: RANG
Az A mátrix rangjának nevezzük az $o(A)$, $s(A)$, $d(A)$ közös értékét.
Jelölés: r(A).

Tétel: RANG KISZÁMOLÁSA
Legyen A ($k \times n$)-es mátrix és az oszlopai legyenek $\underline{a}_1, \ldots, \underline{a}_n$, ekkor $r(A) = dim\langle \underline{a}_1, \ldots, \underline{a}_n \rangle$

Bizonyítás:
Válasszuk ki A oszlopai közül a legtöbbet őgy, hogy ezek lin.flen.-ek legyenek. Oszloprang def. szerint ekkor $r = r(A)$. Állítjuk, hogy $\underline{a}_1, \ldots, \underline{a}_n$ bázist alkot a W = $dim\langle \underline{a}_1, \ldots, \underline{a}_n \rangle$ altérben. Be kell látnunk tehát, hogy $\underline{a}_1, \ldots, \underline{a}_n$ gen.rszr. W-ben. Legyen U = $\langle \underline{a}_1, \ldots, \underline{a}_r \rangle$, célunk belátni, hogy U = W. $r < i \leq n$ esetén $\underline{a}_1, \ldots, \underline{a}_r, \underline{a}_i$ lin.öf, mivel A-ból r+1 lin.flen. oszlopot nem lehet kiválasztani. Az újonnan érkező vektor lemmája szerint ekkor $\underline{a}_i \in \langle \underline{a}_1, \ldots, \underline{a}_r \rangle = U$, tehát $\underline{a}_1, \ldots, \underline{a}_n$ mind U-beli, és mivel U altér, ezért minden W-beli, tehát $\underline{a}_1, \ldots, \underline{a}_n$ vektorokból lin. kombinációval kifejezhető vektor is U-beli kell, hogy legyen. Ezzel $W \subseteq U$ bizonyítottuk, és a tételt is.

Tétel: RANG KISZÁMOLÁSA
Az elemi sorekvivalens lépések a mátrix rangját nem változtatják meg. A lépcsős alakú mátrix sorainak a száma egyenló a mátrix rangjával.

Bizonyítás:
majd

9. tétel

Definíció: LINEÁRIS LEKÉPEZÉS

Az f: $\mathbb{R}^n \to \mathbb{R}^k$ függvényt lineáris leképezésnek hívjuk, ha létezik egy olyan $(k \times n)$-es mátrix, melyre $f(\underline{x}) = A \cdot \underline{x}$ teljesül minden $\underline{x} \in \mathbb{R}^n$ esetén. Az n = k esetben f-et lineáris transzformációnak is nevezzük. Ha f :$\mathbb{R}^n \to \mathbb{R}^k$ lineáris leképezés és $f(\underline{x}) = A \cdot \underline{x}$ minden $\underline{x} \in \mathbb{R}^n$-re, akkor azt mondjuk, hogy a mátrixa A.
Jelölés: $A = [f]$.

Tétel: LINEÁRIS LEKÉPEZÉS FELTÉTELE

Az f: $\mathbb{R}^n \to \mathbb{R}^k$ függvény akkor és csak akkor lineáris leképezés, ha:

- $f(\underline{x} + \underline{y}) = f(\underline{x}) + f(\underline{y})$ igaz minden $\underline{x}, \underline{y} \in \mathbb{R}^n$ esetén;
- $f(\lambda \cdot \underline{x}) = \lambda \cdot f(\underline{x})$ igaz minden $\underline{x} \in \mathbb{R}^n$ és $\lambda \in \mathbb{R}$ esetén.

Ha pedig f teljesíti ezt a két tulajdonságot, akkor az $[f]$ egyértelmű és azonos azzal a $(k \times n)$-es mátrixszal, melynek minden $1 \leq i \leq n$ esetén az i-edik oszlopa $f(\underline{e_i})$.

Bizonyítás:

92. oldal Szeszlér-jegyzet.

Tétel: LINEÁRIS LEKÉPEZÉSEK SZORZATA

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

Bizonyítás:

94. oldal Szeszlér-jegyzet.

Tétel: ADDÍCIÓS TÉTELEK

Tetszőleges α és β szögekre teljesülnek az alábbi összefüggések:

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

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

Bizonyítás:

95. oldal Szeszlér-jegyzet.

10. tétel

Tétel: LINEÁRIS TRANSZFORMÁCIÓ INVERTÁLHATÓSÁGA
Egy f: $\mathbb{R}^n \to \mathbb{R}^n$ lineáris transzformáció akkor és csak akkor invertálható, ha $det[f] \neq 0$. Ha pedig ez a feltétel fennáll, akkor $[f^{-1}] = [f]^{-1}$ - vagyis az f^{-1} inverz transzformáció mátrixa az f mátrixának az inverze.

Bizonyítás:
100. oldal Szeszlér-jegyzet.

Definíció: MAGTÉR, KÉPTÉR
Legyen f: $\mathbb{R}^n \to \mathbb{R}^k$ lineáris leképezés. f magterének nevezzük és Ker$f$-fel jelöljük azon $\mathbb{R}^n$-beli vektorok halmazát, melyeknek a képe az $\mathbb{R}^k$-beli nullvektor:

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

f képterének nevezzük és Imf-fel jelöljük azon $\mathbb{R}^k$-beli vektorok halmazát, melyek megkaphatók (legalább) egy alkalmas $\mathbb{R}^n$-beli vektor f-fel vett képeként.

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

Tétel: MAGTÉR, KÉPTÉR ALTÉR VOLTA
Legyen f: $\mathbb{R}^n \to \mathbb{R}^k$ lineáris leképezés. Ekkor:

- Ker$f \leq \mathbb{R}^n$, vagyis Ker$f$ altér $\mathbb{R}^n$-ben;
- Im$f \leq \mathbb{R}^k$, vagyis Imf altér $\mathbb{R}^k$-ban.

Bizonyítás:
96. oldal Szeszlér-jegyzet.

Tétel: DIMENZIÓTÉTEL
Ha f: $\mathbb{R}^n \to \mathbb{R}^k$ lineáris leképezés, akkor dim Ker$f$ + dim Imf = n.

Bizonyítás:
97. oldal Szeszlér-jegyzet.

11. tétel

Tétel: BÁZISTRANSZFORMÁCIÓ
Legyen f: $\mathbb{R}^n \to \mathbb{R}^n$ lineáris transzformáció és B egy $(n \times n)$-es mátrix, melynek az oszlopai bázist alkotnak $\mathbb{R}^n$-ben. Jelölje g: $\mathbb{R}^n \to \mathbb{R}^n$ azt a függvényt, mely minden $\underline{x} \in \mathbb{R}^n$ esetén $[\underline{x}]_B$-hez $[f(\underline{x})]_B$-t rendeli. Ekkor g is lineáris transzformáció, melynek a mátrixa $[g] = B^{-1} \cdot [f] \cdot B$.

Bizonyítás:
102. oldal Szeszlér-jegyzet.

Tétel: BÁZISTRANSZFORMÁCIÓ
Legyen h: $\mathbb{R}^n \to \mathbb{R}^n$ az a függvény, mely minden $\underline{x} \in \mathbb{R}^n$ esetén $[\underline{x}]_B$-hez $\underline{x}$-et rendeli. Ekkor h lineáris transzformáció, amelynek mátrixa $[h] = B$.

Bizonyítás:
102. oldal Szeszlér-jegyzet.

Definíció: LINEÁRIS TRANSZF. ADOTT BÁZIS SZERINT
Legyen f: $\mathbb{R}^n \to \mathbb{R}^n$ lineáris transzformáció és B bázis $\mathbb{R}^n$-ben. Ekkor a g: $[\underline{x}]_B \mapsto [f(\underline{x})]_B$ lineáris transzformáció mátrixát az f transzformáció B bázis szerinti mátrixának nevezzük.
Jelölés: $[f]_B$

Tétel: BÁZISTRANSZFORMÁCIÓ KISZÁMÍTÁSA
Az $[f]_B$ mátrix i-edik oszlopa egyenlő az $[f(\underline{b}_i)]_B$ koordinátavektorral minden $1 \leq i \leq n$ esetén, ahol f: $\mathbb{R}^n \to \mathbb{R}^n$ tetszőleges lineáris transzformáció és $B = \{\underline{b}_1, \ldots, \underline{b}_n\}$ bázis $\mathbb{R}^n$-ben.

Bizonyítás:
104. oldal Szeszlér-jegyzet.

12. tétel

Definíció: DIAGONÁLIS MÁTRIX

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

Tétel: KAPCSOLAT SAJÁTÉRTÉK ÉS LINEÁRIS LEKÉPEZÉSEK KÖZT

Legyen $B = \{\underline{b}_1, \ldots, \underline{b}_n\}$ tetszőleges bázis és t.f.h. az $[f]_B$ mátrix diagonális, a főátlóban álló elemeket jelölje sorban $\lambda_1, \ldots, \lambda_n$. Ekkor az $[f]_B$ 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 $f(b_i) = 0 \cdot \underline{b}_1 + \ldots + \lambda_i \cdot \underline{b}_i + \ldots + 0 \cdot \underline{b}_n$, vagyis $f(b_i) = \lambda_i \cdot \underline{b}_i$.
ÖSSZEFOGLALVA: $[f]_B$ akkor lesz diagonális, ha B minden tagjára $f(b_i) = \lambda_i \cdot \underline{b}_i$ teljesül valamilyen λ skalárral.

Definíció: SAJÁTÉRTÉK, SAJÁTVEKTOR

Legyen A egy $(n \times n)$-es mátrix.

- A sajátértékének nevezzük a $\lambda \in \mathbb{R}$ skalárt, ha létezik olyan $\underline{x} \in \mathbb{R}^n$, $\underline{x} \neq \underline{0}$ vektor, melyre $A \cdot \underline{x} = \lambda \cdot \underline{x}$
- A sajátvektorának nevezzük az $\underline{x} \in \mathbb{R}^n$ vektort, ha $\underline{x} \neq \underline{0}$ és létezik olyan $\lambda \in \mathbb{R}$ skalár, melyre $A \cdot \underline{x} = \lambda \cdot \underline{x}$

Rövidítve: Ha $A \cdot \underline{x} = \lambda \cdot \underline{x}$ teljesül és $\underline{x} \neq \underline{0}$, akkor λ a sajátértéke és $\underline{x}$ a sajátvektora az A-nak.

Tétel: SAJÁTÉRTÉK MEGHATÁROZÁSA

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

Bizonyítás:

106. oldal Szeszlér-jegyzet.

Definíció: KARAKTERISZTIKUS POLINOM

Az $(n \times n)$-es A mátrix karakterisztikus polinomjának nevezzük a $det(A - \lambda \cdot E)$ determináns értékét, ahol λ változó.
Jelölés: $k_A(\lambda)$.

A sajátérték definíciója átfogalmazva az előző tétel és definíció felhasználásával: A mátrix sajátértékei a $k_A(\lambda)$ karakterisztikus polinom gyökei, tehát a $k_A(\lambda) = 0$ egyenlet megoldásai. Az algebra egyik tétele szerint tehát n-edfokú polinomnak legfeljebb n gyöke lehet, amiből következik, hogy $(n \times n)$-es mátrixnak legfeljebb n sajátértéke van.

13. tétel

Definíció: OSZTHATÓSÁG
Azt mondjuk, hogy az $a \in \mathbb{Z}$ egész osztója $b \in \mathbb{Z}$ egésznek, ha létezik olyan $c \in \mathbb{Z}$, melyre $a \cdot c = b$. Ugyanezt fejezzük ki, ha b-t az a többszörösének mondjuk.
Jelölés: $a|b$, ha pedig a nem osztója b-nek, $a \nmid b$.
Az a valódi osztója b-nek, ha a|b fennál és $1 < |a| < |b|$.

Definíció: PRÍMSZÁM
A $p \in \mathbb{Z}$ egészt prímszámnak nevezzük, ha $|p| > 1$ és p-nek nincsen valódi osztója. 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 számnak nevezzük.

Tétel: SZÁMELMÉLET ALAPTÉTELE
Minden 1-től, 0-tól és (-1)-től különböző egész szám felbontható prímek szorzatára és ez a felbontás a tényezők sorrendjétől és előjelétől eltekintve egyértelmű.

Bizonyítás:
114. oldal Szeszlér-jegyzet.

Tétel: PRÍMEK SZÁMOSSÁGA
A prímek száma végtelen.

Bizonyítás:
117. oldal Szeszlér-jegyzet.

Tétel: SZOMSZÉDOS PRÍMEK KÖZTI HÉZAGOK
Minden $N > 1$ egészhez találhatóak olyan $p < q$ prímek, hogy p és q között nincs további prím és $q - p > N$.

Bizonyítás:
117-118. oldal Szeszlér-jegyzet.

Tétel: NAGY PRÍMSZÁMTÉTEL
$\pi(n) \approx \frac{n}{\ln n}$ vagyis $\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$

Definíció: KONGRUENCIA
legyenek $a, b, m \in \mathbb{Z}$ tetszőleges egészek. Azt mondjuk, hogy a konguens b-vel modulo m, ha a-t és b-t m-mel maradékosan osztva azonos maradékokat kapunk. Az m számot a kongruencia modulusának nevezzük.
Jelölés: $a \equiv b \pmod{m}$

Tétel:
Tetszőleges $a, b, m \in \mathbb{Z}$ egészekre $a \equiv b \pmod{m}$ akkor és csak akkor igaz, ha $m|a - b$.

Bizonyítás:
119. oldal Szeszlér-jegyzet.

Tétel: ALAPMŰVELETEK KONGRUENCIÁKKAL

T.f.h. $a \equiv b$ (mod m) és $c \equiv d$ (mod m) fennállnak a,b,c,d,m egészekre és $k \geq 1$ tetszőleges. Ekkor igazak az alábbiak:

- $a + c \equiv b + d$ (mod m)
- $a - c \equiv b - d$ (mod m)
- $a \cdot c \equiv b \cdot d$ (mod m)
- $a^k \equiv b^k$ (mod m)

Bizonyítás:
120. oldal Szeszlér-jegyzet.

Tétel: KONGRUENCIA

Legyenek a,b,c,m tetszőlegesek és $d = (c, m)$ (lnko). Ekkor $a \cdot c \equiv b \cdot c$ (mod m) akkor és csak akkor igaz, ha $a \equiv b$ (mod $\frac{m}{d}$).

Bizonyítás:
120-121. oldal Szeszlér-jegyzet.

14. tétel

Tétel: LINEÁRIS KONGRUENCIÁK MEGOLDHATÓSÁGA
Az $a \cdot x \equiv b \pmod{m}$ lineáris kongruencia akkor és csak akkor megoldható, ha $(a, m)|b$. Ha pedig ez a feltétel teljesül, akkor $a \cdot x \equiv b \pmod{m}$ megoldásainak a száma modulo m (a,m)-val egyenlő.

Bizonyítás:
124. oldal Szeszlér-jegyzet.

Tétel: EUKLIDESZI ALGORITMUS
Bemenet: a és m (0 < a < m) | Kimenet: (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: az a-t eloszjuk a kapott maradékkal:

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

$\vdots$

i. lépés: az (i-2). lépésben kapott maradékot elosztjuk az (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 a legnagyobb közös osztó.

Tétel: EUKLIDESZI ALGORITMUS
Az Euklideszi algoritmus végrehajtása után $r_k = (a, m)$.

Bizonyítás:
142. oldal Szeszlér-jegyzet.

Tétel: EUKLIDESZI ALGORITMUS LÉPÉSSZÁMA
Az Euklideszi algoritmus polinomiális időben lefut és legfeljebb $2 \cdot [\log_2 a]$ maradékos osztás után megáll.

Bizonyítás:
142. oldal Szeszlér-jegyzet.

A tételhez hozzá tartozik az Euklidesz algoritmus alkalmazása lineáris kongruenciák megoldásához, konkrét példán.

15. tétel

Definíció: EULER-FÉLE φ-FÜGGVÉNY
Ha $n \geq 2$ egész, akkor az $1, \ldots, n-1$ számok között n-hez relatív prímek számát $\varphi(n)$-el jelöljük. Az $n \mapsto \varphi(n)$ függvényt Euler-féle φ függvénynek nevezzük.

Tétel: EULER-FÉLE φ-FÜGGVÉNYRE KÉPLET
Legyen az $n > 1$ egész kanonikus alakja $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ Ekkor

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

Bizonyítás:
130-131. oldal Szeszlér-jegyzet.

Definíció: REDUKÁLT MARADÉKRENDSZER
Az $R = \{c_1, \ldots, c_k\}$ számhalmaz redukált maradékrendszer modulo m, ha a következő feltételeknek eleget tesz:

- $(c_i, m) = 1$ minden i = 1, …, k esetén;
- $c_i \not\equiv c_j$ (mod m) bármely $i \neq j, 1 \leq i, j \leq k$ esetén;
- $k = \varphi(m)$.

Tétel: REDUKÁLT MARADÉKRENDSZER
Legyen $R = \{c_1, \ldots, c_k\}$ redukált maradékrendszer modulo m és legyen tetszőleges egész, melyre (a,m) = 1. Ekkor az $R' = \{a \cdot c_1, \ldots, a \cdot c_k\}$ halmaz szintén redukált maradékrendszer modulo m.

Bizonyítás:
132. oldal Szeszlér-jegyzet.

Tétel: EULER-FERMAT
Ha az a és m $\geq$ 2 egészekre (a,m) = 1, akkor $a^{\varphi(m)} \equiv 1$ (mod m).

Bizonyítás:
132-133. oldal Szeszlér-jegyzet.

Tétel: "KIS" FERMAT-Tétel
Ha p prím és a tetszőleges egész, akkor $a^p \equiv a$ (mod p).

Bizonyítás:
133. oldal Szeszlér-jegyzet.

A tételhez hozzátartozik diofantikus illetve két kongruenciából álló kongruenciarendszerek megoldása is, konkrét példán.

16. tétel

Definíció: POLINOMIÁLIS FUTÁSIDEJŰ ALGORITMUS
Definíció: (vázlatos) A algoritmust polinomiális futásidejűnek tekintjük, ha n méretű bemenethez tartozó f(n) függvényre, mely az algoritmus lépésszámát határozza meg, a következő MINDEN n esetén fennáll:

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

ahol c és k rögzített konstansok.

A Szeszlér-jegyzet 137-141. oldalán található egy hosszas mese a számelméleti algoritmusokról, ezek közül az ALAPMŰVELETEK és a HATVÁNYOZÁS, valamint HATVÁNYOZÁS MODULO M a fontosak.

Tétel: PRÍMTESZTELÉS Fermat-teszt

Bemenet m egész

0. lépés k ← 1

1. lépés Generáljunk véletlen számot 1 és m-1 közt.

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} (mod m) értékét ISMÉTELT NÉGYZETRE EMELÉSEK MÓDSZERÉVEL. Ha nem 1, m NEM prím, STOP.

4. lépés Ha k = 100, m VALÓSZÍNŰLEG prím.

5. lépés k ← k+1, vissza **1. lépés**hez

Tétel: FERMAT-TESZT ÁRULÓK SZÁMA
Ha m > 1 összetett szám és m-nek van árulója, akkor az 1 és m közötti, m-hez relatív prím számoknak legalább a fele áruló.

Bizonyítás:
147. oldal Szeszlér-jegyzet.

Definíció:
Az m > 1 összetett számot univerzális álprímnek, vagy más néven Carmichael-számnak nevezzük, ha nincsen árulója, vagyis, ha minden 1 < a < m, (a,m) = 1 esetén $a^{m-1} \equiv 1$ (mod m).

Nyilvános kulcsú titkosítás és az RSA-algoritmus:
152-154. oldal Szeszlér-jegyzet.

17. tétel

Definíció: NEM KELL - SEGÉDDEFINÍCIÓK
Legyenek A és B tetszőleges halmazok és f : A → B egy függvény. Az f függvényt

- injektívnek nevezzük, ha bármely $x_1, x_2 \in A, x_1 \neq x_2$ esetén $f(x_1) \neq f(x_2)$.
- szürjektívnek nevezzük, ha bármely $y \in B$ esetén létezik olyan $x \in A$, melyre $f(x) = y$.
- bijektívnek nevezzük, ha injektív és szürjektív.

Definíció: HALMAZOK SZÁMOSSÁGÁNAK EGYENLŐSÉGE
Azt mondjuk, hogy a (tetszőleges) A és B halmazok számossága egyenlő, ha létezik egy f : A → B bijekció.
Jelölés: |A| = |B|

Definíció: $\mathbb{N}$ SZÁMOSSÁGA
Az A halmazt megszámlálhatóan végtelennek nevezzük, ha a számossága egyenlő a természetes számok halmazáéval (tehát $|A| = |\mathbb{N}|$).
Jelölés: $|A| = \aleph_0$

Tétel: $\mathbb{Q}$, $\mathbb{Z}$ SZÁMOSSÁGA
Az egész számok $\mathbb{Z}$ halmaza és a racionális számok $\mathbb{Q}$ halmaza egyaránt megszámlálhatóan végtelen.

Bizonyítás:
161. oldal Szeszlér-jegyzet

Tétel: CANTOR
A valós számok $\mathbb{R}$ halmaza nem megszámlálhatóan végtelen, vagyis

$$|\mathbb{N}| \neq |\mathbb{R}|$$

Bizonyítás:
162-164. oldal Szeszlér-jegyzet.

Definíció: $\mathbb{R}$ SZÁMOSSÁGA
Az A halmazt kontinuum számosságúnak nevezzük, ha a számossága egyenlő a valós számok halmazáéval (vagyis $|A| = |\mathbb{R}|$).
Jelölés: |A| = c.

A (0,1) nyílt intervallum is kontinuum számosságú. Ld. 163. oldal Szeszlér-jegyzet.

Definíció:
Legyenek A és B (tetszőleges) halmazok.

- Azt mondjuk, hogy A számossága kisebb vagy egyenlő B számoságánál, ha létezik $f : A \to B$ injektív függvény.
  Jelölés: $|A| \leq |B|$

- Azt mondjuk, hogy A számossága kisebb B számosságánál, ha $|A| \leq |B|$, de $|A| \neq |B|$.
  Jelölés: $|A| < |B|$

Tétel: CANTOR-BERNSTEIN
Az A és B halmazokra |A| = |B| akkor és csak akkor igaz, ha $|A| \leq |B|$ és $|B| \leq |A|$

Tétel: $\mathbb{Q}$ SZÁMOSSÁGA
$|\mathbb{Q}| = |\mathbb{N}|$

Bizonyítás:
167. oldal Szeszlér-jegyzet.

Definíció: HATVÁNYHALMAZ
Tetszőleges A halmaz hatványhalmazának nevezzük az A összes részhalmaza által alkotott halmazt.
Jelölés: P(A)

Tétel: (ismét?) CANTOR-Tétel
Minden A halmazra |A| < |P(A)|.

Bizonyítás:
169. oldal Szeszlér-jegyzet.

Tétel: $\mathbb{N}$ HATVÁNYHALMAZÁNAK SZÁMOSSÁGA
$|P(\mathbb{N})| = |\mathbb{R}|$

Bizonyítás:
170-171. oldal Szeszlér-jegyzet.