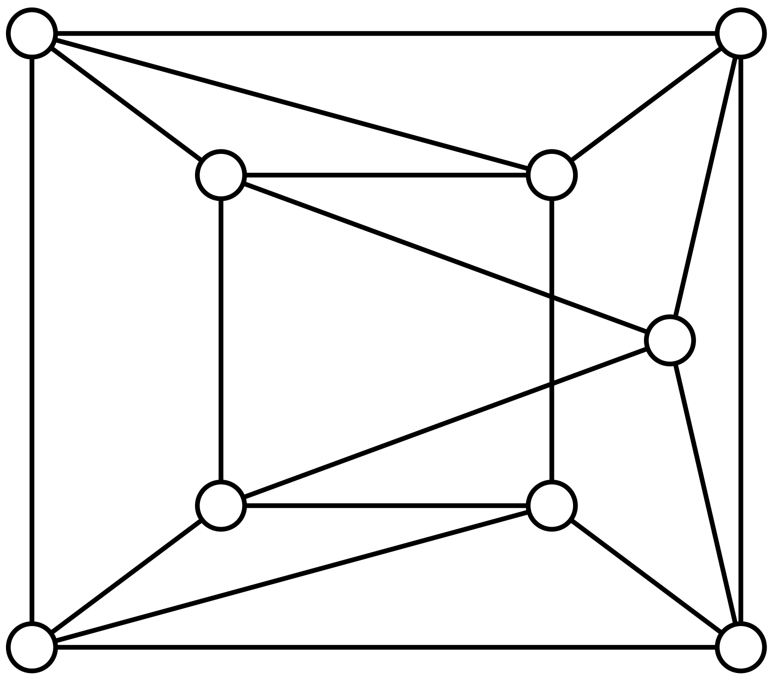
Bevezetés a számításelméletbe I.
A BME I. éves informatikus-hallgatói számára

segédlet a 2005. őszi előadáshoz

Összeállította: Fleiner Tamás



Tartalomjegyzék

Bevezetés

Ez a jegyzet a BME-n, a 2005/2006-os tanév első félévében az informatikus-hallgatók számára előadott „Bevezetés a számításelméletbe” c. előadáshoz kapcsolódik, és elsősorban az említett tárgyból történő vizsgára való felkészülés segédanyaga. Nem pótolja azonban a rendelkezésre álló, könyvformátumú jegyzeteket, amellyekkel számos tekintetben egyezik. Előnye talán mégis annyi, hogy szorosabban kapcsolódik az órán leadott anyaghoz, és így koncentráltabban tartalmazza a vizsgán számonkért tudást. Jelen jegyzet valamennyire túl is mutat azonban az előadáson elhangzottakon, így olyan részeket is tartalmaz, amik nem hangzottak el az előadáson, illetve amiket nem kérünk számon a vizsgán. Ha tehát valaki egészen véletlenül komolyabban érdeklődik egy-egy témakör iránt (bár, őszintén szólva, szkeptikus vagyok ezzel kapcsolatban), azok számára odabiggyesztettem néhány, általam érdekesnek ítélt megjegyzést. Ezek lábjegyzetben[1] ill. apró betűs szedéssel olvashatóak. Ne felejtsük el azonban, hogy ezek csupán a tananyagot kiegészítő megjegyzések: ahhoz, hogy egy adott anyagrészben valaki ténylegesen elmélyülhessen, a megfelelő szakirodalmat (is) célszerű tanulmányoznia.

A bizonyítások végét olyan kiskocka jelzi, mint amilyen pl. ebben a sorban is áll. □

Hogyan is jött létre a jegyzet? Egy előadássorozat tervezésekor az előadónak célszerű saját használatára vázlatot készítenie az elhangzó anyagról, hogy az minél egységesebb és szervesebben felépülő lehessen. Hála a korszerű technológiák elharapózásának, immár ott tartunk, hogy nem lényegesen bonyolultabb egy ilyesfajta anyagot digitálisan szerkeszteni ill. tárolni, mint a hagyományos papíralapon[2]. A jegyzet elsősorban tehát az előadó saját segédanyagaként került összeállításra. Ennek egy következménye, hogy a stílus meglehetősen tömör. Nem kell meglepődni, ha egy-egy mondat teljes megértéséhez akár több dolgot is át kell gondolni. Szerencsére nem bukkannak fel lépten-nyomon ilyen mondatok.

Minden erőfeszítés ellenére valószínűleg számos hiba maradt az alábbi jegyzetben. Lehetne persze több is. Szerencsére voltak, akik segítettek. Úgyogy köszönetet mondok Simonyi Gábornak főleg a síkgráfokkal kapcsolatos részekhez adott tanácsokért, Jüttner Alpárnak a szövegszerkesztéshez nyújtott segítségért, és számos villamosmérnök-hallgatónak, akik a jegyzet korábbi verziójában található problémákra hívták fel a figyelmem. Természetesen minden megmaradt hibáért a felelősség egyedül a szerzőé. Az ezekkel kapcsolatos megjegyzéseket és a konstruktív hozzászólásokat köszönettel fogadom a `fleiner@cs.bme.hu` címen.

Jelen jegyzet jelentős része szellemi termék, és nemcsak a szerzőé. Kizárólagos terjesztője a BME Számítástudományi és Információelméleti Tanszéke, forgalombahozatala önköltségi áron történik. A szerzői jogok tekintetében a szerző elképzelései az alábbiak. A jegyzet szabadon felhasználható, másolható, terjeszthető, de kizárólag a szerző ill. a forrás pontos megjelölésével és ingyenesen. Ugyanez a megkötés öröklődjék minden olyan szerzői jog hatálya alá eső dologra, ami a fenti típusú felhasználásból származik. Az emítettől eltérő célú felhasználáshoz jelen munka szerzőjének engedélye szükséges.

Minden olvasónak sikeres felkészülést és eredményes vizsgázást kívánok.

Fleiner Tamás

[1] Mint pl. ez is, itt.

[2] illetve dehogyisnem... Valaha egy vázlatos anyag volt a jegyzet őse: akkor ez még (többé-kevésbé) igaz volt rá. Később elkezdett bővülni, és egyre inkább jegyzetformája lett. Na ez már egy pinduri kis szöszmötöléssel járt.

1. Komplex számok

Motiváció. Ebben a fejezetben a számfogalom egy kiterjesztéséről lesz szó. Korábbi tanulmányaink során találkoztunk a természetes számokkal ($\mathbb{N} = \{0, 1, 2, \ldots\}$), az egészekkel ($\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$), a racionális számokkal ($\mathbb{Q} = \{\frac{p}{q} : p \in \mathbb{Z}, 0 < q \in \mathbb{N}\}$) illetve a valós számok $\mathbb{R}$ halmazával. Érdemes arra is visszemlékezni, mi motiválta az egyes számhalmazok bevezetését ill. kibővítését. Ha valamit meg akarok számolni, akkor a természetes számokkal dolgozom. Hasznos, ha műveleteket vezetünk be, melyek megkönnyítik annak kiszámolását, hogy mennyi csirkém lesz, ha van most 18 és veszek még (vagy eladok) 5-öt. De megtudhatom azt is, hogy egy 100m×100m-es vagy egy 90m×110m-es földdarab ér-e többet. A negatív egészek bevezetésével egyrészt a tartozás tényét lehet jól leírni, másrészt elérhető, hogy a kivonás művelete gond nélkül elvégezhető legyen. A racionális számok bevezetésével az osztás lesz lényegében elvégezhető (persze a 0 nevezőt kizárjuk), azonban a gyakorlatban is szükség van a törtekre: ha 3 testvér 100 pénzt örököl egyforma arányban, csak úgy tudnak igazságosan megosztozni, ha nem egész szám írja le az örökséget. A valós számok bevezetését indokolja az, hogy elméletileg pontosan akarjuk megmérni mondjuk a négyzet átlóját, a kör területét, vagy más, hasonló mennyiséget.

Az eddigi számfogalmakban közös tehát, hogy mindegyik alkalmas arra, hogy *megmérjen* valamit, azaz a számokon van egy *természetes rendezés*, melynek segítségével bármely két, különböző számról egyértelműen el lehet dönteni, melyik a nagyobb. A számfogalmak bevezetésére alkalmas motiváció, hogy mérhető dolgokat tudjak megmérni. A számokon értelmezett műveletek (összeadás, kivonás, szorzás, osztás, hatványozás, gyökvonás, logaritmus, szögfüggvények, stb) mindegyikéről elmondható, hogy arra valóak, hogy kiszámítsuk egy-egy mennyiség *nagyságát* bizonyos más mennyiségek ismeretében.

A komplex számok bevezetésekor szakítunk az eddigi gyakorlattal. Továbbra is arról van szó, hogy a megismert legbővebb számkört tovább bővítjük, azonban egyszer, s mindenkorra le kell számolnunk azzal az intuícióval, hogy a szám valamely dolog *nagyságát* jelenti: a komplex számokon nem lesz olyasfajta rendezés, mint ami az eddigi nagyságviszony volt.[3] A motiváció itt sokkal inkább az, hogy bizonyos műveletek nem voltak elvégezhetőek a valós számokon, és valamilyen rejtélyes okból szeretnénk pl. a $\sqrt{-1}$-nek értelmet tulajdonítani.

Lássuk mindezt a gyakorlatban. A komplex számok halmaza

$$\mathbb{C} := \{a + bi : a, b \in \mathbb{R}\} ,$$

tehát minden komlex szám egy formális $a + bi$ alakú összegként írható fel, ahol a és b tetszőleges valós számok, az i-t (melynek neve *képzetes egység*) pedig valamiféle „ismeretlenként” tekintjük. Ezt a $z = a+bi$ felírást nevezzük a z komplex szám *kanonikus alakjának*, a z szám *valós része* $Re(z) := a$, *képzetes része* $Im(z) := b$, és a definíció alapján kimondhatjuk, hogy két komplex szám (mondjuk z és z') pontosan akkor egyenlő, ha kanonikus alakjuk $z = a + bi$ és $z' = a' + b'i$ megegyezik, azaz, ha $a = a'$ és $b = b'$.

Ahogy említettük, a valós számok halmaza részhalmaza a komplexekének; konkrétan, ha $a \in \mathbb{R}$, akkor a kanonikus alakja $a = a + 0i$.

Meg kell persze mondani, hogyan végzünk műveleteket a komplex számokkal. Ezeket a műveleteket ráadásul úgy kell definiálnunk, hogy azok a valós számokon végzett műveletek kiterjesztései legyenek. Az alapműveletek esetén úgy járunk el, mintha az i ismeretlen volna, ill. használjuk az $i^2 = -1$ azonosságot:

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \qquad (a + bi) - (c + di) = (a - c) + (b - d)i$$

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

Az osztás azonban nem ilyen egyszerű. Ehhez érdemes definiálni a $z = a + bi$ komplex szám $\overline{z}$-vel jelölt *konjugáltját*, melynek kanonikus alakja $\overline{z} := a - bi$.

Lemma: Tetszőleges $z, w \in \mathbb{C}$ komplex számokra

(1) $\overline{\overline{z}} = z$, ill. (2) $\overline{z + w} = \overline{z} + \overline{w}$, $\overline{z - w} = \overline{z} - \overline{w}$, $\overline{zw} = \overline{z} \cdot \overline{w}$ teljesülnek.

(3) Ha $0 \neq z \in \mathbb{C}$, akkor $0 < z \cdot \overline{z} \in \mathbb{R}$, azaz bármely, nullától különböző komplex számot megszorozva a konjugáltjával, pozitív számot kapunk.

Biz: (1): Triviális. (2): A kanonikus alakokat behelyettesítve könnyen ellenőrizhető.

(3) Legyen $z = a + bi$, ekkor $z \cdot \overline{z} = (a + bi)(a - bi) = a^2 + b^2 + (ab - ab)i = a^2 + b^2 > 0$, hiszen $a^2 \geq 0 \leq b^2$, és $a^2 = b^2 = 0$ esetén $z = 0$ lenne. □

Ezek után osztás is könnyen elvégezhető a konjugálttal való bővítés segítségével. Tegyük fel tehát, hogy $z = a + bi$ és $0 \neq z' = a' + b'i$. Ekkor

$$\frac{z}{z'} = \frac{a + bi}{a' + b'i} = \frac{(a + bi)(a' - b'i)}{(a' + b'i)(a' - b'i)} = \frac{(aa' + bb') + (a'b - ab')i}{a'^2 + b'^2} = \frac{aa' + bb'}{a'^2 + b'^2} + \frac{a'b - ab'}{a'^2 + b'^2}i$$

Könnyen ellenőrizhető, hogy a szokásos műveleti azonosságok továbbra is érvényesek, azaz $z, t, u \in \mathbb{C}$ esetén $z + t = t + z, zt = tz, (z + t) + u = z + (t + u), (zt)u = z(tu)$ ill. $z(t + u) = zt + zu$. A kivonásra és osztásra vonatkozó azonosságok a $z - t = z + (0 - t)$ ill. $\frac{z}{t} = z \cdot \frac{1}{t}$ azonosságokból következnek. Egy fontos tulajdonságot bizonyítunk is:

[3] Természetesen a komplex számoknak is tulajdonítható valamiféle „jelentés”, azonban erre ebben a jegyzetben nem áll módunk részletesen kitérni.

Lemma: A z, w komplex számokra pontosan akkor lesz $zw = 0$, ha $z = 0$ vagy $w = 0$.

Biz: Könnyen ellenőrizhető, hogy $0w = 0$ tetszőleges w komplex számra. Azt kell igazolni, hogy ha a szorzat 0, akkor valamelyik tényezője 0. Tegyük fel tehát indirekt, hogy $zw = 0$ és $z \neq 0 \neq w$. Ekkor

$$0 = \frac{1}{z} \cdot 0 \cdot \frac{1}{w} = \frac{1}{z} \cdot (zw) \cdot \frac{1}{w} = \left(\frac{1}{z} \cdot z\right) \cdot \left(w \cdot \frac{1}{w}\right) = 1 \cdot 1 = 1 ,$$

ellentmondás. □

Láttuk, hogy a komplex számok egyértelműen jellemezhetőek két valós „koordinátával", akárcsak a síkbeli koordinátarendszer pontjai. Természetesen adódik tehát egy kölcsönösen egyértelmű megfeleltetés a komplex számok és a (koordinátarendszerrel ellátott) sík pontjai között: a $z = a + bi$ komplex számnak megfelel az (a, b) koordinátájú pont a *komlex számsíkon*. Vizsgáljuk meg, mi itt az alapműveletek jelentése! Ha z, z' komplex számok a számsíkon, akkor a $z + z'$ komplex számnak megfelelő pontot úgy kapjuk, hogy az origót eltoljuk azzal a vektorral, melyet úgy kapunk, hogy az origóból z-be mutató vektorhoz hozzáadjuk az origóból z'-be mutató vektort. (Kivonásnál az utóbbi vektort kivonjuk.) A szorzás „jelentésének" megértéséhez definiáljuk egy komplex szám szögét. Azt mondjuk, hogy a $z \in \mathbb{C}$ *komplex szám szöge* α, ha az origóból a z-be mutató vektor a valós tengely nemnegatív részével α szöget zár be. Vigyázat: α előjeles, így pl. i szöge $\frac{\pi}{2}$, $(-i)$-é pedig $-\frac{\pi}{2}$, vagy ha úgy tetszik $\frac{3\pi}{2}$. Definiáljuk továbbá a $z = a + bi$ komplex szám *abszolút értékét* a $|z| := \sqrt{z\overline{z}} = \sqrt{a^2 + b^2}$ képlettel. Tegyünk is néhány megfigyelést.

Lemma: (1) Ha $z \in \mathbb{C}$, akkor $|z|$ valós, és $|z| \geq 0$. Továbbá $|z| = 0 \iff z = 0$.

(2) $|z|$ nem más, mint a komplex számsíkon a z komplex számnak megfelelő pont távolsága az origótól.

(3) Ha a z komplex szám szöge α, akkor $z = |z|(\cos\alpha + i \sin\alpha)$.

(4)Ha $z, w \in \mathbb{C}$ komplex számok, akkor $|z + w| \leq |z| + |w|$.

Biz: (1) A $z = a + bi$ kanonikus alakból $z\overline{z} = a^2 + b^2 \geq 0$, így $|z|$ egy nemnegatív szám négyzetgyöke, ami szintén nemnegatív. Pontosan akkor lesz 0, ha $a^2 + b^2 = 0$, azaz $a = b = 0$, tehát, ha $z = 0$.

(2) Az (a, b) koordinátájú pont távolsága az origótól épp az a, b befogókkal rendelkező derékszögű háromszög átfogója, ami Pitagorasz tétele szerint éppen $\sqrt{a^2 + b^2} = |z|$.

(3) Ha a z-nek megfelelő pont a számsíkon $|z|$ távolságra van az origótól, és a nemnegatív valós tengelytől α szögre látszik, akkor z valós koordinátája $Re(z) = |z| \cos\alpha$, képzetes koordinátája pedig $Im(z) = |z| \sin\alpha$.

(4) Legyen O az origója, és legyen Z ill. T a z-nek ill. $z + w$-nek megfelelő pontok a komplex számsíkon. Az abszolút értékről ill. összeadásról tett korábbi megfigyeléseink alapján $|z + w| = |\overline{OT}| \leq |\overline{OZ}| + |\overline{ZT}| = |z| + |w|$, az OZT háromszögre vonatkozó háromszög-egyenlőtlenségből. □

A z komplex számnak a fenti lemma (3) részében megadott felírását a z szám *trigonometrikus alakjának* nevezzük. Jegyezzük meg, hogy míg a kanonikus alak egyértelmű, addig a trigonometrikus nem az: egyrészt α helyett választhatunk $\alpha + 2k\pi$ szöget is (tetszőleges k egész paraméterrel), ill. a $z = 0$ felírásában α tetszőleges valós lehet.

A trigonometrikus alak egyik jelentősége, hogy segítségével a szorzásnak és az osztásnak is szemléletes jelentést tulajdonítható.

Lemma: Legyen a z ill. w komlex számok trigonometrikus alakja $z = |z|(\cos\alpha + i \sin\alpha)$ ill. $w = |w|(\cos\beta + i \sin\beta)$. Ekkor a szorzat ill. hányados trigonometrikus alakja $zw = |z||w|(\cos(\alpha + \beta) + i \sin(\alpha + \beta))$, ill. $\frac{z}{w} = \frac{|z|}{|w|}(\cos(\alpha - \beta) + i \sin(\alpha - \beta))$ lesz. Más szóval: szorzás esetén az abszolút értékek összeszorzódnak, a szögek összeadódnak, míg osztásnál az abszolút érték a két abszolút érték hányadosa, és a szög a két szög különbsége lesz.

Biz: $zw = |z|(\cos\alpha + i \sin\alpha)|w|(\cos\beta + i \sin\beta) = |z||w|(\cos\alpha\cos\beta - \sin\alpha\sin\beta + i(\cos\alpha\sin\beta + \sin\alpha\cos\beta)) = |z||w|(\cos(\alpha + \beta) + i \sin(\alpha + \beta))$ adódik. A hányadosra azt kapjuk, hogy $\frac{z}{w} = \frac{|z|(\cos\alpha + i\sin\alpha)}{|w|(\cos\beta + i\sin\beta)} = \frac{|z|(\cos\alpha + i\sin\alpha)|w|(\cos\beta - i\sin\beta)}{|w|(\cos\beta + i\sin\beta)|w|(\cos\beta - i\sin\beta)} = \frac{|z||w|(\cos\alpha\cos\beta + \sin\alpha\sin\beta + i(-\cos\alpha\sin\beta + \sin\alpha\cos\beta))}{|w|^2(\cos^2\alpha + \sin^2\alpha)} = \frac{|z|(\cos(\alpha-\beta) + i\sin(\alpha-\beta))}{|w| \cdot 1} = \frac{|z|}{|w|}(\cos(\alpha - \beta) + i \sin(\alpha - \beta))$ □

A komplex számok pozitív egész kitevős hatványait is értelmezhetjük, hiszen z^n kiszámításához z-t n-szer kell önmagával összeszorozni, de ehelyett elegendő azt az origótól $|z|^n$ távolsára elhelyezkedő pontot tekinteni, melybe mutató vektor a valós tengely pozitív részével $n\alpha$ szöget zár be, ahol z szöge α. Érdekes megfigyelni, hogy ha $|z| > 1$, akkor z hatványai egy, az origó körüli, táguló spirálvonalon, míg ha $|z| > 1$, akkor z hatványai egy, az origóra szűkülő spirálvonalon helyezkednek el. $|z| = 1$ esetén z minden hatványának abszolút értéke 1, ezért mindezen hatványok az origó közepű, egységsugarú körön találhatóak.

A fentiek szerint tetszőleges $z = |z|(\cos\alpha + i \sin\alpha)$ komplex számnak meg tudjuk határozni az n-dik gyökét (helyesebben: gyökeit), tetszőleges $1 \leq n$ egész esetén. Az $\sqrt[n]{z}$ az a w komplex szám lesz, melyre $w^n = z$. Ha $w = |w|(\cos\beta + i\sin\beta)$, akkor $w^n = |w|^n(\cos(n\beta) + i\sin(n\beta))$, azaz $|w| = \sqrt[n]{|z|}$ és $\alpha = n\beta + 2k\pi$ valamely $k \in \mathbb{Z}$ egészre. Innen $\beta = \frac{\alpha+2k\pi}{n}$ adódik, azaz minden (0-tól különböző) komplex számnak pontosan n db n-dik gyöke van.

A továbbiakban az 1 abszolút értékű komplex számokkal foglalkozunk. Az ε komplex számot *n-dik egységgyök*nek nevezzük, ha $z^n = 1$. A fentiek szerint a komplex egységgyökök abszolút értéke 1, azaz a komplex számsík origó körüli egységsugarú körén helyezkednek el.

Megfigyelés: (1) Az ε komplex szám pontosan akkor n-dik egységgyök, ha $\varepsilon = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ alakúak, valamely k egészre. Pontosan n db n-dik egységgyök van.

(2) A komplex számsíkon az n-dik egységgyököknek megfelelő pontok az origóközepű egységkörön egy szabályos n-szög mentén helyezkednek el úgy, hogy az $\varepsilon = 1$ is egységgyök.

Biz: (1) Az n-dik gyökvonásról elmondottak alapján azonnal adódik, hisz azt $|\varepsilon| = 1$, és $\alpha = 0$-ra kell alkalmazni.

(2) Minden egységgyök az egységkörön van, egymástól $\frac{2\pi}{n}$ szögnyi „távolságra”, és az 1 csakugyan egységgyök. □

Hasznos tudnivaló az egységgyökök összegének és szorzatának ismerete.

Állítás: Ha $\varepsilon_1, \varepsilon_2, \ldots \varepsilon_n$ az n-dik egységgyökök (ahol $\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ és $n > 1$). Ekkor

$$\sum_{k=1}^{n} \varepsilon_k = \varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_n = 0\ , \qquad \text{továbbá} \qquad \prod_{k=1}^{n} \varepsilon_k = \varepsilon_1 \cdot \varepsilon_2 \cdot \ldots \cdot \varepsilon_n = \begin{cases} 1 & \text{ha } n \text{ páratlan} \\ -1 & \text{ha } n \text{ páros} \end{cases}$$

Biz: Legyen $S = \varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_n$. Ekkor $(1 - \varepsilon_1)S = \varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_n - \varepsilon_1(\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_n) = \varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_n - \varepsilon_2 - \varepsilon_3 - \ldots - \varepsilon_n - \varepsilon_1 = 0$, tehát $(1 - \varepsilon_1)S = 0$, ahonnan $S = 0$ adódik. (Felhasználtuk, hogy $\varepsilon_1 \cdot \varepsilon_k = \varepsilon_{k+1}$ a trigonometrikus alakból adódóan.) (Itt tkp azt bizonyítottuk, hogy egy szabályos n-oldalú sokszög középpontjából a csúcspontokba mutató vektorok összege $\underline{0}$. Ez triviális, ha n páros, hisz ekkor a vektorok ellentett párokba rendezhetőek. Egyébként, ha az összeg egy $\underline{v}$ vektor, akkor a csúcsokba mutató vektorok $\frac{2\pi}{n}$-nel való elforgatottjait összeadva az összeg egyrészt a $\underline{v}$ vektor $\frac{2\pi}{n}$-nel való elforgatottja lesz, másrészt pedig nem változik, hisz ugyanazokat a vektorokat adtuk össze. Innen $0 < \frac{2\pi}{n} < 2\pi$ miatt $\underline{v} = \underline{0}$ adódik.)

Az egységgyökök szorzatával kapcsolatban vegyük észre, hogy ha ε n-dik egységgyök, akkor $\overline{\varepsilon}$ is az, hiszen $\overline{\varepsilon}^n = \overline{\varepsilon^n} = \overline{1} = 1$. Az n-dik egységgyökök tehát konjugált párokba állíthatóak, kivéve a valós egységgyököket, amelyek önmagukkal állnak párban. Vegyük észre még, hogy ha $|\varepsilon| = 1$, akkor $\varepsilon \cdot \overline{\varepsilon} = 1$. Ezért minden konjugált pár szorzata 1, és az önmagával párban álló 1 hozzájárulása is 1 a szorzathoz. Tehát az összes n-dik egységgyök szorzata attól függ, hogy az $\varepsilon = -1$ vajon n-dik egységgyök-e: ha igen, akkor a szorzat -1, ha nem, akkor a szorzat 1. A -1 pedig pontosan akkor lesz n-dik egységgyök, ha $(-1)^n = 1$, azaz pontosan akkor, ha n páros. □

Láttuk, hogy a komplex számok alkotta matematikai struktúrában nem igaz számos olyan tulajdonság, amit a valós számokon megszoktunk, pl. nem lehet ugyanolyan értelemben beszélni a számok „nagyságáról”. Azonban nem is ez a komplex számkör bevezetésének igazi jelentősége, hanem sokkal inkább az, hogy a valós számokon megszokott legfontosabb tulajdonságok igazak, azaz $\mathbb{C}$ egy ú.n. testet[4] alkot, ami annyiban „jobb” a valós számtestnél, hogy ebben minden polinomnak van gyöke, más szóval, hogy algebrailag zárt. Erről szól az algebra alaptétele:

Tétel: Ha $p(x)$ egy komplex együtthatós, legalább elsőfokú polinom, akkor létezik olyan α komplex szám, melyre $p(x) = (x - \alpha) \cdot r(x)$ alakba írható, ahol $r(x)$ egy $p(x)$-nél eggyel alacsonyabb fokú, komplex együtthatós polinom. □

Megjegyzés: A fenti tétel következménye, hogy ha $p(x)$ valós együtthatós, akkor találunk egy α gyökét, ami vagy valós (és kiemelhetjük a gyöktényezőt) vagy α képzetes része nemnulla. Utóbbi esetben (mint az könnyen látható) $\overline{\alpha}$ is gyöke $p(x)$-nek, azaz $p(x) = (x - \alpha)(x - \overline{\alpha})r'(x)$ alakba írható, ahol $r'(x)$ egy $p(x)$-nél kettővel alacsonyabb fokú, *valós* együtthatós polinom. (Utóbbi abból adódik, hogy $q(x) = (x - \alpha)(x - \overline{\alpha})$ egy valós együtthatós másodfokú polinom. (Értelemszerűen $q(x)$ diszkriminánsa negatív, és a másodfokú egyenlet megoldóképlete éppen α-t és $\overline{\alpha}$-t adja.))

Az algebra alaptételének ismételt alkalmazásából az adódik, hogy minden valós együtthatós polinom felírható legfeljebb másodfokú valós együtthatós polinomok szorzataként, és ez a tétel bár a valós számkörre vonatkozik, nehezen bizonyítható a komplex számkör megkerülésével.

2. Lineáris egyenletrendszerek

Egy *n-ismeretlenes, m egyenletből álló lineáris egyenletrendszer* alatt m olyan egyenlőséget értünk, melyek mindegyike n rögzített ismeretlen konstansszorosait, konstansokat és ezek összegét (ill. különbségét) tartalmazza. Megtehetjük, hogy minden egyes egyenletet rendezünk, azaz baloldalra gyűjtjük az ismeretlent tartalmazó tagokat, ezeket a bennük szereplő ismeretlenek egy rögzített sorrendjében írjuk fel, és jobbra rendezzük a konstansokat. Ezáltal a lineáris egyenletrendszer egy rendezett alakját kapjuk. Ebben az alakban szereplő együtthatók és konstansok egy táblázatba rendezhetőek. Ezek alkotják az ábrán is jelzett *kibővített együtthatómátrix*ot. A kibővített együtthatómátrixot *lépcsős alak*únak nevezzük, ha minden sorában az első nemnulla elem 1 (a lépcsős alakban ezeket a mátrixelemeket nevezzük *vezéregyeseknek*), ezen kívül bármely két vezéregyes úgy helyezkedik el, hogy a feljebb lévő oszlopa balra legyen a lejjebb lévő oszlopától. Úgy is definiálhatóak a lépcsős alakú mátrixok, mint mindazon mátrixok, amik megkaphatóak a csupa0 mátrixból az alábbi két lépés tetszőleges sorrendben történő, tetszőlegesen sokszori ismételt alkalmazásával. (1): egy M mátrixhoz baloldalt hozzáveszünk egy csupa0 oszlopot, ill. (2): egy M mátrixhoz balról hozzáveszünk egy csupa0 oszlopot, majd a kibővített mátrix tetejére egy 1-gyel kezdődő (egyébként tetszőleges) sort biggyesztünk. Az alábbi ábra hivatott szemléltetni a fenti definíciókat.

[4] Ennek pontos jelentésével a második félévben fogunk megismerkedni; itt legyen elég annyi, hogy a most következő lineáris algebra fejezetekben feltetelezzük ugyan, hogy a skalárokon valós számokat értünk, minden további nélkül működnek az elmondottak komplex skalárokkal is.

Lineáris egyenletrendszer	(kibővített) együtthatómátrix	lépcsős alak
$\begin{array}{c} \alpha_{1,1}x_1 + \alpha_{1,2}x_2 + \ldots + \alpha_{1,n}x_n = b_1 \\ \alpha_{2,1}x_1 + \alpha_{2,2}x_2 + \ldots + \alpha_{2,n}x_n = b_2 \\ \vdots \\ \alpha_{n,1}x_1 + \alpha_{n,2}x_2 + \ldots + \alpha_{n,n}x_n = b_n \end{array}$	$\left(\begin{array}{cccc\|c} \alpha_{1,1} & \alpha_{1,2} & \ldots & \alpha_{1,n} & b_1 \\ \alpha_{2,1} & \alpha_{2,2} & \ldots & \alpha_{2,n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ \alpha_{n,1} & \alpha_{n,2} & \ldots & \alpha_{n,n} & b_n \end{array}\right)$	$\left(\begin{array}{c\|c\|c\|c\|c\|c} & 1\ldots & & & & \\ & & 1\ldots & & & \\ & & & 1\ldots & & \\ & & & & 1\ldots & \vdots \\ 0 & 0 & 0 & 0 & 0\ldots0 & \\ & & & & \ddots & \\ & & & & 0\ldots0 & \end{array}\right)$

A ***redukált lépcsős alak*** olyan lépcsős alak, aminek minden vezéregyesére igaz, hogy az adott vezéregyes az egyedüli nemnulla elem a saját oszlopában, más szóval a vezéregyesek felett is csak 0-k állhatnak a mátrixban.

Azt mondjuk, hogy $(s_1, s_2, \ldots, s_n)$ *megoldása* a fenti lineáris egyenletrendszernek, ha az $x_1 = s_1, x_2 = s_2, \ldots, x_n = s_n$ helyettesítés az egyenletrendszerben szereplő összes egyenlőséget igazzá teszi. A lineáris egyenletrendszer ***egyértelműen megoldható***, ha pontosan egy megoldása van. Célunk egy olyan módszer keresése, aminek segítségével egy lineáris egyenletrendszerről eldönthető, hogy létezik-e megoldása, ha létezik, akkor pedig a megoldás(ok) könnyen megtalálható(ak). Ezért olyan operációkat vizsgálunk, amik a megoldások halmazát nem változtatják, és segítségükkel a lineáris egyenletrendszer egy könnyen megoldható, speciális alakú lineáris egyenletrendszerré alakítható. Célszerű ezeket az operációkat a (kibővített) együtthatómátrixon megadni. A kibővített együtthatómátrix *elemi sorekvivalens átalakításai* tehát az alábbiak:

(1) két sor felcserélése,
(2) valamely sor elemeinek egy $\lambda \neq 0$ számmal történő végigszorzása, ill.
(3) valamely sornak egy másik sorhoz való (elemenkénti) hozzáadása.
(4) (valamely sor konstansszorosának hozzáadása egy másik sorhoz)
(5) (csupa 0-sor elhagyása)

Állítás: Elemi sorekvivalens átalakítás során a lin. egyrsz. megoldásainak halmaza nem változik.

Biz: Elsőként belátjuk, hogy az elemi sorekvivalens átalakítás után minden korábbi megoldás továbbra is megoldás marad, azaz csupán annyi történhet, hogy olyan új megoldások keletkeznek, amik korábban nem voltak megoldások. Ez az állítás világos, ha meggondoljuk, mit jelentenek az egyes lépések az egyenletrendszer szempontjából. (1) két egyenlet felcserélését, (2) egy egyenletnek egy nemnulla számmal való végigszorzását, (3) egy egyenletnek egy másik egyenlethez való hozzáadását, míg (5) egy $0 = 0$ egyenlőség elhagyását jelenti. (4) esetén egy egyenlet konstansszorosának egy másik egyenlethez való hozzáadásáról van szó, ami bár közvetlenül is látszik, de megvalósítható egy (2)-es, egy (3)-as, majd egy (2)-es átalakítás egymásutánjaként is.

Ezt követően azt kell igazolni, hogy egyik átalakítás során sem keletkezhetett új megoldás. Ezt úgy bizonyítjuk, hogy mindegyik fajta átalakításról megmutatjuk, hogy (1),(2) és (3) átalakításokkal visszakaphatjuk az eredeti egyenletrendszert, tehát az újonnan keletkezett megoldások megoldják az eredeti egyenletrendszert is, így új megoldás tényleg sehol sem léphetett be. (1) esetén ez világos, cseréljük ismét fel a megfelelő sorokat, ami egy (1) típusú átalakítás. (2) esetén szorozzuk meg az adott sort $\frac{1}{\lambda}$-val, ami egy (2)-es átalakítás, és az eredeti együtthatómátrixot adja vissza. Ha a (3)-as átalakításban az i-dik sorhoz adtuk hozzá a j-dik sort, akkor szorozzuk meg a j-dik sort (-1)-gyel, adjuk hozzá az i-dik sorhoz, majd ismét szorzzuk végig a j-dik sort (-1)-gyel, miáltal visszakapjuk az eredeti mátrixot, és csak (2)-es ill. (3)-as átalakítást végeztünk. Láttuk, hogy a (4)-es átalakítás (2)-es és (3)-as átalakítások egymásutánja, így az állítás arra is igaz. Az (5)-ös átalakításra az állítás közvetlenül látszik, de ezt nem fogjuk használni a továbbiakban. □

Mielőtt megmutatnánk, hogyan érdemes használni a fenti átalakításokat, rögzítünk néhány mátrixos jelölést. Ha egy M mátrixnak m sora és n oszlopa van, akkor azt mondjuk, hogy M egy $m \times n$ méretű mátrix. $\mathbb{R}^{m\times n}$ a valós, $m \times n$-es mátrixok halmazát jelöli. (Ha $\mathbb{R}$ helyett $\mathbb{C}$-t írunk, akkor komplex mátrixokról beszélünk. Minden, amit ebben a fejezetben elmondunk, komplex mátrixokra ill. komplex együtthatós lineáris egyenletrendszerekre is igaz. Sőt: racionálisakra is.) Ha M egy mátrix, akkor M_i jelöli az M mátrix i-dik sorát, M^j a j-dik oszlopát, M_i^j pedig az (i, j) pozícióban álló elemét.

Tétel: Elemi sorekvivalens átalakításokkal tetszőleges kibővített együtthatómátrix lépcsős alakra hozható.

Biz: Megadjuk a Gauss-elimináció nevű eljárást, ami az (1), (2), (4) átalakítások segítségével a kibővített együtthatómátrixot lépcsős alakra hozza. Az algoritmus inputja tehát az M mátrix, és az algoritmus rekurzív, azaz időnként meghívja önmagát úgy, hogy bemenete egy M-nél kisebb méretű (konkrétan, egy M-nél kevesebb oszloppal rendelkező) mátrix. Az algoritmus kimenete egy, az M-ből elemi sorekvivalens átalakításokkal keletkező lépcsős alak.

Az M mátrix Gauss-eliminációja.

1. Ha $M^1 = \underline{0}$ (azaz M első oszlopa csupa 0), akkor hívjuk meg a Gauss-eliminációt az M első oszlopának elhagyásával keletkező M' mátrixra, és a kapott lépcsős alak elé biggyesszünk egy csupa0 oszlopot.

2. Egyébként (ha $M^1 \neq \underline{0}$), egy esetleges sorcserével ((1)-es átalakítás) érjük el, hogy $M_1^1 \neq 0$ legyen.

3. M_1 (vagyis M első sorának) végigszorzásával (azaz a (2) lépéssel) érjük el, hogy $M_1^1 = 1$ legyen.

4. A (4) lépés segítségével érjük el, hogy $M_i^1 = 0$ legyen minden $i = 2, 3, \ldots$ esetén. („Kinullázzuk az 1-es alatti elemeket.")

5. Hagyjuk el M első oszlopát és első sorát, és hívjuk meg a Gauss-eliminációt az így keletkező M' részmátrixra. A kapott lépcsős alakot egészítsük ki elöl egy csupa0 oszloppal, felül pedig az imént elhagyott sorral.

Ennyi az algoritmus. Az algoritmus véges számú lépés után véget ér, hiszen legfeljebb (kétszer) M elemszámnyi művelet elvégzése után egy kevesebb oszlopból álló mátrixra hívjuk meg az eljárást. (Ezért az algoritmus összességében egy $m \times n$ méretű mátrixon $2mn^2$ műveletet hajt végre.) Könnyen látható, hogy az algoritmus egy $m \times 1$ méretű mátrix esetén nem hívja meg önmagát, hanem egy csupa0 oszlopot vagy egy olyan oszlopmátrixot ad, aminek felső eleme 1, a többi pedig 0. Tehát az algoritmus az egyoszlopú mátrixokat valóban lépcsős alakra hozza. Tegyük fel, hogy ez igaz a legfeljebb n oszlopból álló mátrixokra, és Gauss-elimináljunk egy $(n+1)$-oszlopú mátrixot. Ekkor rekurzív hívás következik, ami az indukció szerint lépcsős alakot szolgáltat. Ezt egy csupa0 oszloppal és esetleg egy 1-essel kezdődő sorral kiegészítve a kapott mátrix nyilván lépcsős alakú.

Annyi van hátra, hogy azt megmutassuk, hogy a Gauss-elimináció által szolgáltatott lépcsős alak valóban elemi sorekvivalens átalakításokkal származtatható M-ből. Ehhez pedig mindössze annyit kell észrevenni, hogy bár a rekurzív hívások során a Gauss elimináció során használt elemi sorekvivalens átalakításokat kisebb mátrixokon hajtjuk végre, az időközben elhagyott sorokat és csupa0 oszopokat „odagondolva" azok nem változnának a lépések során. Tehát amikor visszaírjuk őket, helyesen járunk el.[5] □

Azt kaptuk, hogy a Gauss-elimináció bármely kibővített együtthatómátrixot lépcsős alakra hoz. Ha redukált lépcsős alak a cél, akkor innen már könnyű dolgunk van: pontosan úgy, ahogy a vezéregyesek alatt kinulláztuk az oszlopokat, a vezéregyesek felett is megtehetjük ugyanezt. Könnyen látható, hogy kinullázás során a lépcsős tulajdonság nem sérül, tehát ha minden vezéregyes feletti elemet kinullázunk, akkor megkapjuk a redukált lépcsős alakot. Ez az alak alkalmas arra, hogy leolvassuk a megfelelő lineáris egyenletrendszer megoldásait.

A kibővített együtthatómátrix egy sorát *tilos sor*nak nevezzük, ha benne az együtthatórész csupa-0, a kibővítő elem pedig nemnulla.[6] Világos, hogy a tilos sor egy olyan egyenletnek felel meg, hogy $0x_1 + 0x_2 + \ldots + 0x_n = b \neq 0$, ahonnan azonnal adódik, hogy tilos sor felbukkanása esetén nem létezik az egyenletrendszernek megoldása. *Szabad paraméter*nek nevezzük a (redukált) lépcsős alak vezéregyest nem tartalmazó oszlopához tartozó ismeretlent. Az iménti megfigyelést általánosítja az alábbi tétel.

Tétel: Egy lineáris egyenletrendszer pontosan akkor megoldható, ha a (redukált) lépcsős alakja nem tartalmaz tilos sort. Továbbá, ha a lineáris egyenletrendszer nem tartalmaz tilos sort, akkor a szabad paraméterek értékének tetszőleges megválasztásához egyértelműen létezik megoldás.

Megjegyzés: A tétel első része úgy is kimondható, hogy az egyenletrendszer pontosan akkor megoldható, ha a lépcsős alak kibővítő oszlopa nem tartalmaz vezéregyest. Annak oka, hogy a fenti formát használjuk az, hogy hangsúlyosabbá váljon, hogy egy konkrét feladat (pl Gauss-eliminációval történő) megoldásakor egy tilos sor felbukkanása azt jelenti, hogy nincs megoldás, tehát nem érdemes tovább dolgozni.

Biz: Láttuk, hogy tilos sor esetén nincs megoldás. Az, hogy tilos sor hiányában van megoldás, a tétel második mondatából következik, elegendő tehát csak azt igazolni. Adjunk a szabad paramétereknek tetszőleges értékeket, mondjuk $p_1, p_2, \ldots, p_k$-t. Vizsgáljuk meg, milyen egyenlőségeknek felelnek meg a redukált lépcsős alak egyes sorai. Ha az adott sorban nincs vezéregyes, akkor annak a $0 = 0$ egyenlőség felel meg, ez nem túl izgalmas. Ha az x_i vezéregyese van az adott sorban, akkor a megfelelő egyenlőség nem más, mint $x_i + a_1p_1 + a_2p_2 + \ldots + a_kp_k = b_i$, ahol az a_j-k a szabad paraméterek i-dik sorbeli együtthatói. Tehát a vezéregyesnek megfelelő sorok tekinthetőek a megfelelő x_i ismeretlen egy (egyértelmű) értékadásának. A tétel innen azonnal adódik. □

[5] Ha írásban kell a Gauss-eliminációt végrehajtani, akkor jobb, ha nem próbálkozzunk a fenti rekurzióval, hanem az elhagyandó sorokat és oszlopokat továbbra is akkurátusan kiírjuk.

[6] A tilos sor a (redukált) lépcsős alakban annak felel meg, hogy a kibővíő oszlopban megjelenik egy vezéregyes.

Köv.: (1) A lineáris egyenletrendszer pontosan akkor oldható meg egyértelműen, ha a (redukált) lépcsős alakban nem létezik sem tilos sor, sem szabad paraméter, azaz minden oszlopban van vezéregyes.

(2) Ha egy lineáris egyenletrendszernek létezik és egyértelmű a megoldása, akkor legalább annyi egyenlet van, mint ahány ismeretlen.

Biz: (1): Ha egyértelmű a megoldás, akkor nincs tilos sor, hisz létezik megoldás. Nincs továbbá szabad paraméter sem, hisz az tetszőleges értéket felvehetne. Másfelől, ha nincs tilos sor, akkor létezik megoldás, és ha ezen túlmenően szabad paraméter sincs, akkor azoknak csak egyféleképp lehet tetszőleges értéket adni, így az előző tétel szerint a megoldás egyértelmű.

(2): Ha egyértelmű a megoldás, akkor nincs szabad paraméter, vagyis minden oszlopban van vezéregyes, és ezek a vezéregyesek különböző sorokban találhatóak. A sorok száma (azaz az egyenletek száma) tehát nem lehet kisebb az oszlopok számánál, vagyis az ismeretlenek számánál. □

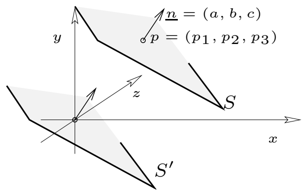
Homogén lineáris egyenletrendszernek nevezünk egy egyenletrendszert, ha a kibővített együtthatómátrix jobb oldali oszlopa csupa0, azaz a megfelelő egyenletek mindegyikének 0 áll a jobb oldalán. Világos, hogy egy homogén lineáris egyenletrendszer kibővített együtthatómátrixában sosem keletkezhet tilos sor az elemi sorekvivalens átalakítások hatására, hisz a jobboldal mindvégig 0 lesz. Csakugyan: minden homogén lineáris egyenletrendszernek létezik megoldása, mégpedig az ú.n. *triviális megoldás*, ami minden ismeretlennek 0 értéket ad. A nemtriviális megoldás létezésének elégséges feltételét adja a következő tétel.

Állítás: Ha egy homogén lineáris egyenletrendszer több ismeretlent tartalmaz, mint ahány egyenletet, akkor van nemtriviális megoldása.

Biz: A kibővített együtthatómátrixnak több oszlopa van, mint sora, így a legfeljebb sorszámnyi vezéregyes nem foglalhat el minden oszlopot, tehát van szabad paraméter. Ezek értékeit nemnullának választva pedig nemtriviális megoldást kapunk. □

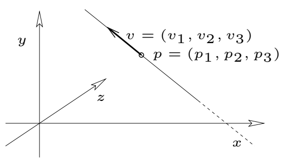
2.1. Koordinátageometria

A koordinátageometriai számítások egy lehetséges példa a lineáris egyenletrendszerek alkalmazására. Tudjuk, hogy a háromdimenziós tér pontjai egyértelműen jellemezhetőek egy valós számhármassal, már persze, amennyiben előzetesen rögzítettünk egy derékszögű koordinátarendszert. Természetes kérdés, hogy hogyan jellemezhetőek különféle térbeli alakzatok, illetve azok metszetei. Térbeli alakzatokon most a pontot, az egyenest és a síkot értjük.



Tegyük fel tehát, hogy S egy sík a térben, és $\underline{n} = (a, b, c)$ egy normálvektora, azaz egy olyan nemnulla vektor, ami az S sík minden egyenesére merőleges. Legyen még $p = (p_1, p_2, p_3)$ az S sík egy pontja, és legyen az S' sík az S sík $(-p_1, -p_2, -p_3)$ vektorral való eltoltja, ami tehát tartalmazza az origót. Világos, hogy S' pontjai pontosan az $(x-p_1, y-p_2, z-p_3)$ alakú pontok lesznek, ahol (x, y, z) az S sík egy tetszőleges pontja.

Azt is tudjuk, hogy az S' sík pontosan azokat a pontokat tartalmazza, amelyekbe az origóból mutató helyvektor merőleges az S' (és így az S) sík $\underline{n}$ normálvektorára, azaz az $(x - p_1, y - p_2, z - p_3)$ és az (a, b, c) vektorok skaláris szorzata 0: $a(x - p_1) + b(y - p_2) + c(z - p_3) = 0$. A sík egyenlete ennek alapján $ax + by + cz = ap_1 + bp_2 + cp_3$ lesz, azaz pontosan azok az (x, y, z) koordinátákkal jellemzett pontok lesznek S-ben, amik megoldják az iménti egyenletet.



Ha egy e egyenes pontjait szeretnénk jellemezni, akkor kiindulhatunk e egy $p = (p_1, p_2, p_3)$ pontjából és az e egy nemnulla $\underline{v} = (v_1, v_2, v_3)$ irányvektorából. Az e egyenes pontjai pontosan azok az (x, y, z) koordinátájú pontok lesznek, amik előállnak $(x, y, z) = (p_1, p_2, p_3) + \lambda(v_1, v_2, v_3)$ alakban valamely $\lambda \in \mathbb{R}$ esetén, azaz a koordináták kielégítik az $x - v_1\lambda = p_1$, $y - v_2\lambda = p_2$ és $z - v_3\lambda = p_3$ egyenletrendszert, ami 3 egyenletből áll és 4 ismeretlent (x, y, z, λ) tartalmaz.

Ha ennek az egyenletrendszernek felírjuk a kibővített együtthatómátrixát, látjuk, hogy ez már egy redukált lépcsős alak, ahol az x, y és z-nek megfelelő oszlpokban vannak a vezéregyesek. Megtehető azonban, hogy a kibővített együtthatómátrix oszlopait nem x, y, z, λ sorrendben írjuk fel, és ekkor elvégezhető lesz a Gauss-elimináció úgy, hogy a λ ne szabad paraméter legyen, hanem az oszlopában vezéregyes álljon. Minthogy mi csak x, y, z-re akarjuk megoldani az egyenletrendszert, az az egyenlőség, ami a λ vezéregyesének sorához tartozik, egyszerűen elhagyható. Marad tehát 2 egyenlet, mindegyikben csak x, y, z a változók, és megoldásai pontosan az e egyenes pontjainak koordinátái lesznek.

Láttuk tehát, hogy a síkot egy egyenlet, az egyenes pontjait két egyenlet írta le. Világos az is, hogy a „pont egyenlete” voltaképpen egy három egyenletből álló lineáris egyenletrendszer: a $p = (p_1, p_2, p_3)$ ponthoz az $x = p_1, y = p_2, z = p_3$ egyenletrendszer tartozik. Ha pedig a fent leírt halmazok (pont, egyenes, sík) közül néhánynak a közös pontjait kell meghatároznunk, akkor az eljárás az lehet, hogy mindegyik ponthalmaznak felírjuk az egyenlet(rendszer)ét, ezeket egy közös egyenletrendszernek tekintve, azt Gauss-eliminációval megoldjuk. Ha nincs megoldás, akkor a metszet értelemszerűen üres, egyébként a redukált lépcsős alakban szereplő egyenletek számától függően a megoldás egy pont, egy egyenes vagy éppen egy sík lesz.

3. Vektorterek

Def: A V halmazt $\mathbb{R}$ *feletti vektortér*nek mondjuk[7], ha
(1) $(V,+)$ kommutatív csoport, azaz az összeadásra az alábbi azonosságok igazak
$\forall u,v,w\in V$ esetén (ö1) $u+(v+w)=(u+v)+w$, (ö2) $u+v=v+u$,
(ö3) létezik $\mathbf{0}\in V$: $u+\mathbf{0}=u$, (ö4) létezik $-u\in V$, amire $u+(-u)=\mathbf{0}$
(2) A skalárral való szorzásra az alábbi szorzásaxiomák teljesülését kívánjuk meg: $\forall\lambda,\kappa\in\mathbb{R}$, $\forall u,v\in V$
(sz1) $(\lambda+\kappa)u=\lambda u+\kappa u$, (sz2) $\lambda(u+v)=\lambda u+\lambda v$, (sz3) $(\lambda\kappa)u=\lambda(\kappa u)$, (sz4) $1u=u$

Megjegyzés: A fenti definíció valójában a *valós* vektortér definíciója. Ha az $\mathbb{R}$ halmaz helyett $\mathbb{Q}$ vagy $\mathbb{C}$ állna, akkor beszélhetnénk *racionális* ill. *komplex* vektortérről. A vektortér skalárjaitól az elvárás, hogy rajtuk legyen egy összeadás és egy szorzásművelet, mellyel ú.n. testet alkotnak. A testekkel később foglalkozunk, itt elegendő a valós vektorterekre koncentrálni.

Példa: (1) $\mathbb{R}$ (és minden test) vektortér önmaga felett.
(2) A síkbeli (térbeli) vektorok vektorteret alkotnak $\mathbb{R}$ felett.
(3) A valós számokból alkotott n hosszú sorozatok is vektorteret alkotnak $\mathbb{R}$ felett, ahol $(x_1,x_2,\ldots,x_n)+(y_1,y_2,\ldots,y_n)=(x_1+y_1,x_2+y_2,\ldots,x_n+y_n)$, illetve $\lambda(x_1,x_2,\ldots,x_n)=(\lambda x_1,\lambda x_2,\ldots,\lambda x_n)$. Világos, hogy az (1) ill. (2) példák a (3) speciális esetei $n=1$ ill. $n=2,3$ esetén.
(4) Az $n\times k$ méretű (valós) mátrixok is vektorteret alkotnak $\mathbb{R}$ felett, ha az összeadást elemenként, a skalárral való szorzást pedig az összes mátrixelem végigszorzásaként értelmezzük.
Az $n=1$ eset épp az előző példát adja.
(5) A valós polinomok is vektorteret alkotnak $\mathbb{R}$ felett, a legfelejebb n-edfokú polinomok szintén.
(6) A valós számok mindegyikéhez egy valós számot rendelő ($f:\mathbb{R}\to\mathbb{R}$ típusú) függvények $\mathbb{R}$ felett vektorteret alkotnak, ahol az összeadás az $(f+g)(x):=f(x)+g(x)$, a skalárral szorzás pedig a $(\lambda\cdot f)(x):=\lambda\cdot f(x)$ azonossággal értelmezhető.

Tétel: Ha V egy valós vektortér, akkor az (1) $\lambda\mathbf{0}=\mathbf{0}$ $\forall\lambda\in\mathbb{R}$, (2) $0v=\mathbf{0}$ $\forall v\in V$,
(3) $(-1)v=-v$ $\forall v\in V$, (4) $\lambda v=\mathbf{0}\Rightarrow(\lambda=0$ vagy $v=\mathbf{0})$ teljesülnek.

Biz: (1): $\mathbf{0}=\lambda\mathbf{0}+(-\lambda\mathbf{0})=\lambda(\mathbf{0}+\mathbf{0})+(-\lambda(\mathbf{0}))=(\lambda\mathbf{0}+\lambda\mathbf{0})+(-\lambda\mathbf{0})=\lambda\mathbf{0}+(\lambda\mathbf{0}+(-\lambda\mathbf{0}))=\lambda\mathbf{0}+\mathbf{0}=\lambda\mathbf{0}$.
(2): $\mathbf{0}=0v+(-0v)=(0+0)v+(-0v)=(0v+0v)+(-0v)=0v+(0v+(-0v))=0v+\mathbf{0}=0v$.
(3): $(-1)v=(-1)v+\mathbf{0}=(-1)v+(v+(-v))=((-1)v+v)+(-v)=((-1)v+1v)+(-v)=(1-1)v+(-v)=0v+(-v)=\mathbf{0}+(-v)=-v$.
(4): Láttuk, hogy $\lambda=\mathbf{0}$ ill. $v=\mathbf{0}$ esetén $\lambda v=\mathbf{0}$. Tegyük fel most, hogy $\lambda v=\mathbf{0}$, és $\lambda\neq 0$. Azt kell igazolnunk, hogy $v=\mathbf{0}$. Tessék: $\mathbf{0}=\frac{1}{\lambda}\mathbf{0}=\frac{1}{\lambda}(\lambda v)=(\frac{1}{\lambda}\lambda)v=1v=v$.[8] □

Def: A $W\subseteq V$ részhalmaz a V valós vektortér *altere*, ha W is valós vektortér a V vektortér műveleteire. Jelölése: $W\leq V$.

Példa:

Tétel: Ha V vektortér, akkor $\emptyset\neq W\subseteq V$ pontosan akkor altere V-nek, ha zárt a vektorösszeadásra és a skalárral való szorzásra.

Biz: Világos, hogy ha W altér, akkor sem a vektorösszeadás, sem a skalárral való szorzás nem vezethet ki W-ből. Az elégségességhez figyeljük meg, hogy a műveletek zártságából azonnal adódnak az (ö1,ö2), ill. az (sz1, sz2, sz3, sz4) axiomák, így csupán (ö3,ö4)-t kell ellenőrizni. Mivel $\emptyset\neq W$, ezért létezik egy $w\in W$, ahonnan $-w=(-1)w\in W$ a skalárral szorzás zártsága miatt. Innen pedig $0=w+(-w)\in W$, tehát (ö3,ö4) is teljesül. □

Def: Legyen V valós vektortér. A $v_1,v_2,\ldots v_n$ vektorok *lineáris kombinációja* a $\sum_{i=1}^n\lambda_iv_i=\lambda_1v_1+\lambda_2v_2+\ldots+\lambda_nv_n$ vektorösszeg, ahol $\lambda_i\in\mathbb{R}$. A $\sum_{i=1}^n\lambda_iv_i$ lin. komb. *triviális*, ha $\forall\lambda_i=0$.

Def: Azt mondjuk, hogy a $v\in V$ vektort *generálja* a V vektortér U részhalmaza, ha v előáll U néhány (véges sok) vektorának lineáris kombinációjaként. (Azaz, ha létezik egy $n\in\mathbb{N}$ szám, és léteznek $u_1,u_2,\ldots,u_n\in U$ vektorok úgy, hogy $v=\sum_{i=1}^n\lambda_iu_i$ teljesül alkalmas λ_i-ket választva.) Az U részhalmaz generálta vektorok halmazát $\langle U\rangle$ jelöli. Egy $g_1,g_2,\ldots g_n$ véges vektorrendszer által generált vektorok halmazát $\langle g_1,g_2,\ldots g_n\rangle$-vel jelöljük. Az $U\subseteq V$ halmaz *generálja* a $W\leq V$ alteret, ha minden vektorát generálja, azaz, ha $W\subseteq\langle U\rangle$. Ha ezen túl még $U\subseteq W$ is teljesül, akkor U-t a W *generátorrendszerének* mondjuk.

A lineáris kombináció valójában annak a ténynek pontos leírása, hogy vektorok egy adott U halmazából a vektortér műveleteinek segítségével hogyan lehet előállítani egy újabb v vektort. Ilyenformán $\langle U\rangle$ nem más, mint mindazon v vektorok halmaza, amiket megkaphatunk az U elemeiből a vektortér

[7] $\mathbb{R}$ elemeit *skalároknak* nevezzük

[8] (3) és (4) bizonyításához szükség volt az (sz4) axiomára is. Ha ez az axioma nem lenne, akkor módosíthatnánk egy tetszőleges vektortéren a skalárral való szorzást úgy, hogy $\lambda v:=\mathbf{0}$ teljesüljön minden $\lambda\in\mathbb{R}$ és minden $v\in V$ esetén. Az így kapott struktúra az (sz4) kivételével minden vektortéraxiomát teljesít.

műveleteinek alkalmazásával. Ezen szemlélet szerint $\langle U\rangle$ bizonyosan zárt a műveletekre, így korábbi tétel szerint altér. Ezt be is bizonyítjuk az alábbiakban.

Tétel: Tetszőleges vektorrendszer által generált vektorok alteret alkotnak, azaz $\langle U\rangle \leq V$ bármely $U \subseteq V$ esetén.

Biz: A műveletekre való zártságot kell ellenőriznünk, azaz, hogy U néhány elemének egy lineáris kombinációját a λ skalárral megszorozva lineáris kombinációt kapunk, illetve, hogy két lineáris kombináció összege is lineáris kombináció. Az első esetben legyen $v := \sum_{i=1}^{n} \lambda_i u_i$, ekkor $\lambda v = \lambda(\lambda_1 u_1 + \lambda_2 u_2 + \dots \lambda_n u_n) = \lambda \cdot \lambda_1 u_1 + \lambda \cdot \lambda_2 u_2 + \dots + \lambda \cdot \lambda_n u_n = \sum_{i=1}^{n} \lambda\lambda_i u_i$, ami valóban lineáris kombináció. Az összeg esetén legyen $v = \sum_{i=1}^{n} \lambda_i u_i$ az egyik, ill. $w = \sum_{j=k}^{m} \kappa_j u_j$ a másik lineáris kombináció. Feltehetjük, hogy $k \leq n$ olyan, hogy az $u_k, u_{k+1}, \dots u_n$ vektorok közösek a két felírásban, a többi vektor pedig nem. Ekkor a lineáris kombinációk átrendezésével (az (ö1, ö2) illetve az (sz1) axiomák felhasználásával) a $v + w = \sum_{i=1}^{k-1} \lambda_i u_i + \sum_{i=k}^{n} (\lambda_i + \kappa_i) u_i + \sum_{i=n+1}^{m} \kappa_i u_i$ alak adódik, ami szintén egy lineáris kombináció, és ilyenformán $v + w \in \langle U\rangle$. □

Def: A $v_1, v_2, \dots, v_n$ vektorrendszer *(lineárisan) független*, ha csak a triviális lineáris kombinációjuk állítja elő a $\mathbf{0}$-t, azaz, ha $\sum_{i=1}^{n} \lambda_i v_i = \mathbf{0} \Rightarrow \forall \lambda_i = 0$. A fenti rendszer *(lineárisan) összefüggő*, ha nem lin.ftn, azaz, ha a $\mathbf{0}$ előáll nemtriv. lin. komb.-ként is: $\sum_{i=1}^{n} \lambda_i v_i = \mathbf{0}$, és $\lambda_i \neq 0$ valamely i-re.[9]

Állítás: A $v_1, v_2, \dots, v_n$ vektorrendszer pontosan akkor független, ha egyik v_k sem áll elő a maradék v_j vektorok lineáris kombinációjaként.

Biz: Világos, hogy ha $v_k = \sum_{i \neq k} \lambda_i v_i$, akkor a $\mathbf{0} = \sum_{i \neq k} \lambda_i v_i + (-1) \cdot v_k$ egy nemtriviális lineáris kombináció, hiszen v_k együtthatója -1. Ha tehát v_k előáll lineáris kombinációként, akkor a rendszer összefüggő. Másfelől, ha $\{v_1, v_2, \dots, v_n\}$ összefüggő, azaz nem lin. ftn, akkor a $\mathbf{0}$ előáll nemtriviális lineáris kombinációként, pl. $\mathbf{0} = \sum_{i=1}^{n} \lambda_i v_i$ alakban, ahol (mondjuk) $\lambda_k \neq 0$. Ekkor átrendezéssel $\lambda_k v_k = \sum_{i \neq k} -\lambda_i v_i$, ahonnan $v_k = \frac{1}{\lambda_k} \sum_{i \neq k} -\lambda_i v_i = \sum_{i \neq k} -\frac{\lambda_i}{\lambda_k} v_i$ adódik, ami épp v_k előállítása a maradék vektorok lineáris kombinációjaként. □

Def: A $\{b_1, b_2, \dots, b_n\}$ vektorrendszer a V vektortér *bázisa*, ha lin. ftn. és generálja V-t.

Tétel: A $\{b_1, b_2, \dots, b_n\}$ pontosan akkor bázisa V-nek, ha $\forall v \in V$ egyértelműen áll elő a b_i-k lin. komb.jaként.

Biz: Tegyük fel, hogy $\{b_1, b_2, \dots, b_n\}$ bázis. Ekkor V minden vektora előáll lineáris kombinációként, hiszen a bázis generátorrendszer. Azt kell látnunk, hogy a lineáris kombinációként történő felírás egyértelmű. Tegyük fel, hogy $v = \sum_{i=1}^{n} \lambda_i b_i = \sum_{i=1}^{n} \kappa_i b_i$ két felírás. Ekkor átrendezéssel $\mathbf{0} = \sum_{i=1}^{n} \lambda_i b_i - \sum_{i=1}^{n} \kappa_i b_i = \sum_{i=1}^{n} (\lambda_i - \kappa_i) b_i$, ahonnan a b_i függetlensége miatt $\lambda_i - \kappa_i = 0$ következik minden i-re. Eszerint $\lambda_1 = \kappa_1, \lambda_2 = \kappa_2, \dots, \lambda_n = \kappa_n$, tehát a felírás csakugyan egyértelmű.

Most tegyük fel, hogy a V bármely eleme egyértelműen állítható elő a $b_1, b_2, \dots, b_n$ vektorok lineáris kombinációjaként. E vektorok tehát generátorrendszert alkotnak, csak a lineáris függetlenséget kell ellenőrizni. Ha lineárisan összefüggőek lennének, akkor valamelyikük (mondjuk b_k) előállna maradék vektorok lineáris kombinációjaként, de ez ellentmondás, ugyanis b_k nem állna elő egyértelműen, hisz $b_k = 1 \cdot b_k$ egy, az említettől különböző előállítás lenne. □

Def: Az $u \in V$ vektor $B = \{b_1, b_2, \dots, b_n\}$ *bázis szerinti koordinátái* $\alpha_1, \alpha_2, \dots, \alpha_n$, ha $u = \sum_{i=1}^{n} \alpha_i b_i$. Az u B szerinti *koordinátavektora* az $[u]_B := \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$ oszlopvektor.

Def: A V vektortér *dimenziója* a V egy tetszőleges B bázisának elemszáma.

Kicserélési tétel: Ha $F = \{f_1, f_2, \dots, f_n\}$ ftn és $G = \{g_1, g_2, \dots, g_k\}$ generálja V-t, akkor tetszőleges f_i-hez $(i = 1, 2, \dots, n)$ létezik g_j $(j = 1, 2, \dots, k)$ úgy, hogy $F \setminus \{f_i\} \cup \{g_j\}$ független.

Biz: Indirekt bizonyítunk, azaz feltesszük, hogy valamelyik f_i-hez nem létezik g_j. Rögzítsük ezt az f_i-t, és vizsgáljuk meg, mit jelent az, hogy $F \setminus \{f_i\} \cup \{g_j\}$ nem lineárisan független. Mivel $F \setminus \{f_i\}$ lineárisan független, ezért ha $F \setminus \{f_i\} \cup \{g_j\}$ egy nemtriviális lineáris kombinációja $\mathbf{0}$-t ad, akkor g_j együtthatója nemnulla, azaz g_j előállítható az $f \setminus \{f_i\}$-beli vektorok lineáris kombinációjaként. Ez minden g_j vektorra igaz, tehát $g_1, g_2, \dots g_k \in \langle F \setminus \{f_i\}\rangle$. Ekkor azonban a g_j-k által generált vektorokat is generálják az $F \setminus \{f_i\}$-beli vektorok (hiszen a generált altér zárt a műveletekre, így a lineáris kombinációra is), tehát $f_i \in \langle g_1, g_2, \dots g_k\rangle \subset \langle F \setminus \{f_i\}\rangle$, ahol az első reláció a g_j-k generátortulajdonságából adódik. Azt kaptuk, hogy f_i-t generálják a maradék F-beli vektorok, ami ellentmond F függetlenségének. □

Köv.: Ha $f_1, f_2, \dots f_n$ lineárisan függetlenek és a $g_1, g_2, \dots g_k$ vektorok generálják V-t, akkor $n \leq k$.

Biz: A kicserélési tétel által biztosított módon (tehát a függetlenség megtartásával) cseréljük ki sorban az $f_1, f_2, \dots, f_n$ vektorokat egy-egy g_j-re. Az f_n cseréje után egy olyan n vektorból álló, lineárisan

[9] Teljesen hasonlóan definiálható egy $U \subseteq V$ részhalmaz lineáris függetlensége is, de mi megelégszünk a fentivel annak okán, hogy csak olyan vektorterekkel fogunk részletesebben foglalkozni, amikben minden lineárisan független halmaz véges. (Más szóval: a számunkra érdekes vektorterek bármely végtelen halmaza lineárisan összefüggő.)

független rendszert kapunk, amiben minden f_i helyett egy-egy g_j áll. Ha két különböző f_i helyére is ugyanaz a g_j kerül, akkor a kapott rendszer nem lesz független: az egyik g_j-nek 1, a másiknak -1 együtthatót adva (a többit pedig 0-nak választva) egy **0**-t adó nemtriviális, lineáris kombinációt kapnánk. Tehát a becserélt g_j-k mindegyike különböző, így a g_j-k száma legalább akkora, mint az f_i-ké. □

Köv.: Vektortér bármely két bázisa azonos elemszámú. A dimenzió fogalma jóldefiniált.

Biz: Legyenek B_1 és B_2 a V tér bázisai. Mivel B_1 ftn, és B_2 generátorrendszer, ezért az előző következmény miatt $|B_1| \leq |B_2|$. B_2 függetlenségéből és B_1 generátortulajdonságából pedig $|B_2| \leq |B_1|$ adódik, ahonnan az állítás rögtön következik. □

Megjegyzés: Jegyezzük meg, hogy a fent kimondott állítások olyan vektorterekre vonatkoznak, amik *végesen generáltak*, azaz létezik véges generátorrendszerük. Nem minden vektortér ilyen: nem végesen generált pl a valós polinomok vektortere, vagy az azt altérként tartalmazó valós függvények vektortere sem. Bár a nem végesen generált vektorterek matematikája legalább olyan érdekes, mint a végesen generáltaké, mi megelégszünk azzal, hogy a továbbiakban csak az utóbbi típusúakkal foglalkozunk. (Így pl. a bázis mindig egy véges halmazt fog jelenteni.)

Tétel: Ha $F \subseteq V$ ftn és a $G \subseteq V$ halmaz generálja a V (végesen generált) vektorteret, akkor léteznek $F \subseteq B_1$ ill. $B_2 \subseteq G$ bázisok. Más szóval: ha a V vektortér végesen generált, akkor tetszőleges lineárisan független részhalmaz kiterjeszthető a teljes tér egy bázisává, ill. tetszőleges generátorrendszer tartalmaz egy bázist.

Biz: Legyen $G' = \{g_1, g_2, \ldots, g_k\}$ a V vektortér egy véges generátorrendszere! „Hízlaljuk fel" az F halmazt úgy, hogy egyesével megpróbáljuk G' soron következő elemét hozzávenni a már eddig felhízlalt halmazhoz, arra ügyelve, hogy csak akkor vesszük be az aktuális g_j-t, ha a keletkező halmaz ezáltal lineárisan független marad. Legyen B_1 az összes G'-beli ellenőrzése után kapott felhízlalt halmaz. Világos, hogy $F \subseteq B_1$, továbbá, hogy B_1 független. Azt kell csupán igazolni, hogy B_1 generálja V-t. Ez abból következik, hogy B_1 generálja a G' generátorrendszer minden elemét. Ha ugyanis $g_j \in B_1$, akkor ez világos, különben pedig g_j ellenőrzésekor egy ftn rendszerből lineárisan összefüggőt kaptunk g_j hozzávételével, tehát g_j már előállt egyszer az aktuális független halmaz elemeinek lineáris kombinációjaként. Így előáll a kibővített B_1 halmaz elemeinek lineáris kombinációjaként is. Márpedig, ha B_1 a G' minden elemét generálja, akkor minden G' által generált vektort is generál, azaz a teljes vektortér generátorrendszerét kaptuk.

A B_2 bázis előállításához válasszuk ki G egy tetszőleges nemnulla elemét, mondjuk b_1-t. Ha $\langle b_1 \rangle = V$, akkor kész vagyunk, hisz máris találtunk egy bázist. Tegyük fel, hogy G-ből már korábban kiválasztottuk a $b_1, b_2, \ldots, b_l$ lineárisan független elemeket. Ha $\langle b_1, b_2, \ldots, b_l \rangle = V$, akkor kész vagyunk, hisz egy lineárisan független generátorrendszert találtunk. Egyébként $\langle b_1, b_2, \ldots, b_l \rangle \neq V = \langle G \rangle$, tehát létezik G-nek olyan eleme (mondjuk b_{l+1}), ami nem áll elő a $b_1, b_2, \ldots b_l$ elemek lineáris kombinációjaként. A lineáris függetlenségre korábban bizonyított összefüggés alapján ekkor $b_1, b_2, \ldots, b_l, b_{l+1}$ is lineárisan független lesz. Mivel G' a V tér egy k-elemű generátorrendszere, minden lineárisan független rendszer legfeljebb k-elemű lehet, tehát a fenti bővítést legfeljebb k-szor tudjuk megtenni. Eszerint legkésőbb a k-dik lépésben a b_i vektorok generálják a teljes V teret, azaz megkaptunk egy $B_2 \subseteq G$ bázist. □

Állítás: (1) $U \leq V \Rightarrow \dim U \leq \dim V$. (2) Az alábbi 5 állítás ekvivalens.
(a) $\dim V = n \iff$ (b) $\exists n$-elemű ftn, és minden n-elemű ftn bázis $\iff$ (c) $\exists n$-elemű generárorrsz., és minden n-elemű gen.rsz. bázis $\iff$ (d) $\exists n$-elemű ftn, és bármely $(n+1)$ vektor öf $\iff$ (e) $\exists n$-elemű gen.rsz., és $\nexists (n-1)$ elemű gen.rsz.

Biz: (1): Legyen B az U altér egy bázisa. Mivel B független V-ben, ezért B kiegészíthető V bázisává, tehát V bázisának legalább annyi eleme van, mint U-énak.

(2): (a) $\Rightarrow$ (b): Ha $\dim V = n$, akkor létezik n-elemű bázis, ami egy n-elemű lineárisan ftn generátorrendszer. Létezik tehát n-elemű ftn. Ha F egy n-elemű független, akkor az létezik F-t tartalmazó bázis, de a bázisok elemszámának egyenlősége miatt ez csak F lehet.

(b) $\Rightarrow$ (c): Létezik n-elemű független, így minden generátorrendszer legalább n-elemű. Mivel létezik n-elemű bázis, ezért ha G egy n-elemű generátorrendszer, akkor bármely G által tartalmazott bázis is n-elemű, tehát az csakis G lehet.

(c) $\Rightarrow$ (d): Létezik n-elemű generátorrendszer, ezért nem létezhet legalább $(n+1)$-elemű független. Azt is tudjuk, hogy létezik n-elemű bázis, ami egyúttal egy n-elemű ftn.

(d) $\Rightarrow$ (e): Mivel van n-elemű független, minden generátorrendszer is legalább n-elemű. Ha pedig G egy generátorrendszer, akkor az általa tartalmazott bázis nem lehet legalább $(n+1)$-elemű, hisz bármely $n+1$ elem öf.

(e) $\Rightarrow$ (a): A vektortér dimenziója nem más, mint egy olyan generátorrendszerének elemszáma, amely generátorrendszer nem tartalmaz valódi részhalmazként generátorrendszert. Az (e) feltétel szerint ez csakis n lehet. □

4. Lineáris leképezések

Def: Az U, V valós vektorterek között ható $\mathcal{A} : U \to V$ függvény egy *lineáris leképezés*, ha
(1) $\mathcal{A}(u+v) = \mathcal{A}(u) + \mathcal{A}(v) \quad \forall u, v \in U$ ill. (2) $\mathcal{A}(\lambda u) = \lambda \mathcal{A}(u) \quad \forall \lambda \in T, \ \forall u \in U$ teljesül.
Lineárisnak tehát a művelettartó leképezést nevezzük. Könnyen látható, hogy az (1,2) tulajdonságok helyett megkívánhatnánk az alábbi tulajdonságot:
(3) $\mathcal{A}(\lambda u + \mu v) = \lambda \mathcal{A}(u) + \mu \mathcal{A}(v) \quad \forall u, v \in V, \forall \lambda, \mu \in \mathbb{R}$. Ha ugyanis $\mathcal{A}$ lineáris, akkor $\mathcal{A}(\lambda u + \mu v) = \mathcal{A}(\lambda u) + \mathcal{A}(\mu v) = \lambda \mathcal{A}(u) + \mu \mathcal{A}(v)$. Másrészt ha (3) fenáll, akkor $\lambda = \mu = 1$ esetén (1), míg $\mu = 0$ helyettesítéssel (2) következik.

Azt is egyszerűen (n szerinti indukcióval) adódik, hogy (3) ekvivalens a formálisan többet kívánó
(3') $\mathcal{A}(\sum_{i=1}^n \lambda_i v_i) = \sum_{i=1}^n \lambda_i \mathcal{A}(v_i) \quad \forall n \in \mathbb{N}, \forall v_1, v_2, \dots, v_n \in V, \forall \lambda_1, \lambda_2, \dots, \lambda_n \in \mathbb{R}$
feltétellel. Eszerint a lineáris leképezés nem más, mint olyan leképezés, ami tetszőleges lineáris kombinációt a képek ugyanolyan együtthatós lineáris kombinációjába képez. Az U és V közötti lineáris leképezések halmazát $\mathrm{Hom}(U, V)$ jelöli. Az $\mathcal{A} : V \to V$ (azonos terek között ható) lineáris leképezést *lineáris transzformáció*nak hívjuk.

Példa: (1) A síkvektorokon az x tengelyre vetítés,
(2) a síkvektorokon az origó körüli (nyújtva)forgatás,
(3) a síkvektoroknak egy origón átmenő egyenesre tükrözése,
(4) a 2×2-es mátrixokhoz 2×3-as mátrixok hozzárendelése $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} b & 0 & 2c-a \\ d & d & 3d \end{pmatrix}$ szerint,
(5) A polinomok vektorterén a deriválás, azaz $p(x) \mapsto p'(x)$. A művelettartás a deriválás azonosságai miatt igaz: $(p+q)'(x) = p'(x) + q'(x)$, ill. $(\lambda p)'(x) = \lambda p'(x)$.

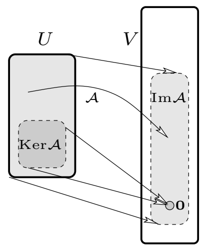
Állítás: A lineáris leképezés egyértelműen meghatározható a báziselemek képeinek megválasztásával. Pontosabban: Ha U és V valós vektorterek, az $u_1, u_2, \dots, u_n$ vektorok az U bázisát alkotják és $v_1, v_2, \dots, v_n$ tetszőleges, V-beli vektorok, akkor pontosan egy olyan $\mathcal{A} \in \mathrm{Hom}(U, V)$ lineáris leképezés létezik, amire $\mathcal{A}(u_i) = v_i \quad \forall i$.

Megjegyzés: A fenti állítás egyik haszna, hogy segítségével könnyen meg tudunk adni egy lineáris leképezést (t.i. egy tetszőleges bázis vektorainak képét kijelölve), és ez remekül jön, ha valamilyen speciális tulajdonságot kielégítő lineáris leképezést kell konstruálnunk például a zh-ban.

Biz: Tegyük fel, hogy létezik a kívánt lineáris leképezés, megmutatjuk, hogy egyértelmű. Legyen ugyanis $u \in U$ tetszőleges vektor. Ekkor u egyértelműen áll elő az U adott bázisának lineáris kombinációjaként, mondjuk $u = \sum_{i=1}^n \lambda_i u_i$ alakban. Ekkor $\mathcal{A}$ feltételezett linearitása miatt $\mathcal{A}(u) = \mathcal{A}(\sum_{i=1}^n \lambda_i u_i) = \sum_{i=1}^n \lambda_i \mathcal{A}(u_i) = \sum_{i=1}^n \lambda_i v_i$, tehát (ha $\mathcal{A}$ valóban létezik, akkor) $\mathcal{A}(u)$ egyértelműen meghatározott.

Csupán azt kell ezek után bebizonyítani, hogy az imént definiált $\mathcal{A}$ leképezés lineáris, azaz művelettartó. Legyen mondjuk $u = \sum_{i=1}^n \lambda_i u_i$, $v = \sum_{i=1}^n \mu_i u_i$ és $\lambda \in \mathbb{R}$. Az összeadásra az adódik, hogy
$\mathcal{A}(u+v) = \mathcal{A}(\sum_{i=1}^n \lambda_i u_i + \sum_{i=1}^n \mu_i u_i) = \mathcal{A}(\sum_{i=1}^n \lambda_i u_i + \mu_i u_i) = \mathcal{A}(\sum_{i=1}^n (\lambda_i + \mu_i) u_i) =$ [10] $\sum_{i=1}^n (\lambda_i + \mu_i) v_i = \sum_{i=1}^n \lambda_i v_i + \mu_i v_i = \sum_{i=1}^n \lambda_i v_i + \sum_{i=1}^n \mu_i v_i =^1 0\mathcal{A}(u) + \mathcal{A}(v)$,
ill. $\mathcal{A}(\lambda\, u) = \mathcal{A}(\lambda \sum_{i=1}^n \lambda_i u_i) = \mathcal{A}(\sum_{i=1}^n \lambda \lambda_i u_i) =$ [10] $\sum_{i=1}^n \lambda \lambda_i v_i = \lambda \sum_{i=1}^n \lambda_i v_i = \lambda \mathcal{A}(u)$. □

Def: Az $\mathcal{A} : U \to V$ lineáris leképezés *magtere* $\mathrm{Ker}\mathcal{A} := \{u \in U : \mathcal{A}(u) = \mathbf{0}\}$, *képtere* pedig $\mathrm{Im}\mathcal{A} := \{\mathcal{A}(u) : u \in U\}$.
Szavakban: a magtér mindazon U-beli vektorokból áll, amik a V tér nullvektorába képződnek, a képtér pedig a V tér mindazon elemeinek halmaza, amik előállnak valamely U-beli vektor képeként. (Ld. az ábrát.)



Példa: A lineáris leképezésre adott korábbi példákban (1) az x tengelyre vetítésnél a képtér az x, a magtér az y tengely, (2-3) az origó körüli (nyújtva)forgatás ill. origón áthaladó tengelyre tükrözéskor a képtér a teljes sík, a magtér pedig egyedül az origót tartalmazza.

A (4)-beli 2×2-es mátrixok leképezésekor rendre az $\begin{pmatrix} x & 0 & y \\ z & z & 3z \end{pmatrix}$ ill. a $\begin{pmatrix} 2x & 0 \\ x & 0 \end{pmatrix}$ alakú mátrixok alkotják a képteret ill. a magteret.

Az (5) deriválás esetén a képtér az összes valós polinom halmaza (hisz minden polinomnak van primitív függvénye, ami polinom), a magtér pedig a konstans polinomok halmaza.

Állítás: Ha $\mathcal{A} \in \mathrm{Hom}(U, V)$, akkor $\mathrm{Ker}\mathcal{A} \leq U$ és $\mathrm{Im}\mathcal{A} \leq V$, tehát a magtér ill. képtér nevükhöz méltóan egyaránt alterek.

Biz: Elegendő azt igazolni, hogy mindkét halmaz zárt a műveletekre. A magtér esetén, ha $u, v \in \mathrm{Ker}\mathcal{A}$ és $\lambda \in \mathbb{R}$, akkor $\mathcal{A}(u+v) = \mathcal{A}(u) + \mathcal{A}(v) = \mathbf{0} + \mathbf{0} = \mathbf{0}$, azaz $u + v \in \mathrm{Ker}\mathcal{A}$, ill. $\mathcal{A}(\lambda u) = \lambda \mathcal{A}(u) = \lambda \mathbf{0} = \mathbf{0}$, tehát $\lambda u \in \mathrm{Ker}\mathcal{A}$. A képtérre pedig tetszőleges $\mathcal{A}(u), \mathcal{A}(v) \in \mathrm{Im}\mathcal{A}$ és $\lambda \in \mathbb{R}$ mellett $\mathcal{A}(u) + \mathcal{A}(v) = \mathcal{A}(u+v) \in \mathrm{Im}\mathcal{A}$, ill. $\lambda \mathcal{A}(u) = \mathcal{A}(\lambda u) \in \mathrm{Im}\mathcal{A}$ adódik. □

Dimenziótétel: Ha $\mathcal{A} : U \to V$ lin. lekép., akkor $\dim \mathrm{Ker}\mathcal{A} + \dim \mathrm{Im}\mathcal{A} = \dim U$.

Biz: Legyen $B' := \{b_1, b_2, \dots, b_k\}$ a $\mathrm{Ker}\mathcal{A}$ vektortér egy bázisa. Mivel B' független az U vektortérben, ezért létezik U-nak egy B'-t tartalmazó bázisa, mondjuk $B = \{b_1, b_2, \dots, b_k, b_{k+1}, \dots, b_n\}$. Világos, hogy $\dim \mathrm{Ker}\mathcal{A} = k$ és $\dim U = n$, így azt kell csupán igazolni, hogy $\dim \mathrm{Im}\mathcal{A} = n - k$. Ezt úgy bizonyítjuk, hogy megmutatjuk, hogy az $\mathcal{A}(b_{k+1}), \mathcal{A}(b_{k+2}), \dots, \mathcal{A}(b_n)$ vektorok az $\mathrm{Im}\mathcal{A}$ tér egy bázisa. Azt kell tehát igazolunk, hogy az említett vektorok generálnak minden $\mathrm{Im}\mathcal{A}$-beli vektort, ráadásul függetlenek. Legyen tehát $\mathcal{A}(u)$ a képtér egy tetszőleges vektora. Legyen az $u = \sum_{i=1}^n \lambda_i b_i$ az u előállítása a B bázisban. Ekkor $\mathcal{A}(u) = \mathcal{A}(\sum_{i=1}^n \lambda_i b_i) = \sum_{i=1}^n \lambda_i \mathcal{A}(b_i) = \sum_{i=k+1}^n \lambda_i \mathcal{A}(b_i)$, hiszen $\mathcal{A}(b_1) = \mathcal{A}(b_2) = \ldots = \mathcal{A}(b_k) = \mathbf{0}$, tehát valóban generátorrendszerrel van dolgunk. A lineáris függetlenséghez tegyük fel, hogy a $\mathbf{0}$ előáll

[10] Itt használjuk, hogy $\mathcal{A}$-t hogyan definiáltuk a bázis lineáris kombinációin.

lineáris kombinációként: $\mathbf{0} = \sum_{i=k+1}^{n} \lambda_i \mathcal{A}(b_i) = \mathcal{A}(\sum_{i=k+1}^{n} \lambda_i b_i)$, tehát $u := \sum_{i=k+1}^{n} \lambda_i b_i \in \mathrm{Ker}\mathcal{A}$. De ekkor az u vektor felírható a B' bázisban, azaz a $b_1, b_2, \ldots b_k$ vektorok lineáris kombinációjaként is: $u = \sum_{i=1}^{k} \mu_i b_i = \sum_{i=k+1}^{n} \lambda_i b_i$, ahonnan $\mathbf{0} = \sum_{i=1}^{k}(-\mu_i) b_i + \sum_{i=k+1}^{n} \lambda_i b_i$, ami a B bázis lineáris függetlensége miatt csakis triviális lineáris kombináció lehet. Eszerint $\lambda_{k+1} = \lambda_{k+2} = \ldots = \lambda_n = 0$, azaz a kiindulási lineáris kombináció is triviális volt, a szóbanforgó rendszer valóban független, így csakugyan az $\mathrm{Im}\mathcal{A}$ tér bázisa. □

Def: Az $\mathcal{A} : U \to V$ leképezés *izomorfizmus* ha lineáris (azaz $\mathcal{A} \in \mathrm{Hom}(U, V)$) és bijekció (azaz kölcsönösen egyértelmű). A $\mathbb{R}$ feletti U és V vektorterek *izomorfak*, ha létezik köztük izomorfizmus. Jelölése: $U \cong V$.

Állítás: (1) Az $\mathcal{A} : U \to V$ lin. lekép. (izomorfizmus) $\iff$ $\mathrm{Ker}\mathcal{A} = \{\mathbf{0}\}$ és $\mathrm{Im}\mathcal{A} = V$.
(2) Ha $\dim V = n$, akkor $V \cong \mathbb{R}^n$. (3) Ha U, V $\mathbb{R}$ feletti, végesen generált, valós vektorterek, akkor $\dim U = \dim V \iff U \cong V$.

Biz: (1): $\Rightarrow$: Ha $\mathcal{A}$ izomorfizmus, akkor bijekció, így $\mathrm{Im}\mathcal{A} = V$, és a dimenziótétel miatt $\dim \mathrm{Ker}\mathcal{A} = 0$, ahonnan $\mathrm{Ker}\mathcal{A} = \{\mathbf{0}\}$.

$\Leftarrow$: A kölcsönös egyértelműséget kell igazolni. Minden elem előáll képként, hisz $\mathrm{Im}\mathcal{A} = V$. Ha $\mathcal{A}(u) = \mathcal{A}(v)$, akkor $\mathbf{0} = \mathcal{A}(u) - \mathcal{A}(v) = \mathcal{A}(u - v)$, azaz $u - v \in \mathrm{Ker}\mathcal{A}$, tehát $\mathbf{0} = u - v$, vagyis $u = v$. Azt kaptuk, hogy $\mathcal{A}$ csakugyan kölcsönösen egyértelmű.

(2): Legyen B a V vektortér egy (n-elemű) bázisa. Könnyen látható, hogy ha minden V-beli vektornak megfeleltetjük a koordinátavektorát (sorvektorként felírva), akkor egy bijektív lineáris leképezést kapunk $\mathbb{R}^n$-be, és ez bizonyítja az izomorfiát.

(3): (2) alapján $U \cong \mathbb{R}^n \cong V$, ami azt jelenti, hogy $U \cong V$. □

4.1. Lineáris leképezések mátrixai

A lineáris leképezések tanulmányozásának fontos eszköze a hozzájuk rendelt mátrixok vizsgálata.

Def: Legyen $\mathcal{A} \in \mathrm{Hom}(U, V)$ lineáris leképezés, $B_1 = \{u_1, u_2, \ldots, u_n\}$ az U, $B_2 = \{v_1, v_2, \ldots, v_m\}$ pedig a V bázisa. Az $\mathcal{A}$ *leképezés mátrixát* a B_1 és B_2 bázisokban az alábbi módon írjuk fel: $[\mathcal{A}]_{B_2}^{B_1} := ([\mathcal{A}(u_1)]_{B_2} | [\mathcal{A}(u_2)]_{B_2} | \cdots | [\mathcal{A}(u_n)]_{B_2})$, azaz egy olyan $m \times n$-es mátrixról van szó, aminek i-dik oszlopa az u_i bázisvektor $\mathcal{A}(u_i)$ képének koordinátavektora. Másképpen kifejezve, ha u_i képe $\mathcal{A}(u_i) = \sum_{j=1}^{m} \lambda_j^i v_j$ alakban áll elő a B_2 bázisban, akkor az $[\mathcal{A}]_{B_2}^{B_1}$ mátrix j-dik sorának i-dik eleme λ_j^i lesz.

Nézzük meg, hogyan kaphatjuk meg a leképezés mátrixának ismeretében egy u vektor koordinátavektorából az $\mathcal{A}(u)$ vektor koordinátavektorát. (Értelemszerűen a B_1 ill. B_2 bázisban felírt koordinátavektorokról beszélünk.) Meg kell határoznunk tehát, hogy egy $u = \sum_{i=1}^{n} \mu_i u_i$ vektor képét hogyan írhatjuk fel a $v_1, \ldots v_m$ bázisban. Hát lássuk:
$\mathcal{A}(u) = \mathcal{A}(\sum_{i=1}^{n} \mu_i u_i) = \sum_{i=1}^{n} \mu_i A(u_i) = \sum_{i=1}^{n} \mu_i (\sum_{j=1}^{m} \lambda_j^i v_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} \mu_i (\lambda_j^i v_j) = \sum_{j=1}^{m} \sum_{i=1}^{n} \mu_i \lambda_j^i v_j = \sum_{j=1}^{m} v_j \sum_{i=1}^{n} \mu_i \lambda_j^i = \sum_{j=1}^{m} (\sum_{i=1}^{n} \mu_i \lambda_j^i) v_j$, tehát a keresett koordinátavektor egy olyan, m-elemű oszlopvektor, aminek j-dik koordinátája $\sum_{i=1}^{n} \mu_i \lambda_j^i$. Ez motiválja a mátrix és oszlopvektor szorzatának definícióját.

Def: Ha $A = (\lambda_j^i)$ egy $m \times n$ méretű mátrix (azaz A j-dik sorának i-dik eleme λ_j^i), és $\underline{u} = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}$ egy m-méretű oszlopvektor, akkor az A mátrix összeszorozható az $\underline{u}$ vektorral, a szorzat egy m-méretű oszlopvektor, aminek j-dik eleme éppen $\sum_{i=1}^{n} \lambda_j^i \mu_i$. Vegyük észre, hogy ez a j-dik elem nem más, mint az A mátrix j-dik sorának és az $\underline{u}$ oszlopvektornak a skaláris szorzata, azaz $A_j \cdot \underline{u}$. Ezt a tulajdonságot szokás a sor-oszlop szorzás kifejezéssel illetni, amin azt értjük, hogy a szorzat egyes koordinátáit úgy kapjuk, hogy a megfelelő sorvektort skalárisan összeszorozzuk a megfelelő oszlopvektorral.

Megjegyzés: Szokás a fenti definíciót a kalapból előhúzni, és megfigyelni, hogy milyen pompásan alkalmazható a lineáris leképezések esetén. A mi felépítésünkben maga a definíció származott abból, hogy megfigyeltük, hogyan kapjuk meg a kép koordinátavektorát az eredeti vektor koordinátavektorából. Az alábbi állítás tehát következik a definíció előtt elhangzottakból.

Állítás: $\mathcal{A} \in \mathrm{Hom}(U, V)$, $B_1 \subseteq U$ és $B_2 \subseteq V$ bázisok $\Rightarrow$ $[\mathcal{A}(u)]_{B_2} = [\mathcal{A}]_{B_2}^{B_1} [u]_{B_1}$ $\forall u \in U$. (Tehát, ha a lineáris leképezés mátrixát megszorozzuk egy u vektor koordinátavektorával, akkor u képének koordinátavektorát kapjuk.)

Megjegyzés: A fenti tétel lényege, hogy ha rögzítjük az U és V terek egy-egy bázisát (és ezáltal e vektorterek vektorait azonosíthatjuk a koordinátavektoraikkal), akkor a lineáris leképezésekre gondolhatunk úgy is, mint $(\dim V \times \dim U)$ méretű mátrixokra, magára a lineáris leképezésre pedig, mint a megfelelő mátrixszal való szorzásra.

A lineáris leképezések $\mathrm{Hom}(U, V)$ halmazán műveleteket is értelmezhetünk.

Def: $\mathcal{A}, \mathcal{B} \in \mathrm{Hom}(U, V)$ és $\lambda \in \mathbb{R}$-re $(\mathcal{A}+\mathcal{B})(u) := \mathcal{A}(u)+\mathcal{B}(u)$ ill. $(\lambda\mathcal{A})(u) := \lambda(\mathcal{A}(u))$ definiálja az $\mathcal{A}+\mathcal{B}, \lambda\mathcal{A}$ leképezéseket.

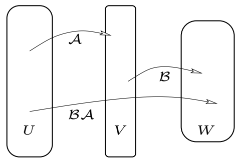
Megfigyelés: Ha $\mathcal{A}, \mathcal{B} \in \mathrm{Hom}(U, V)$ és $\lambda \in \mathbb{R}$, akkor $\mathcal{A}+\mathcal{B}, \lambda\mathcal{A} \in \mathrm{Hom}(U, V)$, azaz lineáris leképezések összege és skalárszorosa is lineáris leképezés. E műveletekkel $\mathrm{Hom}(U, V)$ szintén valós vektortér, és ez a vektortér izomorf a $\dim V \times \dim U$ méretű valós mátrixok alkotta vektortérrel. Konkrétan, $\mathcal{A}+\mathcal{B}$ mátrixa $[\mathcal{A}]_{B_2}^{B_1} + [\mathcal{B}]_{B_2}^{B_1}$, $\lambda\mathcal{A}$ mátrixa pedig $\lambda[\mathcal{A}]_{B_2}^{B_1}$ lesz, ahol B_1 az U és B_2 pedig a V egy bázisa. (Tehát összegleképezés mátrixa a megfelelő mátrixok összege, skalárszoros leképezésé pedig a mátrix skalárszorosa lesz.)

Biz: $(\mathcal{A}+\mathcal{B})(u+v) = \mathcal{A}(u+v)+\mathcal{B}(u+v) = \mathcal{A}(u)+\mathcal{A}(v)+\mathcal{B}(u)+\mathcal{B}(v) = (\mathcal{A}(u)+\mathcal{B}(u))+(\mathcal{A}(v)+\mathcal{B}(v)) = (\mathcal{A}+\mathcal{B})(u)+(\mathcal{A}+\mathcal{B})(v)$, ill. $(\lambda\mathcal{A})(\kappa u) = \lambda(\mathcal{A}(\kappa)u) = \lambda(\kappa\mathcal{A}(u)) = \kappa(\lambda(\mathcal{A}(u))) = \kappa(\lambda\mathcal{A}(u))$, tehát $\mathcal{A}+\mathcal{B}, \lambda\mathcal{A} \in \mathrm{Hom}(U, V)$.

Rögzítsük az U ill. a V tér B_1 ill. B_2 bázisát. A leképezésmátrix definíciója szerint $\mathcal{A}+\mathcal{B}$ mátrixának i-dik oszlopa a B_1 bázis i-dik vektora $(\mathcal{A}+\mathcal{B})(b_i)$ képének koordinátavektora lesz, ám $(\mathcal{A}+\mathcal{B})(b_i) = \mathcal{A}(b_i)+\mathcal{B}(b_i)$ miatt ez nem más, mint a $[\mathcal{A}]_{B_2}^{B_1}$ mátrix i-dik oszlopának és a $[B]_{B_2}^{B_1}$ mátrix i-dik oszlopának összege. A skalárral való szorzásra vonatkozó bizonyítást az olvasóra bízzuk. Ezek szerint a lineáris leképezések mátrixos felírása valóban megadja a mátrixok vektorterével való izomorfiát. $\square$

A fentieken túl értelmezhető lineáris leképezések szorzata is.

Def: $\mathcal{A} \in \mathrm{Hom}(U, V)$, $\mathcal{B} \in \mathrm{Hom}(V, W)$ esetén a $\mathcal{BA} : U \to W$ leképezést a $(\mathcal{BA})(u) := \mathcal{B}(\mathcal{A}(u))$ $(\forall\, u \in U)$ képlettel értelmezzük. (Azaz két lineáris leképezést úgy szorzunk össze, hogy egymás után alkalmazzuk azokat. (Szükséges persze, hogy az elsőnek alkalmazott leképezés képtere benne legyen a másodiknak alkalmazott értelmezési tartományában.))



Megfigyelés: Ha $\mathcal{A} \in \mathrm{Hom}(U, V)$ és $\mathcal{B} \in \mathrm{Hom}(V, W)$, akkor $\mathcal{BA} \in \mathrm{Hom}(U, W)$, azaz lineáris leképezések szorzata is lineáris leképezés.

Biz: Ha $u, v \in U$ és $\lambda \in \mathbb{R}$, akkor $(\mathcal{BA})(u+v) = \mathcal{B}(\mathcal{A}(u+v)) = \mathcal{B}(\mathcal{A}(u)+\mathcal{A}(v)) = \mathcal{B}(\mathcal{A}(u))+\mathcal{B}(\mathcal{A}(v)) = (\mathcal{BA})(u) + (\mathcal{BA})(v)$, ill. $(\mathcal{BA})(\lambda u) = \mathcal{B}(\mathcal{A}(\lambda u)) = \mathcal{B}(\lambda\mathcal{A}(u)) = \lambda\mathcal{B}(\mathcal{A}(u)) = \lambda(\mathcal{BA})(u)$. $\square$

Vizsgáljuk meg, mi is lesz a fenti megfigyelésben szereplő $\mathcal{BA}$ leképezés mátrixa. Rögzítsük ezért rendre az U, V ill. W terek egy-egy bázisát: B_1-t, B_2-t ill. B_3-at. Vizsgáljuk meg, mi lesz a $[\mathcal{BA}]_{B_3}^{B_1}$ mátrixnak (mondjuk) a j-dik oszlopa, azaz, mi lesz a B_1 bázisbeli b_j vektor képének (azaz a $(\mathcal{BA})(b_j) = \mathcal{B}(\mathcal{A}(b_j))$ vektornak) a B_3 bázis szerinti koordinátavektora! A leképezés mátrixáról korábban tanultakat a $\mathcal{B}$ leképezésre alkalmazva az adódik, hogy a kérdéses oszlopot úgy kapjuk, hogy a $\mathcal{B}$ leképezésnek a B_2 és B_3 bázisokban felírt $[\mathcal{B}]_{B_3}^{B_2}$ mátrixát megszorozzuk a b_j vektor $\mathcal{A}$ leképezés szerinti $\mathcal{A}(b_j)$ képének B_2 bázis szerinti koordinátavektorával (azaz az $[\mathcal{A}(b_j)]_{B_2}$ oszlopvektorral). Ám vegyük észre, hogy $\mathcal{A}(b_j)$ definíció szerint nem más, mint az $[\mathcal{A}]_{B_2}^{B_1}$ mátrix j-dik oszlopvektora. Eszerint a keresett $[\mathcal{BA}]_{B_3}^{B_1}$ mátrix j-dik oszlopa éppen a $[\mathcal{B}]_{B_3}^{B_2}$ mátrixnak és az $[\mathcal{A}]_{B_2}^{B_1}$ mátrix j-dik oszlopának szorzata. Ha pedig konrétan a j-dik oszlop i-dik elemére vagyunk kíváncsiak, akkor ezt a fentiek szerint úgy kaphatjuk meg, mint a $[\mathcal{B}]_{B_3}^{B_2}$ mátrix i-dik sorának és az $[\mathcal{A}]_{B_2}^{B_1}$ mátrix j-dik oszlopának szorzata. Ez motiválja a mátrixszorzás definícióját.

Def: Legyenek $B \in \mathbb{R}^{n\times k}$ és $A \in \mathbb{R}^{k\times l}$ tetszőleges mátrixok. Ekkor (vagyis ha B-nek pontosan annyi oszlopa van, mint ahány sora A-nak) a B és A mátrixok összeszorozhatóak, $B \cdot A \in \mathbb{R}^{n\times l}$, és $(B \cdot A)_i^j = B_i \cdot A^j$, azaz a szorzatmátrix i-dik sorának j-dik elemét úgy kapjuk, hogy a B mátrix i-dik sorát (mint sorvektort) skalárisan összeszorozzuk a A mátrix j-dik oszlopával (mint oszlopvektorral).

A fenti definíciót éppen az motiválta, hogy két lineáris leképezés szorzatának mátrixát írja le, tehát a fenti gondolatmenet alapján a következőt igazoltuk.

Állítás: Ha $\mathcal{A} \in \mathrm{Hom}(U, V)$, $\mathcal{B} \in \mathrm{Hom}(V, W)$ és B_1, B_2 ill. B_3 rendre az U, V ill. W terek egy-egy bázisai, akkor $[\mathcal{BA}]_{B_3}^{B_1} = [\mathcal{B}]_{B_3}^{B_2} \cdot [\mathcal{A}]_{B_2}^{B_1}$, azaz lineáris leképezések szorzatának mátrixa azonos a leképezések mátrixainak szorzatával (egyező bázisok esetén). $\square$

Köv.: Ha $C \in \mathbb{R}^{m\times n}$, $B \in \mathbb{R}^{n\times k}$ és $A \in \mathbb{R}^{k\times l}$ tetszőleges mátrixok, akkor $(C \cdot B) \cdot A = C \cdot (B \cdot A)$, azaz a mátrixszorzás asszociatív (feltéve, hogy a műveletek elvégezhetőek).

Biz: A megfelelő mátrixokat tekinthetjük egy-egy lineáris leképezésnek, nevezetesen $C \in \mathrm{Hom}(\mathbb{R}^n, \mathbb{R}^m)$, $B \in \mathrm{Hom}(\mathbb{R}^k, \mathbb{R}^n)$ ill. $A \in \mathrm{Hom}(\mathbb{R}^l, \mathbb{R}^k)$, és ekkor $(C \cdot B) \cdot A$ a annak a lineáris leképezésnek lesz a mátrixa, amit az $u \mapsto (CB)(A(u))$ formula definiál tetszőleges $u \in \mathbb{R}^n$ esetén, míg a $C \cdot (B \cdot A)$ mátrix annak a lineáris leképezésnek lesz a mátrixa, amit az $u \mapsto C(BA)(u)))$ formula ad meg. Mivel $(A, B, C$-t most lineáris leképezéseknek gondolva) $(CB)(A(u)) = C(B(A(u))) = C((BA)(u))$, ezért a két fenti lineáris leképezés azonos, így (az ugyanazon bázisokban felírt) mátrixaik sem különbözhetnek. $\square$

5. Permutációk, determinánsok

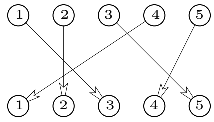
5.1. Permutációk, inverziószám

Def: Jelölje $[n]$ az $\{1, 2, \ldots, n\}$ halmazt. A $\sigma : [n] \to [n]$ bijektív (azaz kölcsönösen egyértelmű) leképezés neve *permutáció*. Az $[n]$ permutációinak halmazát S_n jelöli.

Megjegyzés: A permutáció a definíció szerint egy olyan függvény, ami az 1 és n közötti számok mindegyikéhez egy 1 és n közötti számot rendel úgy, hogy minden 1 és n közötti szám pontosan egy másik számhoz van hozzárendelve. Szokásos a permutációt egy $2 \times n$ méretű táblázat segítségével megadni:

az első sorban vannak 1-től n-ig a számok, és minden szám alatt az a szám áll, amit a permutáció hozzárendel.

Szemléltethetjük a permutációt úgy is, hogy felveszünk egymás alatt két sorban $n - n$ db pettyet, mindkét sorban megszámozzuk a pettyeket 1-től n-ig (balról jobbra), és nyilat vezetünk a felső sorban levő i-dik pettyből az alsó sor j-dik pettyébe, ha $\sigma(i) = j$.



Egy ilyen ábra akkor „kódol” permutációt, ha minden felső pontból pontosan egy nyíl indul, és minden alsó pontba pontosan egy nyíl érkezik. (Az ábra pl. a $\sigma(1) = 3, \sigma(2) = 2, \sigma(3) = 5, \sigma(4) = 1, \sigma(5) = 4$ permutáció diagramja.)

Def: Ha $\sigma \in S_n$, akkor a σ permutációból a $k, l \in [n]$ elemek cseréjével keletkező permutációt $\sigma_{k,l}$ jelöli, azaz $\sigma_{k,l}(i) = \sigma(i)$, ha $k \neq i \neq l$, $\sigma_{k,l}(l) = \sigma(k)$, és $\sigma_{k,l}(k) = \sigma(l)$. (A permutáció diagramján a k-ból és l-ből induló nyilakat kell úgy átirányítani, hogy végpontjaikat felcseréljük.)
A $\sigma \in S_n$ permutáció inverze az a $\sigma^{-1} \in S_n$ permutáció, amire $\sigma^{-1}(i) = j \iff \sigma(j) = i$. (A diagramon a nyilak irányát meg kell fordítani, és az egész ábrát a feje tetejére kell állítani.)
A k, l elemek *inverzióban állnak* $\sigma \in S_n$ szerint, ha k, l ill. $\sigma(k), \sigma(l)$ nagyságviszonya fordított. A σ permutáció $I(\sigma)$ *inverziószáma* a $\sigma \in S_n$ szerint inverzióban álló számpárok száma. Egy $\sigma \in S_n$ permutáció *páros*, ha $I(\sigma)$ páros, és *páratlan*, ha $I(\sigma)$ páratlan.

Megfigyelés: Az a tény, hogy két elem inverzióban áll a σ permutáció szerint, könnyen megállapítható a σ diagramjáról. Nevezetesen, i és j pontosan akkor áll inverzióban, ha az i-ből és j-ből induló élek metszik egymást. (Ha ugyanis nem metszik egymást, akkor a nagyobbik számhoz a permutáció nagyobbat rendel, ha pedig metszik, akkor a nagyobbhoz rendelt szám kisebb lesz, mint a kisebbhez rendelt.) Ezért a σ permutáció diagramjáról könnyen leolvasható az $I(\sigma)$ inverziószám, ami nem más, mint a diagramban található nyilak páronkénti metszéspontjainak száma[11].

Tétel: Tetszőleges $\sigma \in S_n$ permutációra $I(\sigma) = I(\sigma^{-1})$, továbbá, ha $k, l \in [n]$ különbözőek, akkor a σ és $\sigma_{k,l}$ permutációk különböző paritásúak.

Biz: Láttuk, hogy σ^{-1} diagramját úgy kapjuk, hogy a σ diagramját a feje tetejére állítjuk, és a nyilak irányát megfordítjuk. Világos, hogy ettől a páronkénti metszéspontok száma nem változik, azaz $I(\sigma) = I(\sigma^{-1})$.

Ha a diagramon a k-ból és l-ből induló nyilak végpontjait felcseréljük, akkor könnyen látható, hogy minden olyan nyílon, amit nem bántottunk, a metszéspontok száma 0-val vagy 2-vel, azaz mindenképpen páros számmal változik. Tehát itt a metszéspontok számának változása összességében is páros. Azt kell még megfigyelni, hogy a k-ból és l-ből induló eredeti nyilak és módosított nyilak közül pontosan egy pár lesz metsző. Eszerint a páronkénti metszéspontok számának különbsége a két diagramon páratlan, azaz σ és $\sigma_{k,l}$ ellentétes paritásúak. □

5.2. Determinánsok

Ebben részben definiálunk egy mennyiséget négyzetes mátrixokra, amit számos helyen tudunk majd haszonnal alkalmazni a továbbiakban. Legyen tehát $A = (a_{i,j})$ egy $n \times n$ méretű mátrix, és tegyük fel, hogy elemein értelmezett az összeadás és a szorzás, amik kommutatív műveletek. Az A mátrix *determinánsán* az alábbi szorzatösszeget értjük:

$$\det(A) := |A| := \sum_{\sigma \in S_n} (-1)^{I(\sigma)} \prod_{i=1}^{n} a_{i,\sigma(i)}$$

Tehát annyi szorzatot adunk össze, ahány permutációja van az $1, 2, \ldots, n$ számoknak. Egy ilyen szorzatban az adott permutáció inverziószámának paritása határozza meg az előjelet, a szorzat további tényezői pedig a mátrix bizonyos elemei. Világos, hogy minden sorból egy elemet választunk a szorzatba, és a permutáció kölcsönösen egyértelmű leképezés volta miatt az sem történhet meg, hogy $\sigma(i) = \sigma(j)$ valamely $i \neq j$ esetén. Tehát az egyes szorzatokba kiválasztott elemek különböző oszlopokból származnak. *Bástyaelhelyezés*nek hívjuk az A mátrix n elemének kiválasztását, ha közül semelyik két elem sem esik ugyanabba a sorba vagy oszlopba. Tehát a determináns definíciójában szereplő szorzatok mindegyike egy bástyaelhelyezésnek felel meg. Ez fordítva is igaz, ha ugyanis adott egy bástyaelhelyezés, akkor definiáljuk $\sigma(i)$-t úgy, mint az i-dik sorban álló bástya oszlopindexét. Ezáltal σ egy permutáció lesz (hiszen $i \neq j$ esetén $\sigma(i) \neq \sigma(j)$), tehát minden bástyaelhelyezés egyúttal meg is határoz egy, a determináns definíciójában szereplő szorzatot.

[11]Tehát $I(\sigma)$ azonos a metsző nyílpárok számával. Ha a diagram olyan, hogy semelyik három nyíl nem megy át ugyanazon a ponton, akkor $I(\sigma)$ azonos a metszéspontok számával. Egyébként minden olyan metszéspontot, amin k nyíl megy át, $\frac{1}{2}k(k-1)$-szer kell megszámolni.

A determináns definícióját tehát úgy is megfogalmazhatjuk, mint az összes bástyaelhelyezéshez tartozó mátrixelem-szorzatok előjeles összege. Ez a definíció azért nem pontos, mert az előjelek megválasztását nem írja le pontosan. Ez hát most a célunk. Mit jelent egy adott bástyaelhelyezés szempontjából, hogy a megfelelő σ permutációban i és j inverzióban állnak? Feltehetjük, hogy mondjuk $i < j$. Ha e két elem nem áll σ szerint inverzióban, akkor $\sigma(i) < \sigma(j)$, azaz a megfelelő bástyaelhelyezésben a j-dik sorbeli bástya jobbra van az i-dik sorbelitől, másképpen mondva e két bástya egymástól ÉNY-DK irányban helyezkedik el. Ha azonban i és j a σ permutáció szerint inverzióban áll, akkor $\sigma(i) > \sigma(j)$, tehát a j-dik sorban álló bástya balra van az i-dik sorban találhatótól, azaz a két bástya ÉK-DNY irányt határoz meg. Pontosíthatjuk tehát a determináns alternatív definícióját: az összes bástyaelhelyezés szerinti szorzatokat úgy kell összegeznünk, hogy egy szorzat előjele aszerint lesz pozitív ill. negatív, hogy az ÉK-DNY irányt meghatározó bástyapárok száma páros-e vagy páratlan.

Ennek fényében néhány további megfigyelést teszünk a determinánssal kapcsolatban. Az $A = (a_{i,j})$ mátrix *transzponáltja* az az A^T mátrix, amely i-dik sorának j-dik eleme $a_{j,i}$. (Úgy is mondhatjuk, hogy $(A^T)_i^j = A_j^i$.) A négyzetes A mátrix *főátlója* a bal felső sarkot és a jobb alsó sarkot összekötő átló mentén elhelyezkedő mátrixelemek halmaza. A négyzetes A mátrix *(szigorú) felső háromszögmátrix*, ha főátlója alatt csak 0-k állnak (és főátlója is csupa-0).

Tétel: Legyen A $n \times n$-es mátrix. (1) $\det(A) = \det(A^T)$
(2) Ha A felső háromszögmátrix, akkor $\det(A)$ az A főátlóbeli elemeinek szorzata.
(3) Ha A egy sora/oszlopa csupa-0, akkor $\det(A) = 0$.
(4) Ha A egy sorát/oszlopát λ-val végigszorozzuk, akkor a determináns is λ-szoros lesz.
(5) Ha A két sorát/oszlopát felcseréljük, a determináns (-1)-szeres lesz.
(6) Ha A két sora/oszlopa azonos, determinánsa 0.
(7) Ha A egy sorának λ-szorosát hozzáadjuk egy másik sorhoz, a determináns nem változik.

Biz: (1) Az A mátrixhoz tartozó tetszőleges bástyaelhelyezés meghatározza egy olyan bástyaelhelyezését az A^T mátrixnak, ami ugyanazon elemek szorzatához tartozik. (A bástyaelhelyezésben szereplő bástyákat a főátlóra kell tükrözni). Tehát A és A^T determinánsának definíciójában ugyanazok a szorzatok szerepelnek, ezért mindössze azt kell igazolnunk, hogy az előjeleik is azonosak. Ez utóbbi pedig azért igaz, mert a tükrözés során egy ÉK-DNY-i bástyapár ÉK-DNY-i marad, és az ÉNY-DK-iek is megmaradnak ugyanolyanoknak. (Ez a bizonyítás egyébként elmondható úgy is, hogy észrevesszük, hogy az A-beli σ-hoz tartozó bástyaelyezésnek megfelelő A^T-beli bástyaelhelyezés a σ^{-1} permutációhoz tartozik (ha az i-dik sorból a j-dik elemet választottuk A-ban, akkor A^T-ban a j-dik sor i-dik elemére lesz szükségünk), és a permutációk fejezetben láttuk, hogy $I(\sigma) = I(\sigma^{-1})$.)

(2) A determináns definíciójában szereplő szorzatok közül azok, amik tartalmaznak a főátló alól elemet, nem érdekesek, hiszen értékük 0. Igy csak azokat kell összegeznünk a megfelelő előjellel, amiknek minden eleme a főátlóból vagy a fölül kerül ki. Az utolsó sorból tehát kénytelenek vagyunk az utolsó elemet választani. Az utolsóelőtti sorban már nem választhatunk az utolsó oszlopból, hisz onnan már választottunk, így marad itt is a főátlóbeli elem. Általában, ha az i-dik sorból választunk, és a nagyobb sorszámú sorokból már kiválasztottuk a főátlóbeli elemet, akkor az i-dik sorban is kénytelenek vagyunk a főátlóból választani. Tehát a determináns definíciójában legfeljebb egyetlen nemnulla szorzat van, mégpedig a főátlóbeli elemeké. Mivel a megfelelő bástyaelhelyezésben bármely pár ÉNY-DK irányt határoz meg, az előjel pozitív.

(3) Ha mondjuk az i-dik sor csupa-0, akkor minden bástyaelhelyezésben lesz innen bástya, ami az adott szorzatot 0-vá teszi. Tehát 0 értékű szorzatokat kell előjelesen összegezni, de így sem kaphatunk mást, mint 0-t a determinánsra. (Csupa-0 oszlop esetén az érvelés hasonló. De hivatkozhatunk akár a transzponáltra is, aminek egy csupa-0 sora lesz.)

(4) Ha egy sorban minden elemet λ-val megszorzunk, akkor a determináns definíciójában szereplő minden egyes szorzatban pontosan egy tényező jön ebből a sorból, tehát minden szorzat éppen λ-szorosára változik, vagyis az előjeles összeg, a determináns is λ-szoros lesz.

(5) Ha adott az A mátrixon egy bástyaelhelyezés, és két sort felcseréljük, akkor egy olyan bástyaelhelyezést kapunk a felcseréltsorú A' mátrixban, amihez ugyanaz a szorzat tartozik. Ha tehát az A' determinánsát akarjuk kiszámítani, azt kell meghatároznunk, hogy a sorcsere hogyan változtatja egy bástyaelhelyezésben az ÉK-DNY-i bástyapárok számát. Világos, hogy a felcserélés által nem érintett bástyák alkotta párok esetén ez a szám nem változik. Könnyen ellenőrizhető, hogy egy nem érintett bástya ha nincs benne a két felcserélt bástya feszítette téglalapban, akkor a két érintett bástyával ugyanannyi ÉNY-DK-i párt alkot a csere előtt, mint a csere után. Ha egy nem érintett bástya a megfelelő téglalapban van, akkor viszont vagy mindkét felcserélt bástyával ÉNY-DK-i párt alkotott, és a csere után ÉK-DNY-it fog alkotni, vagy fordítva. Tehát az ÉNY-DK-i párok számának paritása csak attól fog megváltozni, hogy a két felcserélt bástya alkotta pár hogyan viselkedik. E két bástyára viszont az igaz, hogy ha a csere előtt

ÉK-DNY-i párt alkottak, akkor a csere után ÉNY-DK-it fognak alkotni, és viszont. Azt kaptuk, hogy sorcsere után minden bástyaelhelyezésben megváltozik az ÉK-DNY-i párok számának paritása, azaz a definícióban minden szorzat előjelet vált. Tehát a determináns is (-1)-szeresre változik. (Oszlopokra hasonló érvelés igaz, de áttérhetünk a transzponáltra is, hisz a oszlopcsere abban sorcserének felel meg.)

(6) Ha A-nak felcseréljük a két azonos sorát, akkor ugyanazt a mátrixot kapjuk, tehát a determináns nem változik, másfelől (5) miatt a determináns előjelet vált. Tehát a determináns azonos a saját ellentettjével, azaz csak 0 lehet. (Ugyanez a bizonyítás az oszlopokra is, de ízlés szerint lehet a transzponálttal is indokolni.)

(7) Legyen A' az a mátrix, amit A-ból úgy kapunk, hogy A i-dik sorának λ-szorosát hozzáadjuk A j-dik sorához. A $\det A'$ definíciójában minden bástyaelhelyezéshez tartozó szorzatban a j-dik tényező egy összeg. Ha felbontjuk a zárójelet, akkor két szorzat összegét kapjuk: az egyik szorzat az A determinánsának megfelelő tagja, a másik pedig azé az A'' mátrixé, amit úgy kapunk A-ból, hogy a j-dik sort helyettesítjük az i-dik sor λ-szorosával. Azt kaptuk tehát, hogy $\det A' = \det A + \det A''$. Ha $\lambda = 0$, akkor $\det A'' = 0$ a (3) miatt, egyébként pedig ha A'' j-dik sorát $\frac{1}{\lambda}$-val végigszorozzuk, akkor a kapott determináns (6) miatt 0 lesz, tehát $\det A'' = \lambda \cdot 0 = 0$, ismét. Innen $\det A' = \det A$ adódik. □

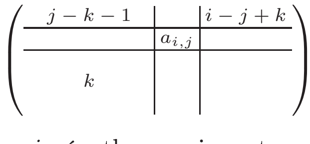
A most bizonyított tétel abban segít, hogy hatékonyan kiszámítsuk egy négyzetes mátrix determinánsát. Ha a definícióval próbálkoznánk, akkor a lépések száma nem volna korlátozható n polinomjával. Megtehetjük azonban, hogy a mátrixon elemi sorekvivalens átalakításokat végzünk. Az előző tétel megmutatja, hogy egy-egy lépésnél mi történik a determinánssal. Ha tehát elvégezzük a Gauss-eliminációt a mátrixon, akkor tudjuk, hogy a kapott mátrix determinánsa hányszorosa lesz az eredetiének. Ráadásul egy felső háromszögmátrixot kapunk, aminek egy jól meghatározott n-tényezős szorzat a determinánsa. Mivel a Gauss-elimináció hatékonyan elvégezhető, ez a módszer általában gyorsabb, mint a definíció alapján történő kiszámítás. (Hátránya sajnos ennek a módszernek, hogy nem mindig alkalmazható. Egy olyan mátrix esetén pl, aminek elemei polinomok, a determináns értelmes, de mégsem tudjuk elvégezni az elemi sorekvivalens átalakításokat, így marad a kiszámításhoz a gyalogos út. Az alábbiakban mutatunk egy másik módszert, ami ebben az esetben is működik, és sokszor segít.)

Az A négyzetes mátrix i-dik sorának és j-dik oszlopának elhagyásával keletkező mátrix determinánsának $(-1)^{i+j}$-szeresét az $A_{i,j}$ *előjeles aldeterminánsnak* nevezzük. Az előjeles aldetermináns nem tévesztendő össze az A mátrix *aldeterminánsával*, amit akkor kapunk, ha az A mátrixnak elhagyjuk néhány (akár 1-nél több) sorát, és ugyanennyi oszlopát, és a keletkező négyzetes mátrix determinánsát nézzük.

Kifejtési tétel: Ha A $n \times n$-es mátrix és i rögzített, akkor $\det(A) = \sum_{j=1}^{n} a_{i,j} \cdot A_{i,j}$ (*az i-dik sor szerinti kifejtés*). Rögzített j-re $\det(A) = \sum_{i=1}^{n} a_{i,j} \cdot A_{i,j}$ (*a j-dik oszlop szerinti kifejtés*). Ha $k \neq l$, akkor $\sum_{j=1}^{n} a_{k,j} \cdot A_{l,j} = 0 = \sum_{i=1}^{n} a_{i,k} \cdot A_{i,l}$ (*ferde kifejtés*).

Biz: Elegendő csak a sor szerinti kifejtéssel foglalkozni, hisz az oszlop szerinti kifejtés nem más, mint a transzponált sor szerinti kifejtése. Csoportosítsuk a $\det A$-beli szorzatokat a szerint, hogy az i-dik sorból az $a_{i,1}, a_{i,2}, \ldots, a_{i,n}$ tényezők közül melyiket tartalmazzák. Ha most a j-dik csoportban minden szorzatból kiemeljük $a_{i,j}$-t akkor pontosan azokat a szorzatokat kapjuk meg, amik az $A_{i,j}$ előjeles aldetermináns definíciójában szerepelnek. Azt kell tehát megvizsgálni, hogy hogyan változik egy szorzat előjele akkor, ha nem az determinánsban, hanem az eggyel kisebb mátrixban tekintjük.

Megszámoljuk tehát, hogy ha egy, az $a_{i,j}$ elemet tartalmazó bástyaelhelyezésben elhagyjuk az i-dik sort és a j-dik oszlopot, akkor a kapott bástyaelhelyezésben hogyan változik az ÉK-DNY-i bástyapárok száma az eredeti elhelyezéshez képest. Mivel itt lényegében csak az (i,j) mező feletti bástyát hagytuk el, azt kell megszámolni, hogy hány olyan ÉK-DNY-i bástyapár van az eredeti bástyaelhelyezésben, ami az (i,j) bástyát tartalmazza. Az ilyen párok (i,j) bástyától különböző bástyái az A mátrix két, téglalap alakú részmátrixban helyezkednek el.



Tegyük fel, hogy az (i,j) bástyától DNY-ra k bástya van az elhelyezésben. Mivel az első $j-1$ oszlop mindegyikében pontosan egy bástya van, az (i,j)-től ÉNY-ra $j-k-1$ bástya található. Az első $i-1$ sorban is éppen $i-1$ bástya áll, tehát (i,j)-től ÉK-re $i-j+k$ bástya található. A keresett bástyapárok száma tehát $k+i-j+k = 2k+i-j$.

Azt kaptuk tehát, hogy az előjel pontosan akkor változik meg, ha $2k+i-j$ páratlan, ami pontosan akkor teljesül, ha $i+j$ páratlan. Ezzel igazoltuk, hogy az előjeles aldeterminánsok definíciójában szereplő szorzatokat a megfelelő $a_{i,j}$-vel és $(1)^{i+j}$-vel megszorozva, az A mátrix determinánsát kapjuk. □

Természetes kérdés, hogy az A és B $(n \times n)$-es mátrixok esetén mondhatunk-e valamit $\det(A+B)$-ről $\det A$ és $\det B$ függvényében. A naív várakozás ellenére semmit nem mondhatunk. Nem így azonban az $A \cdot B$ szorzatmátrix esetén, aminek a determinánsa az eredeti determinánsok szorzata lesz. Erről szól az alábbi fontos tétel, amit itt nem bizonyítunk.

Tétel: Ha A, B $n \times n$-es, valós mátrixok, akkor $|A \cdot B| = |A| \cdot |B|$.

6. Mátrix rangja

Egy mátrixnak fontos paramétere, mennyire „függetlenek” az elemei. Mindjárt meg is adunk háromféle módszert ennek „mérésére”, majd megmutatjuk, hogy ugyanarról van szó mindhárom esetben.

Legyen A egy tetszőleges mátrix. Az A mátrix $s(A)$ *sorrangján* az A mátrixból kiválasztható lineárisan független sorok maximális számát értjük. (A sorrang tehát megegyezik az A mátrix sorvektorai által generált vektortér dimenziójával.) Az A $o(A)$ *oszloprangja* az A mátrixból kiválasztható lineárisan független oszlopok maximális száma. (Hasonlóan, A oszloprangja nem más, mint az A oszlopvektorai generálta tér dimenziója.) Végül A $d(A)$ *determinánsrangja* megegyezik A legnagyobb, nemnulla aldeterminánsának méretével. (Emlékeztetünk, hogy aldeterminánson egy olyan determinánst értünk, ami A-ból azonos számú sor és oszlop elhagyásával keletkezik.)

Tétel: Tetszőleges mátrix sor-, oszlop- és determinánsrangja megegyezik.

Biz: Megmutatjuk, hogy mindhárom rangfogalom azonos az A mátrix Gauss-eliminációja után kapott vezéregyesek számával. Ezt úgy tesszük meg, hogy tetszőleges A mátrixról megmutatjuk, hogy $s(A) = d(A)$. Ha ez sikerül, akkor kész vagyunk, ugyanis $d(A) = d(A^T) = s(A^T) = o(A)$ miatt az oszloprang is egyenlő a sor és determinánsrang közös értékével.

Világos, hogy ha A lépcsős alakú és k vezéregyest tartalmaz, akkor a vezéregyeseket tartalmazó sorok lineárisan függetlenek, és a vezéregyeseket tartalmazó sorok és oszlopok közös elemei egy olyan $k \times k$ méretű részmátrixot adnak, ami felső háromszögmátrix, és főátlója csupa-1, tehát determinánsa sem 0. Ha legalább $k + 1$ sort választunk ki, akkor azok lineárisan összefüggőek, hiszen tartalmaznak egy csupa-0 sort. Ha egy legalább $(k + 1) \times (k + 1)$ méretű aldeterminánst választunk, akkor az is 0 lesz, hisz az is tartalmaz csupa-0 sort. Eszerint $s(A) = k = d(A)$.

Megmutatjuk, hogy a Gauss-elimináció nem változtatja sem a sor, sem a determinánsrangot. Ha ezt megtesszük, akkor megmutattuk, hogy $s(A) = d(A)$, hiszen mindkét rang azonos lesz az elimináció után kapott mátrix vezéregyeseinek számával. A Gauss-elimináció elemi sorekvivalens átalakításokból áll, tehát elegendő ezekről kimutatni, hogy megőrzik a rangokat.

A sorcserénél világos, hogy a sorrang nem változik. Az aldeterminánsok értékei esetleg az ellentettek lesznek, de 0-voltuk nem változik. Ha egy sort nemnullával végigszorzunk, akkor ettől szintén nem változhat meg a sorrang. Az aldeterminánsok értéke vagy nem változik, vagy λ-szoros lesz, tehát pontosan akkor lesz 0, ha előzőleg is 0 volt.

Vizsgáljuk meg végül azt a transzformációt, amikor az i-dik sor λ-szorosát hozzáadjuk a j-dik sorhoz. Ekkor voltaképp a j-dik sorvektort helyettesítjük egy olyan sorvektorral, ami benne van a sorok által generált vektortérben, tehát a sorrang (a sorok által generált tér dimenziója) nem növekedhetett. Mivel az i-dik sor $-\lambda$-szorosának ismételt hozzáadásával visszanyerhető az eredeti A mátrix (miközben ismét csak csökkenhet a sorrang), ezért a sorrang a transzformáció során nem változhat.

Állítjuk, hogy a determinánsrang sem változik. Tekintsünk ugyanis egy A' aldeterminánst a transzformáció előtt, legyen A'' a transzformáció után ugyanitt elhelyezkedő aldetermináns! Ha A' nem tartalmazza a j-dik sort, akkor $\det A' = \det A''$, vagyis pontosan akkor lesz 0 az aldetermináns, ha előzőleg is 0 volt. Ha A' tartalmazza a j-dik sort, akkor a j-dik sor szerint kifejtve A''-t azt kapjuk, hogy $\det A'' = \det A' + \lambda \cdot \det A^*$, ahol a A^* az a determináns, amit úgy kapunk A'-ből, hogy a j-dik sort helyettesítjük az i-dikkel. Ez utóbbi A^* vagy kétszer tartalmazza az i-dik sort, és ekkor determinánsa 0, vagy determinánsa (előjeltől eltekintve) megegyezik azzal az aldeterminánssal, amit akkor kapunk, hogy az j-dik sor helyett az i-diket választjuk. Azt kaptuk tehát, hogy ha a transzformáció előtt minden $k \times k$ méretű aldetermináns 0 volt, akkor ez így lesz a sorhozzáadás után is. Ha pedig a sorösszeadás után létrejött egy nemnulla $k \times k$ méretű aldetermináns, akkor a eredetileg is volt egy ilyen. Mindezek alapján a determinánsrang sem változhatott, a tételt igazoltuk. □

A fenti tétel szerint definiálhatjuk az A mátrix $r(A) := s(A) = o(A) = d(A)$ *rangját.*

Köv.: Tetszőleges mátrix rangja megegyezik a transzponáltjának rangjával.

Biz: $r(A) = s(A) = o(A^T) = r(A^T)$ □

7. Mátrix inverze

A B $n \times n$ méretű mátrix az $A \in \mathbb{R}^{n \times n}$ mátrix *balinverze*, ha $B \cdot A = I_n$, ahol I_n az $n \times n$ méretű egységmátrix, aminek a főátlója csupa-1, egyéb elemei 0-k. A $J \in \mathbb{R}^{n \times n}$ mátrix az A *jobbinverze*, ha $A \cdot J = I_n$.

Állítás: Ha az $A \in \mathbb{R}^{n \times n}$ mátrixnak létezik jobb- és balinverze is, akkor azok egyenlőek.

Biz: Legyen B bal-, J pedig jobbinverz. Ekkor $B = BI_n = B(AJ) = (BA)J = I_nJ = J$. □

Köv.: Ha egy mátrixnak van jobb és balinverze is, akkor azok egyértelműek. $\square$

Tétel: Az alábbi három állítás ekvivelens. (1) $\det A \neq 0$. (2) A-nak létezik balinverze. (3) A-nak létezik jobbinverze.

Lemma: Ha A és B összeszorozható mátrixok, akkor $(A \cdot B)^T = B^T \cdot A^T$.

Biz: Emlékeztetünk, hogy az alsó index a sort, a felső az oszlopot jelenti. Azt kell megmutatni, hogy a két mátrix elemnként azonos. És valóban: $((A \cdot B)^T)_i^j = (A \cdot B)_j^i = A_j \cdot B^i = (B^T)_i \cdot (A^T)^j = (B^T \cdot A^T)_i^j$. $\square$

Biz: Megmutatjuk, hogy (1) és (3) ekvivalens. Ez elegendő, mert a fenti lemma szerint A-nak pontosan akkor van balinverze, ha A^T-nak létezik jobbinverze. Ez (1) és (3) egyenértékűsége miatt azt jelenti, hogy $\det(A^T) \neq 0$, azaz $\det A \neq 0$. Tehát ekkor (1) és (2) is ekvivalens.

Ha J az A $n \times n$ méretű mátrix jobbinverze, akkor a J mátrix i-dik oszlopa megfelel egy olyan lineáris egyenletrenszer egy megoldásának, aminek A az együtthatómátrixa, a jobboldalakon pedig csupa 0-k állnak, kivéve az i-dik helyet, aholis 1 található. Tehát ha létezik jobbinverz, akkor az összes ilyen lineáris egyenletrendszernek van megoldása. Másfelől, ha mindezen lineáris egyenletrendszerek megoldhatóak, akkor a megoldásokat oszlopvektorokba rendezve, az oszlopokból olyan J' mátrix képződik, amire $AJ' = I_n$ áll, tehát A-nak van jobbinverze. Próbáljuk tehát megoldani ezeket az egyenletrendszereket. Az az észrevétel, hogy ehhez nem kell n Gauss-eliminációt elvégezni, megtehetjük ezeket „szimultán": A mellé írunk egy I_n egységmátrixot, és így végezzük el a Gauss-eliminációt. Amikor az i-dik egyenletrendszer megoldását keressük, akkor egyszerűen elhagyjuk a feleslegesen hozzávett oszlopokat, és leolvassuk a megoldást.

Nézzük tehát a Gauss-elimináció utáni kapott redukált lépcsős alakot! Ha az első n oszlop egy egységmátrixot alkot (vagyis mindegyik tartalmaz vezéregyest), az pontosan azt jelenti, hogy A rangja (így determinánsrangja) n, azaz $\det A \neq 0$. De a baloldali egységmátrix egyszersmind azt is mutatja, hogy az összes vizsgált lineáris egyenletrendszer megoldható, tehát A-nak létezik jobbinverze. Tehát ha $\det A \neq 0$, akkor létezik jobbinverz. Most tegyük fel, hogy az első n oszlop alkotta RLA nem az egységmátrix, vagyis az utolsó sor n db 0-val kezdődik. Mivel a kiindulási $n \times 2n$ méretű mátrix rangja n volt (a jobboldalra hozzávett egységmátrix miatt), és ez a rang nem csökkenhetett, ezért a teljes RLA utolso sora nem lehet csupa-0. Van tehát egy olyan oszlop, aminek az utolsó eleme nem 0, és akkor ezt az oszlopot kiválasztva a megfelelő lineáris egyenletrendszernek tilos sora lesz. Van tehát egy olyan a lineáris egyenletrendszerek között, amelyiknek nincs megoldása, vagyis A-nak nem létezik jobbinverze. $\square$

Megjegyzés: Az iménti tételnek az a része, hogy ha $\det A = 0$, akkor A-nak nincs se jobb-, se balinverze, könnyen igazolható a determinánsok szorzástételéből. Tegyük fel, ugyanis, hogy mondjuk B balinverz. Ekkor $1 = \det I_n = \det(BA) = \det B \cdot \det A$, tehát $\det A \neq 0$. Ellentmondás.

Köv.: Az $A \in \mathbb{R}^{n \times n}$ mátrixnak pontosan akkor van inverze, ha $(A|I_n)$ Gauss-eliminációjával a RLA $(I_n|B)$ alakú. Ekkor $B = A^{-1}$.

Biz: Az előző tétel bizonyításakor láttuk az első mondat érvényességét. A második rész abból következik, hogy ha egy lineáris egyenletrendszer megoldásakor a kibővített egységmátrix redukált lépcsős alakja egységmátrix, akkor a megoldás egyértelmű és azt éppen a jobboldalon található oszlopvektor adja meg. Ezek az oszlopvektorok pedig a jobbinverz oszlopai lesznek, amint azt a tétel bizonyításában láttuk. $\square$

8. Lineáris egyenletrendszerek tárgyalása mátrixokkal

Tétel: Legyen $A \in \mathbb{R}^{n \times k}$, tetszőleges valós mátrix. Az alábbi állítások ekvivalensek.
(1) Az $(A|b)$ kibővített egyómátrix leírta lineáris egyenletrendszernek (egyértelműen) létezik megoldása.
(2) (Egyérteműen) létezik $x \in \mathbb{R}^k$, amire $Ax = b$. (3) $b \in \mathrm{Im}(A)$ (és $\mathrm{Ker}(A) = \{\mathbf{0}\}$) .
(4) (Egyérteműen) létezik $x \in \mathbb{R}^k$ úgy, hogy $b = \sum_{i=1}^k A^i x_i$.
(5) $b \in \langle A^1, \ldots, A^k \rangle$ (és $A^1, \ldots A^k$ lineárisan független vektorok).
(6) $\langle A^1, \ldots, A^k \rangle = \langle b, A^1, \ldots, A^k \rangle$ (és $A^1, \ldots A^k$ lineárisan független vektorok).
(7) $\dim(\langle A^1, \ldots, A^k \rangle) = \dim(\langle b, A^1, \ldots, A^k \rangle)(= k)$. (8) $r(A) = r(A|b)(= k)$.

Biz: (1) $\iff$ (2): A definíciókból adódik. (2) $\iff$ (3): A képtér definíciója szerint $Ax = b \iff b \in \mathrm{Im}(A)$. Világos, hogy ha $Ax = b = Ay$ akkor $A(x - y) = \mathbf{0}$, illetve ha $Ax = b$ és $Az = \mathbf{0}$, akkor $A(x + z) = Ax + Az = Ax = b$. Tehát ha az $Ax = b$ megoldása egyértelmű, akkor $\mathrm{Ker}(A) = \{\mathbf{0}\}$. Ha pedig $\mathrm{Ker}(A) = \{\mathbf{0}\}$, akkor nem lehet két különböző megoldása az egyenletrendszernek.
(2) $\iff$ (4): Világos, hogy $Ax = b \iff b = \sum_{i=1}^k A^i x_i$.
(4) $\iff$ (5): b-t (definíció szerint) pontosan akkor generálják az oszlopvektorok, ha előáll lineáris kombinációjukként. Az oszlopvektorok által generált térben pontosan akkor egyértelmű a felírás, ha e vektorok

bázisát alkotják az általuk generált térnek, azaz, ha lineárisan függetlenek.
(5) $\iff$ (6): b pontosan akkor van benne az oszlopvektorok terében, ha az oszlopvektorokhoz b-t hozzávéve nem tudunk további vektort generálni.
(6) $\iff$ (7): Az $A^1, \dots, A^k$ vektorok pontosan akkor lineárisan függetlenek, ha az általuk generált térben bázist alkotnak, azaz, ha a generátum dimenziója k.
(7) $\iff$ (8): Egy oszlopvektorai által generált tér dimenziója nem más, mint az oszlopvektorokból kiválasztható lineárisan független vektorok száma, azaz az oszloprang. Erről pedig tudjuk, hogy a ranggal egyenlő. $\square$

9. Mátrixok sajátértékei, sajátvektorai és sajátalterei

Def: Legyen $\mathcal{A} : V \to V$ egy lineáris transzformáció, $v \in V$ egy vektor a térből és $\lambda \in \mathbb{R}$ egy skalár. A $v \in V$ vektort az $\mathcal{A}$ transzfomáció λ ***sajátértékhez*** tartozó ***sajátvektorának*** nevezzük, ha (1) $v \neq \mathbf{0}$ és (2) $\mathcal{A}(v) = \lambda \cdot v$ teljesül. Ha λ az $\mathcal{A}$ transzformáció egy sajátértéke (azaz tartozik hozzá sajátvektor) akkor a λ-hoz tartozó ***sajátaltér*** a nullvektorból és a λ-hoz tartozó sajátvektorokból áll: $\{v \in V : \mathcal{A}(v) = \lambda \cdot v\}$.

Tétel: (1) Lineáris transzformáció minden sajátvektora pontosan egy sajátértékhez tartozik.
(2) Fix sajátértékhez tartozó sajátvektorok a $\mathbf{0}$-val együtt alteret alkotnak.

Biz: (1): Ha v sajátvektor, akkor $0 \neq v$. Tegyük fel, hogy $\mathcal{A}(v) = \lambda v$ és $\mathcal{A}(v) = \mu v$. Ekkor $\lambda v = \mu v$, azaz $(\lambda - \mu)v = \mathbf{0}$. Tanultuk, hogy skalár és vektor szorzata csak úgy lehet $\mathbf{0}$, ha $v = \mathbf{0}$ vagy $\lambda - \mu = 0$. Az első eset kizárt, ezért $\lambda = \mu$, tehát minden sajátvektor pontosan egy sajátértékhez tartozik.
(2): Legyen $V_\lambda := \{v \in V : \mathcal{A}(v) = \lambda \cdot v\}$ a vizsgált halmaz, melynek altér voltát kell igazolnunk. Azt kell csupán megmutatni, hogy ha $u, w \in V_\lambda$, és $\mu \in \mathbb{R}$ tetszőleges skalár, akkor $u + w, \mu u \in V_\lambda$. Természetesen ez is a linearitásból következik: $\mathcal{A}(u + w) = \mathcal{A}(u) + \mathcal{A}(w) = \lambda \cdot u + \lambda \cdot w = \lambda \cdot (u + w)$ ill. $\mathcal{A}(\mu u) = \mu \cdot \mathcal{A}(u) = \mu \cdot (\lambda \cdot u) = (\mu\lambda)u = \lambda \cdot (\mu u)$. $\square$

Vizsgáljuk meg, mit jelent az, hogy v egy $\mathcal{A}$ transzformáció sajátértéke! Ekkor $\mathcal{A}(v) = \lambda v$, azaz $\mathcal{A}(v) - \lambda v = \mathbf{0}$. Jelölje id azt az (ún. identikus) lineáris transzformációt, ami minden vektorhoz önmagát rendeli. Nyilván λid is lineáris transzformáció, ami minden vektorhoz a λ-szorosát rendeli, és a legutóbbi összefüggés úgy írható fel, hogy $(\mathcal{A} - \lambda \cdot id)v = \mathbf{0}$. Könnyen látható, hogy $\mathcal{A} - \lambda id$ is egy lineáris transzformáció (konkrétan, egy w vektorhoz $(\mathcal{A}(w) - \lambda w)$-t rendel), és az a tény tehát, hogy λ az $\mathcal{A}$ transzformáció sajátértéke, úgy fogalmazható meg, hogy az $\mathcal{A} - \lambda id$ lineáris transzformáció egy nemnulla vektort a $\mathbf{0}$-ba képez. Legyen B a V vektortér egy bázisa, és tekintsük az $\mathcal{A}$ transzformáció $[\mathcal{A}]_B^B$ mátrixát. Tudjuk, hogy a koordinátavektorokon az $\mathcal{A}$ leképezés úgy működik, hogy ezzel a mátrixszal kell balról szorozni, ezért az a tény, hogy λ sajátérték, azaz, hogy $\mathcal{A} - \lambda id$ egy nemnulla vektort $\mathbf{0}$-ba visz, úgy mondható el, hogy a $[\mathcal{A}]_B^B - \lambda I$ mátrixot egy nemnulla koordinátavektorral jobbról megszorozva megkaphatjuk a csupa-0 vektort. Ez pedig pontosan azt jelenti, hogy a $[\mathcal{A}]_B^B - \lambda I$ mátrix oszlopai nem lineárisan függetlenek (az előbbi vektor koordinátái adják meg a $\mathbf{0}$-t előállító nemtriviális lineáris kombináció együtthatóit). Azt kaptuk, hogy az oszloprang kisebb, mint az oszlopok száma, és mivel négyzetes mátrixról van szó, ez a determinánsranggal kifejezve azt jelenti, hogy a $[\mathcal{A}]_B^B - \lambda I$ mátrix determinánsa 0. Bebizonyítottuk tehát, hogy $\det([\mathcal{A}]_B^B - \lambda I) = 0$ pontosan akkor teljesül, ha λ az $\mathcal{A}$ transzformáció sajátértéke, ráadásul ez a tény függetlenül a felíráshoz használt B bázistól.

Def: Az $\mathcal{A} : V \to V$ lineáris transzformáció ***karakterisztikus polinomja*** $k_\mathcal{A}(\lambda) := \det([A]_B^B - \lambda \cdot I)$, ahol B a V vektortér egy tetszőleges bázisa.

Tétel: (1) A karakterisztikus polinom a λ változónak egy n-edfokú polinomja, ahol $n = \dim V$.
(2) A karakterisztikus polinom független a felírásához használt bázistól.
(3) A $\lambda \in \mathbb{R}$ skalár pontosan akkor sajátértéke az $\mathcal{A}$ transzformációnak, ha $k_\mathcal{A}(\lambda) = 0$, azaz λ gyöke a karakterisztikus polinomnak.

Biz: (1): A determináns definíciójára gondolva a karakterisztikus polinom olyan n-tényezős szorzatok előjeles összege, ahol a szorzatok tényezői az $[A]_B^B - \lambda \cdot I$ mátrix elemei. E mátrix minden eleme egy legfeljebb elsőfokú polinomja λ-nak, ezért minden szorzat egy legfeljebb n-edfokú polinom, így a determináns is az. Egy szorzat pontosan akkor lesz n-edfokú, ha minden tényezője elsőfokú. Márpedig pontosan a főátlóban szerepelnek az elsőfokú elemek (-1 a főegyütthatójuk), így pontosan egyetlen n-edfokú tagja lesz a determinánst meghatározó összegnek (aminek a főegyütthatója egyébként $(-1)^n$ lesz). A determináns tehát csakugyan λ egy pontosan n-edfokú polinomja.
(2): Nem bizonyítjuk. (Jegyezzük meg, hogy maga az állítás fontos (hiszen ez mutatja, hogy a karakterisztikus polinom fogalma jóldefiniált), bizonyítása nemtriviális.)
(3): A karakterisztikus polinom definíciója előtti gondolatmenet pontosan ezt igazolja. $\square$

Cayley-Hamilton tétel: Minden lineáris transzformáció gyöke a karakterisztikus polinomjának, azaz $k_\mathcal{A}(\mathcal{A})(v) = \mathbf{0}$ minden $v \in V$ vektorra. (Más szóval, $k_\mathcal{A}(\mathcal{A})$ a nulla transzformáció. Egy harmadik megfogalmazás szerint, ha $k_\mathcal{A}(\lambda) = a_n\lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_1\lambda + a_0$, akkor tetszőleges $v \in V$ vektorra $a_n \cdot \mathcal{A}^n(v) + a_{n-1}\mathcal{A}^{n-1}(v) + \ldots + a_1 \cdot \mathcal{A}(v) + a_0 \cdot v = \mathbf{0}$ teljesül, ahol az $\mathcal{A}^k$ lineáris transzformációt az $\mathcal{A}^k(v) := \mathcal{A}(\mathcal{A}(\ldots\mathcal{A}(v)\ldots))$ k-szoros iterált definiálja.) □

10. Végtelen halmazok, számosság

Ez a fejezet nem lett külön kidolgozva, az érdeklődő olvasó a `http://cs.bme.hu/~sali/halmaz.pdf` webhelyen letöltheti.

11. Elemi leszámlálások

Def: Legyenek $k, n \in \mathbb{N}$ és $0 \le k \le n$. Az n *elem k-adosztályú (ismétlés nélküli) variációján* n db, rögzített, egymástól megkülönböztethető elemből kiválasztott k db elem egy sorrendjét értjük. Azaz kiválasztunk egy első elemet az n közül, egy tőle különböző másodikat, stb, végül az eddigiektől különböző k-adikat. $V(n,k)$ jelöli n elem k-adosztályú variációinak számát.

Példa: A fenti variációfogalomra egy lehetséges példa, ha azt kérdezzük, hogy egy n versenyző részvételével megrendezett kerékpárversenyen hányféle sorrendje lehet az első k befutónak.

A kérdés értelemszerűen $V(n,k)$ értéke. Világos, hogy $V(n,0) = 1, V(n,1) = n$. Az is látszik, hogy $V(n,k) = V(n,k-1) \cdot (n-k+1)$, hiszen minden szóbajövő sorrendet meghatározhatunk úgy, hogy először $k-1$ elemet rakunk sorba, majd a k-dik elemet kiválasztjuk az eddig ki nem választott $n-k+1$ elem közül. Innen $V(n,k) = n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$ adódik.

Def: Az n természetes szám *faktoriálisa* $n! := \begin{cases} 1 & \text{ha } n = 0 \\ 1 \cdot 2 \cdot \ldots \cdot n & \text{ha } n > 0 \end{cases}$.

A fenti jelöléssel $V(n,k) = \frac{n!}{(n-k)!}$ adódik.

Def: Legyen $k, n \in \mathbb{N}$. Ekkor *n elem k-adosztályú, ismétléses variációja* alatt egy olyan k hosszú sorozatot értünk, aminek tagjai n db, egymástól megkülönböztethető elem közül kerülnek ki, úgy, hogy az n elem bármelyikét tetszőlegesen sokszor felhasználhatjuk a sorozatban. Az említett ismétléses variációk számát $V_{ism}(n,k)$ jelöli.

Példa: Az ismétléses variáció kapcsán a Tour de France kerékpáros vetélkedő egy versenynapjára gondolhatunk, és megkérdezhetjük, hogy ha az adott napon n versenyző indult, és k etap volt (ezek mindegyikénél az első néhány befutó pontokat szerez), akkor hányféle lehet az aznapi etapgyőztesek sorrendje.

Hasonlóan a fenti gondolatmenethez, itt $V_{ism}(n,0) = 1, V_{ism}(n,1) = n$, ill. $k \ge 1$ esetén $V_{ism}(n,k) = V_{ism}(n,k-1) \cdot n$, ahonnan $V_{ism}(n,k) = n^k$.

Def: Legyen $n \in \mathbb{N}$. Ekkor n elem egy *permutációja* az n db, egymástól megkülönböztethető elem egy sorbarendezését jelenti.

Példa: A permutációra korábban láttunk már példát: egy $n \times n$ méretű táblán egy bástyaelhelyezést ír le. De ha pl. n ellenőrzésen kell átjutnunk, mindegyiken egy-egy jelszó bemondásával (ha rossz jelszóval próbálkozunk, azonnal veszítünk), és ismerjük az n jelszót, de nem tudjuk, melyik ellenőrzési pontokhoz tartozik, akkor a siker esélye (további információ hiányában) éppen $\frac{1}{n!}$.

A definíciókból azonnal adódik, hogy n elem permutációi azonosak az n elem n-edosztályú variációival, így a fentiek szerint a számuk $\frac{n!}{0!} = n!$.

Def: Legyen $k_1, k_2, \ldots, k_l \in \mathbb{N}$ rögzített számok és $n := \sum_{i=1}^{n} k_i$. Ekkor n elem *ismétléses permutációja* alatt egy olyan n hosszú sorrendet értünk, amiben az i-dik elem pontosan k_i-szer jelenik meg minden $1 \le i \le l$ esetén.

Példa: Ha tudjuk, hogy egy héten minden nap öt óránk van az általános iskolában, és ismerjük az egyes tárgyak heti óraszámait ($k_1, k_2, \ldots, k_n$, ezekre értelemszerűen $k_1 + k_2 + \ldots + k_n = 25$ teljesül), akkor a lehetséges órarendek száma éppen a 25 óra ismétléses permutációinak száma. (A példa pindurit sánta, mert nem valószínű olyan nap, hogy testnevelés-ének-rajz-technika-osztályfőnöki legyen a beosztás.)

Megjegyzés: 1. Az „n elem ismétléses permutációja” elnevezése nem teljesen pontos. Ugyanis amikor erről beszelünk, akkor azt mindig úgy értjük, hogy az l és a k_i-k értékek is rögzítettek.
2. Ha minden k_i értéke 1, akkor az ismétlés nélküli permutáció fogalmához jutunk vissza. Az ismétlés nélküli permutációnak tehát két lehetséges általánosítását láttuk: az ismétlés nélküli variációt, ill. az ismétléses permutációt.

Az ismétléses permutációk számának kiszámításához tekintsünk n megkülönböztethető elemet, és rögzítsük ezeknek egy l csoportra történő szétosztását, úgy, hogy a csoportok mérete rendre $k_1, k_2, \ldots, k_l$ legyen. Ekkor az n elem minden permutációja egyértelműen meghatároz egy ismétléses permutációt ha a sorbarakott elemek helyett azok csoportját tekintjük. Az a lényeges megfigyelés, hogy minden ismétléses permutációt ugyanannyi ismétlés nélküli permutáció határoz meg: ha ugyanis egy rögzített ismétléses permutációt szeretnénk megkapni, akkor az egyes csoportokat adott helyekre kell szétosztani, amit egy k_i méretű csoport esetén k_i!-féleképp tehetünk meg. Mivel minden csoportra ezt egymástól függetlenül megtehetjük, ezért minden ismétléses permutációt pontosan $k_1! \cdot k_2! \cdot \ldots \cdot k_l!$-féle ismétlés nélküli permutáció határoz meg. Ezért az ismétléses permutációk száma $\frac{n!}{k_1! \cdot k_2! \cdot \ldots \cdot k_l!}$.

Megjegyzés: 1. A $\frac{(k_1+k_2+\ldots+k_l)!}{k_1! \cdot k_2! \cdot \ldots \cdot k_l!}$ kifejezésről ránézésre nem világos, hogy egész szám. Láttuk azonban, hogy az ismétléses permutációk számát írja le, ezért bizonyosan egész. Ezzel tehát egy algebrai tényt kombinatorikus úton igazoltunk.
2. Figyeljük meg, hogy az „ismétléses" jelző a variációk ill. permutációk esetén különböző dolgot jelent: variációk esetén tetszőleges számú ismétlődés megengedett, permutációknál minden elemről adott, hogy hányszor ismétlődik.

Def: Legyen $k, n \in \mathbb{N}$, $k \leq n$. Ekkor *n elem k-adosztályú kombinációján* egy (rögzített) n elemből álló halmaz egy k-elemű részhalmazát értjük. Az elem k-adosztályú kombinációinak számát (azaz az n-elemű halmaz k-elemű részhalmazainak számát) $C(n, k)$ jelöli.

Példa: A legkézenfekvőbb példa talán a lottóhúzások lehetséges kimeneteleinek száma, $C(90, 5)$.

Vegyük észre, hogy n elem minden k-adosztályú variációja egyértelműen meghatároz egy k-adosztályú kombinációt: egyszerűen el kell feledkezni kiválasztott k elem sorrendjéről. Az is azonnal látszik, hogy minden egyes k-adosztályú kombináció annyi k-adosztályú variációból származtatható, ahányféleképpen a kiválasztott k db elemet sorba lehet rakni, azaz k! db-ból. Ezért $C(n, k) = \frac{n!}{(n-k)! \cdot k!}$.

Megjegyzés: Az fenti kombinációfogalom ismét speciális esete az ismétléses permutációnak: ha n elemből akarok k-t kiválasztani, akkor feltehetem, hogy az n elemnek van egy rögzített sorrendje. Ebben a sorrendben minden elemről meg kell mondanom, kiválasztottam-e vagy sem, rááadásul ezt úgy, hogy pontosan k-t válasszak ki. Vagyis egy olyan n hosszú sorrendről van szó, amiben a **„kiválasztva"** k-szor, a **„nem kiválasztott"** pedig $(n-k)$-szor jelenik meg. Ez pedig az n elem egy olyan ismétléses permutációja, amire $k_1 = k$ és $k_2 = n - k$.

Def: Jelölje $\binom{n}{k} := \frac{n!}{(n-k)! \cdot k!}$ az „n alatta k" (vagy „n alatt a k" ?) *binomiális együtthatót.*

A fenti jelöléssel $C(n, k) = \binom{n}{k}$ adódik.

Megjegyzés: 1. Ránézésre itt sem világos, hogy $\binom{n}{k} \in \mathbb{N}$, de kombinatorikus úton ez azonnal adódik, hisz egy halmaz méretét adja meg. (Persze ezt már láttuk az ismétléses permutációknál.)
2. $\binom{n}{k} = \binom{n}{n-k}$: algebrai úton is világos, de abból is látszik, hogy n elem közül k elem kiválasztása ugyanaz, mint $n - k$ elem „otthagyása", vagyis a megmaradó $n - k$ elem kiválasztása.
3. Ha $k \geq 1$, akkor $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. Rögzítsünk ugyanis egy x elemet az n elem közül. Ha most n elem közül k-t választunk ki, akkor ebben a k elemben vagy nincs benne az x, és akkor tkp $n-1$ elemből választottunk k-t ($\binom{n-1}{k}$-féleképp), vagy benne van az x, és ekkor az x-től különböző $n-1$ elem közül kellett $(k-1)$-t kiválasztani, amit $\binom{n-1}{k-1}$-féleképp tehetünk meg. Az azonosság persze algebrai úton is igazolható, de az az út unalmas és fárasztó.

Def: Legyen $k, n \in \mathbb{N}$. Ekkor *n elem k-adosztályú, ismétléses kombinációja* n-féle elemtípusból k db kiválasztását jelenti, ahol bármely típusból tetszőlegesen sokat választhatunk. Tehát az ismétléses kombinációk kölcsönösen megfeleltethetőek az $a_1 + a_2 + \ldots a_n = k$ összegeknek, ahol $a_i \in \mathbb{N}$ írja le, hogy az i-dik típusból hányat választottunk. Az n elem k-adosztályú ismétléses variációinak száma $C_{ism}(n, k)$.

Példa: Ha egy cukrászdában n-féle süteményt árulnak, akkor k db-t éppen $C_{ism}(n, k)$-féleképpen vásárolhatunk.

Az n elem tetszőleges k-adosztályú, ismétléses kombinációja egyértelműen megfeleltethető egy $(n + k - 1)$ hosszúságú 0/1-sorozatnak: először leírunk a_1 db 1-t, majd egy 0-t, utána a_2 db 1-t, egy 0-t, a_3 db 1-t, 0-t, stb. (Tkp. minden a_i-t a_i db 1-essel, és minden +-t egy 0-val kódolunk.) Összesen tehát k db 1-t és $(n - 1)$ db 0-t írunk le. Ráadásul, minden $n + k - 1$ hosszúságú, k db 1-est tartalmazó 0/1 sorozatból egyértelműen adódik egy ismétléses kombináció. Ezért az ismétléses kombinációk száma azonos a lehetséges 0/1-sorozatok számával. Egy ilyen sorozatot pedig úgy kapunk, hogy a lehetséges $n + k - 1$ helyből kiválasztjuk azt a k helyet, ahova 1-t írunk, a maradék helyeken értelemszerűen 0-k állnak. Eszerint n elem k-adosztályú ismétléses kombinációinak száma $\binom{n+k-1}{k}$.

A binomiális együtthatókkal kapcsolatos a binomiális tétel.

Binomiális tétel: Ha $1 \leq n \in \mathbb{Z}$, akkor $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$.

Biz: Amikor a zárójeleket felbontjuk, akkor a keletkező kifejtési tagok úgy adódnak, hogy az n tényező mindegyikéből kiválasztjuk az a ill. b valamelyikét, és ezeket összeszorozzuk. Tehát minden kifejtési tag $a^i \cdot b^{n-i}$ alakú lesz valamely $0 \leq i \leq n$ egészre. Konkrétan: $a^i b^{n-i}$ annyiszor fog adódni, ahányféleképpen i db a-t tudok választani a lehetséges n-ből, azaz $\binom{n}{i}$-szer. $\square$

Köv.: 1. $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = \sum_{i=0}^{n} \binom{n}{i} = (1+1)^n = 2^n$.
2. $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots \pm \binom{n}{n} = \sum_{i=0}^{n} (-1)^i \binom{n}{i} = (1-1)^n = 0^n = 0$.

A Pascal háromszög. A binomiális együtthatókat elrendezhetjük piramisalakzatban úgy, hogy a piramis csúcsán áll az $\binom{0}{0} = 1$ együttható, alatta az $\binom{1}{0} = 1$ ill. $\binom{1}{1} = 1$ együtthatók, a harmadik sorban találhatóak a $\binom{2}{0}, \binom{2}{1}, \binom{2}{2}$ együtthatók. Általában, az i-dik sorban az $\binom{i}{0}, \binom{i}{1}, \ldots, \binom{i}{i}$ együtthatók állnak. A legutóbbi következmény mutatja, hogy a Pascal háromszög i-dik sorában található elemek összege 2^{i-1}. Ez azonban belátható abból a tényből is, hogy minden sorösszeg kétszerese az előzőnek, ugyanis a pascal háromszög egy elemét úgy kapjuk, hogy összeadjuk a fölötte álló két elemet. (Ez a korábban látott $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ összefüggésből adódik.) A Pascal háromszögnek további érdekes tulajdonságai vannak.

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
... ...

A Pascal háromszög

12. Gráfok

A $G = (V, E)$ *egyszerű gráf*, ha (1) $V \neq \emptyset$ és (2) $E \subseteq \binom{V}{2} := \{\{u, v\} : u, v \in V, u \neq v\}$.

Egy G gráf esetén $V(G)$ jelöli G *csúcsainak (pontjainak)*, $E(G)$ pedig G *éleinek* halmazát, azaz $G = (V(G), E(G))$. A G egyszerű gráf *véges*, ha V véges halmaz.

A G gráf egy *diagramja* egy olyan lerajzolása, amiben a csúcsoknak (síkbeli) pontok felelnek meg, éleknek pedig olyan görbék[12], amik a két végpontot kötik össze, önmagukat nem metszik, és más végpontokat elkerülnek. A G gráf *szomszédossági mátrixa* az a $V(G) \times V(G)$ méretű mátrix, aminek (u, v) pozícióján az u és v közti élek száma áll ($u = v$ esetén a hurokélek számának kétszerese).

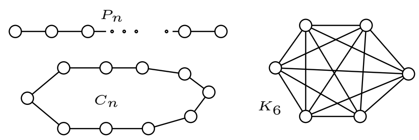
Az $e = \{u, v\}$ élt röviden $e = uv$-vel jelöljük; u és v az e él *végpontjai.* u és v *szomszédos*, ha $uv \in E$. e és f *párhuzamos élek*, ha végpontjaik azonosak[13]. *Hurokél* az olyan él, aminek végpontjai azonosak[14]. A $G = (V, E)$ pár *gráf*, ha $V \neq \emptyset$, E élhalmaz V-n, és párhuzamos és hurokél is megengedett. A G gráf *véges*, ha $V(G)$ és $E(G)$ is véges halmazok.

A G gráf v csúcsának $d(v)$ *foka* a v végpontú élek száma (hurokél kétszer számít): $d(v) := |\{e \in E : v \text{ végpontja } e\text{-nek}\}| + |\{e \in E : e \text{ hurokél és } v\text{-n}\}|$. A G gráf *maximális* ill. *minmális fokszámát* $\Delta(G) := \max\{d(v) : v \in V(G)\}$, ill. $\delta(G) := \min\{d(v) : v \in V(G)\}$ jelöli. A G gráf *(r-)reguláris*, ha minden pontjának ugyanannyi (r) a foka: $\Delta(G) = \delta(G)(= r)$.

Tétel: Ha G véges gráf, akkor $\sum_{v \in V(G)} d(v) = 2|E(G)$.

Biz: $\sum_{v \in V} d(v) = \sum_{v \in V} \sum_{\substack{e \in E \\ e = vx}} 1 = \sum_{e \in E} \sum_{\substack{v \in V \\ e = vx}} 1 = \sum_{e \in E} 2 = 2|E|$. (Szavakban: ha minden fokszámot összeadunk, akkor minden élt kétszer számolunk meg: egyszer az egyik, másszor a másik végpontjánál.) □

K_n az n-pontú *teljes gráf*: $|V(G)| = n$, és bármely két pont (egyszer) össze van kötve. P_n az n*-pontú út* C_n az n*-pontú kör*: $V(P_n) = V(C_n) = \{v_1, \ldots, v_n\}$, $E(P_n) = \{v_i v_{i+1} : 1 \leq i < n\}$, $E(C_n) = E(P_n) \cup \{v_1 v_n\}$. (ld. az ábrát)



Megfigyelés: $K_2 = P_2, K_3 = C_3$

$D = (V, A)$ *irányított gráf*, ha (1) $V \neq \emptyset$ és (2) $A \subseteq V^2$. (Minden élnek van egy irányítása. A diagramon nyilakkal jelölhető. Párhuzamos és hurokél itt is értelmezhető, akár kétféle irányú él is lehet két pont között. Az irányítatlan fogalmak többsége értelemszerűen kiterjeszthető.)

A G_1 és G_2 gráfok *izomorfak* ($G_1 \cong G_2$), ha létezik egy-egy $\varphi_V : V(G_1) \to V(G_2)$ és $\varphi_E : E(G_1) \to E(G_2)$ bijekció úgy, hogy $uv \in E(G) \iff \varphi_V(u)\varphi_V(v) = \varphi_E(uv)$. (Tkp. kölcs. egyért. megfelelés a pontok között, úgy, hogy tetsz. u és v annyiszor van összekötve G_1-ben, mint a megfelelőik G_2-ben.)

A G egyszerű gráf *komplementere* a $\overline{G} := (V(G), \binom{V}{2} \setminus E(G))$ gráf.

Példa: Önkomplementer (komplemeterükkel izomorf) gráfok. (Pl. P_4, C_5 ill. az 5-pontú „bika”.)

Tétel: Gráfok izomorfiája ekvivalenciareláció: tetszőleges G_1, G_2, G_3 gráfokra (1) $G_1 \cong G_1$, (2) $G_1 \cong G_2 \Rightarrow G_2 \cong G_1$ és (3) $G_1 \cong G_2 \cong G_3 \Rightarrow G_1 \cong G_3$.

A G gráf *élsorozata* egy olyan $(v_1, e_1, v_2, e_2, \ldots, v_k)$ sorozat, amire $e_i \in E(G)$ és $e_i = v_i v_{i+1}$ ($\forall 1 \leq i < k$). A *séta* olyan élsororzat, aminek minden éle különböző. A *körséta* olyan séta, aminek kiinduló és végpontja azonos: $v_1 = v_k$. Az *út* (ill. *kör*) olyan (kör)séta, aminek csúcsai (a végpontok azonosságától eltekintve) különbözőek.

Egyszerű gráf esetén az út (kör) azonosítható a hozzátartozó pontsorozattal vagy élsorozattal.

A G gráf *összefüggő (öf)*, ha bármely két pontja között vezet séta.

Állítás: A G gráfban pontosan akkor létezik u és v között séta, ha létezik u és v között út.

$u, v \in V(G)$-re $u \sim v$, ha létezik u és v között séta. A G gráf *komponense* a $\sim$ ekvivalenciareláció ekvivalenciaosztálya.

---

[12] Görbe helyett szerencsésebb töröttvonalról beszelni. Egy görbe egészen váratlan módon is tud viselkedni. Hagyjuk.

[13] Ezek értelmezéséhez vagy $E(G)$-t „multihalmaznak” tekintjük (egy él többszörös multiplicitással lehet eleme), vagy E csak az élek „neveinek” halmaza, és odagondolunk egy $E \to \binom{V}{2}$ leképezést is, ami megmutatja az élek végpontjait. Nem kínlódunk a fogalom precíz definíciójával: megelégszünk azzal, hogy lehetséges formalizálni azt, amit szemléletesen leírunk.

[14] Ehhez is módosítani kéne az él definícióját, de itt sem az absztrakt formalizmus a cél.

Állítás: A $\sim$ reláció ekvivalenciareláció: (1) $u \sim u$, (2) $u \sim v \Rightarrow v \sim u$, (3) $u \sim v \sim w \Rightarrow u \sim w$ tetszőleges $u, v, w \in V(G)$-re.

Következmény: $K \subseteq V(G)$ a G gráf komponense, ha bármely $u, v \in K$ között létezik G-séta, de nem létezik $u - v$ séta ha $u \in K$, $v \in V(G) \setminus K$.

Következmény: Minden gráf egyértelműen komponensekre bontható.

$G = (V, E)$ gráf, $e \in E$, $E' \subseteq E$, $v \in V$, $V' \subseteq V$. $G - e := (V, E \setminus \{e\})$ az e él törlésével keletkező gráf. $G - E' := (V, E \setminus E')$ az E' éleinek törlésével keletkező gráf. Legyen $E_v := \{e \in E : v \text{ végpontja } e\text{-nek}\}$. $G - v := (V \setminus \{v\}, E \setminus E_v)$ a v pont törlésével keletkező gráf. $E_{V'} := \{e \in E : e\text{nek van } V'\text{-beli végpontja}\}$. $G - V' := (V \setminus V', E \setminus E_{V'})$ a V' törlésével keletkező gráf.

Legyen G egy gráf és $V' \subseteq V(G)$, ill. $V^* := V \setminus V'$. G^* a *G gráf V^* által feszített részgráfja*, ha $G^* = G - V'$. H a *G részgráfja*, ha $H = (G - V') - E'$ alkalmas $V' \subseteq V(G)$ és $E' \subseteq E(G)$-re.

13. Fák alaptulajdonságai

A G gráf *erdő*, ha körmentes, azaz nem tartalmaz kört. A G gráf *fa*, ha öf erdő, azaz ha körmentes és összefüggő.

Tétel: Tegyük fel, hogy G n-pontú, körmentes gráf. G pontosan akkor összefüggő, ha $n - 1$ éle van.

Biz: Építsük fel F-t az n-pontú üresgráfból élek behúzásával. A körmentesség miatt mindig két különböző komponens közt kell élt behúzni (különben kört kapnánk). Két komponens közé behúzott él 1-gyel csökkenti a komponensek számat. Ha G öf, akkor n-ről 1-re csökken a komponensek száma, tehát $n - 1$ élt húztunk be. Másfelől, ha G $(n-1)$-élű, akkor komponenseinek száma $n - (n-1) = 1$, tehát G öf. $\square$

Tétel: Legyen G n-pontú, $(n-1)$-élű, összefüggő, egyszerű gráf. Ekkor G körmentes.

Biz: Indirekt. Ha G-ben van egy k-pontú kör, akkor e kör k élének behúzása után $n-k+1$ komponens van. A további $n-1-k$ él mindengyike legfeljebb 1-gyel csökkenti a kompontensek számát, végül tehát legalább $n - k + 1 - (n - 1 - k) = 2$ komponens lesz, azaz G nem öf. Ellentmondás. $\square$

Köv.: F fa $\iff$ G körmentes, öf $\iff$ $|E(G)| = |V(G)| - 1$, G körmentes $\iff$ $|E(G)| = |V(G)| - 1$, G öf $\iff$ G minimális öf (bármely élt elhagyva G szétesik) $\iff$ G maximális körmentes (tetsz. új élt behúzva kör keletkezik.)

Köv.: Minden véges, öf G gráfnak létezik *feszítőfája*, azaz olyan F részgráfja, amire F fa és $V(G) = V(F)$.

Biz: Hagyjunk el éleket, míg a gráf öf marad. Végül egy min. öf gráfot, azaz fát kapunk. Ez fesz.fa lesz, hisz nem hagytunk el pontot. $\square$

Def: F fa, $v \in V(F)$ az F *levele*, ha $d(v) = 1$.

Tétel: Minden, legalább 2-pontú fának van legalább két levele.

Biz: Tekintsünk egy leghosszabb P utat. P végpontjából sem indulhat további él: ha ugyanis újabb pontba futna, akkor P nem lenne leghosszabb, ha pedig P egy pontjába, akkor a gráf nem lenne körmentes. $\square$

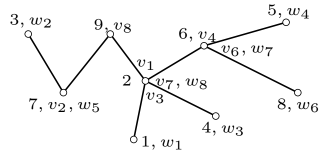
14. A Cayley tétel

Alapprobléma: Hány n-pontú fa van? Izomorfia erejéig: n = 1-re 1, n = 2-re 1, n = 3-ra 1, n = 4-re 2 ($K_{1,3}$ és P_4), n = 5-re 3 (2-levelű, 3-levelű, 4-levelű), n = 6-ra 6 (2-levelű, $2 \times$ 3-levelű, $2 \times$ 4-levelű, 5-levelű), ... Nehéz.

Számozott csúcsokon (izomorf fákat többször megszámolva) n = 1-re 1, n = 2-re 1, n = 3-ra 3, n = 4-re 16 ($4 \times K_{1,3}$ és $12 \times P_4$), n = 5-re 125 ($60 \times$ 2-levelű, $60 \times$ 3-levelű, $5 \times$ 4-levelű), n = 6-ra sok.

Cayley tétel: Az $\{1, 2, \ldots, n\}$ ponthalmazon n^{n-2} különböző fa adható meg.

Biz: (A Prüfer-kód segítségével) Részfák egy $F = F_1 > F_2 > \ldots > F_{n-1}$ sorozatát konstruáljuk az alábbiak szerint. Legyen $i \in [n-1]$-re w_i az F_i legkisebb sorszámú levele, v_i pedig w_i F_i-beli szomszédja. Legyen továbbá $F_{i+1} := F_i - w_i$. (Az aktuális F_i fának a legkisebb w_i levelét hagyjuk el, ami v_i-hez csatlakozik.)



Levéltörlési sorrend: 1, 3, 4, 5, 7, 8, 6, 2
Prüfer kód: (2, 7, 2, 6, 9, 6, 2)

Megfigyelés: $F_{n-1} = \{n\}$, azaz $v_{n-1} = n$.

Biz: Az n csúcsot sosem hagytuk el, hisz mindig legl. 2 levél volt. $\square$

A fenti F fa *Prüfer-kódja* $P(F) = (v_1, v_2, \ldots, v_{n-2})$. A definícióból adódik, hogy az F_i fa Prüfer-kódja $P(F_i) = (v_i, v_{i+1}, \ldots, v_{n-2})$. Az is világos, hogy minden fához egyértelműen tartozik Prüfer-kód. Azt kell igazolni, hogy minden $(n-2)$-hosszú sorozat pontosan egy fa Prüfer-kódja, hisz ekkor a lehetséges n^{n-2} Prüfer-kód kölcs. egyért. megfelel a vizsgált fáknak.

Megfigyelés: Az F fa Prüfer-kódjában F bármely v csúcsa $(d(v)-1)$-szer szerepel.

Biz: Láttuk, hogy $F_{n-1} = \{n\}$, ezért a $v = n$ pont éppen annyiszor szerepel a $v_1, v_2, \dots, v_{n-1}$ pontok között, ahányszor egy-egy szomszédja törlésre került, azaz $d(n)$-szer. Mivel $v_{n-1} = n$, ezért a Prüfer-kódban $d(n)-1$-szer szerepel az n.

Legyen most $k < n$. A k csúcs pontosan akkor szerepel a Prüfer-kódban, ha töröljük egy szomszédját, azaz, ha fokszáma eggyel csökken. Amikor k fokszáma 1-re csökken, akkor az utolsó k-ból induló él már k-nak (és nem a szomszédjának) a törlése miatt lesz törölve, tehát ekkor már nem k kerül a Prüfer-kódba. (Ez az él egyébként a k-ból az n csúcs felé vezető út első éle, hisz a részfák n-re zsugorodnak.) Tehát k is $d(k)-1$-szer bukkan fel a Prüfer-kódban. □

Köv.: Az F fa levelei pontosan F-nek a Prüfer-kódban nem szereplő csúcsai.

Biz: A levelek az 1-fokú csúcsok, vagyis pontosan azok az 1 és n közti számok, amik 0-szor szerepelnek a Prüfer-kódban. □

Köv.: w_1 a legkisebb olyan természetes szám, ami nem szerepel a $v_1, v_2, \dots, v_{n-1}$ sorozatban. □

Láttuk, hogy az F Prüfer-kódjának k-dik jegytől induló végszelete az F_k fa Prüfer-kódja. Ezért w_k (az F_k fa legkisebb indexű levele), a legkisebb olyan szám, $\{1, 2, \dots, n\} \setminus \{w_1, w_2, \dots, w_{k-1}\}$ között, ami nem szerepel a F_k Prüfer-kódjában, azaz $v_k, v_{k+1}, \dots, v_{n-2}$ között. Más szóval, a legkisebb olyan szám, ami nem szerepel a $w_1, w_2, \dots, w_{k-1}, v_k, v_{k+1}, \dots, v_{n-1}$ sorozatban. (Ez $k = n-1$-re is igaz.) Ha tehát a Prüfer-kód csakugyan egy F fához tartozik, F egyértelműen rekonstruálható: be kell húzni a $v_{n-1}w_{n-1}, v_{n-2}w_{n-2}, \dots, v_1w_1$ éleket az $[n]$ ponthalmazon. (Az éleket ebben a sorrendben érdemes behúzni, mert így mindig egy fát bővítünk, amit emiatt könnyű élkereszteződés nélkül lerajzolni.)

Azt kell még igazolni, hogy a $(v_1, v_2, \dots, v_{n-2})$ Prüfer-kódból egyértelműen rekonstrukálható F gráf olyan fa, aminek Prüfer-kódja $(v_1, v_2, \dots, v_{n-2})$.

Legyen F'_k a $w_{n-1}v_{n-1}$, $w_{n-2}v_{n-2}$, …, w_kv_k élek feszítette gráf. Azt mutatjuk meg k szerinti indukcióval, hogy F'_k olyan fa, aminek Prüfer-kódja $(v_k, v_{k+1}, \dots v_{n-2})$. (Ez $k = 1$ esetén épp azt adja, amit szeretnénk.) Az indukciós állítás $k = n-1$-re világos, hisz F'_{n-1} egypontú, és Prüfer-kódja üres.

Megfigyelés: (1) $w_1, w_2, \dots, w_{n-1}, n$ különbözőek. (Hisz w_j választásakor w_i tiltott ha $i < j$.)
(2) $v_k \notin \{w_1, w_2, \dots, w_k\}$ (w_i választásakor $i \le k$-ra $w_i \neq v_k$) , így $v_k \in \{w_{k+1}, w_{k+2}, \dots, w_{n-1}, n\}$. □

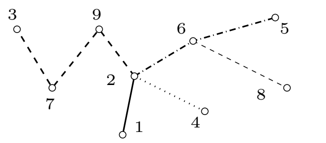
Tegyük fel, hogy F_{k+1} fa, és hogy Prüfer-kódja csakugyan $(v_{k+1}, \dots v_{n-2})$. (1) és (2) miatt $V(F'_{k+1}) = \{n, w_{n-1}, v_{n-2}, w_{n-2}, \dots, v_{k+1}, w_{k+1}\} = \{n, w_{n-2}, w_{n-3}, \dots, w_{k+1}\}$, ezért (1) miatt F'_k csakugyan fa, aminek w_k levele. Azt csupán bizonyítani, hogy w_k az F'_k legkisebb levele. F'_{k+1} Prüfer-kódjából a fenti Következmény alapján az látszik, hogy F'_{k+1} leveleinek halmaza

$$L(F'_{k+1}) = \{w_{k+1}, \dots, w_{n-1}, n\} \setminus \{v_{k+1}, \dots, v_{n-1}\} = [n] \setminus (\{w_1, w_2, \dots, w_k\} \cup \{v_{k+1}, \dots, v_{n-1}\}) \ .$$

Világos, hogy $L(F'_k) = (L(F'_{k+1}) \setminus \{v_k\}) \cup \{w_k\} = [n] \setminus (\{w_1, w_2, \dots, w_{k-1}\} \cup \{v_k, v_{k+1}, \dots, v_{n-1}\})$, és az F_k Prüfer-kódjára vonatkozó megfigyelés szerint w_k-t éppen e halmaz legkisebb eleme. □

Alkalmazás: Véletlen fa generálása n ponton: Egy n-oldalú dobókockát $(n-2)$-szer feldobva, a keletkező sorozat egy egyenletes eloszlás szerinti véletlen fa Prüfer-kódja. □

A Cayley tételre megadunk egy nemsztenderd, alternatív bizonyítást is. Előnye, hogy valamivel közvetlenebbül látszik a kölcsönösen egyértelmű megfeleltetés a fák és az azokat leíró ismétléses variációk között, továbbá, hogy a fa rekonstrukciója a kód alapján valamivel egyszerűbb.



$P_1 = \{1\}$, $P_2 = \{\mathbf{1}, 2\}$, $P_3 = \{\mathbf{2}, \mathbf{9}, \mathbf{7}, 3\}$
$P_4 = \{\mathbf{2}, 4\}$, $P_5 = \{\mathbf{2}, \mathbf{6}, 5\}$, $P_6 = \{6\}$
$P_7 = \{7\}$, $P_8 = \{\mathbf{6}, 8\}$, $P_9 = \{9\}$
Refürp kód: $(1, 2, 9, 7, 2, 2, 6, 6)$

Legyen tehát F egy fa az $v_1, v_2, \dots, v_n$ pontokon. Az F fában (egyértelműen) létezik egy P_2 irányított út v_1-ből v_2-be. A P_2 út valamelyik pontjából létezik egy egyértelmű irányított P_3 út v_3-ba úgy, hogy P_3 minden (irányítatlan) éle különböző a P_2-beliektől. (Ha v_3 rajta van P_2-n, akkor P_3-nak egyetlen pontja és 0 éle van.) Általában, ha már ismerjük a $P_2, P_3, \dots, P_i$ utakat, akkor P_{i+1} az az (egyértelműen létező) v_{i+1}-be vezető út lesz, aminek kiindulópontja rajta van a $P_2, P_3, \dots, P_i$ utak által alkotott részfán, de ettől eltekintve diszjunkt tőle. Világos, hogy a fenti eljárás az F fát a $P_2, P_3, \dots, P_n$ utak uniójára bontja fel, és ezen utak élei páronként különbözőek.

Ha $P_i = (v_{a(1)}, v_{a(2)}, \dots, v_{a(k)}, v_i)$ egy felbontásbeli út, akkor legyen P_i *kódja* $a(1), a(2), \dots, a(k)$. (Ha tehát $P_i = (v_i)$ egy egypontú út, akkor a kódja üres.) Legyen az F fa ***Refürp-kódja*** az F felbontásában szereplő $P_2, P_3, \dots, P_n$ irányított utak kódjainak egymásutánja. Világos, hogy ha F egy fa a $v_1, v_2, \dots, v_n$ pontokon, akkor egyértelműen létezik Refürp-kódja. E Refürp-kód ráádásul $n-1$ számból áll, hiszen minden P_i út kódja megegyezik P_i éleinek számával, tehát az F fa Refürp-kódja is épp olyan hosszú, mint ahány éle van F-nek.

Világos, hogy a Refürp-kód első jegye 1 (hisz P_2 a v_1 csúcsból kiindulva fut a $v_1 \neq v_2$ csúcsba), és a kód további $n-2$ jegyének mindegyike az 1 és n közti egészek közül kerül ki. Így az ismétléses variációkról tanultak alapján legfeljebb n^{n-2}-féle Refürp-kód kódolhat n-pontú fát.

Azt kell csupán igazolni, hogy ha $1 = r(1), r(2), r(3), \dots, r(n-1)$ egy olyan számsorozat, amiben minden $r(i)$ egy 1 és n közti egész, akkor egyértelműen létezik egy olyan F fa, aminek Refürp-kódja $r(1), r(2), r(3), \dots, r(n-1)$. A cél tehát nem más, mint az $r(1), r(2), \dots, r(n-1)$ számsorozatot felbontani $n-1$ sorozat egymásutánjára (ezek némelyike üres lesz), úgy, hogy e sorozatok rendre a $P_2, P_3, \dots, P_n$ utak kódjai legyenek. Az első kérdés tehát, hogy az $r(1), r(2), \dots, r(n-1)$ számsorozatban melyik $r(i)$ lesz a P_2 út kódjának utolsó jegye, azaz melyik $r(i+1)$ lesz a P_3 kódjának első jegye, más szóval a P_3 út kiindulópontjának indexe[15]. A P_3 út kétféle lehet: kiindulópontja vagy v_2, vagy a P_2 útnak egy v_2-től

[15]ha P_3 egypontú, akkor itt P_3 helyett az első nemegypontú P_i útról van szó, hiszen annak a kódja kezdődik $r(i+1)$-gyel.

különböző pontja, aminek indexe tehát szerepel P_2 kódjában. Ezért a P_3 út kódjának kezdete (vagyis az ominózus $r(i+1)$) az első olyan jegye lesz F Refürp-kódjának, amire $r(i+1)=2$, vagy $r(i+1)$ már korábban előfordult F Refürp-kódjában.

A fenti módszer általánosságban is működik. Tegyük fel, hogy az $r(1),\ldots,r(n-1)$ sorozatból már meghatároztuk a $P_2,P_3,\ldots,P_i$ utak kódjait. A cél a P_{i+1} út kódjának meghatározása. Legyen a P_i kódjának utolsó jegye az F Refürp-kódjának k-dik jegye, vagyis $r(k)$. Világos, hogy ha már valamelyik korábbi P_j út használta a v_{i+1} csúcsot, akkor $i+1$ már korábban szerepelt a P_j kódjában, azaz $r(l)=i+1$ valamely $l\le k$ esetén. Ekkor P_{i+1} kódja üres, és rátérhetünk P_{i+2}-re. Ellenkező esetben, vagyis ha $i+1$ nem szerepelt a Refürp-kód $r(k)$-ig tartó részében, akkor v_{i+1} nem pontja a $P_2,P_3,\ldots,P_i$ utak egyikének sem, tehát P_{i+1} legalább kétpontú, és csupán azt kell megállapítani, hogy P_{i+1} ($r(k+1)$-gyel kezdődő) kódja hol ér véget, azaz melyik $r(s+1)$-gyel kezdődik a P_{i+1}-t követő, első, legalább kétpontú P_m út kódja. A P_m út kétféle lehet: vagy a $v_2,v_3,\ldots,v_{i+1}$ csúcsok valamelyike a kiindulópontja, vagy egy olyan pont, aminek indexe a $P_2,P_3,\ldots P_{i+1}$ útak valamelyikének kódjában már szerepelt korábban. Ezért $s+1$ olyan szám, amire

$$s>k \qquad \text{és} \qquad r(s+1)\in\{2,3,\ldots,i+1\}\cup\{r(1),r(2),\ldots,r(s)\} \tag{1}$$

teljesül. Világos, hogy ha $s+1$-re (1) fennáll, akkor $r(s+1)$ nem lehet benne P_{i+1} kódjában, tehát $s+1$ a legkisebb olyan szám, ami teljesíti az (1) feltételt. Ezzel pedig egyértelműen meghatároztuk P_{i+1} kódját: $r(k+1),r(k+2),\ldots,r(s)$.

Ha pedig ismerjük a $P_2,P_3,\ldots,P_n$ utak kódjait, akkor mindezen utak rekonstruálhatóak, tehát uniójuk, az F' gráf is. Kell, hogy F' fa. Világos, hogy minden P_i kiindulópontja egy előző P_j útnak pontja, tehát a F' összefüggő. Minden P_i-nek annyi éle van, mint a kódjának hossza, tehát F'-nek $n-1$ éle van, továbbá F' tartalmazza minden P_i út végpontjait, tehát a $v_2,v_3,\ldots,v_n$ pontokat, valamint P_2 kezdőpontját, v_1-t. Tehát F' egy n-pontú, $(n-1)$-élű összefüggő gráf, azaz F csakugyan fa. Az F' konstrukciójából pedig azonnal adódik, hogy P_i egy olyan irányított út, aminek a kiindulópontja egy korábbi P_j pont valamelyike, végpontja v_i, tehát F' Refürp kódja csakugyan $r(1),r(2),r(3),\ldots,r(n-1)$.

Megjegyzés: A Refürp-kódból a fa rekonstrukciója valójában még egyszerűbb. Legyen $r(1),r(2),\ldots,r(n-1)$ egy Refürp-kód. A rekonstrukció $n-1$ lépésben történik: az i-dik lépésben $v_{r(i)}$-ből indítunk egy e_i élt. Az e_i él másik végpontja $v_{r(i+1)}$ lesz, ha $i+1\le n-1$ és $v_{r(i+1)}$ nem szerepel a már felépített fában. Egyébként az a v_j lesz az e_i másik végpontja, amire j a legkisebb olyan pozitív csúcsindex, ami nem szerepel a már felépített fában.

Alkalmazás: Hány olyan F fa van n címkézett ponton, amiben az 1 és 2 címkéjű pontok között futó út F-nek pontosan k élét tartalmazza? (Világos, hogy a Refürp-kód első $k+1$ jegyét nem választhatjuk teljesen szabadon, így $(n-1)\cdot(n-2)\cdot\ldots\cdot(n-k)\cdot(k+1)\cdot n^{n-k-3}$ adódik. Az is látszik, hogyan kell ilyen tulajdonságú véletlen fát generálni.)

Szorgalmi házi feladat: Mi köze a Prüfer-kódnak a Refürp-kódhoz? (A helyes megfejtők díja a szerző elismerése.)

15. A Kruskal algoritmus

Alapprobléma: Egy vízműből kell n várost ivóvízzel ellátni. Úgy kell a vezetékhálózatot megépíteni, hogy csak városokon belül lehet vezetékeket elágaztatni, és a költségminimalizálás a cél.

Formálisan: Adott $G=(V,E)$ lehetséges utak öf gráfja, $k:E\to\mathbb{R}_+$ költségfv. $F\subseteq E$-re $k(F):=\sum_{f\in F}k(f)$. Keressünk egy olyan $F\subseteq E$ élhamazt, amire (V,F) fa, és ezen belül $k(F)$ minimális. Az ilyen (V,F) fát *minimális költségű feszítőfának* nevezzük.

Kruskal algoritmusa:

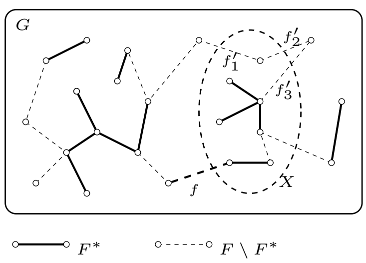
Input: $G=(V,E)$ öf gráf, $k:E\to\mathbb{R}_+$ költségfv. Output: $F=F_m$ min. ktg-ű feszítőfa.

Az algoritmus működése:

Legyen $E=\{e_1,e_2,\ldots,e_m\}$, növekvő költség szerint sorbarendezve (azaz $k(e_1)\le k(e_2)\le\ldots\le k(e_m)$) és legyen $F_0:=\emptyset$. Sorban minden e_i-ről eldöntjük, hogy bevesszük-e az F_i élhalmazba: ha F_{i-1} az e_i él hozzávételével körmentes marad, akkor $F_i:=F_{i-1}\cup\{e_i\}$ különben, ha F_{i-1}-be e_i-t behúzva kör keletkezik, akkor $F_i:=F_{i-1}$.

Def: Adott $G=(V,E)$ öf gráf ill $k:E\to\mathbb{R}$ költségfüggvény esetén egy $F^*\subseteq E$ élhalmazt *optimális*nak nevezünk, ha létezik G-nek olyan minimális költségű (V,F) feszítőfája, amire $F^*\subseteq F$.

Lemma: Legyen $G=(V,E),k:E\to\mathbb{R}_+$. Tegyük fel, $F^*\subseteq E$ optimális, továbbá, hogy $X\subset V$ olyan, hogy nem vezet X és $V\setminus X$ között F^*-beli él. Legyen az X és $V\setminus X$ között vezető élek között f egy minimális költségű. Ekkor $F^*\cup\{f\}$ is optimális.



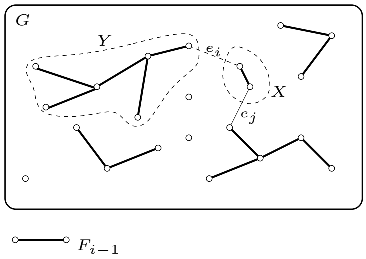
Biz: F^* optimalitása miatt létezik egy (V,F) minimális költségű feszítőfa, amire $F^*\subseteq F$. Ha $f\in F$, akkor (V,F) az $F^*\cup\{f\}$ optimalitását is bizonyítja. Ha $f\notin F$, akkor a (V,F) fában létezik egy út f két végpontja között. Ez az út X-ből indul, és $V\setminus X$-ben ér véget, tehát tartalmaz legalább egy f' élt, ami X és $V-X$ között vezet. Az f él választása miatt $k(f)\le k(f')$ áll. Ha a (V,F) fából elhagyjuk f'-t, akkor a fa két komponensre esik, ráadásul f végpontjai különböző komponensekben lesznek.

Ezért f behúzásával $(V,F\setminus\{f'\}\cup\{f\})$ szintén fa lesz, és a költsége sem lehet több, mint (V,F) költsége volt. Tehát egy, az $F^*\cup\{f\}$ élhalmazt tartalmazó, minimális költségű feszítőfát kaptunk. □

Tétel: A Kruskal algoritmus konstruálta (V,F) a G gráf egy minimális költségű feszítőfája.

Biz: Az F_i definíciójából világos, hogy F körmentes. A (V,F) gráfba bármely $e_j\in E\setminus F$-beli élt behúzva kört kapunk, hiszen már az F_{j-1}-be behúzva is kör keletkezett. Mivel G öf, ezért (V,F) is öf, tehát csakugyan feszítőfája G-nek.

Teljes indukcióval igazoljuk (i szerint), hogy F_i optimális. Ez elegendő, hisz ekkor az F_m feszítőfa is optimális, és az ezt bizonyító minimális költségű feszítőfa csakis maga (V, F_m) lehet. Az állítás $F_0 = \emptyset$ esetén triviális.



Tegyük fel, hogy F_{i-1} optimális. Ha $F_i = F_{i-1}$, akkor F_i nyilvánvalóan optimális. Egyébként $F_i = F_{i-1} \cup \{e_i\}$. Figyeljük meg, hogy az e_i a (V, F_{i-1}) gráf két komponense (mondjuk X és Y) között fut (egyébként kört hozna létre). Az is világos, hogy e_i előtt egyetlen X és $V \setminus X$ között futó e_j él sem került sorra, hisz akkor e_j-t be kellett volna venni, és a komponens X-nél bővebb volna. Tehát e_i az X és $V \setminus X$ között futó élek küzül az egyik legolcsóbb. De ekkor az előző lemma szerint $F_i = F_{i-1} \cup \{e_i\}$ is optimális. □

Alkalmazás: $G = (V, E)$ véges gráf, $V_1, V_2, \ldots, V_k \subseteq V$. Létezik-e G-nek olyan feszítőfája, ami minden egyes V_i-nek tartalmazza egy feszítőfáját?

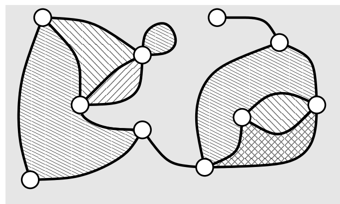
Legyen $k(e)$ azon V_i-k száma, amik e mindkét végpontját tartalmazzák, azaz $k(e) = k_1(e) + k_2(e) + \ldots + k_s(e)$, ahol $k_i(e) = 1$, ha e végpontjai V_i-ben vannak, egyébként $k_i(e) = 0$. Ha F fa G-ben, akkor

$$k(F) = \sum_{f \in F} k(f) = \sum_{f \in F} \sum_{j=1}^{s} k_j(f) = \sum_{j=1}^{s} \sum_{f \in F} k_j(f) \leq \sum_{j=1}^{s} |V_j| - 1 =: c\ ,$$

és pontosan akor áll egyenlőség, ha F egy olyan feszítőfája G-nek, ami minden H_i-t belülről feszít.

Keressünk egy maximális k-költségű F feszítőfát G-ben. Ha ennek költsége c, akkor F jó fa, ilyet kerestünk. Ha a költség c-nél kisebb, akkor nem létezik megfelelő fa. □

16. Síkgráfok



A G gráf egy ***síkbarajzolása*** a G egy olyan diagramja, amiben az éleknek megfelelő görbék (töröttvonalak) csak végpontokban metszhetik egymást. G ***síkbarajzolható (sr)***, ha létezik síkbarajzolása. A síkbarajzolás a síkot *tartományokra (lapokra)* osztja. Lesz egy végtelen tartomány, az ún. *külső* tartomány. Gömbre rajzoláson lényegében ugyanezt értjük, csak sík helyett a gömb felszínén dolgozunk, külső tartományról nem beszélünk.

Tétel: A G gráf pontosan akkor síkbarajzolható, ha gömbre rajzolható.

Biz: *Sztereografikus projekcióval.* (A gömböt úgy helyezzük el, hogy a síkot a déli sarkon érintse, és az északi sarokból (egyenes) vetítéssel a sík pontjai bijektíven megfelelnek az északisark-mentes gömbfelszín pontjainak. (A síkbeli inverzió általánosítása. Vicces tulajdonságai vannak: a sík egyeneseit a gömbfelszín északi sarkon átmenő köreibe viszi, a sík köreit a gömbfelszín északi sarokra nem illeszkedő köreibe, és viszont. Ráadásul szögtartó: térképészek ezért szeretik.))

Tetszőleges síkbarajzolást a sztereografikus projekció gömbre rajzolásba visz, továbbá, ha az északi sarok egy gömbi tartomány belsejében fekszik, akkor gömbre rajzolást síkbarajzolásba képez. A gömböt odébbgurítva és az új északi sarokról visszavetítve látszik, hogy tetszőleges síkbarajzolás bármely T tartományához létezik egy másik síkbarajzolás, amiben T a külső tartomány. □

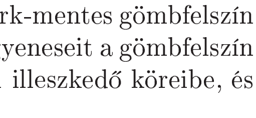
Köv.: Tetszőleges konvex poliéder élhálója síkbarajzolható.

Biz: Vetítsük az élhálót a poliéder egy belső P pontjából egy P közepű gömbre. Ezáltal az élháló gráfja gömbre rajzolható, azaz síkbarajzolható.

Megjegyzés: A fenti állítás megfordítása úgy igaz, hogy tetszőleges G sr gráfhoz létezik egy P konvex poliéder, úgy, hogy G a P élhálójának egy *részgráfjával* izomorf.

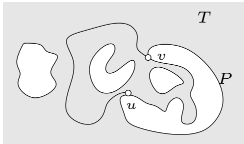
Tétel: Ha a G síkbarajzolható gráf csúcsainak, tartományainak, éleinek és komponenseinek száma rendre n, t, e és k, akkor $n + t = e + k + 1$.

Biz: Élszám szerinti indukcióval bizonyítjuk, hogy ha G egy n-csúcsú, e-élű síkbarajzolható gráf, akkor igaz rá az állítás. Ha a G_0 gráf élszáma $e_0 = 0$, akkor komponenseinek száma $k_0 = n$ (hisz minden csúcs önálló komponens) és a létrejövő síktartományok száma $t_0 = 1$, tehát igaz az állítás. Tegyük fel, hogy az n-pontú, i éllel rendelkező, síkbarajzolható gráfokra már bebizonyítottuk az állítást. Legyen G_i egy tetszőleges n-pontú síkbarajzolható gráf, éleinek, tartományainak ill. komponenseinek száma pedig legyen rendre $e_i = i$, t_i ill. k_i. Húzzunk be G_i-be egy $(i+1)$-dik élt (mondjuk uv-t). Így kapjuk a G_{i+1} gráfot. Vizsgáljuk meg, G_{i+1} megfelelő paramétereit, azaz az $e_{i+1}, t_{i+1}, k_{i+1}$ számokat!



Világos, hogy $e_{i+1} = i + 1$. Két esetet különböztetünk meg. Ha u és v a G_i gráf két különböző komponensében található, akkor az uv él G_i két komponensét köti össze, tehát $k_{i+1} = k_i - 1$. Az uv él a G_i egy tartományán (mondjuk T-n) belül halad, tehát G_i minden T-től különböző tartománya egyúttal G_{i+1}-nek is tartománya lesz.

Azt kell csupán látni, hogy T (elhagyva belőle az uv élt) szintén tartománya lesz a G_{i+1} gráfnak, hiszen ha T-t a behúzott uv él kettévágná, akkor az egyik keletkező T' tartomány határa tartalmazna u-t a v-vel összekötő élsorozatot a G_i gráfban, ami ellentmond annak, hogy u és v a G_i különböző tartományaiban található. Tehát $t_{i+1} = t_i$, azaz $n + t_{i+1} = n + t_i = e_i + k_i + 1 = i + k_i + 1 = (i+1) + (k_i - 1) + 1) = e_{i+1} + k_{i+1} + 1$, vagyis az indukciós lépést bebizonyítottuk.



A másik eset az, amikor u és v egyazon komponensbe esnek, azaz létezik u és v közé behúzott tartomány határán egy u-ból v-be vezető P út. Ekkor $k_{i+1} = k_i$, hiszen egy komponensen belül élt behúzva ugyanazok a ponthalmazok maradtak a G_{i+1} gráf komponensei, amik G_i-é voltak. Legyen T a G_i gráfnak az a tartománya, aminek a belsejében vezet az imént behúzott uv él.
Világos, hogy G_i minden T-től különböző tartománya tartománya lesz G_{i+1}-nek is, továbbá a T tartomány két tartományra esik szét, amik az uv él mentén határosak. (Az egyik tartományt az uv él és a P út alkotta kör határolni fogja. Azt kaptuk tehát, hogy $t_{i+1} = t_i + 1$ ezért $n + t_{i+1} = n + t_i + 1 = e_i + k_i + 1 + 1 = i + 1 + k_{i+1} + 1 = e_{i+1} + k_{i+1} + 1$. Igazoltuk az indukciós lépést, a tételt beláttuk. □

Köv.: (**Euler-formula**) Ha egy összefüggő, n-pontú, e-élű gráf t tartománnyal síkbarajzolható, akkor $n + t = e + 2$.

Biz: Ha G összefüggő, akkor $k = 1$ komponense van, tehát az előző tétel szerint $n + t = e + k + 1 = e + 1 + 1 = e + 2$. □

Köv.: Ha G sr, akkor bármely síkbarajzolásának ugyanannyi tartománya van. □

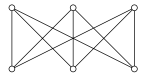
Köv.: Ha G egyszerű, legalább 3-pontú, sr gráf, akkor $e \leq 3n - 6$.

Biz: Húzzunk be annyi további élt a síkbarajzolhatóság megtartásával, amennyit csak tudunk. A kapott gráfnak e' db éle, t tartománya és n csúcsa lesz. Minden tartományt 3 él, és minden él 2 tartományt határol, ezért $2e' = 3t = 3(e' + 2 - n) = 3e' + 6 - 3n \Rightarrow 3n - 6 = e' \geq e$. □

Megjegyzés: Ha G sr és egyszerű, akkor $(|E(G)| = 3|V(G)| - 6) \iff (G$ minden lapja háromszög).

Köv.: Ha G sr és egyszerű, akkor van legfeljebb 5-ödfokú csúcsa, azaz $\delta(G) \leq 5$.

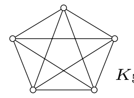
Biz: Indirekt. Ha $d(v) \geq 6\ \forall v \in V \Rightarrow 2e = \sum_{v \in V} d(v) \geq 6n \Rightarrow e \geq 3n$, ellentmondás. □



$K_{3,3}$

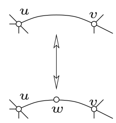
Köv.: Sem K_5, sem $K_{3,3}$ nem síkbarajzolható.

Biz: Indirekt. K_5-re: $n = 5, e = 10 \Rightarrow t = 7 \Rightarrow 21 = 3t \leq 2e = 20$, ellentmondás. $K_{3,3}$-ra: $n = 6, e = 9 \Rightarrow t = 5$. Mivel $K_{3,3}$ C_3-mentes, ezért minden tartományt legalább 4 él határol: $20 = 4t \leq 2e = 18$, ellentmondás. □



K_5

Def: A G és H gráfok *topologikusan izomorfak*, ha H megkapható G-ből az alábbi lépések ismételt alkalmazásával:



1. Törlünk egy uv gráfélt, és beveszünk egy új, másodfokú csúcsot, aminek a szomszédai u és v. (Ha úgy tetszik, egy w csúcsot ültetünk az uv élre.)
2. Törlünk egy másodfokú x csúcsot, és éllel összekötjük x két szomszédját.

Megjegyzés: A fenti definícióban a két lépés egymás „inverze”, azaz ha G-ből az 1. lépés egy G' gráfot képez, akkor G'-ből egy 2. lépés konstruálja meg G-t, és viszont.

Kuratowski tétel: A G gráf pontosan akkor sr, ha nem tartalmaz sem $K_{3,3}$-mal, sem K_5-tel topologikusan izomorf részgráfot.

Biz: Szükségesség: ha G sr, akkor minden H részgráfja sr, továbbá ha H és K topologikusan izomorf, és H sr, akkor K is sr. Így $K = K_5$ ill. $K = K_{3,3}$ nem lehetséges. Az elégségesség nem triviális, itt nem bizonyítjuk. □

Fáry-Wagner tétel: Ha G egyszerű, sr gráf, akkor G úgy is síkba rajzolható, hogy minden él egyenes szakaszként van lerajzolva.

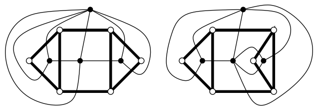
„**Biz:** ” (Vázlat) A síkbarajzolhatóság megtartásával új éleket behúzva feltehető, hogy G-nek maximálisan sok $(3n-6)$ éle van, így tetszőleges síkbarajzoláskor G minden lapját három él határolja. Rajzoljuk le G-t a síkba úgy, hogy az éleknek megfelelő görbék töröttvonalak legyenek. Vegyünk fel a síkon egy olyan ABC háromszöget, aminek a lerajzolt G teljes egészében a belsejében van. Töröttvonalak segítségével kössük össze G külső lapjának három csúcsát az A, B, C csúcsokkal úgy, hogy a síkbarajzoltságot megtartjuk és A, B, C mindegyikével G külső lapjának egy-egy csúcsát kötjük össze.

Legyenek a G' gráf csúcsai a lerajzolásbeli töröttvonalak törés- és végpontjai, G' élei pedig a töröttvonalak szakaszai. Világos, hogy G' is síkbarajzolt gráf. Ha ennek a síkbarajzolásnak van olyan lapja, ami nem háromszög, akkor azt a sokszöget húrjai segítségével fel tudjuk darabolni háromszögekre. (Ugyanis tetszőleges sokszögbe be tudunk húzni olyan húrt, ami teljes egészében a sokszög belsejében halad: vagy egy konvex X csúcs két szomszédja összeköthető, vagy X összeköthető a hozzá legközelebbi, a konvex szögtartományba eső csúccsal.)

Igy megkapjuk egy G'-t részgráfként tartalmazó, csupa háromoldalú tartománnyal rendelkező G^* gráf egyenes szakaszokkal való síkbarajzolását. Helyettesítsük G^* minden élét egy gumiszalaggal, majd hagyjuk, hogy a gumik összehúzódásával a rendszer egyensúlyba kerüljön, azaz a tárolt rugalmas energia minimális legyen. Nem triviális, de igaz, hogy ez bekövetkezik. Miközben a rendszer egyensúlyba kerül, nem történhet meg, hogy egy csúcspont átkerül egy gumiszalag túloldalára. Az egyensúlyi helyzetben minden gumi egyenes lesz, és csak G^* csúcsaiban metszik egymást.

Egyenként hagyjuk el $E(G^*) \setminus E(G')$ éleit, és hagyjuk, hogy a rendszer egyensúlyba kerüljön. Itt sem történik meg, hogy csúcs egy gumiszalag túloldalára kerül, ezért az összes szükséges elhagyás után G' olyan síkbarajzolását kapjuk, amiben minden él egy-egy szakasz, és a G éleinek egy egyenesbe eső szakaszok felelnek meg. Ez pedig G kívánt lerajzolását adja. (Ha G-nek nemcsak háromszöglapjai voltak, akkor G részgráfja a lerajzolt gráfnak, ami nem változtat azon, hogy az élek szakaszok.) $\square$

17. Síkgráfok dualitása



Különböző síkbarajzolásokhoz különböző duális tartozik. (Egyszer van 6-odfokú csúcs, másszor nincs.)

Legyen $G = (V, E)$ síkbarajzolt gráf, legyen V^* G lapjainak halmaza. $G^* = (V^*, E^*)$ a G *duálisa*, ahol $E^* = \{e^* : e \in E\}$ és e^* az e-t határoló tartomány(oka)t összekötő él.

Megjegyzés: A G^* duális gráf nem(csak) G-től, hanem G adott síkbarajzolásától függ. Adott síkgráf különböző síkbarajzolásai nemizomorf duálisokat definiálhatnak.

Def: A G gráf e és e' élei *soros élek*, ha van olyan közös pontjuk, amihez nem csatlakozik más él. A $Q \subseteq E(G)$ élhalmaz *vágás*, ha Q egy olyan élhalmaz, hogy elhagyásakor G komponenseinek száma megnő, és Q egy legszűkebb ilyen élhalmaz, azaz Q semelyik valódi részhalmazára ez nem teljesül. Az e él *elvágó él*, ha $\{e\}$ vágás.

Tétel: Legyen $G = (V, E)$ sr. (1) Ha G^* a G duálisa, akkor G^* sr és öf.

(2) $f(e) := e^*$ egy $f : E(G) \to E(G^*)$ természetes bijekciót definiál.

(3) G lapjai bijektíven G^* pontjainak felelnek meg.

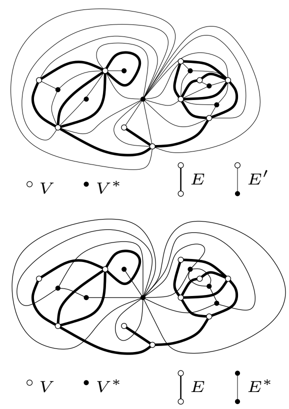
(4) $e, e' \in E(G)$ párhuzamos (soros) élek $\iff$ $f(e), f(e')$ soros (párhuzamos) élek.

(5) $e \in E(G)$ a G hurokéle (elvágó éle) $\iff$ $f(e)$ a G^* elvágó éle (hurokéle).

(6) Ha G öf, akkor $G = (G^*)^*$, és ekkor G pontjai bijektíven G^* lapjainak felelnek meg.

(7) $C \subseteq E(G)$ a G köre (vágása) $\iff$ $f(C)$ G^* vágása (köre).

(8) Ha G öf, akkor $F \subseteq E(G)$ a G feszítőfája $\iff$ $f(F)$ a G^* egy feszítőfájának komplementere.



A G' és G^* gráfok

Biz: (1): Elkészítünk egy $G' = (V', E')$ gráfot az alábbiak szerint. A síkbarajzolt G gráf minden l lapján felveszünk egy v_l pontot, legyen $V^* := \{v_l : l \text{ } G \text{ lapja}\}$, és legyen $V' := V \cup V^*$. A G' gráf minden éle egy V-beli és egy V^*-beli pont között fut. Az éleket úgy kapjuk, hogy minden V-beli v csúcsból annyi E'-élt indítunk, ahány E-beli indul v-ből, mégpedig úgy, hogy v körül felváltva következzenek az E-beli ill. E'-beli élek. Ha egy v-ből induló E'-beli él az l lapon indul, akkor ezen él másik végpontja v_l lesz. Feltehető, hogy minden vv_l élt az adott l lapon belül rajzoltunk, így G' síkbarajzolt gráf lesz. Sőt: $G' \cup E$ olyan síkbarajzolt gráf, aminek kétféle lapja lehetséges: ha egy lapját E-beli uv él határolja, akkor u és v is ugyanazzal a V^*-beli ponttal van összekötve, ezért ezen a lapon körbejárva két E'-beli és egy E-beli élen haladunk végig. Ezen kívül $G' \cup E$-nek olyan lapjai lehetnek még, amiket kizárólag E'-beli élek határolnak. Az is látszik, hogy ha egy első típusú lapról az E-beli élt elhagyjuk, akkor két háromszöglapot olvasztunk egy négyszöglappá.

Azt kaptuk tehát, hogy G' egy síkbarajzolt gráf, és G egy síkbarajzolását úgy kaphatjuk meg, hogy G bizonyos négyszöglapjaiba (a lapon belül haladva) behúzunk egy átlót. Világos, hogy azt is megtehetjük, hogy ugyanezen négyszöglapoknak nem a V-beli csúcsait összekötő átlóját húzzuk be, hanem (szintén a lapon belül maradva) a V^*-belieket összekötőt. Ezáltal újfent egy síkbarajzolt gráfot kapunk, ami definíció szerint épp a G^* duális gráf lesz.

Azt kell még igazolni, hogy a G^* gráf összefüggő, azaz bármely v_l és v_k csúcsa között vezet út. Tekintsünk a síkon egy olyan görbe vonalat, ami ezek között a csúcsok között vezet, de nem megy át G egyetlen csúcsán sem. Ez a görbe a G gráfon tartományról-tartományra halad, mindig a G élét átmetszve. Világos, hogy minden ilyen tartományugrásnál a duálisban a megfelelő tartományokhoz tartozó csúcsok szomszédosak, tehát a görbe definiál egy élsorozatot a duális gráfon, amiből már könnyen készíthető egy v_l-t a v_k-val összekötő út is.

(2,3,4,5): A definícióból világos, ill. (1)-ből látszik.

(6)Mivel G^* minden éle pontosan egy élet metszi G-nek pontosan egyszer, ezért G^* bármely tartománya tartalmazza G-nek legalább egy pontját. Mivel G öf, ezért az Euler-formula szerint $n = e + 2 - t$, ahol n, t, e jelöli G pont-, tartomány- és élszámát. (1) szerint G^* is öf, ahonnan $t^* = e^* + 2 - n^*$, ahol n^*, t^* és e^* a G^* pont-, tartomány- és élszáma. (2) miatt $e = e^*$, (3) szerint $t = n^*$, így $n = t^*$, azaz G^* minden lapja pontosan egy V-beli pontot tartalmaz. Innen az látszik, hogy $(G^*)' = G'$, tehát $(G^*)^* = G$. Az állítás második része (3)-ból következik.

(7): Ha C a G köre, akkor C lerajzolása 2 részre osztja a síkot. Ezért $f(C)$ éleit elhagyva a kör belsejében lévő duális csúcsokból nem lesznek elérhetőek a körön kívüli csúcsok. Az is könnyen látható, hogy mind a kör belsejében levő, mind a C körlapon kívüli duális csúcsok összefüggő gráfot feszítenek $G*$-ban. Ezért, ha $f(C)$ valódi részhalmazát hagyjuk el, akkor G^* öf marad, tehát a C éleinek megfelelő élek G^* egy vágását adják.

Ha Q a G vágása, akkor Q a G egy K komponensét vágja szét egy K_1 és egy K_2 komponensre. Ha Q tartalmaz egy uv elvágó élt, akkor Q minimalitása miatt $Q = \{uv\}$, és $f(Q)$ (5) miatt hurokél, ami kör. Egyébként Q minden éle két *különböző* tartományt határol, így K_1-t legalább 2 tartomány határolja. A K_1 komponenst körüljárása a határolótarományok egy ciklikus sorrendjét adja, és belátható, hogy ebben minden határoló tartomány pontosan egyszer szerepel. Ezért az $f(Q)$ duális élhalmaz a G^* egy köre. Az ekvivalenciák másik iránya a fentiekhez hasonlóan bizonyítható.

(8) F a G max körmentes részgráfja $\iff$ $f(F)$ a G^* max (elvágó élhalmaz)-mentes részgráfja $\iff$ $F^* := G^* - f(F)$ a G^* min öf részgráfja, $\iff$ F^* feszítőfa (hisz G^* (1) miatt öf). □

A fentiekben azt láttuk, hogy a síkbarajzolható gráfokhoz el tudunk készíteni egy duális gráfot, ami nemcsak a síkbarajzolása révén kötődik az eredeti gráfhoz, hanem a vágás-kör dualitás alapján is. Ez a megfigyelés teremt lehetőséget a fogalom általánosítására.

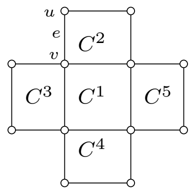
Def: A G gráf a H gráf ***absztrakt duálisa***, ha létezik egy $\varphi : E(G) \to E(H)$ bijekció úgy, hogy C a G köre $\iff$ $\varphi(C)$ a H vágása és Q a G vágása $\iff$ $\varphi(Q)$ a H köre.

Világos, hogy minden síkbarajzolható G gráfnak létezik absztrakt duálisa (akár több, nemizomorf is), hiszen tetszőleges síkbarajzoláshoz tartozó G^* duálisgráf megfelel. Nem világos azonban, hogy vajon létezik-e nem síkbarajzolható gráfoknak duálisa.

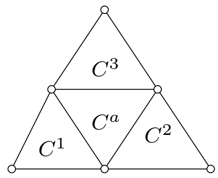
Whitney tétel: A G gráfnak pontosan akkor létezik absztrakt duálisa, ha G sr.

Biz: (Vázlat) Világos, hogy ha $G^{(*)}$ a G gráf absztrakt duálisa, és H a G részgráfja, akkor az $E(H)$-nak megfelelő élek $G^{(*)}$-nak egy olyan $H^{(*)}$ részgráfját alkotják, ami a H gráf absztrakt duálisa. A Kuratowski tétel szerint Whitney fenti tételét bebizonyíthatjuk úgy, hogy igazoljuk, hogy sem a K_5-tel, sem pedig a $K_{3,3}$-mal topologikusan izomorf gráfoknak nincs absztrakt duálisa. Világos, hogy a szóbanforgó gráfok úgy keletkeznek, hogy K_5 vagy $K_{3,3}$ éleit soros élekkel helyettesítjük. Ezen soros éleknek az absztrakt duálisban párhuzamos éleknek kell megfelelniük. Ha most e párhuzamos élekből csak $1-1$ példányt tartunk meg, akkor a K_5 vagy a $K_{3,3}$ absztrakt duálisát kapnánk. A Whitney tételt tehát visszavezettük arra, hogy két konkrét gráfról (a K_5-ről ill. a $K_{3,3}$-ról) kell igazolni, hogy nincs absztrakt duálisuk.

Nézzük a K_5-t! Ennek van 5 db olyan vágása, amelyek mindegyike $1-1$ pontot vág le, és ezek $4-4$ élt tartalmaznak. Ha indirekt létezik egy $K_5^{(*)}$ absztrakt duális, akkor ennek pontosan 5 db 4-hosszú köre van (mondjuk $C^1, C^2, \ldots, C^5$) úgy, hogy azok páronkét $1-1$ közös éllel rendelkeznek, amit elhagyva egy 6-hosszú kört kapunk. Legyen a C^1 és C^2 közös éléhez csatlakozó C^2-él $e = uv$! (Ld. az ábrát.) Ha v a C^1 körön van, akkor u biztosan nem pontja C^1-nek, hiszen $C^1 \cup C^2$-ből elhagyva a közös élt egy 6-hosszú kört kapunk. Tudjuk, hogy uv a C^2-nek és egy másik körnek a közös éle. A fentiek szerint az u végpont csakis a C^3 kör v-ből induló élének másik végpontja lehet. A fenti gondolatmenet a C^1 bármely szomszédos körével elmondható. Ebből az adódik, hogy a $K_5^{(*)}$ gráf szükségképpen a kocka élhálója, de ennek 6 db 4-hosszú köre van, ami ellentmondás.



Tegyük fel ezután indirekt, hogy a $K_{3,3}$ gráfnak létezik egy $K_{3,3}^{(*)}$ absztrakt duálisa. A $K_{3,3}$-nak 6 db 3-élű vágása van (amik egy-egy csúcs levágásával keletkeznek). E 6 vágás két 3-as csoportra osztható úgy, hogy az egy csoporton belüli vágások páronként éldiszjunktak. A duális megfelelőjük 6 db 3-hosszú kör lesz, mondjuk C^1, C^2, C^3 és C^a, C^b, C^c úgy, hogy sem a számozott, sem a betűzött köröknek nincs közös éle, de bármely számozottnak pontosan egy közös éle van bármely betűzöttel. Nézzük a C^a kört és a hozzá élen csatlakozó C^1, C^2, C^3 köröket. Az ábrán látható csúcsok közül semelyik kettő sem eshet egybe a fent elmondottak miatt. Ekkor azonban nem létezhet olyan C^b kör, aminek a három számozott C^i mindegyikével közös éle van. Az kaptt ellentmondás igazolja a Whitney tételt. □

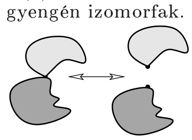


Korábban már láttunk példát arra, hogy egy öf, sr G gráfnak lehetnek nemizomorf G_1^*, G_2^* duálisai. A fenti, 8 pontból álló tétel persze azokra is igaz, így G vágásai bijektíven G_1^* ill. G_2^* köreinek is megfelelnek. Tehát G_1^* és G_2^* élei között körtartó bijekció van. Ez motiválja a következő fogalmat.

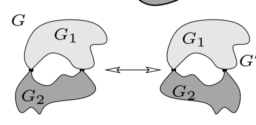
Def: G és H gráfok ***gyengén izomorfak (2-izomorfak)***, ha létezik egy $\varphi : E(G) \to E(H)$ bijekció úgy, hogy C pontosan akkor köre a G gráfnak, ha $\varphi(C) = \{\varphi(c) : c \in C\}$ a H köre.

Whitney tétele: Ha G síkbarajzolható, továbbá G és H gyengén izomorf, akkor
(1) H is síkbarajzolható, (2) G^* és H^* is gyengén izomorf, végül (3) G és $(G^*)^*$ gyengén izomorf.

Biz: (Vázlat) (1): Legyen G^* a G gráf egy duálisa. Világos, hogy G^* egyúttal a H absztrakt duálisa is, ezért az elsőnek kimondott Whitney tétel miatt H sr. (2): Minthogy G^* és H^* egyaránt absztralt duálisai H-nak (hisz a duális is absztrakt duális), ezért egymással gyengén izomorfak a 8 pontból álló tétel (7) állítása szerint. (3): Az idézett tétel (1) állítása miatt $(G^*)^*$ öf, a (6) állítás szerint tehát G^* duálisa $(G^*)^*$-nak és persze G-nek is. De ekkor G és $(G^*)^*$ egymással gyengén izomorfak. □



Hogyan kaphatunk gyengén izomorf gráfokat? Ha G két különböző komponensének egy-egy pontját azonosítjuk, akkor a körök halmaza nem változik. Az inverzoperáció, amikor egy elvágó pontot széthúzunk szintén 2-izomorf gráfot eredményez. Ha G a pontdiszjunkt G_1 és G_2 gráfokból keletkezik úgy, hogy G_1 u_1 pontját azonosítjuk G_2 u_2 pontjával *és* G_1 v_1 pontját azonosítjuk G_2 v_2 pontjával, akkor G és G' is gyengén izomorf, ahol G'- úgy kapjuk, hogy G_1 u_1 pontját azonosítjuk G_2 v_2 pontjával *és* G_1 v_1 pontját azonosítjuk G_2 u_2 pontjával.



Tétel: (Whitney) Ha G és H gyengén izomorf, akkor H előállítható G-ből a fenti 3 operáció ismételt alkalmazásával. □

18. Gráfok mátrixai

Def: A $G = (V, E)$ (irányított) gráf *szomszédossági (adjacencia) mátrixa* $A(G) = (a)_{i,j} \in \mathbb{R}^{V \times V}$, ahol $a_{i,j} :=$ az i-ből j-be futó élek száma.

Megfigyelés: Ha G (irányított) gráf, akkor v pontjának (ki)-foka $A(G)$ mátrix v-hez tartozó sorában levő elemek összege. A v-hez tartozó oszlopösszeg a v (be)-foka. Ha G irányítatlan, akkor $A(G)$ szimmetrikus: $A(G) = A(G)^T$.

Tétel: Ha $G = (V, E)$ (irányított) gráf, akkor az A^k mátrix (u, v) pozícióban álló $(A^k)^v_u$ eleme megegyezik az u-ból v-be vezető, k élű séták számával.

Biz: Teljes indukcióval: $k = 1$-re ez $A(G)$ definíciójából közvetlenül következik. Tegyük fel, hogy $A(G)^k$-ra már bizonyítottuk az állítást. Világos, hogy az u-ból v-be vezető $(k+1)$-élű utak száma $\sum_{w\in V}$(a k élű uw séták száma) $\cdot$ (a wv élek száma) $= \sum_{w\in V}(A(G)^k)^w_u \cdot A(G)^v_w = (A(G)^{k+1})^v_u$. □

Köv.: Ha G egyszerű, irányítatlan gráf, akkor $(A(G)^2)^v_v = d(v)\ \forall v \in V(G)$. □

Tétel: Ha G irányítatlan gráf, és λ_1 az $A(G)$ legnagyobb sajátértéke, akkor $\lambda_1 \leq \Delta(G)$, továbbá ha G Δ-reguláris, akkor $\Delta = \lambda_1$. (Emlékeztetünk, hogy $\Delta(G)$ a legnagyobb G-beli fokszámot jelöli.)

Biz: Legyen $\underline{x} = (x_1, x_2, \dots, x_n)$ egy λ_1-hez tartozó sajátvektor, és legyen $x_k = \max\{x_1, x_2, \dots, x_n\}$. Mivel $\underline{x} \neq \mathbf{0}$, ezért (esetleg a $-\underline{x}$ sajátvektorra áttérve) feltehető, hogy $x_k > 0$. Ekkor $\lambda_1 \cdot x_k = A(G)_k \cdot \underline{x} = \sum_{i=1}^n a_{k,i}x_i \leq \sum_{i=1}^n a_{k,i}x_k = x_k \cdot \sum_{i=1}^n a_{k,i} = x_k \cdot d(v_k) \leq \Delta \cdot x_k$.

Másrészt, ha G Δ-reguláris, akkor $\underline{1}$ a Δ sé-hez tartozó sv, ugyanis a fenti egyenlőtlenségek végig egyenlőséggel teljesülnek. □

Def: A $G = (V, E)$ irányított gráf *illeszkedési (incidencia) mátrixa* $B(G) \in \mathbb{R}^{V\times E}$, amire

$$(B(G))^e_v = \begin{cases} 1 & \text{ha } v \text{ az } e \text{ kezdőpontja} \\ -1 & \text{ha } v \text{ az } e \text{ végpontja} \\ 0 & \text{egyébként ,} \end{cases} \qquad \text{irányítatlanra} \quad (B(G))^e_v = \begin{cases} 1 & \text{ha } v \text{ az } e \text{ végpontja} \\ 0 & \text{egyébként.} \end{cases}$$

Tétel: A G irányított gráf $B(G)$ illeszkedési mátrixának néhány oszlopa pontosan akkor lineárisan független, ha a megfelelő élek irányítatlan megfelelői erdőt alkotnak.

Biz: Egy körnek megelelő oszlopvektorok megfelelő, ± 1 együtthatókkal vett lineáris kombinációja a nullvektort adja, ezért minden független oszloprendszer erdőnek felel meg.

Ha egy oszloprendszer erdőnek felel meg, akkor egy tetszőleges, levélből induló él független a többi oszloptól, hisz a levélhez tartozó koordinátában a többi oszlop 0, a vizsgált oszlop pedig nem. Ezen él elhagyásával egy kisebb erdőt kapunk; ennek éleihez tartozó oszlopokról pedig indukcióval bizonyítható, hogy a lineárisan függetlenek. □

Köv.: Ha G irányított, hurokélmentes, n-pontú gráf c komponenssel, akkor $r(B(G)) = n - c$.

Biz: $B(G)$ rangja azonos $B(G)$ oszloprangjával, azaz feszítő erdejének élszámával, ami $n - c$. □

Tétel: Ha B a G gráf $B(G)$ illeszkedési mátrixából egy sor elhagyásával keletkező mátrix, akkor $\det(BB^T)$ a G feszítőfáinak száma.

A bizonyításhoz szükséges az alábbi, a determinánsok szorzástételét általánosító segédtétel.

Lemma: (Binet-Cauchy tétel) Ha $M \in \mathbb{R}^{[n]\times[m]}$, $N \in \mathbb{R}^{[m]\times[n]}$ és $n \leq m$, akkor $\det(M \cdot N) = \sum_{H\in\binom{[m]}{n}} \det(N^H) \cdot \det(M_H)$, ahol N^H az N mx H-beli oszlopai, M_H pedig az M mx H-beli sorai meghatározta részmátrix. □

A B mátrix oszlopainak egy részhalmazát pontosan akkor alkot reguláris mátrixot (az előző tétel szerint), ha az adott oszlopok egy feszítőfának felelnek meg. Ekkor pedig a determináns ± 1, u.i. pontosan egy nemnulla kifejtési tag van. (Az elhagyott sornak megfelelő pontot gyökérnek tekintve, minden oszlophoz azt a sort választjuk, ami az oszlopnak megfelelő él gyökértől távolabbi végpontjához tartozik.) A B^T mátrix ugyanezen *sor*részhalmazhoz tartozó részmátrixának a determinánsa ugyanannyi, ezért $H \in \binom{E}{n-1}$-re

$$\det(B^H) \cdot \det(B^T_H) = \begin{cases} 1 & \text{ha } H \text{ feszítőfa} \\ 0 & \text{ha } H \text{ nem feszítőfa ,} \end{cases}$$

ezért a Binet-Cauchy tétel miatt $\det(B \cdot B^T)$ csakugyan G feszítőfáinak száma. □

Köv.: Cayley tétel: A K_n gráfnak n^{n-2} feszítőfája van.

Biz: A az előző tétel szerint BB^T mátrix determinsa adja a feszítőfák számát, ahol a B a mátrix úgy keletkezik, hogy a $B(K_n)$ illeszkedési mátrixból egy sort elhagyunk. A mátrixszorzás definíciója miatt a $(BB^T)^v_v = d(v) = n - 1$, ill. $u \neq v$-re $(BB^T)^u_v = d(v) = -1$. Így

$$\begin{vmatrix} n-1 & -1 & \dots & -1 \\ -1 & n-1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & -1 \\ -1 & \dots & -1 & n-1 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \dots & 1 \\ -1 & n-1 & -1 \dots & -1 \\ -1 & \ddots & n-1 \ \ddots & \vdots \\ \vdots & & \ddots \ \ddots & -1 \\ -1 & \dots & \dots -1 & n-1 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \dots & 1 \\ 0 & n & 0 \dots & 0 \\ 0 & \ddots & n \ \ddots & \vdots \\ \vdots & & \ddots \ \ddots & 0 \\ 0 & \dots & \dots \ 0 & n \end{vmatrix} = n^{n-2} \qquad \square$$