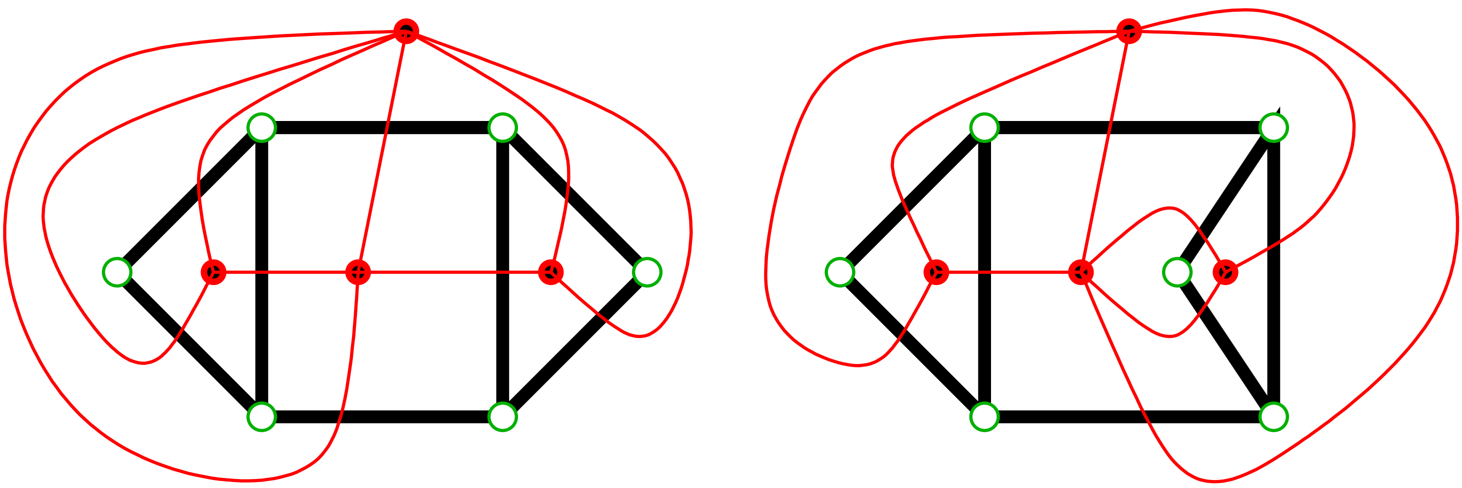
Bevezetés a számításelméletbe 1.

A BME I. éves mérnök-informatikus hallgatói számára

segédlet a 2007. őszi előadáshoz

Összeállította: Fleiner Tamás



Utolsó frissítés: 2012. február 7.

Tartalomjegyzék

Bevezetés

Ez a jegyzet nagyjából a BME-n, a 2007/2008-as tanév első félévében a mérnök-informatikus hallgatók számára előadott, VISZA 103 fedőnevű, „Bevezetés a számításelméletbe” c. előadás anyagát tartalmazza. A jegyzet elsődleges célja a vizsgára való felkészülés. Nem pótolja a rendelkezésre álló, könyvformátumú jegyzetet, amellyel számos tekintetben egyezik. Előnye mégis talán annyi, hogy szorosabban kapcsolódik az órán leadott anyaghoz, és így koncentráltabban tartalmazza a vizsgán számonkért tudást. A jegyzet valamennyire túl is mutat azonban az előadáson elhangzottakon, így olyan részeket is tartalmaz, amelyek ismeretét nem követeljük meg a vizsgán. Ha tehát valaki egészen véletlenül komolyabban érdeklődik egy-egy témakör iránt, 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 valódi szakirodalmat (is) érdemes tanulmányoznia.

Hogyan célszerű a jegyzetet használni, és egyáltalán: hogyan folyik a vizsga?

A jegyzetet igyekeztem úgy összeállítani, hogy abban minden szerepeljen, amit a vizsgán kérdezhetünk. Valószínűleg ez nem sikerült tökéletesen, de a szándék megvolt. A jegyzet a definíció-tétel-bizonyítás szentháromság alapján nyugszik: a definiált fogalmakat *dőlt betűs szedéssel* jeleztem, a tétel (állítás, megfigyelés, lemma) előtt **félkövéren** adom meg, miről is van szó, a bizonyítások végét pedig olyan kiskocka jelzi, mint amilyen pl. e sor végén is áll. □

Az is cél volt, hogy ne legyen túl száraz az anyag. A jegyzet ezért tartalmaz a tananyagot kiegészítő, ill. ahhoz kapcsolódó, érdekesnek ítélt információkat is. Az így közölt ismereteket a vizsgán tehát nem követeljük meg: az az általános irányelv, hogy az apró betűvel szedett részeket még a jeles osztályzatért sem kell tudni. Talán nem túl kockázatos azt kijelenteni, hogy a normál szedésű részek beható ismerete elegendő a jeles osztályzathoz. A spektrum másik végének teljesítésére már lényegesen több lehetőség kínálkozik. Elégtelent pl. úgy lehet szerezni, hogy a vizsgázó nem tudja pontosan kimondani valamelyik lényeges definíciót, tételt vagy állítást. Eredményes módszer az is, ha a definíciókat és tételeket szó szerint bemagolja a hallgató, de a vizsgán bizonyságát adja annak, hogy nem érti, miről beszél. Más szóval, a legalább elégséges osztályzatnak feltétele a törzsanyaghoz tartozó fogalmak, állítások pontos ismerete, azaz, hogy a hallgató ezeket ki tudja mondani, képes legyen azokat alkalmazni és azokra szükség esetén példát mutatni. Az elégséges osztályzatnak nem feltétele, hogy minden ismertetett bizonyítást tökéletesen ismerjen a vizsgázó. Sőt: akár egyet sem kell tudni. Azonban aki ennek alapján próbál levizsgázni, az azt üzeni az őt vizsgáztatónak, hogy nagyon nem érdekli őt az anyag. Mint gyakorló vizsgáztató elmondhatom, hogy ez engem arra ösztönöz, hogy alaposan győződjek meg a definíciók és tételek kellő szintű ismeretéről, mert azt gondolom, hogy számos olyan állítást tartalmaz a tananyag, amit úgy a legkönnyebb megérteni, ha ismerjük a bizonyítást, vagy legalább annak vázlatát. Általánosságban elmondható, hogy sokkal fontosabb (értsd: elengedhetetlen), hogy egyetlen témakörben se lehessen zavarba hozni a vizsgázót, mint egy-egy bizonyítás részletes ismerete. Akinek „sajnos” nem jut ideje a topologikus izomorfia obskurus definícióját megtanulni, de hatosra tudja a kontinuum hipotézist, az éppúgy megbukik, mint az, aki semmit sem tud a gráf definícióján kívül, és azt is csak alig.

A vizsga lebonyolítása úgy történik, hogy minden vizsgára jelentkező hallgatónak kisorsolunk egy tételt az itt is megtalálható tételsorból. Ezt követően legalább 45 perc felkészülési idő alatt a hallgató kidolgozhatja a tételét, célszerűen vázlatot ír. A számonkérés abból áll, hogy a kidolgozott vázlat alapján ki kell tudni mondani a vizsgatételben szereplő definíciókat és tételeket, illetve reprodukálni kell tudni a bizonyításokat. Ha nem megy magától, a vizsgáztató segít. Számítani kell arra is, hogy másik tétellel kapcsolatos fogalmakra, állításokra is rákérdez a vizsgáztató. A vizsgáztató személye a helyszínen dől

[1] Mint pl. ez is, itt.

el, az esetek többségében valamelyik előadó vagy gyakorlatvezető előtt kell számot adni a tudásról.

Hogyan is jött létre a jelen segédlet? A jegyzet írása 2004 tavaszán kezdődött, azóta hízik az anyag. Akkoriban még csak naiv elképzelésem volt a dolgról, miszerint

> „Egy előadássorozat tervezésekor az előadónak célszerű leírnia az elhangzó anyagot, hogy az minél egységesebb 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 eleinte a saját segédanyagomként került összeállításra. Értelmesnek tűnt ezt közreadni, és ha már ez megtörtént, akkor jó befektetésnek látszott kicsit olvasmányosabbá, jegyzetszerűbbé tenni a szöveget. Mindemellett a jelentős számban felbukkanó hibákat is igyekeztem folyamatosan gyomlálni. (Volt, van, lesz belőlük bőven.) Ebben a harcban múlhatatlan érdemeket szereztek azok a hallgatók (és kollégák), akik jelezték, ha elírást vagy hibát találtak. Munkájukat ezúton is köszönöm. Remélem, hogy ennek nyomán a jegyzet használhatósága jelentősen javult, és számos későbbi hallgató felkészülését könnyíti meg. Természetesen mindehhez én is hozzáteszem a magamét: minden átdolgozáskor újabb elírásokat és tévedéseket illesztek az anyagba az egyensúly megőrzése érdekében.

A saját felhasználású segédanyagtól a mostani jegyzetformátumig van még néhány lépés. Általános hiba –mondják–, hogy ezt a „pár lépést" nagyságrendekkel alábecslik a szerzők. Több kollégától hallottam hogy egy tudományos könyv megírásához szükséges erőfeszítésnek kb. 70%-a az anyag megírása. Ennek egy következménye, hogy az „utolsó simítások" fázis az *addigi* munkának hozzávetőleg a fele. Így aztán minden erőfeszítés ellenére valószínűleg számos hiba maradt a most közreadott jegyzetben. Természetesen minden ilyen hibáért a felelősség egyedül az enyém. A jegyzettel, az abban található akár helyesírási, nyelvhelyességi, akár módszertani, akár matematikai hibákkal kapcsolatos megjegyzéseket és a konstruktív hozzászólásokat köszönettel fogadom a `fleiner@cs.bme.hu` címen. Ünnepélyesen ígérem, hogy az érdemi kritika figyelembevételével igyekszem tovább javítani az anyagot. A jegyzet reményeim szerint karbantartott változata a `www.cs.bme.hu/~fleiner/jegyzet` weblapról tölthető le.

Pár szó végül a szerzői jogokról.

> A jelen munka jelentős része szellemi termék, és nemcsak a szerzőé. A szerzői jogok tekintetében a szerző elképzelései az alábbiak. E munka jelenlegi formájában szabadon másolható, terjeszthető, de kizárólag a szerző és a forrás pontos megjelölésével és ingyenesen. Ugyanez a megkötés öröklődjék minden olyan szerzői jog hatálya alá eső dologra, ami a jelen munka fenti típusú felhasználása során származik. A fent említettől eltérő célú felhasználás (pl. az anyag szerkesztése, átdolgozása, árusítása) kizárólag a jelen munka szerzőjének engedélyével lehetséges.

Minden olvasónak sikeres felkészülést és eredményes vizsgázást kívánok.

Budapest, 2007. december 14.

Fleiner Tamás

Jegyzetevolúció-blog

`2007. 12. 14. 12.00: Meg par ora, es elkeszul a jegyzet. Turelem....`

`2007. 12. 14. 18.15: Letoltheto a 0. verzio. Lesz meg nehany apro valtozas, pl. a Cayley tetel meg nem vegleges.`

`2007. 12. 18. 15.00: Jegyzet0.1 Jópár elírást ki lett javítva. Köszönet Rádi Attilának, Velinszky Lászlónak és Csöndes Lászlónak. A Cayley tétellel még nem foglalkoztam. A hiperlinkek nem túl jók, és a pdf sem vektoros. Ezeken is dolgozom, addig is lesz .ps változat.`

`2007. 12. 20. 13.00, jegyzet1.0: További bosszantó elírásoktól sikerült megszabadulni. M■ködnek a hiperlinkek, vektoros a pdf, és a Cayley tétel is frissült.`

`2007. 12. 29. 14.35, jegyzet1.1: Újabb elírások t■ntek el, a halmazelmélet rész b■vült.`

2008. 01. 14. 12.00 jegyzet1.2: Egyéb javítások mellett immár a Pitagorasz tétel is rendben van. Mindebben Velinszky László, Hidasi Péter, Tóth Zoltán és Keresztes László segítettek. Újabb mérföldkő, hogy van a blogban ő és ű.

2008. 01. 24. 12.30 jegyzet1.3: Zsolnay Károly, Szelei Tamás és Tauber Ádám segítettek.

2008. 02. 06. 15.00 jegyzet1.4: Rádi Attila volt szemfüles.

2009. 01. 02. 11.10 jegyzet1.5: Szabó Bálint vett észre egy súlyos ostobaságot a koordinátageometriában.

2009. 01. 05. 11.24 jegyzet 1.6: Vőneki Balázs talált hibát a 37. oldalon szereplő, dualitást tárgyaló tétel bizonyításában.

2009. 01. 09. 16.20 jegyzet 1.7: A mátrixok sajátértékeiről szóló szakaszban már a mátrixok sajátértékeiről is szó van, köszönet Varga Juditnak.

2009. 01. 12. 14.40 jegyzet 1.8: Szárnyas Gábor olvasott gondosan.

2009. 06. 22. 19.00 jegyzet 1.9: Molnár Gergely, Sweidan Omar, Nagy Gábor és Pintér Olivér segítettek.

2010. 01.12. 11.30 jegyzet 1.10: Benei Viktor talált számos sajtóhibát.

2012. 02. 07. 12.05 jegyzet 1.11: Baranyai Balázs talált egy felesleges egyest. Tarnay Kálmán és WolframAlpha mutattak rá a másodfokú egyenlet hibás megoldására ill. Szedelényi János és Joó Ádám olvastak figyelmesen. Még a címlapábra is meghízott.

[2] Ma már ezzel nem értek egyet. Bonyolultabb. Azért remélem, talán mégsem haszontalan a befektetett munka.

Bevezetés a Számításelméletbe I. vizsgatételek
2007/2008. tanév első félév

1. Térbeli koordinátageometria: sík egyenlete, egyenes egyenletrendszerei. Metszéspontok, metszésvonalak számítása. Vektortér definíciója, a definíció egyszerű következményei, példák.
2. Altér, lineáris kombináció, generált altér, generátorrendszer, lineáris függetlenség.
3. Bázis és dimenzió fogalma, kicserélési tétel.
4. Lineáris egyenletrendszer megoldása Gauss-eliminációval, redukált lépcsős alak. Megoldhatóság, a megoldás egyértelműségének feltétele.
5. Permutációk inverziószáma. Determináns definíciója, alaptulajdonságai, kiszámítása. Kifejtési tétel. Mátrixok, műveletek mátrixokkal, ezek tulajdonságai. Determinánsok szorzástétele (biz. nélkül).
6. Lineáris egyenletrendszerek tárgyalása mátrixokkal, $n \times n$-es lineáris egyenletrendszer egyértelmű megoldhatóságának jellemzése a determináns segítségével. Mátrix inverze, létezésének szükséges és elégséges feltétele. Inverz meghatározása Gauss-eliminációval.
7. Mátrix rangja, a rangfogalmak egyenlősége, rang meghatározása Gauss-eliminációval. Lineáris leképezés fogalma, egyszerű tulajdonságai.
8. Lineáris leképezés mátrixa, vektor képének meghatározása a mátrix segítségével. Lineáris leképezések szorzata, szorzat mátrixa.
9. Lineáris leképezések magtere, képtere. Dimenziótétel.
10. Lineáris transzformációk sajátértékei, sajátvektorai, ezek meghatározása.
11. Komplex számok: kanonikus (algebrai) és trigonometrikus alak, alapműveletek komplex számokkal, abszolút érték (hossz), konjugált. Komplex szám n-edik gyöke, egységgyökök.
12. Kombinatorikus leszámlálási alapfeladatok: ismétlés nélküli és ismétléses permutáció, variáció, kombináció; példák. Binomiális tétel. Gráfelméleti alapfogalmak: gráf, egyszerű gráf, izomorfia, részgráf, feszített részgráf.
13. Gráfok összefüggősége, élsorozat, út, kör, komponens, fa. Fák egyszerű tulajdonságai, Prüfer-kód, Cayley-tétel.
14. Síkbarajzolhatóság, kapcsolat a gömbre rajzolhatósággal, Euler-tétel, Kuratowski-tétel (bizonyítás csak a könnyebbik irányban).
15. Síkbarajzolható gráf duálisának fogalma. Példa olyan gráfra, melynek léteznek nem izomorf duálisai. Gyenge izomorfia, Whitney tétele (biz. nélkül).
16. Végtelen halmazok számossága: $|A| = |B|$, $|A| \leq |B|$ és $|A| < |B|$ definíciója, Cantor-Bernstein-tétel (biz. nélkül). Megszámlálhatóan végtelen és kontinuum számosságú halmaz fogalma. Példák: $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$ számossága. Hatványhalmaz számossága (Cantor tétele), $\mathbb{N}$ hatványhalmazának számossága. Kontinuum-hipotézis.

1. fejezet

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 valók, 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.[1] 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!

Def.: A komplex számok halmaza $\mathbb{C} := \{a + bi : a, b \in \mathbb{R}\}$, tehát minden komplex 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.

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

(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:

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

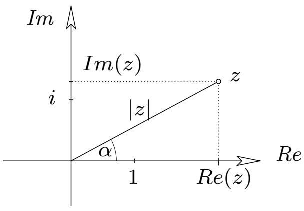
Biz.: Könnyen ellenőrizhető, hogy $0w = 0$ tetszőleges w komplex számra. Azt kell igazolni, hogy ha a szorzat 0, akkor valamelyik tényezője 0. Tegyük fel tehát indirekt, hogy $zw = 0$ és $z \neq 0 \neq w$. Ekkor

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

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 *komplex 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 és persze valós. 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 komplex 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 $|z|^n$ távolságra 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 $1 \le n$ 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 $\varepsilon^n = 1$. 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 soksög 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[2] 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] Ennek pontos jelentéséről a második félévben lesz szó; bár a most következő lineáris algebra szakaszokban feltételezzük, hogy a skalár valós számot jelent, az ott elmondottak pl komplex skalárokkal is működnek.

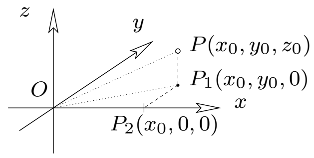
2. fejezet

Lineáris algebra

2.1 Koordinátageometria

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.

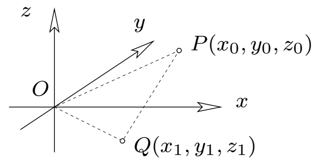
Lemma: Ha a P pont koordinátái (x_0, y_0, z_0), és O az origó, akkor $|OP|^2 = x_0^2 + y_0^2 + z_0^2$.



Biz.: Legyen $P_1(x_0, y_0, 0)$ a P vetülete az xy síkra, és legyen $P_2(x_0, 0, 0)$ a P_1 vetülete az x tengelyre! Világos, hogy OP_2P_1 és OP_1P derékszögű háromszögek, ezért Pitagorasz tétele szerint $|OP_1|^2 = |OP_2|^2 + |P_2P_1|^2 = x_0^2 + y_0^2$, ill. $|OP|^2 = |OP_1|^2 + |P_1P|^2 = x_0^2 + y_0^2 + |P_1P|^2 = x_0^2 + y_0^2 + z_0^2$.□

A lemma segítségével jellemezhetjük két vektor merőlegességét.

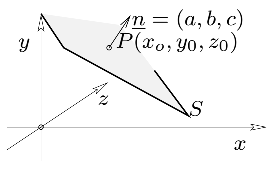
Tétel: Legyenek $P(x_0, y_0, z_0)$ és $Q(x_1, y_1, z_1)$ a koordinátarendszer tetszőleges pontjai, O pedig legyen az origó. Ekkor $OP \perp OQ \iff (x_0x_1 + y_0y_1 + z_0z_1 = 0)$.



Biz.: OP és OQ pontosan akkor merőlegesek, ha az $OPQ\triangle$ O-nál levő szöge $\frac{\pi}{2}$, ami Pitagorasz tétele szerint pontosan akkor teljesül, ha $|OP|^2 + |OQ|^2 = |PQ|^2$. Beírva a megfelelő koordinátákat, az előző lemma alapján ez pontosan azt jelenti, hogy $x_0^2+y_0^2+z_0^2+x_1^2+y_1^2+z_1^2 = (x_0-x_1)^2 + (y_0-y_1)^2 + (z_0-z_1)^2 = x_0^2 + x_1^2 - 2x_0x_1 + y_0^2 + y_1^2 - 2y_0y_1 + z_0^2 + z_1^2 - 2z_0z_1$ teljesül. Ez utóbbi pedig azzal ekvivalens, hogy $x_0x_1 + y_0y_1 + z_0z_1 = 0$. Mi pedig éppen ezt akartuk bizonyítani. □

Def.: Ha S a háromdimenziós tér egy síkja, akkor az $\underline{n}$ vektort az S *normálvektorának* nevezzük, ha $\underline{n} \neq \mathbf{0}$ és $\underline{n}$ merőleges minden S-beli vektorra. (A $\mathbf{0}$ jelölés a 0 hosszúságú nullvektort jelenti.)

Tétel: Legyen S a koordinátarendszer síkja, legyen $P(x_0, y_0, z_0)$ az S sík egy pontja, $\underline{n} = (a, b, c)$ pedig S egy normálvektora. Ekkor egy $Q(x, y, z)$ pont pontosan akkor van az S síkban, ha $ax + by + cz = ax_0 + by_0 + cz_0$ teljesül.

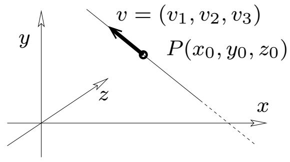


Biz.: $Q \in S \iff \underline{n} \perp \vec{PQ} = (x - x_0, y - y_0, z - z_0) \iff 0 = a(x - x_0) + b(y - y_0) + c(z - z_0) \iff ax + by + cz = ax_0 + by_0 + cz_0$. □

A fenti tétel mutatja az alábbi definíció érvényességét.

Def.: Az $\underline{n} = (a, b, c)$ normálvektorú $P(x_0, y_0, z_0)$ ponton átmenő *sík egyenlete* $ax + by + cz = konst$, ahol $konst = ax_0 + by_0 + cz_0$.

Def.: Ha e egy egyenes, akkor a $\underline{v}$ vektor az e *irányvektora*, ha $\underline{v} \neq \mathbf{0}$ és $\underline{v} \parallel e$.



Tetszőleges e egyenest egyértelműen meghatároz, ha megadjuk egy pontját és e egy irányvektorát.

Megfigyelés: Legyen $P(x_0, y_0, z_0)$ a $\underline{v} = (v_1, v_2, v_3)$ irányvektorú e egyenes egy pontja. Ekkor $Q \in e \iff \exists \lambda \in \mathbb{R} : \vec{OQ} = \vec{OP} + \lambda \underline{v} \iff (x, y, z) = (x_0, y_0, z_0) + \lambda(v_1, v_2, v_3) \iff$

$$\begin{aligned} x &= x_0 + \lambda v_1 \\ y &= y_0 + \lambda v_2 \\ z &= z_0 + \lambda v_3 \ . \end{aligned} \tag{2.1}$$

Def.: A (2.1) megfogalmazást az e *egyenes paraméteres egyenletrendszerének* nevezzük.

Vizsgáljuk meg a (2.1) egyenletrendszert. Ha az irányvektor egyik koordinátasíkkal sem párhuzamos, azaz $v_1 v_2 v_3 \neq 0$, akkor az alábbi ekvivalens formát kapjuk:

$$\lambda = \frac{x - x_0}{v_1} = \frac{y - y_0}{v_2} = \frac{z - z_0}{v_3} \ .$$

Ha $\underline{v}$-nek pontosan egy koordinátája 0 (mondjuk v_3), akkor az egyenletrendszer a

$$\lambda = \frac{x - x_0}{v_1} = \frac{y - y_0}{v_2} \qquad z = z_0$$

alakot ölti. Végül ha az irányvektor valamelyik (mondjuk az x) koordinátatengellyel párhuzamos (azaz $v_2 = v_3 = 0$), akkor a

$$\lambda = \frac{x - x_0}{v_1} \qquad y = y_0, z = z_0$$

alakot kapjuk. Vegyük észre, hogy a fenti három eset mindegyikére igaz, hogy az egyenest két sík egyenletének együttes teljesülése írja le, a λ paraméterrel nem foglalkozunk.

2.2 Vektorterek

Def.: A V halmazt $\mathbb{R}$ *feletti vektortér*nek mondjuk[1], 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 $\mathbf{0} \in V$: $u + \mathbf{0} = u$ $\forall u \in U$-ra, (ö4) $\forall u \in U$-ra létezik egy $-u \in V$, amire $u + (-u) = \mathbf{0}$.
(2) A skalárral való szorzásra a szorzásaxiómák teljesülését kívánjuk meg: $\forall \lambda, \kappa \in \mathbb{R}$, $(\lambda, \kappa \in \mathbb{R})$ $\forall u, v \in V$
(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: Az (ö4) feltételben szereplő $-u$ vektort az u vektor *ellentettjének* hívjuk.

Példa: (1) $\mathbb{R}$ (és minden test) vektortér önmaga felett.
(2) A síkbeli (térbeli) helyvektorok vektorteret alkotnak $\mathbb{R}$ felett a szokásos „vektorösszeadásra” és skalárral való szorzásra.
(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 $\lambda(x_1, x_2, \ldots, x_n) = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n)$. A nullvektor az csupa-0 sorozat, az ellentett a (-1)-szeresek sorozata.
(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. A nullvektor az azonosan 0 mátrix, az ellentett az elemenként (-1)-gyel végigszorzott mátrix.
Az $n = 1$ eset épp az előző példát adja.
(5) A valós polinomok is vektorteret alkotnak $\mathbb{R}$ felett, a legfeljebb n-edfokú polinomok szintén. Nullvektor az azonosan 0 polinom, ellentett a (-1)-szeres.
(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. Nullvektor az azonosan 0 leképezés, ellentett pedig a függvény (-1)-szerese.

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

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

Biz.: (1): Világos, hogy $\mathbf{0} = \mathbf{0}+\mathbf{0}$. Mindkét oldalt λ-val megszorozva azt kapjuk, hogy $\lambda\mathbf{0} = \lambda(\mathbf{0}+\mathbf{0}) = \lambda\mathbf{0} + \lambda\mathbf{0}$. Mindkét oldalhoz a $\lambda\mathbf{0}$ vektor $-(\lambda\mathbf{0})$ ellentettjét hozzáadva adódik, hogy $\mathbf{0} = -(\lambda\mathbf{0}) + \lambda\mathbf{0} = -(\lambda\mathbf{0}) + (\lambda\mathbf{0} + \lambda\mathbf{0}) = (-(\lambda\mathbf{0}) + \lambda\mathbf{0}) + \lambda\mathbf{0} = \mathbf{0} + \lambda\mathbf{0} = \lambda\mathbf{0}$, és éppen ezt kellett igazolnunk.
(2): Hasonlóan járunk el, csak a vektor és skalár szerepet cserél. Mivel $0 = 0 + 0$, ezért v-t megszorozva ezzel az egyenlőség fennmarad: $0v = (0 + 0)v = 0v + 0v$. Most mindkét oldalhoz hozzáadhatjuk a $0v$ vektor $-(0v)$ ellentettjét, azaz $\mathbf{0} = -(0v) + 0v = -(0v) + (0v + 0v) = (-0v + 0v) + 0v = \mathbf{0} + 0v = 0v$, győztünk.
(3): Az előzőek szerint $\mathbf{0} = 0v = (1 - 1)v = 1v + (-1)v = v + (-1)v$, így mindkét oldalhoz $-v$-t adva $-v = -v + \mathbf{0} = -v + (v + (-1)v) = (-v + v) + (-1)v = \mathbf{0} + (-1)v = (-1)v$ adódik, és nekünk ezt kellett igazolnunk.
(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: $\mathbf{0} = \frac{1}{\lambda}\mathbf{0} = \frac{1}{\lambda}(\lambda v) = (\frac{1}{\lambda}\lambda)v = 1v = v$.[2] □

Def.: A $W \subseteq V$ részhalmaz a V valós vektortér *altere*, ha W is valós vektortér a V vektortér műveleteire. Jelölése: $W \leq V$. *Triviális altér* alatt magát a V vektorteret, ill. az egyedül a $\mathbf{0}$-ból álló alteret értjük.

Példa: (1) A síkbeli helyvektorok alkotta vektortérnek alterei a triviális altereken kívül úgy kaphatóak, hogy tekintünk egy origón átmenő e egyenest, és pontosan azon vektorok lesznek az altérben, melyek e-re illeszkednek.
(2) A 2×3-as mátrixok között alteret alkotnak azok a mátrixok, amelyek első sorában álló elemek összege 0.
(3) A legfeljebb 10-edfokú valós polinomok vektorterének alterét alkotják azok a polinomok, amelyekben csak olyan tagok szerepelnek, amiknek a kitevője prímhatvány (és persze legfeljebb 10-edfokúak). Ebből az altérből egy polinom pl a $p(x) = 24x^2 - x^3 + 4x^7$.

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) axiómák, 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. □

Állítás: Ha $U, W \leq V$ alterek, akkor $U \cap W \leq V$, azaz alterek metszete altér. Ez végtelen sok altérre is igaz, azaz ha $U_\alpha \leq V$ minden $\alpha \in I$ esetén (ahol I akár végtelen halmaz is lehet, akkor $\bigcap_{\alpha\in I} U_\alpha \leq V$ szintén altér.

Biz.: A műveletzártságot kell ellenőrizni. Ha $u, v \in U \cap W$, akkor $u, v \in U$, ezért $u + v \in U$ és $u, v \in V$ így $u + v \in V$, azaz $u + v \in U \cap W$. Ha pedig $\lambda \in \mathbb{R}$, akkor $u \in U$ miatt $\lambda u \in U$ és $u \in V$ miatt $\lambda u \in W$, ezért $\lambda u \in U \cap W$.

A végtelen változathoz $u, v \in \bigcap_{\alpha\in I} U_\alpha)$ esetén $u, v \in U_\alpha$ miatt $u + v \in U_\alpha$ teljesül minden $\alpha \in I$-re, ezért $u + v \in \bigcap_{\alpha\in I} U_\alpha$. Tetszőleges $\lambda \in \mathbb{R}$ esetén pedig $u \in U_\alpha$ miatt $\lambda u \in U_\alpha$ teljesül minen $\alpha \in I$-re, ezért $\lambda u \in \bigcap_{\alpha\in I} U_\alpha$ adódik ha $u \in \bigcap_{\alpha\in I} U_\alpha$. □

Def.: Legyen V valós vektortér. A $v_1, v_2, \ldots v_n$ vektorok *lineáris kombinációja* a $\sum_{i=1}^n \lambda_i v_i = \lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_n v_n$ vektorösszeg, ahol $\lambda_i \in \mathbb{R}$. A $\sum_{i=1}^n \lambda_i v_i$ 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 $v = \sum_{i=1}^n \lambda_i u_i$ 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 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.

---

[2](3) és (4) bizonyításához szükség volt az (sz4) axiómára is. Ha ennek az axiómának nem kellenne teljesülni, 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 nem túl izgalmas struktúra az (sz4) kivételével minden vektortéraxiómát teljesít.

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 $\lambda v = \lambda(\lambda_1 u_1 + \lambda_2 u_2 + \ldots \lambda_n u_n) = \lambda \cdot \lambda_1 u_1 + \lambda \cdot \lambda_2 u_2 + \ldots + \lambda \cdot \lambda_n u_n = \sum_{i=1}^{n} \lambda\lambda_i u_i$, ami valóban lineáris kombináció. Az összeg esetén legyen $v = \sum_{i=1}^{n} \lambda_i u_i$ az egyik, ill. $w = \sum_{i=k}^{m} \kappa_i u_i$ a másik lineáris kombináció, ahol a generáló u_i vektorok közül néhányat esetleg a v és a w előállításához is felhasználtunk, néhányat pedig esetleg csak az egyikhez. Az adott előállításhoz fel nem használt u_i-k együtthatóját 0-nak választva feltehető, hogy az előállításaink $v = \sum_{i=1}^{m} \lambda_i u_i$ ill. $w = \sum_{i=1}^{m} \kappa_i u_i$ alakúak. Ekkor a lineáris kombinációk átrendezésével (az (ö1, ö2) illetve az (sz1) axiómák felhasználásával) a $v + w = \sum_{i=1}^{m} \lambda_i u_i + \sum_{i=1}^{m} \kappa_i u_i = \sum_{i=1}^{m} (\lambda_i + \kappa_i) u_i$ alak adódik, ami szintén egy lineáris kombináció, és ilyenformán $v + w \in \langle U \rangle$. □

Def.: A $v_1, v_2, \ldots, v_n$ vektorrendszer *(lineárisan) független*, ha csak a triviális lineáris kombinációjuk állítja elő a **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 **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.[3]

Megjegyzés: (1) Nem győzzük elégszer hangsúlyozni, hogy a lineáris függetlenség nem egy vektor tulajdonsága, hanem vektorok egy halmazáról lehet eldönteni, hogy független-e vagy sem.[4] (Éppenséggel egyelemű halmazokról is beszélhetünk, és ebben a tekintetben mondhatjuk, hogy a $\{v\}$ halmaz pontosan akkor lineárisan független, ha $v \neq \mathbf{0}$.)

(2) Igaz viszont az az állítás, hogy ha vektorok egy rendszere lineárisan független, akkor ennek a rendszernek bármely részhalmaza szintén lineárisan független rendszert alkot.

Állítás: A $v_1, v_2, \ldots, v_n$ 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 $\{v_1, v_2, \ldots, v_n\}$ összefüggő, azaz nem lin. ftn., akkor a **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 $\{b_1, b_2, \ldots, b_n\}$ vektorrendszer a V vektortér *bázisa*, ha lin. ftn. és egyúttal V generátorrendszere.

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

Biz.: Tegyük fel, hogy $\{b_1, b_2, \ldots, b_n\}$ 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 $\lambda_1 = \kappa_1, \lambda_2 = \kappa_2, \ldots, \lambda_n = \kappa_n$, tehát a felírás csakugyan egyértelmű.

Most tegyük fel, hogy a V bármely eleme egyértelműen állítható elő a $b_1, b_2, \ldots, b_n$ 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 $B = \{b_1, b_2, \ldots, b_n\}$ *bázis szerinti koordinátái* $\alpha_1, \alpha_2, \ldots, \alpha_n$, 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.

Megfigyelés: Érdemes utánagondolni, hogy ha B a V vektortér bázisa, $u, v \in V$ és $\lambda \in \mathbb{R}$, akkor $[u + v]_B = [u]_B + [v]_B$ ill. $[\lambda u]_B = \lambda \cdot [u]_B$.

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

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

[3] 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.)

[4] A gyors vizsgázás egy lehetséges módja a következő kijelentés: *„Ha az u lineárisan független vektor és a v is lineárisan független, akkor az u és v vektorok lineárisan függetlenek."*

független, ezért ha $F \setminus \{f_i\} \cup \{g_j\}$ egy nemtriviális lineáris kombinációja **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 $n \le k$.

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 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 $|B_1| \le |B_2|$. B_2 függetlenségéből és B_1 generátortulajdonságából pedig $|B_2| \le |B_1|$ 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 $G' = \{g_1, g_2, \dots, g_k\}$ 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 $b_1, b_2, \dots, b_l$ lineárisan független elemeket. Ha $\langle b_1, b_2, \dots, b_l\rangle = V$, akkor kész vagyunk, hisz egy lineárisan független generátorrendszert találtunk. Egyébként $\langle b_1, b_2, \dots, b_l\rangle \ne V = \langle G\rangle$, tehát létezik G-nek olyan eleme (mondjuk b_{l+1}), ami nem áll elő a $b_1, b_2, \dots b_l$ elemek lineáris kombinációjaként. A lineáris függetlenségre korábban bizonyított összefüggés alapján ekkor $b_1, b_2, \dots, b_l, b_{l+1}$ 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) $U \le V \Rightarrow \dim U \le \dim V$. (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 generátorrsz., 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 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. □

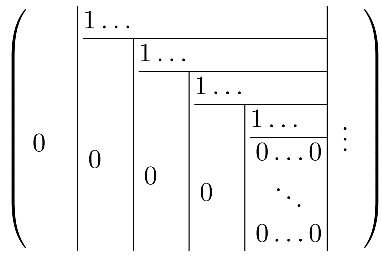
2.3 Lineáris egyenletrendszerek

Egy *k egyenletből álló, n-ismeretlenes lineáris egyenletrendszer* alatt k olyan egyenletet 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.

Def.: A kibővített együtthatómátrixot *lépcsős alak*únak nevezzük, ha
(1) minden sorában az első nemnulla elem 1 (a lépcsős alakban ezeket a mátrixelemeket nevezzük *vezéregyeseknek*), ill.
(2) bármely vezéregyesre igaz, hogy tetszőleges felette álló sorban van a vizsgált vezéregyestől balra vezéregyes.

Úgy is definiálhatóak a lépcsős alakú mátrixok, mint mindazon mátrixok, amik megkaphatóak valamely $k \in \mathbb{N}$ esetén egy elfajuló $k \times 0$ méretű mátrixból kiindulva 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 szemlélteti a fenti definíciókat.

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

Def.: A *redukált lépcsős alak (RLA)* 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.

Def.: 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). Első megfigyelésünk, hogy ha egy lineáris egyenletrendszer kibővített együtthatómátrixa RLA, akkor a megoldás pofonegyszerű. Nem árt azért egy definíció.

Def.: Ha a kibővített együtthatómátrix RLA akkor a lineáris egyenletrendszer azon ismeretlenjeit, amelyekhez tartozó oszlopban nincs vezéregyes, *szabad paramétereknek* hívjuk. Ha egy lépcsős alakú kibővített együtthatómátrixnak az utolsó („kibővítő") oszlopában van vezéregyes, akkor azt a sort *tilos sornak* nevezzük. Ha a kibővített együtthatómátrix nem feltétlenül lépcsős alakú, akkor tilos sor alatt olyan sort értünk, amiben az utolsó nemnulla elem kivételével csupa 0 áll.

Megfigyelés: (1) A tilos sor egy olyan egyenletnek felel meg, ami az ismeretlenek 0-szorosainak összegét egy nemnulla számmal teszi egyenlővé. Világos, hogy ha a kibővített együtthatómátrixnak van tilos sora, akkor az adott lineáris egyenletrendszernek nem lehet megoldása.
(2) Ha a RLA-nak nincs tilos sora, akkor a mátrix által reprezentált egyenletek mindegyike vagy a $0 = 0$ egyenlet, vagy pedig olyan egyenlet, ami egy vezéregyesnek megfelelő ismeretlen és szabad paraméterek vmilyen együtthatós összegét egy konstanssal teszi egyenlővé. Ez az egyenlet a vezéregyesnek megfelelő ismeretlen egy értékadásának is tekinthető.

Példa: Tegyük fel, hogy a kibővített együtthatómátrix a redukált lépcsős alakja a jobboldali ábrán látható. Ekkor z és u a szabad paraméterek, a megoldás pedig $z, u \in \mathbb{R}$ tetszőleges, $x = 6 + 3z - 2u$, $y = 2 - 4u$ és $v = 7$.

$$\begin{array}{ccccc|c} x & y & z & u & v & \\ 1 & 0 & -3 & 2 & 0 & 6 \\ 0 & 1 & 0 & 4 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

Köv.: Ha a kibővített együtthatómátrix RLA, akkor pontosan akkor van megoldása az egyenletrendszernek, ha nincs tilos sor, azaz nem szerepel vezéregyes az utolsó oszlopban. Ebben az esetben a szabad paraméterek tetszőleges választásához egyértelműen létezik az egyenletrendszernek megoldása.□

A továbbiakban tehát az a célunk, hogy a kibővített együtthatómátrixot redukált lépcsős alakra hozzuk, mégpedig olyan operációk segítségével, amik a megoldások halmazát nem változtatják meg. Mielőtt azonban megadnánk a szóban forgó átalakításokat, saját használatra rögzítünk néhány mátrixokkal kapcsolatos praktikus jelölést. Ha egy M mátrixnak k sora és n oszlopa van, akkor azt mondjuk, hogy M egy $k \times n$ méretű mátrix. $\mathbb{R}^{k\times n}$ a valós, $k \times n$-es mátrixok halmazát jelöli. (Ha $\mathbb{R}$ helyett $\mathbb{C}$-t írunk, akkor komplex mátrixokról beszélünk. Minden, amit ebben a szakaszban 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.

Def.: A kibővített együtthatómátrix *elemi sorekvivalens átalakításai* 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)

A (4) és (5) átalakítások azért szerepelnek zárójelben, mert a hagyományos felépítésben azokat is elemi sorekvivalens átalakításnak tekintjük. Nekünk a továbbiakban azonban elegendő az (1-3) átalakításokra szorítkozni. Figyeljük meg ugyanis, hogy a (4) átalakítás megkapható egy (2) egy (3) és egy (2) átalakítás egymásutánjaként. Az (5) átalakítás elhagyása pedig csak a 0-sorok cipelését eredményezi, komoly kárt nem okoz.

Megfigyelés: Ha A' az A mátrixból az (1-4) elemi sorekvivalens átalakítások egymásutánjával kapható, akkor A is megkapható A'-ből az (1-4) átalakítások segítségével.

Biz.: Láttuk, hogy (4) megkapható (2) és (3) segítségével, ezért elegendő az (1-3) átalakításokra bizonyítani. Sőt, elegendő csak azt igazolni, hogy ha A' az A-ból egyetlen átalakítással keletkezik, akkor az „visszaalakítható”. Az (1) sorcserénél ez világos, hisz még egyszer elvégezzük ugyanazt a sorcserét. A (2) sorszorzásnál $\lambda \neq 0$ miatt ugyanezt a sort $\frac{1}{\lambda}$-val végigszorozva újfent visszakapjuk az eredeti mátrixot. A (3) sorhozzáadás az legkeményebb dió. Ha a A_i-t adtuk A_j-hez, akkor először egy (2) átalakítással A_i-t (-1)-gyel végigszorozzuk, majd egy (3) operáció segítségével az i-dik sort a j-dikhez adjuk, végül ismét (2)-t alkalmazzuk az i-dik sorra $\lambda = -1$ választással. Győztünk. $\square$

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

Biz.: Megmutatjuk, hogy ESÁ után megoldás nem veszhet el, azaz minden korábbi megoldás az ESÁ után keletkező egyenletrendszernek is megoldása marad. Ez több, mint világos, ha arra gondolunk, mit is jelent egy ESÁ az egyenletek nyelvén megfogalmazva: (1) két egyenlet felcserélését, (2) egy egyenlet végigszorzását, míg (3) egy egyenletnek egy másikhoz való hozzáadását. Nem meglepő, hogy minden eredeti megoldás az így kapott rendszernek is megoldása lesz.

Mivel megoldás nem veszhet el, ezért legfeljebb annyi történhet, hogy új megoldások is bekerülnek a megoldások halmazába. Ha azonban az előző megfigyelés szerint ESÁ-kkal visszaalakítjuk a rendszerünket az eredetire, akkor az „újonnan bejött” megoldás nem veszhet el, tehát az már az eredeti rendszernek is megoldása volt. $\square$

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.

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

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

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

2d 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 akkor ér véget, ha 0 oszlopa marad a mátrixnak. Mivel az ilyen mátrixok lépcsős alakúak, a 0 oszlopú mátrixokon az algoritmus megfelelően működik. 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 kiegészíve 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 azokat, 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. A korábban a RLA-ról tett megállapításunk igazolja az alábbi tételt.

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 természetesen 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 $p_1, p_2, \ldots, p_m$-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 $x_i + a_1p_1 + a_2p_2 + \ldots + a_mp_m = b_i$, ahol az a_j a p_j szabad paraméter i-dik sorbeli együtthatója. Tehát a vezéregyesnek megfelelő sorok tekinthetőek a megfelelő x_i ismeretlen egy (egyértelmű) értékadásának. A tétel innen azonnal adódik. □

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. □

[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.

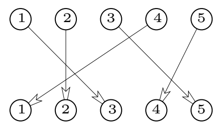
2.4 Permutációk, determinánsok

2.4.1 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 nyíldiagramja.)

Def.: 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 nyíldiagramon 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 nyíldiagramjáról. Nevezetesen, i és j pontosan akkor áll inverzióban, ha az i-ből és j-ből induló nyilak 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 nyíldiagramjáról könnyen leolvasható az $I(\sigma)$ inverziószám, ami nem más, mint a nyíldiagramban található nyilak páronkénti metszéspontjainak száma[6].

Tétel: Tetszőleges $\sigma \in S_n$ permutációra $I(\sigma) = I(\sigma^{-1})$.

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

2.4.2 Determinánsok

Ebben a részben négyzetes mátrixokhoz egy olyan mennyiséget definiálunk, 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 közülük 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.

[6] Tehát $I(\sigma)$ azonos a metsző nyílpárok számával. Ha a nyíldiagram 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 ezek szerint úgy is megfogalmazhatjuk, mint az összes bástyaelhelyezéshez tartozó mátrixelem-szorzatok előjeles összege. Ez a definíció a miatt hiányos, hogy nem írja le pontosan az előjelek megválasztását. 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.

Példa: A jobb oldalon látható 3×3 méretű mátrix determinánsa pl $|A| = (-1)^0 \cdot aei + (-1)^1 \cdot afh + (-1)^1 \cdot bdi + (-1)^2 \cdot bfg + (-1)^2 \cdot cdh + (-1)^3 \cdot ceg$.
$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

A fentiek 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 $(A^T)^j_i = A^i_j$.) A négyzetes A mátrix *főátlója* a bal felső sarkot és a jobb alsó sarkot összekötő átló mentén elhelyezkedő mátrixelemek halmaza. A négyzetes A mátrix *felső háromszögmátrix*, ha főátlója alatt csak 0-k állnak. Ugyanez az A mátrix *szigorú* felső háromszögmátrix, ha olyan felső háromszögmátrix, aminek a főátlójában is csak 0-k állnak.

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 egyes szorzatokhoz ugyanazok az előjelek tartoznak a két definícióban. 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 szakaszban 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 a determinánsra, mint 0-t. (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, azaz $(A')_k = A_k$, ha $k \neq j$, és $(A')_j = A_j + \lambda A_i$. Ekkor
$|A'| = \sum_{\sigma \in S_n} (-1)^{I(\sigma)} \cdot \prod_{s=1}^n (A')_s^{\sigma(s)} = \sum_{\sigma \in S_n} (-1)^{I(\sigma)} \cdot \left((A)_j^{\sigma(j)} + \lambda A_i^{\sigma(j)} \right) \prod_{1 \leq s \leq n, s \neq j}^n (A')_s^{\sigma(s)} =$
$\sum_{\sigma \in S_n} (-1)^{I(\sigma)} \cdot (A)_j^{\sigma(j)} \cdot \prod_{1 \leq s \leq n, s \neq j}^n (A')_s^{\sigma(s)} + \lambda \cdot \sum_{\sigma \in S_n} (-1)^{I(\sigma)} \cdot (A)_i^{\sigma(j)} \cdot \prod_{1 \leq s \leq n, s \neq j}^n (A')_s^{\sigma(s)} =$
$|A| + \lambda \cdot 0 = |A|$, ugyanis a második szumma annak a mátrixnak a determninánsa, amit A-ból úgy kapunk, hogy a j-dik sor helyett is az i-dik sort írjuk.

A fenti nem túl átlátható levezetés szavakban úgy mondható el, hogy $\det A'$ 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 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. $\square$

A most bizonyított tétel egy négyzetes mátrix determinánsának hatékony kiszámításához segít minket. 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.

Példa:
$$\begin{vmatrix} 2 & 6 & 0 & 4 \\ 1 & 4 & 5 & 3 \\ 3 & 3 & 0 & 0 \\ 2 & 3 & 6 & 2 \end{vmatrix} = 2 \cdot \begin{vmatrix} 1 & 3 & 0 & 2 \\ 1 & 4 & 5 & 3 \\ 3 & 3 & 0 & 0 \\ 2 & 3 & 6 & 2 \end{vmatrix} = 2 \cdot \begin{vmatrix} 1 & 3 & 0 & 2 \\ 0 & 1 & 5 & 1 \\ 0 & -6 & 0 & -6 \\ 0 & -3 & 6 & -2 \end{vmatrix} = 2 \cdot \begin{vmatrix} 1 & 3 & 0 & 2 \\ 0 & 1 & 5 & 1 \\ 0 & 0 & 30 & 0 \\ 0 & 0 & 21 & 1 \end{vmatrix} = 30 \cdot 2 \cdot \begin{vmatrix} 1 & 3 & 0 & 2 \\ 0 & 1 & 5 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 21 & 1 \end{vmatrix} = 60 \cdot \begin{vmatrix} 1 & 3 & 0 & 2 \\ 0 & 1 & 5 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} = 60 \cdot 1 = 60$$

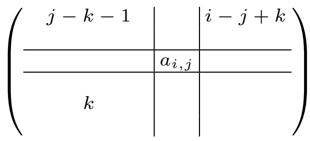
Hátránya sajnos a fenti módszernek, hogy nem mindig alkalmazható. Egy olyan mátrix esetén pl, aminek elemei polinomok, a determináns értelmes, de mivel osztani nem tudunk, az elemi sorekvivalens átalakításokat sem tudjuk elvégezni. Így marad a kiszámításhoz a gyalogos út. Az alábbiakban mutatunk egy 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
(1) $\det(A) = \sum_{j=1}^n a_{i,j} \cdot A_{i,j}$ (*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*), ill.
(2) 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.: (1) 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 a 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.

(2) A ferde kifejtés egy olyan determináns kiszámítása sor szerinti kifejtéssel, amely determinánsnak két azonos sora van. Láttuk, hogy a determináns értéke ilyenkor 0, ezért azt ily módon kiszámítva sem kaphatunk mást. □

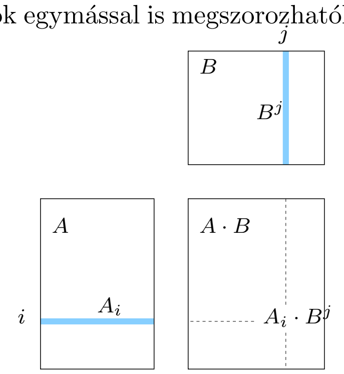
2.5 Mátrixműveletek, térbeli vektorok szorzása

A determinánsok tárgyalása után érdemes a mátrixok között műveleteket bevezetni.

Def.: Ha $A, B \in \mathbb{R}^{n\times k}$, azaz A és B $n \times k$ méretű mátrixok, akkor összeadhatóak, ami elemenkénti összeadást jelent. Azaz $A + B \in \mathbb{R}^{n\times k}$, amire $(A + B)_i^j = A_i^j + B_i^j$.

Állítás: Ha az $A, B, C \in \mathbb{R}^{n\times k}$, akkor $A + B = B + A$ (vagyis az összeadás felcserélhető, más szóval *kommutatív*) és $(A + B) + C = A + (B + C)$, ami az összeadás átzárójelezhetőségi tulajdonsága, idegen szóval *asszociativitása.* □

A mátrix skalárszorosát a vektortereknél megismert módon értelmezzük, azaz az elemeit végigszorozzuk a skalárral: $(\lambda\cdot A)_i^j := \lambda\cdot A_i^j$. Ennél sokkal izgalmasabb, hogy mátrixok egymással is megszorozhatók.



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

Fontos megfigyelés: Ha az A és B mátrixok összeszorozhatók, akkor az AB szorzatmátrix oszlopai az A mátrix oszlopainak lineáris kombinációi lesznek. Konkrétan az i-dik oszlop olyan lineáris kombináció, amelynek együtthatói a B mátrix i-dik oszlopában vannak felsorolva: $(A\cdot B)^i = B_1^i\cdot A^1 + B_2^i\cdot A^2 + \dots$ A továbbiakban többször lesz szükség erre a megfigyelésre.

Megjegyzés: Ha A és B mátrixok, akkor általában nem igaz, hogy $A \cdot B = B \cdot A$, hiszen ha az első szorzás elvégezhető, a második nem feltétlenül, ráadásul a szorzatok mérete sem lesz azonos. $n \times n$ méretű mátrixokra sem igaz a kommutativitás. Igaz viszont, amit a valós számokon megszoktunk, hogy a szorzás disztributív az összeadás felett: $A(B + C) = A \cdot B + A \cdot C$ ill. $(A + B)C = A \cdot C + B \cdot C$. Ha a szorzások elvégezhetők, akkor az asszociativitás is igaz: $A \cdot (B \cdot C) = (A \cdot B) \cdot C$. Míg a disztributivitás közel triviális, az asszociativitás bizonyítása ezen a ponton meglehetősen keserves lenne.

A fenti definíció azt is megmutatja, hogy egy mátrixot és egy oszlopvektort hogyan szorozhatunk össze, amennyiben az oszlopvektort egy egyoszlopú mátrixnak tekintjük.

Megjegyzés: Mátrix és oszlopvektor összeszorzására egy fontos példa a lineáris egyenletrendszerek megadása. Figyeljük meg, hogy ha adott egy lineáris egyenletrendszernek az $(A|b)$ kibővített együtthatómátrixa, akkor ha az ismeretleneket (a mátrixban megadott sorrend szerint egy $x = (x_1, x_2, \dots, x_n)^T$ oszlopvektorba gyűjtjük, akkor az $Ax = b$ szorzat pontosan azt írja le, hogy a lineáris egyenletrendszerben minden egyes egyenletnek teljesülnie kell.

A determinánsok és a mátrixműveletek közti összefüggésre példa, hogy ha A egy $n\times n$ méretű mátrix, akkor $|\lambda A| = \lambda^n \cdot |A|$, hiszen $\lambda \cdot A$ minden sorából kiemelhető a λ a szakasz első tételének (4) pontja miatt. Jegyezzük meg, hogy a determinánsnak nincs sok köze a mátrixok összeadásához, és *nagyon* nem igaz, hogy a $\det(A+B)$ determináns $\det A + \det B$ lenne. A szorzással viszont érdekes kapcsolat áll fenn.

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

Koordinátageometriai számításoknál roppant hasznos lehet a vektoriális szorzat fogalma.

Def.: Az (α szöget bezáró) $\underline{a}, \underline{b} \in \mathbb{R}^3$ vektorok *vektoriális szorzata* az az $\underline{a} \times \underline{b}$ vektor, ami merőleges az $\underline{a}$ és $\underline{b}$ síkjára, azokkal jobbsodrású rendszert alkot, és hossza $|\underline{a}| \cdot |\underline{b}| \cdot \sin\alpha$, azaz az a és b által feszített paralelogramma területe.

Állítás: Az $\underline{a} = (a_1, a_2, a_3)$ és $\underline{b} = (b_1, b_2, b_3)$ vektorok vektoriális szorzata az $\begin{vmatrix} e_x & e_y & e_z \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix}$ determináns értéke, ahol e_x, e_y és e_z a tér három koordinátatengelyének egységvektorai.

Bizonyítás vázlat: Könnyű ellenőrizni, hogy $\underline{a}, \underline{b} \in \{e_x, e_y, e_z\}$ esetén igaz az állítás, sőt, ez akkor is látszik, ha az $\underline{a}$ és $\underline{b}$ vektorok a koordinátatengelyek egységvektorainak konstansszorosai. Figyeljük meg, hogy az $\underline{a} \times \underline{b}$ vektoriális szorzatot úgy kapjuk, hogy a $\underline{b}$ vektor $|\underline{a}|$-szorosát az $\underline{a}$-re merőleges síkra vetítjük, és ezt a vetületet a merőleges síkban $\underline{a}$ „hegye felől nézve” $+90°$-kal elforgatjuk. Hasonló megfontolással látszik, hogy ugyanezt a szorzatot úgy is megkaphatjuk, hogy az $\underline{a}$ vektor $|\underline{b}|$-szeresét vetítjük a $\underline{b}$-re merőleges síkra, és ezt a vetületet forgatjuk a merőleges síkon $\underline{b}$ felől nézve $90°$-kal. Ebből az adódik, hogy a vektoriális szorzás disztributív az összeadás felett, azaz $\underline{a} \times (\underline{b} + \underline{b}') = \underline{a} \times \underline{b} + \underline{a} \times \underline{b}'$ ill., hogy $(\underline{a} + \underline{a}') \times b = \underline{a} \times b + \underline{a}' \times b$ teljesül. Ezért $\underline{a} \times \underline{b} = (a_1e_x + a_2e_y + a_3e_z) \times (b_1e_x + b_2e_y + b_3e_z) = a_1e_x \times b_1e_x + a_1e_x \times b_2e_y + a_1e_x \times b_3e_z + a_2e_y \times b_1e_x + a_2e_y \times b_2e_y + a_2e_y \times b_3e_z + a_3e_z \times b_1e_x + a_3e_z \times b_2e_y + a_3e_z \times b_3e_z$. Az alábbi levezetést pedig pl a determinánsok kifejtési tétele igazolja: $\begin{vmatrix} e_x & e_y & e_z \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix} = \begin{vmatrix} e_x & e_y & e_z \\ a_1 & 0 & 0 \\ b_1 & b_2 & b_3 \end{vmatrix} + \begin{vmatrix} e_x & e_y & e_z \\ 0 & a_2 & 0 \\ b_1 & b_2 & b_3 \end{vmatrix} + \begin{vmatrix} e_x & e_y & e_z \\ 0 & 0 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix} =$
$\begin{vmatrix} e_x & e_y & e_z \\ a_1 & 0 & 0 \\ b_1 & 0 & 0 \end{vmatrix} + \begin{vmatrix} e_x & e_y & e_z \\ a_1 & 0 & 0 \\ 0 & b_2 & 0 \end{vmatrix} + \begin{vmatrix} e_x & e_y & e_z \\ a_1 & 0 & 0 \\ 0 & 0 & b_3 \end{vmatrix} + \begin{vmatrix} e_x & e_y & e_z \\ 0 & a_2 & 0 \\ b_1 & 0 & 0 \end{vmatrix} + \begin{vmatrix} e_x & e_y & e_z \\ 0 & a_2 & 0 \\ 0 & b_2 & 0 \end{vmatrix} + \begin{vmatrix} e_x & e_y & e_z \\ 0 & a_2 & 0 \\ 0 & 0 & b_3 \end{vmatrix} + \begin{vmatrix} e_x & e_y & e_z \\ 0 & 0 & a_3 \\ b_1 & 0 & 0 \end{vmatrix} + \begin{vmatrix} e_x & e_y & e_z \\ 0 & 0 & a_3 \\ 0 & b_2 & 0 \end{vmatrix} + \begin{vmatrix} e_x & e_y & e_z \\ 0 & 0 & a_3 \\ 0 & 0 & b_3 \end{vmatrix}$
Az első megfigyelés szerint a két rémséges kifejezés jobboldalai megegyeznek, ezért a baloldalak is, ami épp a bizonyítandó állítás. □

Def.: Az $\underline{a}, \underline{b}, \underline{c} \in \mathbb{R}^3$ vektorok *vegyesszorzata* $(\underline{a}, \underline{b}, \underline{c}) := \underline{a} \cdot (\underline{b} \times \underline{c})$.

Állítás: (1) Ha $\underline{a} = (a_1, a_2, a_3)$, $\underline{b} = (b_1, b_2, b_3)$ és $\underline{c} = (c_1, c_2, c_3)$, akkor az $(\underline{a}, \underline{b}, \underline{c})$ vegyes szorzat értékét az $\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}$ determináns adja meg.
(2) A vegyes szorzat felírható $(\underline{a}, \underline{b}, \underline{c}) = (\underline{a} \times \underline{b}) \cdot c$ alakban is.
(3) A vegyes szorzat értéke az $\underline{a}, \underline{b}$ és $\underline{c}$ vektorok feszítette paralelepipedon előjeles térfogata (ami akkor pozitív, ha $\underline{a}, \underline{b}, \underline{c}$ jobbsordású rendszert alkotnak).

Biz.: (1) Ha a determinánst az első sor szerint fejtjük ki, akkor a_i-t éppen azzal a determinánssal kell megszorozni, ami a megfelelő egységvektor együtthatója lenne a $\underline{b} \times \underline{c} = \begin{vmatrix} e_x & e_y & e_z \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}$ determináns kiszámításakor. Az állítás a skaláris szorat definíciójából adódik.
(2) Az imént bizonyított (1) állításból és a determinánsokra vonatkozó $\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} = - \begin{vmatrix} a_1 & a_2 & a_3 \\ c_1 & c_2 & c_3 \\ b_1 & b_2 & b_3 \end{vmatrix} = \begin{vmatrix} c_1 & c_2 & c_3 \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix}$ azonosságból közvetlenül következik.
(3) A $\underline{b} \times \underline{c}$ vektor hossza a $\underline{b}$ és $\underline{c}$ vektorok feszítette paralelogramma területe. Ebből úgy kapjuk a paralelepipedon térfogatát, hogy ezt megszorozzuk az $\underline{a}$ vektor hosszával és $\cos\alpha$-val, ahol α az $\underline{a}$ vektor és a $\underline{b}$ és $\underline{c}$ vektorok által feszített sík által bezárt szöget jelenti. Világos, hogy a $\underline{b} \times \underline{c}$ és $\underline{a}$ vektor szöge $\beta = \frac{\pi}{2} \pm \alpha$, hiszen a vektoriális szorzat merőleges a $\underline{b}, \underline{c}$ síkra. Ez azt mutatja, hogy $\sin\beta = \pm\cos\alpha$, vagyis a vegyesszorzat abszolút értéke csakugyan megegyezik a paralelepipedon területével. Az előjellel most nem piszmogunk. □

Megjegyzés: Három dimenzióban tehát a determináns a sorvektorok feszítette paralelepipedon előjeles térfogatát adja meg, és ezt a vektoriális szorzat segítségével láttuk be. Magasabb dimenzióban azonban nem tudjuk két vektor „értelmes” vektoriális szorzatát definiálni. Azonban nem is ez az az út, ami a determináns szemléletes jelentéséhez vezet. Ha n dimenziós térről van szó, akkor a vektoriális szorzat mintájára lehetséges tetszőleges $n-1$ vektor „szorzatát” definiálni, ahol akárcsak a vektoriális szorzásnál, számít az „összeszorzott” vektortényezők sorrendje. (Valami olyasmiről lenne szó, hogy $n-1$ vektor egy ú.n. *hipersíkot* feszít, a szorzat erre merőleges, mégpedig úgy, hogy az n dimenzióban élő alienek számára jobbsordású rendszert kapjunk. A szorzatvektor hossza pedig a feszített $n-1$ dimenziós paralelepipedon térfogata lenne. (Minden valamirevaló ufókutató előtt jól ismert, hogy az n dimenziós űrlényeknek két karjuk van és mindegyik kezükön legalább n ujjuk, hiszen egyébként nem tudnának dolgokat szilárdan megfogni.)) Nos, ezt az általános vektoriális szorzást felhasználva be lehet éppenséggel vezetni az n dimenziós vegyesszorzást, ami nem volna más, mint az első „tényező” skaláris szorzata a további tényezők vektoriális szorzatával. A fenti lemma értelemszerű általánosítása igaz lenne erre a műveletre, és így azt kapnánk, hogy az $n \times n$-es determináns a sorvektorok feszítette sokdimenziós paralelelpipedon (szaknyelven *paralelotóp*) előjeles térfogatát adja meg.

2.6 Mátrix inverze

Def.: 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. □

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

Köv.: Az A mátrixnak pontosan akkor van jobbinverze, ha A-nak létezik balinverze.

A bizonyításhoz egy segédtételre van szükség.

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

Biz.: Emlékeztetünk, hogy az alsó index sort, a felső oszlopot jelent. Azt kell megmutatni, hogy a két mátrix elemenként azonos. És valóban: $((A \cdot B)^T)_i^j = (A \cdot B)_j^i = A_j \cdot B^i = (B^T)_i \cdot (A^T)^j = (B^T \cdot A^T)_i^j$. (A formalizmus valamennyire elrejti, mennyire triviális az állítás. Könnyen meggyőzhetjük erről magunkat, ha lerajzoljuk, hogyan állnak a mátrixok a szorzáskor.) □

A következmény bizonyítása a tétel felhasználásával: A-nak a tétel szerint pontosan akkor van jobbinverze, ha $\det A \neq 0$, azaz, a determinánsokról tanultak alapján $\det A^T \neq 0$. Utóbbi a tétel miatt azzal ekvivalens, hogy A^T-nak létezik egy X jobbinverze, ami a lemma szerint éppen azt jelenti, hogy X^T az A balinverze. □

Lemma: Tegyük fel, hogy A' az A négyzetes mátrixból elemi sorekvivalens átalakítások egymásutánjával kapható meg. Ekkor a $\det A = 0$ és $\det A' = 0$ állítások ekvivalensek.

Biz.: A lemma bizonyításához feltehetjük, hogy A' egyetlen elemi sorekvivalenssal kapható A-ból, hiszen ha egyetlen ESÁ sem tudja elrontani determináns 0 voltát ill. a sorok lin. ftnségét, akkor ESÁ-k sorozata sem képes erre.

A determináns tulajdonságairól tanultak alapján sorcserénél a determináns (-1)-szeres lesz, sorszorzásnál a determináns nemnullával szorzódik, míg sor másik sorhoz hozzáadásakor a determináns nem változik, tehát nem kaphatunk 0-ból nemnullát vagy fordítva. □

A tétel bizonyítása: Tekintsük azt a lineáris egyenletrendszert, aminek kibővített együtthatómátrixa az A mátrix, jobbról az e_i egységvektorral (azaz azzal az oszlopvektorral, aminek az i-dik koordinátája 1, az összes többi 0) kibővítve. Vegyük észre, hogy ha J az A jobbinverze, akkor a J mátrix i-dik oszlopa egy megoldását adja ennek az egyenletrendszernek, hiszen $A \cdot J^i = e_i$ a jobbinverz definíciója szerint. Tehát ha létezik jobbinverz, akkor minden i-re megoldható a fenti lineáris egyenletrendszer. Másfelől, ha ezen lineáris egyenletrendszerek mindegyike megoldható, akkor a megoldásokat oszlopvektorokba rendezve, az oszlopokat pedig egy J mátrixba gyűjtve $AJ = I_n$ adódik, tehát A-nak van jobbinverze.

Az inverz meghatározásához tehát ezeket az egyenletrendszereket próbáljuk megoldani. Azt a hasznos észrevételt tesszük, hogy ehhez nem szükséges nekünk sorban n Gauss-eliminációt elvégezni, mert eliminálhatunk „szimultán" is: jobbról 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 az $(A|I_n)$ mátrix Gauss-eliminációja utáni kapott $(A'|J')$ redukált lépcsős alakot! Ha $A' = I_n$, akkor az egyfelől azt jelenti, hogy A' mindegyik oszlopában van vezéregyes és nincs szabad paraméter, ezért mindegyik lineáris egyenletrendszer egyértelműen megoldható, azaz létezik jobbinverz, és az nem más, mint J'. Másfelől, $\det A' \neq 0$, és mivel A'-t A-ból ESÁ-k sorozatával kaptuk, ezért a lemma szerint $\det A \neq 0$ is fennáll.

A másik lehetőség, hogy $A' \neq I_n$. Ez azt jelenti, hogy A'-nek van olyan oszlopa, amiben nincs vezéregyes, ezért A' utolsó sorában sincs vezéregyes. Tehát $\det A' = 0$, és a lemma miatt pedig $\det A = 0$. Azt kell még megmutatnunk, hogy A-nak nem létezik jobbinverze, azaz valamelyik lineáris egyenletrendszer nem megoldható. Mivel J' az I_n mátrixból ESÁ-k sorozata után jött létre, ezért $\det I_n \neq 0 \neq \det J'$. Eszerint nem lehet J'-nek csupanulla sora, így ha J' utolsó sorában mondjuk az i-dik koordnináta nem 0, akkor az i-dik lineáris egyenletrendszer nem lesz megoldható a kapott tilos sor miatt. Ezek szerint nem létezik A-nak jobbinverze sem. □

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 $B = A^{-1}$. □

2.7 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.

Def.: Az A $n \times k$ méretű mátrix *sorrangján* az A mátrixból kiválasztható lineárisan független sorok maximális számát értjük: $s(A) := \dim\langle A_1, A_2, \dots A_n\rangle$. Az A mátrix *oszloprangja* az A mátrixból kiválasztható lineárisan független oszlopok maximális száma: $o(A) := \dim\langle A^1, A^2, \dots A^k\rangle$. Végül az A mátrix $d(A)$ *determinánsrangja* megegyezik A legnagyobb, nemnulla aldeterminánsának méretével. (Emlékeztetünk, hogy aldeterminánson egy olyan (természetesen négyzetes) determinánst értünk, amit A néhány sorának és oszlopának elhagyásával kapunk.)

Állítás: Tetszőleges A mátrixra $d(A) = d(A^T)$.

Biz.: Mivel négyzetes mátrix determinánsa megegyezik a transzponáltjának determinánsával, ezért az A-beli legnagyobb nemnulla aldetermináns az A^T-beli legnagyobb nemnulla aldetermináns transzponáltja lesz, ezért méretük megegyezik. $\square$

Megfigyelés: Ha az A mátrix lépcsős alakú és k vezéregyest tartalmaz, akkor a vezéregyeseket tartalmazó sorok lineárisan függetlenek. Ha A-nak legalább $k+1$ sorát választjuk ki, akkor azok lineárisan összefüggőek, hiszen van köztük (legalább) egy csupa-0 sor. Ha az A mátrix vezéregyeseket nem tartalmazó sorait és oszlopait elhagyjuk, akkor egy $k \times k$ méretű felső háromszögmátrixot kapunk, aminek a főátlója csupa-1, tehát ennek determinánsa sem 0. Ha pedig egy legalább $(k+1) \times (k+1)$ méretű részmátrixot tekintünk, akkor annak ugyancsak lesz csupa-0 sora, így a determinánsa is 0-nak adódik. Eszerint lépcsős alakú mátrixokra $s(A) = k = d(A)$. Az alábbi tétel ezt a megfigyelést általánosítja.

Tétel: Tetszőleges A mátrixra $s(A) = d(A)$.

A bizonyítás előtt rámutatunk egy fontos következményre.

Köv.: Tetszőleges A mátrixra $o(A) = d(A) = s(A)$.

Biz.: A tétel szerint $o(A) = \dim\langle A^1, A^2, \ldots\rangle = \dim\langle (A^T)_1, (A^T)_2, \ldots\rangle = s(A^T) = d(A^T) = d(A) = s(A)$, használva az előző tételt és állítást. $\square$

A következmény szerint mindegy, hogy egy mátrix esetében melyik rangfogalomról beszélünk, ezért helytálló az alábbi definíció.

Def.: Az A mátrix *rangja* $r(A) := s(A) = o(A) = d(A)$.

A tétel bizonyításához az alábbi segédtételt használjuk.

Lemma: Tegyük fel, hogy A' az A mátrixból elemi sorekvivalens átalakítások egymásutánjával kapható. Ekkor $s(A) = s(A')$ és $d(A) = d(A')$.

Biz.: Ahogy ezt korábban láttuk, elegendő azt az esetet igazolni, hogy ha A' egyetlen ESÁ-sal kapható A-ból. Az ESÁ definíciójából adódóan A' minden sora előáll A sorainak lineáris kombinációjaként, vagyis $A'_1, A'_2, \ldots \in \langle A_1, A_2, \ldots\rangle$, így $\langle A'_1, A'_2, \ldots\rangle \leq \langle A_1, A_2, \ldots\rangle$, tehát $\dim\langle A'_1, A'_2, \ldots\rangle \leq \dim\langle A_1, A_2, \ldots\rangle$, más szóval $s(A') \leq s(A)$. adódik. Korábban már láttuk, hogy minden ESÁ fordítottja is elvégezhető ESÁ-k sorozataként, ezért A'-ből megkapható A is. Ebből a fenti gondolatmenet szerint $s(A) \leq s(A')$ következik, amit az imént kapott $s(A') \leq s(A)$ egyenlőtlenséggel összevetve $s(A) = s(A')$ adódik.

Lássuk a determinánsrangot! Elegendő azt igazolni, hogy A minden $k \times k$ méretű aldeterminánsa pontosan akkor 0, ha A' minden $k \times k$ méretű aldeterminánsa 0. Tegyük fel, hogy ez A-ra igaz, és tekintsük A' egy $k \times k$ méretű B' részmátrixát. Ha A'-t egy sorcsere vagy egy sor konstanssal való szorzásával kaptuk meg, akkor látjuk, hogy A-ban van egy B'-nak megfelelő B részmátrix, amire $|B'| = |B| = 0$ vagy $|B'| = -|B| = -0 = 0$ vagy $|B'| = \lambda|B| = \lambda \cdot 0 = 0$ teljesül, utóbbi arra a λ konstansra, amivel az ESÁ során a sort szoroztuk. Tehát sorcsere vagy sorszorzás után minden $k \times k$ méretű determináns 0 marad. Ha az ESÁ sorhozzáadás volt, akkor vagy $|B'| = |B| = 0$, vagy $|B|$ felírható két A-beli $k \times k$ méretű determináns összegeként. Ismét azt kapjuk, hogy $|B'| = 0 + 0 = 0$.

Hátra van még annak igazolása, hogy ha A' minden $k \times k$ méretű aldeterminánsa 0, akkor ez A-ra is igaz. Ez a fenti gondolatmenetből úgy következik, hogy ismét megfigyeljük, hogy minden ESÁ fordítottja elvégezhető ESÁ-k sorozataként. $\square$

A tétel bizonyítása: Láttuk, hogy ESÁ-kkal sem $s(A)$, sem pedig $d(A)$ nem változik. Végezzük el A Gauss-eliminációját, így kapjuk A' lépcsős alakú mátrixot. A fenti lemma és megfigyelés miatt $s(A) = s(A') = d(A') = d(A)$, és nekünk pontosan ezt kellett igazolnunk. $\square$

2.8 Lineáris egyenletrendszerek tárgyalása mátrixokkal

Tétel: Legyen $A \in \mathbb{R}^{k \times n}$, tetszőleges valós mátrix. Az alábbi állítások ekvivalensek.

(1) Az $(A|b)$ kibővített együtthatómátrix leírta lineáris egyenletrendszernek (egyért.) megoldása van.
(2) (Egyértelműen) létezik $x \in \mathbb{R}^n$, amire $Ax = b$.
(3) (Egyértelműen) létezik $x \in \mathbb{R}^n$ úgy, hogy $b = \sum_{i=1}^n A^i x_i$.
(4) $b \in \langle A^1, \ldots, A^n\rangle$ (és $A^1, \ldots A^n$ lineárisan független vektorok).
(5) $\langle A^1, \ldots, A^n\rangle = \langle b, A^1, \ldots, A^n\rangle$ (és $A^1, \ldots A^n$ lineárisan független vektorok).
(6) $\dim(\langle A^1, \ldots, A^n\rangle) = \dim(\langle b, A^1, \ldots, A^n\rangle)(= n)$. (7) $r(A) = r(A|b)(= n)$.

Biz.: (1) $\iff$ (2): A definíciókból adódik. (2) $\iff$ (3): A mátrixszorzásnál tett fontos megfigyelés alkalmával láttuk, hogy $Ax = b \iff b = \sum_{i=1}^n A^i x_i$. (3) $\iff$ (4): 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.
(4) $\iff$ (5): b pontosan akkor van benne az oszlopvektorok terében, ha az oszlopvektorokhoz b-t hozzávéve nem tudunk további vektort generálni.
(5) $\iff$ (6): Az $A^1, \ldots, A^n$ vektorok pontosan akkor lineárisan függetlenek, ha az általuk generált térben bázist alkotnak, azaz, ha a generátum dimenziója n.
(6) $\iff$ (7): 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. $\square$

Tétel: Az $n \times n$ méretű A együtthatómátrixszal megadott lineáris egyenletrendszer pontosan akkor oldható meg egyértelműen, ha $|A| \neq 0$.

Biz.: Ha $|A| \neq 0$, akkor a mátrixok inverze kapcsán tanultak szerint A-nak létezik inverze. Innen $x = (A^{-1} \cdot A)x = A^{-1} \cdot (Ax) = A^{-1}b$, tehát x (ha létezik), akkor egyértelmű. Az $x = A^{-1}b$ vektor viszont megoldás, hiszen $Ax = A(A^{-1}b) = (A \cdot A^{-1})b = I \cdot b = b$. Ezzel az elégségességet igazoltuk.

A szükségességhez tegyük fel, hogy a megoldás egyértelmű. Az előző tétel (4) része szerint ekkor A oszlopai lineárisan függetlenek. Ekkor A rangja n lesz, ezért létezik A-nak $n \times n$ méretű nemnulla determinánsú részmátrixa, ami csakis maga A lehet. Eszerint $|A| \neq 0$. $\square$

2.9 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) $\mathcal{A}(\lambda u) = \lambda\mathcal{A}(u) \quad \forall \lambda \in \mathbb{R},\ \forall u \in U$ teljesül.
Lineárisnak tehát a műveletartó 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.

Az is egyszerűen (n szerinti indukcióval) bizonyítható, hogy (3) ekvivalens a formálisan többet kívánó
(3') $\mathcal{A}(\sum_{i=1}^n \lambda_i v_i) = \sum_{i=1}^n \lambda_i \mathcal{A}(v_i) \quad \forall n \in \mathbb{N}, \forall v_1, v_2, \ldots, v_n \in V, \forall \lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{R}$
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.

Megfigyelés: Ha $\mathcal{A} : U \to V$ egy lineáris leképezés, akkor szükségképpen $\mathcal{A}(\mathbf{0}) = \mathbf{0}$ teljesül, ahol az első $\mathbf{0}$ az U, a második pedig a V tér nullvektora, hiszen $\mathcal{A}(\mathbf{0}) = \mathcal{A}(\mathbf{0} + \mathbf{0}) = \mathcal{A}(\mathbf{0}) + \mathcal{A}(\mathbf{0})$, és mindkét oldalhoz az $\mathcal{A}(\mathbf{0})$ vektor ellentettjét hozzáadva $\mathbf{0} = \mathcal{A}(\mathbf{0})$ adódik. $\square$

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 műveletartás a deriválás azonosságai miatt igaz: $(p + q)'(x) = p'(x) + q'(x)$, ill. $(\lambda p)'(x) = \lambda p'(x)$.

Állítás: A lineáris leképezést egyértelműen meghatározzák a báziselemek képei. Pontosabban: Ha U és V valós vektorterek, az $u_1, u_2, \ldots, u_n$ vektorok az U bázisát alkotják és $v_1, v_2, \ldots, v_n$ 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.

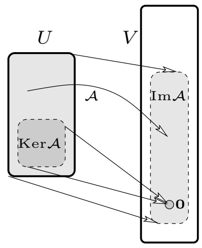
Biz.: Tegyük fel, hogy létezik a kívánt lineáris leképezés, megmutatjuk, hogy egyértelmű. Legyen ugyanis $u \in U$ tetszőleges vektor. Ekkor u egyértelműen áll elő az U adott bázisának lineáris kombinációjaként, mondjuk $u = \sum_{i=1}^n \lambda_i u_i$ alakban. Ekkor $\mathcal{A}$ feltételezett linearitása 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 műveletartó. 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
$\mathcal{A}(u + v) = \mathcal{A}(\sum_{i=1}^n \lambda_i u_i + \sum_{i=1}^n \mu_i u_i) = \mathcal{A}(\sum_{i=1}^n \lambda_i u_i + \mu_i u_i) = \mathcal{A}(\sum_{i=1}^n (\lambda_i + \mu_i) u_i) =$ [7] $\sum_{i=1}^n (\lambda_i +$

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

$\mu_i)v_i = \sum_{i=1}^n \lambda_i v_i + \mu_i v_i = \sum_{i=1}^n \lambda_i v_i + \sum_{i=1}^n \mu_i v_i =^7 \mathcal{A}(u) + \mathcal{A}(v)$,
ill. $\mathcal{A}(\lambda\ u) = \mathcal{A}(\lambda \sum_{i=1}^n \lambda_i u_i) = \mathcal{A}(\sum_{i=1}^n \lambda\lambda_i u_i) =^7 \sum_{i=1}^n \lambda\lambda_i v_i = \lambda \sum_{i=1}^n \lambda_i v_i = \lambda\mathcal{A}(u)$. □

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 $\mathcal{A} : U \to V$ lineáris leképezés, akkor $\dim \mathrm{Ker}\mathcal{A} + \dim \mathrm{Im}\mathcal{A} = \dim U$.

Biz.: Legyen $B' := \{b_1, b_2, \ldots, b_k\}$ a $\mathrm{Ker}\mathcal{A}$ vektortér egy bázisa. Mivel B' független az U vektortérben, ezért létezik U-nak egy B'-t tartalmazó bázisa, mondjuk $B = \{b_1, b_2, \ldots, b_k, b_{k+1}, \ldots, b_n\}$. 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 $\mathcal{A}(b_{k+1}), \mathcal{A}(b_{k+2}), \ldots, \mathcal{A}(b_n)$ vektorok az $\mathrm{Im}\mathcal{A}$ tér egy bázisa. Azt kell tehát igazolnunk, 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 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 $\mathcal{A}^{-1}(\mathbf{0}) = \mathbf{0}$ miatt $\mathrm{Ker}\mathcal{A} = \{\mathbf{0}\}$.

$\Leftarrow$: 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 $U \cong V$. □

2.9.1 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 koordiná-

tavektorokról 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 $\sum_{i=1}^n \mu_i \lambda_j^i$. Ha jól megfigyeljük, éppen azt kaptuk, hogy a leképezés mátrixával való szorzás megadja a leképezést a koordinátavektorokon. Ezt írja le az alábbi tétel.

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.

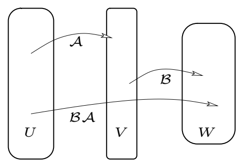
Megfigyelés: Ha $\mathcal{A}, \mathcal{B} \in \mathrm{Hom}(U, V)$ és $\lambda \in \mathbb{R}$, akkor $\mathcal{A} + \mathcal{B}, \lambda\mathcal{A} \in \mathrm{Hom}(U, V)$, azaz lineáris leképezések összege és skalárszorosa is lineáris leképezés. E műveletekkel $\mathrm{Hom}(U, V)$ szintén valós vektortér, 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 $[\mathcal{B}]_{B_2}^{B_1}$ 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. Honnan is ismerős ez a sor-oszlop szorzás? Az alábbi állítás adja meg a választ.

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. □

2.10 Lineáris transzformációk és mátrixok sajátértékei, sajátvektorai és sajátalterei

Egy $\mathcal{A}$ lineáris leképezés esetén egy vektor „különlegesnek” számított, ha a nullvektorba képződik (hisz a nullvektor egy „különleges” vektora a vektortérnek). Ezek a vektorok alkották a Ker$\mathcal{A}$ magteret. Ha azonban lineáris transzformációról van szó, akkor amint rögzítünk egy v vektort, az értelmezési tartományban már nem csak a $\mathbf{0}$ lesz „különleges” vektor, hanem v (és annak konstansszorosai) is. Tehát nemcsak úgy jöhet létre érdekes szituáció, ha egy vektor a $\mathbf{0}$-ba képződik, hanem úgy is, ha egy vektor fix pontja a leképezésnek, azaz önmagába képződik. Sőt, az is érdekes szituáció, ha egy vektor képe a saját konstansszorosa. Ez motiválja a most következő szakaszt.

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: $\{v \in V : \mathcal{A}(v) = \lambda \cdot v\}$.

Az $\mathbb{R}^n$ vektortéren ható lineáris transzformációra példa egy tetszőleges $n \times n$ méretű $A \in \mathbb{R}^{n\times n}$ méretű mátrixszal való szorzás, azaz az $x \mapsto A \cdot x$ hozzárendelés. (Az előző szakaszban azt láttuk egyébként, hogy minden véges dimenziós vektorterek között ható lineáris leképezés a koordinátavektorokon mátirxszorzásként hat, ezért az $\mathbb{R}^n$ tér minden lineáris transzformációja egy $n\times n$ méretű mátrixszal való balszorzás.) Így speciális lineáris transzformációkra: a négyzetes mátrixszal való szorzásra is elmondhatjuk a fenti definíciót.

Def.: Legyen $A \in \mathbb{R}^{n\times n}$ egy négyzetes mátrix, $v \in \mathbb{R}^n$ egy oszlopvektor, és $\lambda \in \mathbb{R}$ egy skalár. A v vektort az A mátrix λ *sajátértékhez* tartozó *sajátvektorának* mondjuk, ha (1) $v \neq \mathbf{0}$ és (2) $A \cdot v = \lambda \cdot v$.

(A fenti definícióban $\mathbf{0}$ a szokásos módon a csupa 0-kból álló oszlopvektort jelöli.) A továbbiakban általában foglalkozunk a lineáris transzformációkkal, így a megállapításaink az iménti definícióban szereplő mátrixszorzás esetére is érvényesek lesznek.

Megjegyzés: Vegyük észre, hogy $\lambda = 0$ pontosan akkor sajátérték, ha a Ker$\mathcal{A}$ magtér nem csak a nullvektorból áll. Ebben az esetben a $\lambda = 0$-hoz tartozó sajátaltér megegyezik a magtérrel.

A definíció (1) feltétele valójában technikai dolog, azért vettük előre, hogy ne felejtsük el (mondjuk a vizsgán). Azért van rá szükség, mert e nélkül nem volna igaz az alábbi tétel.

Tétel: (1) Lineáris transzformáció minden sajátvektora pontosan egy sajátértékhez tartozik.
(2) Bármely λ sajátértékhez tartozó sajátaltér a V vektortér altere.

Biz.: (1): Ha v sajátvektor, akkor $\mathbf{0} \neq v$. 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. $\mathcal{A}(\mu u) = \mu \cdot \mathcal{A}(u) = \mu \cdot (\lambda \cdot u) = (\mu\lambda)u = \lambda \cdot (\mu u)$. □

Vizsgáljuk meg, mit jelent az, hogy λ egy $\mathcal{A}$ transzformáció sajátértéke! Ekkor a λ-hoz tartozó bármely v sajátvektorra$\mathcal{A}(v) = \lambda v$ teljesül, 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 a $v \neq \mathbf{0}$ vektort a $\mathbf{0}$-ba képzi. 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 független 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. □

Hogyan számíthatjuk ki egy adott $\mathcal{A}$ lineáris transzformáció sajátértékeit és sajátvektorait? Rögzítünk egy B bázist, és felírjuk a transzformáció $[\mathcal{A}]_B^B$ mátrixát ebben a bázisban. A mátrix főátlóelemeiből kivonunk λ-t, és az így kapott mátrixnak kiszámítjuk a determinánsát, azaz meghatározzuk a karakterisztikus polinomot. Valahogyan meghatározzuk a karakterisztikus polinom gyökeit. Pontosan ezek a gyökök lesznek $\mathcal{A}$ sajátértékei. Egy adott λ-hoz tartozó sajátaltér meghatározása pedig úgy történik, hogy megoldjuk az $([\mathcal{A}]_B^B - \lambda I)x = 0$ lineáris egyenletrendszert, és a megoldásul kapott x-ek lesznek a λ-hoz tartozó sajátaltérbeli vektorok koordinátavektorai.

Példa: Tegyük fel, hogy az $\mathcal{A}$ leképezés mátrixa $A = \begin{pmatrix} 2 & 0 & -3 \\ 0 & 2 & 5 \\ 1 & 1 & 0 \end{pmatrix}$ valamely bázisban. A karakterisztikus polinom (oszlop szerint kifejtve) $\begin{vmatrix} 2-\lambda & 0 & -3 \\ 0 & 2-\lambda & 5 \\ 1 & 1 & -\lambda \end{vmatrix} = (2-\lambda) \cdot \begin{vmatrix} 2-\lambda & 5 \\ 1 & -\lambda \end{vmatrix} + 1 \cdot \begin{vmatrix} 0 & -3 \\ 2-\lambda & 5 \end{vmatrix} = (2-\lambda)(-\lambda \cdot (2-\lambda) - 5) + 3(2-\lambda) =$ $(2-\lambda)(\lambda^2 - 2\lambda - 2) = (2-\lambda)(\lambda - (1+\sqrt{3}))(\lambda - (1-\sqrt{3}))$. Eszerint a sajátértékek $\lambda = 2$, $\lambda = 1 + \sqrt{3}$ és $\lambda = 1 - \sqrt{3}$. A $\lambda = 2$-höz tartozó sajátérvektorokra az igaz, hogy $(A - 2 \cdot I)x = 0$, vagyis olyan lineáris egyenletrendszer megoldásait keressük, amelynek kibővített együtthatómátrixa és annak Gauss-eliminációja az alábbiak szerint néz ki:
$\left.\begin{matrix} 0 & 0 & -3 \\ 0 & 0 & 5 \\ 1 & 1 & -2 \end{matrix}\right| \begin{matrix} 0 \\ 0 \\ 0 \end{matrix} \quad \to \quad \left.\begin{matrix} 1 & 1 & -2 \\ 0 & 0 & -3 \\ 0 & 0 & 5 \end{matrix}\right| \begin{matrix} 0 \\ 0 \\ 0 \end{matrix} \quad \to \quad \left.\begin{matrix} 1 & 1 & -2 \\ 0 & 0 & 1 \\ 0 & 0 & 5 \end{matrix}\right| \begin{matrix} 0 \\ 0 \\ 0 \end{matrix} \quad \to \quad \left.\begin{matrix} 1 & 1 & -2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{matrix}\right| \begin{matrix} 0 \\ 0 \\ 0 \end{matrix}$ A sajátaltér elemei az $x = (x_1, x_2, x_3)$ megoldások lesznek, tehát $x_2 \in \mathbb{R}$ szabad paraméter, $x_3 = 0$ és $x_1 = -x_2$ adódik. Vagyis a sajátaltér elemei a $(-x_2, x_2, 0)$ alakú vektrok lesznek, és $x_2 \neq 0$ esetén ezek éppen a $\lambda = 2$ sajátértékhez tartozó sajátvektorokkal lesznek azonosak.

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.) □

3. fejezet

Kombinatorika, gráfelmélet

3.1 Elemi leszámlálások

Def.: Legyenek $k, n \in \mathbb{N}$ és $0 \leq k \leq n$. Az *n elem k-adosztályú (ismétlés nélküli) variációján* n db, rögzített, egymástól megkülönböztethető elemből kiválasztott k különböző 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 az első k befutó sorrendje hányféle lehet.

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 tetszőlegesen 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 (azaz résztáv) 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. $k \geq 1$ 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: Tegyük fel, hogy n ellenőrzésen kell átjutnunk, mindegyiken egy-egy jelszó bemondásával, és ha rossz jelszóval próbálkozunk, azonnal veszítünk. Ha ismerjük az n jelszót, de nem tudjuk, hogy azok melyik ellenőrzési pontokhoz tartoznak, akkor a feladatunk az, hogy eltaláljuk a jelszavak azon permutációját, ami szerint azokat bemondva átjutunk az ellenőrzéseken.

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 $n := k_1 + k_2 + \ldots + k_l$. Ekkor n elem *ismétléses permutációja* alatt l féle elem egy olyan n hosszú sorrendet értünk, amiben az i-dik elem pontosan k_i-szer jelenik meg minden $1 \leq i \leq l$ esetén.

Példa: Ha tudjuk, hogy egy héten minden nap öt óránk van az általános iskolában, és ismerjük az egyes tárgyak heti óraszámait (legyenek ezek $k_1, k_2, \ldots, k_l$, amikre természetesen $k_1 + k_2 + \ldots + k_l = 25$ 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 beszélünk, 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 az $\{1, 2, \ldots, n\}$ halmaz minden eleméhez rendeljük a sorbarendezendő l-féle elem valamelyikét úgy, hogy az i-dik fajta elemet pontosan k_i db számhoz rendeljük. Világos, hogy a fenti hozzárendeléssel az $\{1, 2, \ldots, n\}$ halmaz elemeinek minden egyes permutációja meghatároz egy ismétléses permutációt. Másfelől, minden egyes ismétléses permutáció az $\{1, 2, \ldots, n\}$ elemeinek pontosan ugyanannyi permutációjából kapható meg: ha ugyanis egy rögzített ismétléses permutációt szeretnék megkapni, akkor minden egyes k_i méretű halmaz elemeit az ismétléses permutáció által meghatározott pozíciókra kell tetszőlegesen szétosztani. Ezt csoportonként $k_i!$-féleképp tehetjük meg, a csoportonkon egymástól függetlenül, tehát minden egyes ismétléses permutációt éppen $k_1! \cdot k_2! \cdot \ldots \cdot k_l!$ permutáció határoz meg. Mivel az $\{1, 2, \ldots, n\}$ ismétlés nélküli permutációinak száma $n!$, ezért az ismétléses permutációk számára a $\frac{n!}{k_1! \cdot k_2! \cdot \ldots \cdot k_l!}$ formula adódik.

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 n 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: 90 lehetséges számból az 5 nyerőszámot $C(90, 5)$-féleképp lehet kivállasztani, hisz a kihúzás sorrendje nem számít.

Vegyük észre, hogy n elem minden k-adosztályú variációja egyértelműen meghatároz egy k-adosztályú kombinációt: egyszerűen el kell feledkezni a 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 $C(n, k) = \frac{V(n,k)}{k!} = \frac{n!}{(n-k)! \cdot k!}$.

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, ráádásul 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" ?) módon kiolvasott ú.n. *binomiális együtthatót.* A fenti jelöléssel $C(n, k) = \binom{n}{k}$ adódik.

Megjegyzés: 1. Ránézésre itt sem világos, hogy $\binom{n}{k}$ egész szám, 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 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 kombinációinak száma $C_{ism}(n, k)$.

Példa: Ha egy cukrászdában n-féle süteményt árulnak, és mindegyik fajtából korlátlan számú áll rendelkezésre, akkor k db süteményt 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. egy $a_1 + a_2 + \ldots + a_n = k$ ismétléses permutációt úgy alakítunk át, hogy minden a_i-t a_i db 1-essel, és minden +-t egy db 0-val kódolunk, az $= k$ végződést pedig elhagyjuk. Pl a $0 + 0 + 3 + 2 + 0 + 5 + 0 = 10$ összegnek megfelelő ismétléses permutációt a 0011101100111110 sorozat kódolja.) 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 $(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} = \binom{n}{0} b^n + \binom{n}{1} a b^{n-1} + \ldots + \binom{n}{i} a^i b^{n-i} + \ldots + \binom{n}{n} a^n$.

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 $0 \le i \le n$ egészre. Konkrétan: $a^i b^{n-i}$ annyiszor fog adódni, ahányféleképpen ki lehet választani i db a-t a lehetséges n-ből, azaz $\binom{n}{i}$-szer. □

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 $(i+1)$-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
... ...

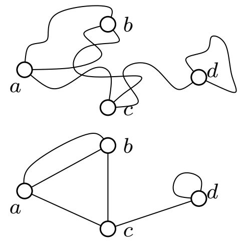
A Pascal háromszög

3.2 Gráfok

Def.: A $G = (V, E)$ pár egy *egyszerű gráf*, ha (1) $V \neq \emptyset$ és (2) $E \subseteq \binom{V}{2} := \{\{u, v\} : u, v \in V, u \neq v\}$, azaz E elemei V bizonyos kételemű részhalmazai. Ha G egy gráf, akkor $V(G)$ jelöli G *csúcsainak* (néha *pontjainak)*, $E(G)$ pedig G *éleinek* halmazát, azaz $V(G)$ az a V halmaz, és $E(G)$ az az E halmaz, amire $G = (V, E)$.

Def.: A G gráf egy *diagramja* a G egy olyan lerajzolása, amiben a csúcsoknak (síkbeli) pontok felelnek meg, éleknek pedig olyan síkgörbék[1], amik az adott él két végpontját kötik össze, önmagukat nem metszik, és más végpontokat elkerülnek. Az $e = \{u, v\}$ élt röviden $e = uv$-vel jelöljük, u-t és v-t az e él ***végpontjainak*** mondjuk. Az u és v csúcsok *szomszédosak*, ha $uv \in E$. Az e és f éleket *párhuzamosnak* nevezzük, ha végpontjaik azonosak[2]. *Hurokél* az olyan él, aminek két végpontja megegyezik[3]. A $G = (V, E)$ pár *gráf*, ha $V \neq \emptyset$, E élhalmaz V-n, és párhuzamos és hurokél is megengedett.

$$\begin{pmatrix} 0 & 2 & 1 & 0 \\ 2 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$$



A $G = (\{a, b, c, d\}, \{ab, ab, ac, bc, cd, dd\})$ gráf szomszédossági mátrixa és két lehetséges diagramja.

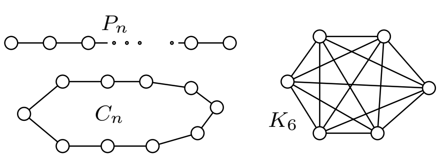
Def.: A G gráf *szomszédossági mátrixa* az a $V(G) \times V(G)$ méretű mátrix, aminek (u, v) pozícióján az u és v közti élek száma áll ($u = v$ esetén a hurokélek számának kétszerese). A G gráf *véges*, ha $V(G)$ és $E(G)$ is véges halmazok.

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

Tétel: Ha G véges (nem feltétlenül egyszerű) gráf, akkor $\sum_{v \in V(G)} d(v) = 2|E(G)|$, azaz egy véges gráf fokszámainak összege éppen az élszám kétszerese.

Biz.: Ha G-nek nincs éle, akkor a fokszámösszeg is és az élszám (kétszerese) is 0. Építsük fel G-t úgy, hogy egyenként húzzuk be az éleket. Minden egyes új él behúzása eggyel növeli az élszámot, és kettővel a fokszámösszeget, hisz két ponton növekszik egyet a fokszám (vagy hurokél esetén egy csúcsnál 2-vel). Eszerint amikor G-t felépítettük, akkor is igaz lesz ez a tulajdonság, épp, ahogy a tétel állítja. □

Def.: K_n az n pontú *teljes gráf*: $|V(G)| = n$, és bármely két pont össze van kötve (egyszer).
Világos, hogy a K_n gráf $(n-1)$-reguláris, és $|E(K_n)| = \binom{n}{2}$.
P_n az n *pontú út*, C_n az n *pontú kör*:
$V(P_n) = V(C_n) = \{v_1, \ldots, v_n\}$, $E(P_n) = \{v_i v_{i+1} : 1 \le i < n\}$, $E(C_n) = E(P_n) \cup \{v_1 v_n\}$. (ld. az ábrát)



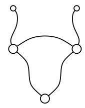
Megfigyelés: $K_2 = P_2, K_3 = C_3$

[1]Görbe helyett szerencsésebb töröttvonalról beszelni. Egy görbe egészen váratlan módon is tud viselkedni. Hagyjuk.
[2]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.
[3]Ehhez is módosítani kéne az él definícióját, de itt sem az absztrakt formalizmus a cél.

Def.: $D = (V, A)$ *irányított gráf*, ha (1) $V \neq \emptyset$ és (2) $A \subseteq V^2$. (Minden élnek van egy irányítása. A diagramon nyilakkal szokás jelölni. Párhuzamos és hurokél itt is értelmezhető, és akár mindkét irányú él be lehet húzva két pont között. Az irányítatlan fogalmak jó része értelemszerűen kiterjed.)

Def.: 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. $u, v \in V(G_1)$ esetén u-ból pontosan annyi él vezet v-be G_1-ben, mint a $\varphi(u)$-ból $\varphi(v)$-be G_2-ben.)

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



a bika

Példa: A P_4, a C_5 ill. a „bika” *önkomplementer* (saját komplemeterével izomorf) gráf.

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) $G_1 \cong G_2 \cong G_3 \Rightarrow G_1 \cong G_3$. □

Def.: 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.

Def.: 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. □

Def.: $u, v \in V(G)$-re $u \sim v$, ha létezik u és v között séta.

Állítás: Irányítatlan gráfon 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. □

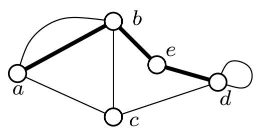
Def.: A G gráf *komponense* a $\sim$ ekvivalenciareláció ekvivalenciaosztálya.

A komponens fogalma a fenti absztrakt definíció helyett az alábbi módon is definiálható.

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 bontható komponensekre. □

Def.: Legyen $G = (V, E)$ gráf, $e \in E$, $E' \subseteq E$, $v \in V$, $V' \subseteq V$. Ekkor $G - e := (V, E \setminus \{e\})$ az e él törlésével keletkező gráf, $G - E' := (V, E \setminus E')$ pedig az E'-beli élek 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'-beli pontok törlésével keletkező gráf. Tehát él (ill. élek) törlésekor csak az élhalmaz változik, ha pontot (ill. pontokat) törlünk, akkor a törölt pont(ok)ra illeszkedő éleket is törölnünk kell.



Legyen G egy gráf és $V' \subseteq V(G)$, ill. $V^* := V \setminus V'$. G^* a *G gráf V^* által feszített részgráfja*, ha $G^* = G - V'$. A feszített részgráfot tehát úgy kapjuk, hogy néhány csúcsot törlünk a gráfból.

Részgráfot pedig úgy kapunk, hogy a csúcsok mellett élek törlése is megengedett, azaz H a *G részgráfja*, ha $H = (G - V') - E'$ alkalmas $V' \subseteq V(G)$ és $E' \subseteq E(G)$-re.

A jobboldali ábrán látható gráf vastagított élei a csúcsaikkal együtt egy részgráfot alkotnak. Ez nem feszített részgráf, ugyanis ehhez a hurokélt és az ab él párhuzamos példányát is tartalmaznia kellene.

Hagyományosan úgy szokás definiálni a fenti fogalmakat, hogy a $H = (V', E')$ gráf a $G = (V, E)$ részgráfja, ha $V' \subseteq V$ és $E' \subseteq E$. A H részgráfot pedig akkor nevezik feszítettnek, ha E' minden olyan E-beli élt tartalmaz, aminek végpontjai V'-ben vannak. Könnyen látható, hogy az általunk használt definíció ekvivalens a „hagyományossal”.

3.2.1 Fák alaptulajdonságai

Def.: 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, hiszen egy komponens két pontja közé élt húzva kört kapnánk. Azonban két különböző komponens közé behúzott él pontosan 1-gyel csökkenti a gráf komponenseinek számát. Ha végül 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. □

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

Biz.: Szokás szerint építsük fel G-t élek egymás utáni behúzásával. Tudjuk, hogy minden él behúzása legfeljebb 1-gyel csökkenti a komponensek számát, így a kezdeti n izolált pontból csakis akkor kaphatunk egy 1 komponensű gráfot, ha mind az $n-1$ élt két addigi komponens közé húztuk be. Ez azt jelenti, hogy egyik él behúzása sem hozott létre kört, a gráfunk körmentes. □

Köv.: G 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 $V(G) = V(F)$. (Jegyezzük meg, hogy a feszítőfa általában nem *feszített* részgráf.)

Biz.: Hagyjunk el egymás után G éleit, míg a gráf öf marad. Végül egy minimális öf gráfot, azaz fát kapunk. Ez feszítőfa lesz, hisz nem hagytunk el pontot. □

Def.: Egy F fa v csúcsa *levél*, ha $d(v) = 1$.

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

Biz.: Tekintsünk F egy leghosszabb útját, mondjuk az u-t és v-t összekötő P-t! Ekkor sem u-ból, sem v-ből nem indulhat további él: ha az ugyanis egy P-n kívüli pontba futna, akkor P nem lenne leghosszabb, ha pedig P egy pontjába, akkor a F nem lenne körmentes. □

3.2.2 A Cayley tétel

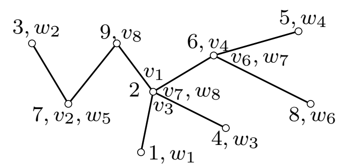
Alapprobléma: Hány n-pontú fa van? Izomorfia erejéig: n = 1-re, n = 2-re és n = 3-ra 1, hisz nincs sok választásunk. n = 4-re 2 (a $K_{1,3}$ és a P_4), n = 5-re pedig 3 (a 2-levelű, a 3-levelű és a 4-levelű), n = 6-ra 6 (a 2-levelű út, kétféle 3-levelű, kétféle 4-levelű és egy 5-levelű), magasabb n-ekre ezt már fáradságos folytatni.

Számozott csúcsokon (vagyis egyébként izomorf fákat többször megszámolva) azt kapjuk, hogy n = 1-re és n = 2-re 1, n = 3-ra 3 (szabadon választjuk, melyik két csúcs összekötetlen), n = 4-re 16 (négyféle $K_{1,3}$ és 12-féle P_4), n = 5-re 125 (60-féle P_5, 60-féle 3-levelű és ötféle 4-levelű), n = 6-ra pedig jó sok. Mi a szabály? Az alábbi tétel mutatja meg.

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

Biz.: (A Prüfer-kód segítségével) Ha egy F fa csúcsai különböző számokkal vannak címkézve, akkor definiáljuk az F fa $P(F)$-fel jelölt *Prüfer-kódját* az alábbiak szerint. Ha F-nek legfeljebb két csúcsa van, akkor a kód üres: $P(F) := \emptyset$. Ha F-nek legalább 3 csúcsa van, akkor legyen w_1 az F legkisebb címkéjű levele, legyen c_1 a w_1 levél v_1 szomszédjának címkéje, és legyen $P(F) := (c_1, P(F - w_1))$. Más szóval: töröljük a legkisebb címkéjű levelet, írjuk le a szomszédjának a címkéjét, és ezt az eljárást addig iteráljuk, amíg a fának végül két csúcsa lesz.

Megfigyelés: Amikor a fának a törlések után már csak két csúcsa van, akkor ezek egyike a legnagyobb címkéjű (jelen esetben n-es) csúcs. Ez azért van így, mert az n címkéjű csúcsot sosem törölhettük, hisz mindig legalább két levél közül választottuk ki a minimális címkéjűt. Vagyis ha a Prüfer-kód képzését nem a kétcsúcsú fánál hagynánk abba, hanem az egycsúcsúnál (amikoris elfogynak a törölhető levelek), akkor az utolsónak törölt levél szomszédja bizonyosan az n címkéjű csúcs lenne.



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

Világos, hogy a Prüfer-kód tetszőleges 1-től n-ig címkézett fához egyértelműen rendel egy $n-2$ hosszúságú sorozatot úgy, hogy a sorozat minden tagja egy 1 és n közötti címke. Az ismétléses variációkról tanultak szerint ilyen sorozatból n^{n-2}-féle létezik. A továbbiakban tehát két dolgot kell igazolnunk: (1) különböző fákhoz különböző Prüfer-kódok tartoznak ill. (2) tetszőleges $n-2$ hosszúságú, $1, 2, \ldots, n$ jeleket tartamazó sorozathoz létezik olyan fa, aminek ez a sorozat a Prüfer-kódja. Ez igazolja, hogy a címkézett fák bijektíven megfelelnek az említett ismétléses variációknak, és így a számuk pontosan n^{n-2}. Mi csak az (1)-t fogjuk igazolni, azaz, hogy tetszőleges Prüfer-kódból egyértelműen lehet a fát „visszakódolni". A bizonyításhoz egy segédtételre is szükség lesz.

Lemma: A Prüfer-kódban tetszőleges v csúcs címkéje pontosan $(d(v) - 1)$-szer szerepel.

Biz.: Tegyük fel, hogy v címkéje n-nél kisebb. Amikorra a Prüfer-kódolást befejezzük, akkorra már vagy töröltük v-t, vagy v levél maradt, és az n címkéjű csúcshoz csatlakozik. Az első esetben v-t egy olyan állapotában töröltük, amikor v levél volt, és innentől kezdve nem írtuk be v címkéjét a kódba. Ahhoz azonban, hogy v levéllé váljon, pontosan $d(v) - 1$ szomszédját kellett törölni, és pontosan ezen alkalmakkor írtuk le v címkéjét a Prüfer-kódba. Tehát v címkéje pontosan $(d(v) - 1)$-szer szerepel. Ha v végül levél maradt, akkor is igaz a fenti érvelés, hiszen odáig $d(v) - 1$ (levél)szomszédját töröltük.

Ha pedig v az n címkéjű csúcs, akkor a Prüfer-kódolás befejezésekor v-nek egy szomszédja maradt, addig tehát $d(v) - 1$ szomszédja lett törölve, így az n címkét éppen $(d(v) - 1)$-szer írtuk le a kód legyártásakor. □

Köv.: Tetszőleges (különböző számokkal címkézett csúcsú) F fának a Prüfer-kódjában nem szereplő címkék azonosak F leveleinek címkéivel.

Biz.: Egy v csúcs pontosan akkor levele F-nek, ha $d(v) = 1$, azaz, ha v címkéje nem szerepel F Prüfer-kódjában. □

Tegyük fel tehát, hogy csúcscímkék valamely $(c_1, c_2, \ldots, c_{n-2})$ sorozata egy F fa Prüfer-kódja. Legyen $c_{n-1} = n$, a Prüfer kód ki nem írt, befejező eleme. Az F fa meghatározásához mindössze F $n-1$ élét kell megtalálnunk, azaz minden egyes c_i címkéhez meg kell mondanunk azt, hogy mi volt a c_i leírásakor törölt w_i levél l_i címkéje. Mi sem egyszerűbb ennél. A fenti következmény miatt az elsőnek törölt levél l_1 címkéje nem más, mint a legkisebb olyan címke, ami nem fordul elő a $c_1, c_2, \ldots, c_{n-2}$ sorozatban. (Mivel $l_1 < n$, ezért azt is mondhatjuk, (ami a gyakorlatban történő visszafejtést kicsit egyszerűsíti), hogy l_1 a legkisebb olyan címke, ami nem fordul elő a $c_1, c_2, \ldots, c_{n-1}$ sorozatban.)

Mi lesz ezek után a másodiknak törölt levél l_2 címkéje? Világos, hogy az első levél törlése után kapott $F - w_1$ fa címkéi az $\{1, 2, \ldots, n\} \setminus \{l_1\}$ halmaz elemei. Tehát a másodiknak törölt levél l_2 címkéje nem más, mint ennek a halmaznak a legkisebb olyan eleme, ami nem szerepel a $F - w_1$ Prüfer kódját meghatározó $c_2, c_3, \ldots, c_{n-2}$ címkék között. Mivel a törölt levél címkéje most sem lehetett n, ezért itt is a legkisebb olyan címkét kell venni, ami nem szerepel az $l_1, c_2, c_3, \ldots, c_{n-1}$ elemek között. Az eddigi gondolatmenetet alkalmazva, ha már meghatároztuk a törölt levelek $l_1, l_2, \ldots, l_i$ címkéit, akkor az l_{i+1} címke nem más, mint az aktuális fa Prüfer-kódjában nem szereplő címkék legkisebbike, azaz a legkisebb olyan pozitív egész, ami nincs a $l_1, l_{,} \ldots, l_i, c_{i+1}, c_{i+2}, \ldots, c_{n-1}$ halmazban.

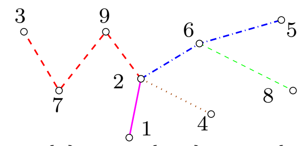
A fentiek szerint minden egyes l_i címke egyértelműen adódik, ezért bebizonyítottuk, hogy ha egy sorozat egy F fa Prüfer kódja, akkor a sorozat F-t meghatározza, más szóval különböző fákhoz különböző $P(F)$ kód tartozik.

A (2) bizonyításához azt kellene belátnunk, hogy tetszőleges ismétléses variációból kiindulva a fenti eljárással kapott G gráf egyrészt fa lesz, másrészt G Prüfer-kódja azonos lesz a kiindulási sorozattal. Ezzel itt nem kínlódunk. □

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

A Cayley tételre megadunk egy nemsztenderd, alternatív bizonyítást is. Előnye, hogy 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.

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



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

Ha $P_i = (v_{a(1)}, v_{a(2)}, \ldots, v_{a(k)}, v_i)$ egy felbontásbeli út, akkor legyen P_i *kódja* $a(1), a(2), \ldots, a(k)$. (Ha tehát a $P_i = (v_i)$ út egypontú, akkor a kódja üres.) Legyen az F fa *Refürp-kódja* az F felbontásában szereplő $P_2, P_3, \ldots, P_n$ irányított utak kódjainak egymásutánja. Világos, hogy ha F egy fa a $v_1, v_2, \ldots, v_n$ pontokon, akkor egyértelműen létezik Refürp-kódja. E Refürp-kód ráadásul $n-1$ 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 $1 = r(1), r(2), r(3), \ldots, r(n-1)$ egy olyan számsorozat, amiben minden $r(i)$ egy 1 és n közti egész, akkor egyértelműen létezik egy olyan F fa, aminek Refürp-kódja $r(1), r(2), r(3), \ldots, r(n-1)$. A cél tehát nem más, mint az $r(1), r(2), \ldots, r(n-1)$ számsorozatot felbontani $n-1$ sorozat egymásutánjára (ezek némelyike üres lesz), úgy, hogy e sorozatok rendre a $P_2, P_3, \ldots, P_n$ utak kódjai legyenek. Az első kérdés tehát, hogy az $r(1), r(2), \ldots, r(n-1)$ 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[4]. A P_3 út kétféle lehet: kiindulópontja vagy v_2, vagy a P_2 útnak egy v_2-től 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 amire $r(i+1)$ 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 $l \leq k$ 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 $P_2, P_3, \ldots P_{i+1}$ utak valamelyikének kódjában már szerepelt korábban. Ezért $s+1$ olyan szám, amire

$$s > k \qquad \text{és} \qquad r(s+1) \in \{2, 3, \ldots, i+1\} \cup \{r(1), r(2), \ldots, r(s)\} \tag{3.1}$$

[4]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.

teljesül. Világos, hogy ha $s+1$-re (3.1) fennáll, akkor $r(s+1)$ nem lehet benne P_{i+1} kódjában, tehát $s+1$ a legkisebb olyan szám, ami teljesíti az (3.1) feltételt. Ezzel pedig egyértelműen meghatároztuk P_{i+1} kódját: $r(k+1), r(k+2), \dots, r(s)$.

Ha pedig ismerjük a $P_2, P_3, \dots, P_n$ 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 $v_2, v_3, \dots, v_n$ 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 $r(1), r(2), r(3), \dots, r(n-1)$.

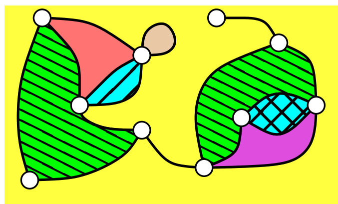
Megjegyzés: A Refürp-kódból a fa rekonstrukciója valójában még egyszerűbb. Legyen $r(1), r(2), \dots, r(n-1)$ egy Refürp-kód. A rekonstrukció $n-1$ lépésben történik: az i-dik lépésben $v_{r(i)}$-ből indítunk egy e_i élt. Az e_i él másik végpontja $v_{r(i+1)}$ lesz, ha $i+1 \le n-1$ és $v_{r(i+1)}$ nem 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.)

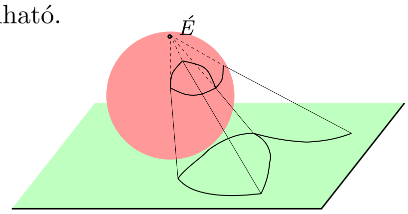
3.2.3 Síkgráfok

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.



Megjegyzés: Könnyen látható, hogy bármely fa síkbarajzolható: tetszőlegesen felvéve a diagram csúcsait a síkon, láttuk, hogy ha egyenként behúzzuk a fa éleit, akkor mivel sosem hozunk létre kört, a síknak egyetlen tartománya lesz, tehát egy új él behúzásakor a két végpont ugyanazon a tartományon van, ezért lehetséges közéjük egy, a korábban behúzott éleket nem metsző élt berajzolni.

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. $\square$

Köv.: Tetszőleges konvex poliéder élhálója síkbarajzolható.

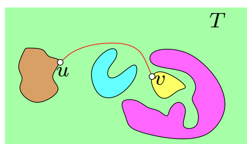
Biz.: Vetítsük az élhálót a poliéder egy belső P pontjából egy P közepű gömbre. Ezáltal az élháló gráfja gömbre rajzolható, azaz síkbarajzolható.

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 síkbarajzolt gráf csúcsainak, tartományainak, éleinek és komponenseinek száma rendre n, t, e és k, akkor $n+t = e+k+1$.

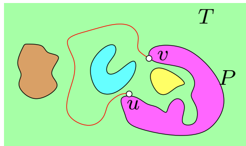
Biz.: Élszám szerinti indukcióval bizonyítjuk, hogy ha G egy n-csúcsú, e-élű síkbarajzolható gráf, akkor igaz rá az állítás. Ha a G_0 gráf élszáma $e_0 = 0$, akkor komponenseinek száma $k_0 = n$ (hisz minden csúcs önálló komponens) és a létrejövő síktartományok száma $t_0 = 1$, tehát igaz az állítás. 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 komponenseiben 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 között egy P út. Erről a P útról az is feltehető, hogy annak a T tartománynak a határán halad, amelyikbe behúzni készülünk az uv élt. 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.



Világos, hogy G_i minden T-től különböző tartománya tartománya marad G_{i+1}-nek is, továbbá a T tartomány két olyan tartományra esik szét, amik az uv él mentén határosak. (Az egyik ilyen tartományt az uv él és a P út alkotta kör fogja határolni. Azt kaptuk tehát, hogy $t_{i+1} = t_i + 1$ ezért $n + t_{i+1} = n + t_i + 1 = e_i + k_i + 1 + 1 = i + 1 + k_{i+1} + 1 = e_{i+1} + k_{i+1} + 1$. Ezzel igazoltuk az indukciós lépést, a tételt tehát beláttuk. $\square$

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

Biz.: Ha G öf, akkor $k = 1$, tehát az előző tétel szerint $n + t = e + k + 1 = e + 1 + 1 = e + 2$. $\square$

Köv.: Ha G sr, akkor bármely síkbarajzolásának ugyanannyi tartománya van. $\square$

Köv.: Ha G egyszerű, legalább 3-pontú, sr gráf, akkor $e \leq 3n - 6$. Ha mindezen túl G minden lapját legalább 4 él határolja, akkor $e \leq 2n - 4$.

Biz.: Feltehető, hogy G-be nem lehet további éleket behúzni a sr és egyszerű tulajdonságok megtartásával. Ekkor G minden lapját (a külsőt is beleértve) 3 él határolja, hisz ha volna egy ennél több csúcsot tartalmazó lap, akkor azon egy újabb élt rajzolhatnánk. Világos, hogy G öf, hiszen ha nem az lenne, további éleket tudnánk behúzni. Teljesül tehát, hogy $3t = 2e$, hisz a lapok mentén megszámolva az éleket minden élt éppen kétszer számolunk le. Az öf tulajdonság miatt az Euler-formula is igaz, tehát $e = n + t - 2$, azaz $3e = 3n + 3t - 6 = 3n + 2e - 6$, ahonnan $e = 3n - 6$.

Azt kaptuk, hogy ha G egy olyan egyszerű sr gráf, amibe újabb él nem húzható be az egyszerűség és sr tulajdonság megtartásával, akkor $e = 3n - 6$. A következmény első része innen azonnal adódik.

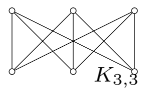
A második részhez feltehető, hogy G öf, hisz két komponens közé (a sr-ság megtartásával) újabb élt behúzva nem kaphatunk háromszöglapot. Ezért $4t \leq 2e$, hisz a lapok mentén az éleket leszámolva minden élt kétszer számolunk meg, és minden lapot legalább 4 él határol. Mivel G öf, ismét használhatjuk az Euler-formulát: $e = n + t - 2$, azaz $2e = 2n + 2t - 4 \leq 2n + e - 4$, és az állítás közvetlenül adódik. $\square$

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

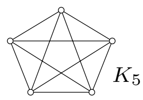
Köv.: Ha G sr és egyszerű, akkor van legfeljebb 5-ödfokú csúcsa, azaz $\delta(G) \leq 5$.

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. $\square$

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



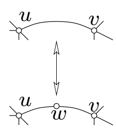
Biz.: Indirekt. K_5-re: $n = 5, e = 10 \Rightarrow t = 7 \Rightarrow 21 = 3t \leq 2e = 20$, ellentmondás. $K_{3,3}$-ra: $n = 6, e = 9 \Rightarrow t = 5$. Mivel $K_{3,3}$ C_3-mentes, ezért minden tartományt legalább 4 él határol: $20 = 4t \leq 2e = 18$, ellentmondás. $\square$



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. Ha H sr és K topologikusan izomorf H-val, akkor K is sr. Így $K = K_5$ ill. $K = K_{3,3}$ nem lehetséges ha G sr volt. Az elégségesség nem triviális, itt nem bizonyítjuk. $\square$

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

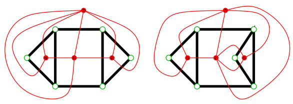
„**Biz.:** ” (Vázlat) A síkbarajzolhatóság megtartásával új éleket behúzva feltehető, hogy G-nek maximálisan sok $(3n-6)$ éle van, így tetszőleges síkbarajzoláskor G minden lapját három él határolja. Rajzoljuk le G-t a síkba úgy, hogy az éleknek megfelelő görbék töröttvonalak legyenek. Vegyünk fel a 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, rögzítsük az A, B és C csúcsok helyzetét, 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.) □

3.2.4 Síkgráfok dualitása



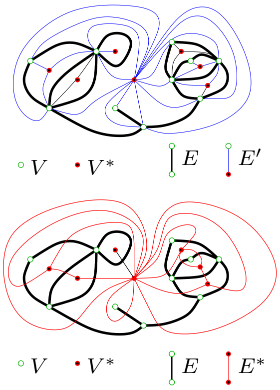
Különböző síkbarajzolásokhoz különböző duális tartozik. (Egyszer van 6-odfokú csúcs, másszor nincs.)

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 $Q \subseteq E(G)$ 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. A G gráf e és e' élei *soros élek*, ha $\{e, e'\}$ vágás.

Tétel: Legyen $G = (V, E)$ sr. (1) Ha G^* a G duálisa, akkor G^* sr és öf.
(2) $\varphi(e) := e^*$ egy $\varphi : E(G) \to E(G^*)$ természetes bijekciót definiál.
(3) G lapjai bijektíven G^* pontjainak felelnek meg.
(4) Ha G öf, akkor G a G^* duálisa, így ekkor G pontjai bijektíven G^* lapjainak felelnek meg.
(5) $e \in E(G)$ a G hurokéle (elvágó éle) $\iff$ $\varphi(e)$ a G^* elvágó éle (hurokéle).
(6) $e, e' \in E(G)$ párhuzamos (soros) élek $\iff$ $\varphi(e), \varphi(e')$ soros (párhuzamos) élek.
(7) $C \subseteq E(G)$ a G köre (vágása) $\iff$ $\varphi(C)$ G^* vágása (köre).
(8) Ha G öf, akkor $F \subseteq E(G)$ a G feszítőfája $\iff$ $\varphi(F)$ 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 $V^* := \{v_l : l\ G \text{ lapja}\}$, 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 e' 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): A duális definíciójából világos.

(4) 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.

(5,6, 7) Elegendő (7)-t bizonyítani, (5,6) ebből következik. Ha C a G köre, akkor C lerajzolása 2 részre osztja a síkot. Ezért $\varphi(C)$ 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 $\varphi(C)$ 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 $\varphi(Q)$ (5) miatt hurokél, ami kör. Egyébként Q minden éle két *különböző* tartományt határol, így K_1-t legalább 2 tartomány határolja. A K_1 komponens körüljárása a határolótartományok egy ciklikus sorrendjét adja, és belátható, hogy ebben minden határoló tartomány pontosan egyszer szerepel. Ezért a $\varphi(Q)$ 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). $\square$

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.

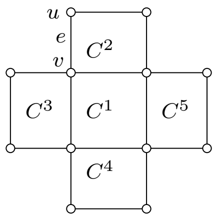
Def.: A G gráf a H gráf *absztrakt duálisa*, ha létezik egy $\varphi : E(G) \to E(H)$ bijekció úgy, hogy C a G köre $\iff$ $\varphi(C)$ a H vágása és Q a G vágása $\iff$ $\varphi(Q)$ a H köre.

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.

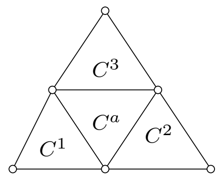
Whitney tétel: A G gráfnak pontosan akkor létezik absztrakt duálisa, ha G sr.

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 páronként $1-1$ 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. A kapott ellentmondás igazolja a Whitney tételt. $\square$



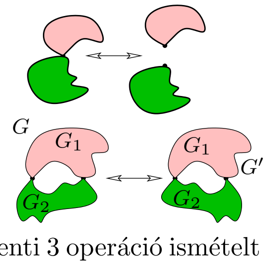
Korábban már láttunk példát arra, hogy egy öf, sr G gráfnak lehetnek nemizomorf G_1^*, G_2^* duálisai. A fenti, 8 pontból álló tétel persze az ilyen gráfokra is igaz, így G vágásai bijektíven G_1^* ill. G_2^* köreinek is megfelelnek. Tehát G_1^* és G_2^* élei között körtartó bijekció van. Ez motiválja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

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 ez eredetivel gyengén 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. $\square$

4. fejezet

Halmazelmélet

A modern matematika alapjának manapság a halmazelméletet és a matematikai logikát szokás tekinteni. Mi ebben a fejezetben a halmazelméletnek egy speciális részét villantjuk fel, mégpedig a számosságok elméletét. Nincs arra mód, hogy számottevő mélységben foglalkozzunk az elméletnek akár ezzel a szeletével, de a tárgyalás talán elegendő ahhoz, hogy megértsünk valamit e a rendkívül absztrakt és mély tudományágban szokásos gondolkodásmódból.

E fejezet célja a számfogalomnak a komplex számoktól különböző irányú általánosítása: a végtelennek mint számnak a kezelése. Most nem a természetes szám, egész szám, racionális szám, komplex szám vonalon próbáljuk bővíteni a számkört, hanem azt figyeljük meg, hogy a véges halmazok bármelyikéhez egyértelműen hozzárendelhető egy természetes szám: az adott halmaz elemszáma. Más szóval, ha két halmazhoz ugyanazt rendeltük, akkor ugyanannyi elemük van. De vajon miért csak a véges halmazokhoz tudunk így elemszámot rendelni? Miért ne próbálkozhatnánk meg a végtelen halmazok elemszámának meghatározásával is? Ezt tesszük az alábbiakban.

Def.: Tegyük fel, hogy az f függvény az A halmaz elemeihez a B halmaz elemeit rendeli. Az f függvény *injektív*, ha különböző elemekhez különböző elemeket rendel, azaz $x \neq y \Rightarrow f(x) \neq f(y)$ teljesül tetszőleges $x, y \in A$ esetén. Azt mondjuk, hogy f *szürjektív* (magyarul *ráképezés*), ha a B halmaz minden eleme előáll képként, vagyis $\forall b \in B \exists a \in A : f(a) = b$. Ha egy f függvény injektív és szürjektív, akkor f-t *bijekció*nak (magyarul *kölcsönösen egyértelmű leképezés*nek vagy *egy-egyértelmű leképezés*nek) mondjuk.

Ha f egy A és B közti bijekció, akkor f voltaképpen párokba rendezi A és B elemeit, így szemléletesen világos, hogy A-nak és B-nek ugyanannyi eleme van. Ha f injekció A-ból B-be, akkor B-nek nem feltétlenül áll elő minden eleme képként, tehát A-nak annyi eleme van, mint B egy részhalmazának, azaz B elemeinek száma legalább akkora, mint A-éié. Erről szól az alábbi definíció.

Def.: Azt mondjuk, hogy A *számossága azonos* B *számosságával* (jelölésben $|A| = |B|$), ha létezik A és B között bijekció. Ha létezik A-ból B-be injekció akkor A *számossága kisebb vagy egyenlő, mint* B*-é*, és ezt az $|A| \leq |B|$ jelölés írja le.

Cantor-Bernstein tétel:[1] Ha $|A| \leq |B|$ és $|B| \leq |A|$, akkor $|A| = |B|$.

Biz.: Feltehetjük, hogy az A és B halmazok diszjunktak. Legyenek $f : A \to B$ és $g : B \to A$ injekciók, amik a tétel feltételei szerint léteznek. Legyen $A \cup B$ a G (esetleg végtelen) gráf csúcshalmaza, és $a \in A$, $b \in B$ esetén legyen $ab \in E(G)$, ha $f(a) = b$ vagy ha $g(b) = a$. Világos, hogy a G gráf bármely csúcsából legfeljebb két él indul. Az A és B halmazok közötti φ bijekciót G minden egyes komponensén belül külön-külön definiáljuk. A G gráf komponensei ötfélék lehetnek:

(1) a, b egy komponens, ha $f(a) = b$ és $g(b) = a$. Legyen ekkor $\varphi(a) = b$.

(2) Komponens lehet az $a_1, b_1, a_2, b_2, \ldots, a_n, b_n$ kör, ahol tehát $b_n a_1$ is G éle. Definiáljuk ekkor a komponensen belül a φ leképezést a $\varphi(a_i) = b_i$-nek. Ezáltal φ bijekció a komponensen belül.

Ezzel a véges komponenseket elintéztük. Ha G egy komponense végtelen, akkor az egy végtelen út, ami vagy mindkét irányban végtelen, vagy csak az egyikben. Három eset van tehát:

(3) G egy komponense a $\ldots, a_{-2}, b_{-2}, a_{-1}, b_{-1}, a_0, b_0, a_1, b_1, a_2, b_2, \ldots$, mindkét irányban végtelen út. Ekkor a $\varphi(a_i) := b_i$ bijekció a komponensen belül.

(4) Ha G egy egyirányban végtelen út komponensének végpontja A-beli, azaz a komponens $a_1, b_1, a_2, b_2, \ldots$ alakú, és a $\varphi(a_i) := b_i$ ismét bijekció.

(5) Az az eset marad, amikor a komponens egy B-beli csúcsból induló végtelen út, azaz $b_1, a_1, b_2, a_2, \ldots$. Ekkor legyen $\varphi(a_i) = b_i$ ismét bijekciót ad a komponensen.

A fenti öt eset valamelyike G bármely komponensére ráhúzható, ezért a φ leképezést az A minden elemére definiáltuk, és az is világos, hogy B minden eleme pontosan egy A-beli elem képe lesz. Más szóval φ egy A és B közti bijekció, nekünk pedig pontosan egy ilyen függvény létezését kellett igazolnunk. □

A Cantor-Bernstein tétel ereje abban rejlik, hogy két halmaz számosságának egyenlőségét nem muszáj egy konkrét bijekció sokszor fáradságos megadásával igazolni. Elegendő mindössze két injekciót mutatni

[1] Ennek az időnként Schröder-Bernstein ill. Bernstein-Schröder néven emlegetett tételnek a története 1887-ben kezdődik, amikoris Richard Dedekind ezt bebizonyította magának. Akkortájt még lényegében nem létezett halmazelmélet, így szinte senkit sem érdekelt az eredmény. 1895-ben azonban a halmazelmélet másik nagy alakja, a Dedekinddel ekkor már haragban álló Georg Cantor ugyanezt sejtésként mondta ki. Ernst Schröder 1896-ban adott egy hibás bizonyítást, majd Felix Bernstein 1898-ban talált egy helyeset. A tétel számos elnevezése abban minden esetre közös, hogy a „Dedekind” karaktersorozat egyikben sem fordul elő.

a két kérdéses halmaz között.

Def.: Azt mondjuk, hogy A *számossága kisebb, mint* B *számossága* (jelölésben $|A| < |B|$), ha $|A| \leq |B|$ és $|A| \neq |B|$ (azaz ha $|A| = |B|$ nem teljesül).

Világos, hogy ha A és B két véges halmaz, akkor vagy ugyanannyi elemük van (azaz $|A| = |B|$), vagy az egyiknek több eleme van, mint a másiknak, más szóval az egyik halmaznak van a másik halmazzal egyező elemszámú részhalmaza (azaz $|A| < |B|$ vagy $|B| < |A|$). Nem világos azonban, hogy végtelen halmazokra is általánosítható-e ez a megfigyelés. Elképzelhető éppenséggel, hogy az A és a B „annyira végtelen" halmazok, hogy egyiket sem lehet a másikba injektálni. Nos, hogy ez csakugyan megtörténhet-e, az a halmazelmélet leginkább vitatott ú.n. *kiválasztási axiómáján* múlik. Ez az 1904-ben Ernst Zermelo által megfogalmazott axióma a következőt mondja ki:
Ha A egy halmaz, akkor létezik egy olyan f leképezés, amelyik az A halmaz nemüres részhalmazaihoz az A elemeit rendeli úgy, hogy tetszőleges $X \subseteq A$ esetén $f(X) \in X$ teljesüljön. Más szóval az A halmaz összes részhalmazából *szimultán* kiválasztható egy-egy elem.

Ha ezt az axiómát bevesszük a halmazelmélet szokásos axiómarendszerébe, akkor egy hihetetlenül hatékony eszközt kapunk. Ez az axióma ekvivalens az ú.n. *jólrendezési tétellel.* E tétel szerint minden halmaz jólrendezhető, azaz tetszőleges H halmaz elemeinek létezik olyan sorrendje, amely szerint H tetszőleges K részhalmazának van a sorban legkisebb eleme. A valós számok szokásos rendezése pl nem jólrendezés, mert a valós számok $\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\}$ részhalmazának nincs első (legkisebb) eleme. A kiválasztási axiómával ekvivalens a teljes indukció végtelen általánosításának, az ú.n. *transzfinit indukciónak* a létjogosultsága. Érdekes számunkra a kiválasztási axiómának az a következménye is, mely szerint tetszőleges vektortérnek létezik bázisa. (Végesen generált vektortérre ez világos, nem végesen generáltakra ez korántsincs így.) A számosságok összehasonlíthatósága kapcsán pedig azt érdemes megjegyezni, hogy a kiválasztási axióma ekvivalens a számosságok *trichotómiájával* is, ami pontosan azt mondja ki, hogy bármely két halmaz összehasonlítható, azaz létezik injekció valamelyikükből a másikba. Ha igaz a kiválasztási axióma, akkor tehát nem történhet olyasfajta csúfság, hogy két halmaz számossága ne volna összehasonlítható.

Felmerül tehát a kérdés: a kiválasztási axióma vajon igaz vagy sem. Ha a kiválasztási axiómát feltesszük, akkor igen erős tételek igazolhatók. Egy meglepő következmény például a Banach-Tarski paradoxon, mely szerint a háromdimenziós egységgömb szétdarabolható véges sok részre úgy, hogy a keletkező részekből (pontosabban azok eltoltjaiból és elforgatottjaiból) két (értelemszerűen tömör) egységgömb rakható össze (természetesen úgy, hogy minden darabot a két új gömb közül pontosan egyhez használunk fel). (Érdekes epizód a paradoxon történetéből a Scientific American 1989-es áprilisi száma Arlo Lipof levelével, mely egy közelebbről meg nem nevezett dél-amerikai ország szupertitkos akciójáról számol be: a Banach-Tarski tétel felhasználásával aranygömböket kettőznek. A kérdés persze csak az, hogy Arlo Lipof melyik angol kifejezés anagrammája.)

A kiválasztási axióma egy másik meglepő következménye az alábbi. Egy börtön összes rabjával közlik, hogy másnap reggel mindenkinek egy pozitív egész számot írnak a homlokára. Mindazokat, akik a többiek számainak ismeretében helyesen tippelik meg a saját számukat, szabadon engedik. Ekkor a rabok megállapodhatnak egy olyan „stratégiában", amivel elérhetik, hogy bármilyen számokat is kapnak másnap reggel, véges sok kivételtől eltekintve mindegyikük helyesen tippeljen. Más szóval, ha végtelen sok rab volt bezárva, akkor 100% fogja kitatlálni a saját számát.

Mi tehát a kiválasztási axióma státusza? Ha igaz, váratlan következményei vannak, ha nem igaz, akkor nincs pl. trichotómia. Kurt Gödel és Paul Cohen munkájának nyomán derült ki, hogy a kiválasztási axióma logikailag független a halmazelmélet szokásos Zermelo-Fraenkel féle axiómarendszerétől (röviden ZF-től), azaz sem a kiválasztási axióma, sem annak tagadása nem bizonyítható az említett axiómákból. Ezért akár a kiválasztási axiómát, akár annak tagadását vesszük hozzá a ZF-hez, pusztán ettől nem kapunk ellentmondást. Ha tehát a ZF ellentmondásmentes, akkor a kiválasztási axiómával együtt is az marad. Miután nem várható, hogy a kiválasztási axiómát bárki megcáfolná (hisz ez a ZF ellentmondásosságát jelentené), azért semmi hátrányunk sem származik abból, ha igaznak tekintjük. Így számos érdekes állítás eldönthetővé válik, amiket remekül be lehet bizonyítani.

Pontosan ugyanarról van itt is szó, mint amit a geometriában a párhuzamossági axiómának a „többi" axiómához való viszonya kapcsán feszegettek évszázadokon keresztül. Sokan és sokáig próbálkoztak eredménytelenül a párhuzamossági axióma bizonyításával a maradék axiómák segítségével (köztük Bolyai Farkas is), majd (az atyai tiltás ellenére ezzel foglalkozó) Bolyai János és az orosz Nyikolaj Lobacsevszkij egymástól függetlenül demonstrálták, hogy a párhuzamossági axióma tagadását feltéve egy éppoly mély és érdekes geometriát kapunk, mint amilyen a megszokott euklideszi. Később aztán szigorúan matematikai eszközökkel is sikerült igazolni, hogy a párhuzamossági axióma logikailag független a többi axiómától, és akár az axiómát, akár annak a tagadását vesszük hozzá a többihez, ez nem hoz ellentmondást a rendszerbe.

Def.: Az A halmaz *megszámlálható*, ha $|A| \leq |\mathbb{N}|$. Az $\mathbb{N}$ halmaz számosságát $\aleph_0$ (alef null) jelöli[2].

Állítás: Ha az A halmaz megszámlálható, akkor A véges, vagy A megszámlálhatóan végtelen halmaz, és ekkor $|A| = \aleph_0$.

Ha egy A halmaz megszámlálható, akkor létezik belőle az $\mathbb{N}$ halmazba injekció, vagyis A elemeinek különböző természetes számokat tudunk megfelelteni. Ezzel egyúttal sorba is rendezzük A elemeit: $A = \{a_1, a_2, \ldots\}$. Az is világos, hogy ha $A = \{a_i : i \in \mathbb{N}\}$, akkor A megszámlálható halmaz. Vagyis egy halmaz pontosan akkor megszámlálható, ha elemei felsorolhatók (sorba rendezhetők) úgy, hogy a felsorolásban mindegyik elem előbb-utóbb sorra kerüljön.

Köv.: A négyzetszámok halmaza vagy a prímszámok halmaza bár valódi részhalmaza a természetes számok halmazának, számosságuk mégis $\aleph_0$, azaz ugyanannyi van belőlük, mint a természetes számokból. Az egész számok $\mathbb{Z}$ halmaza tartalmazza $\mathbb{N}$-t, de számossága annak sem több $\aleph_0$-nál, hisz az egészek felsorolhatók: $0, 1, -1, 2, -2, 3, \ldots$ Ez utóbbi általánosítása következik.

Állítás: Ha A és B megszámlálható halmazok, akkor $A \cup B$ is megszámlálható.

[2]Az $\aleph$ (alef) a héber ABC első betűje. Követi a $\beth$ (bet), $\gimel$ (gimel), $\daleth$ (dalet), és 18 további betű. Ne nézzünk bután, hogy csak az alefet ismerjük.

Biz.: Tudjuk, hogy A és B elemei felsorolhatók, azaz $A = \{a_0, a_1, \ldots\}$ és $B = \{b_0, b_1, \ldots\}$. Ekkor $A \cup B = \{a_0, b_0, a_1, b_1, a_2, b_2, \ldots\}$, tehát $|A \cup B| \leq \aleph_0$. $\square$

Köv.: Véges sok megszámlálható halmaz uniója is megszámlálható.

Ennél azonban több is igaz.

Tétel: Megszámlálható sok megszámlálható halmaz uniója megszámlálható, azaz, ha $|A_i| \leq \aleph_0$ minden $i \in \mathbb{N}$ esetén, akkor $|\bigcup_{i\in\mathbb{N}} A_i| \leq \aleph_0$.

Biz.: Feltehetjük, hogy $A_i = \{a(i,0), a(i,1), a(i,2), \ldots\}$ az elemek egy sorbarendezése. Ekkor $\bigcup_{i\in\mathbb{N}} A_i = \{a(0,0), a(1,0), a(0,1), a(2,0), a(1,1), a(0,2), a(3,0), a(2,1), a(1,2), a(0,3), \ldots\}$, azaz először azokat az elemeket soroljuk fel, ahol az zárójelen belüli számok összege 0, majd azokat, ahol 1, majd 2, s.í.t. (Ezt gyakran úgy teszik szemléletessé, hogy az $a(i,j)$ elemet a koordinátarendszer pozitív síknegyedének (i,j) pontja reprezentálja, és a nemnegatív rácspontokat kell sorba rendeznünk, amit számos módszerrel meg tudunk tenni. Nincs most kedvem erről ábrát készíteni, remélem, világos.) Azt kaptuk, hogy $\bigcup_{i\in\mathbb{N}} A_i$ elemei sorba rendezhetők, ezért a halmaz megszámlálható. $\square$

Köv.: $|\mathbb{Q}| = \aleph_0$.

Biz.: Világos, hogy a $\mathbb{Q}$ halmaz előáll $\mathbb{Q} = \bigcup_{i=1}^{\infty} \mathbb{Q}_i$ alakban, ahol $\mathbb{Q}_i := \{\frac{n}{i} : n \in \mathbb{Z}\}$ az i nevezőjű törtek halmaza. Világos, hogy $|\mathbb{Q}_i| = |\mathbb{Z}| = \aleph_0$, ezért uniójuk ($\mathbb{Q}$) is megszámlálható. $\square$

Az órán a fenti tétel alábbi bizonyításával illusztráltuk a Cantor-Bernstein tétel alkalmazását.

2. bizonyítás: Mivel $\mathbb{N} \subseteq \mathbb{Q}$, ezért $\aleph_0 = |\mathbb{N}| \leq |\mathbb{Q}|$. Az egyenlőség bizonyításához azt kell megmutatnunk, hogy $|\mathbb{Q}| \leq |\mathbb{N}|$, azaz $\mathbb{Q}$ elemeihez különböző természetes számokat kell rendelnünk. Ezt az alábbiak szerint tehetjük meg. Tetszőleges $r \in \mathbb{Q}$ felírható $r = \frac{p}{q}$ alakban, ahol $0 < q \in \mathbb{N}$ és $(p,q) = 1$, azaz p és q relatív prímek. Legyen ekkor

$$f(r) = \begin{cases} 0 & \text{ha } p = 0, \\ 2^p \cdot 5^q & \text{ha } p > 0, \\ 3^{-p} \cdot 5^q & \text{ha } p < 0. \end{cases}$$

Világos, hogy minden racionális számhoz egyértelműen rendelünk természetes számot, és különböző racionálisak képe (a prímfelbontás egyértelműsége miatt) különböző lesz. $\square$

A következő célunk, hogy megszámlálhatónál nagyobb számosságú halmazt találjunk.

Def.: A H halmaz *hatványhalmazának* elemei a H halmaz részhalmazai: $\mathcal{P}(H) := \{X : X \subseteq H\}$.

Állítás: $|\mathcal{P}(\mathbb{N})| = |(0,1)|$, ahol $(0,1)$ a valós számegyenes 0 és 1 végű nyílt intervallumát jelöli.

Biz.: A Cantor-Bernstein tételt alkalmazzuk, azaz mindkét irányba megadunk egy-egy injekciót. Ha tehát $A \subseteq \mathbb{N}$ akkor legyen $f(A) := \sum_{a\in A} 10^{-(a+1)}$. Más szóval az A részhalmaznak az a szám fog megfelelni, amit úgy kapunk, hogy leírunk egy 0-t, és utána sorra 1-t vagy 0-t írunk a szerint, hogy az $\mathbb{N}$ soron következő eleme benne van-e az A halmazban. (Pl. ha A a prímszámok halmaza , akkor $f(A) = 0,00110101000101\ldots$-nak adódik.) Világos, hogy különböző részhalmazokhoz különbözőképpen felírt számok tartoznak, raádásul minden $f(A)$ pozitív és $0,2$-nél nem nagyobb lesz. f tehát injekció.

Legyen most $x \in (0,1)$ tetszőleges szám, melynek 2-es számrendszerbeli alakja $x = 0, x_1x_2\ldots$. Legyen $g(x) := \{n \in \mathbb{N} : x_n = 1\}$. Mivel különböző számok 2-es számrendszerbeli alakja különböző, ezért a g függvény is injekció. $\square$

Megjegyzés: A fenti bizonyításban a g függvény nem bijekció, ugyanis jópár olyan $A \subseteq \mathbb{N}$ halmaz van, ami nem áll elő $g(x)$ alakban. Konkrétan azok az A halmazok tartoznak ide, amikre létezik olyan N küszöb, hogy minen N-nél nagyobb szám A-ban van. Az ilyen halmaz az olyan 2-es számrendszerbeli alaknak felelne meg, amiben egy helyiértéktől kezdve csupa 1-esek állnak. Márpedig ilyen szám nincs, ahogyan 10-es számrendszerben sincs olyan szám, ami a tizedesvessző után valahonnantól csupa 9-esből áll.

Az f függvény konstrukciójakor is pontosan a fenti anomáliát igyekszünk elkerülni: 10-es számrendszerben nincs olyan szám, ami „tizedesvessző" után valahonnantól csupa 9-eseket tartalmaz. Persze ilyen számot nem is konstruáltunk.

Def.: A $\mathcal{P}(\mathbb{N})$ halmaz számosságát *kontinuum* számosságnak nevezzük, és (ritkábban) $\mathfrak{c}$-vel (gót „c"-vel) vagy (gyakrabban) $2^{\aleph_0}$-lal[3] jelöljük.

Létezik-e vajon nem megszámlálható halmaz? Az alábbi tétel szerint a válasz igen.

Tétel: $|\mathcal{P}(\mathbb{N})| > |\mathbb{N}|$, avagy $\mathfrak{c} > \aleph_0$.

Ennél azonban jóval több igaz.

Cantor tétele: Tetszőleges H halmazra $|\mathcal{P}(H)| > |H|$.

---

[3]Ez a jelölés összhangban van azzal, hogy egy n elemű halmaznak 2^n részhalmaza van.

Biz.: Az alábbi bizonyítás a híres *Cantor-féle átlós módszer*. Indirekt bizonyítunk, tegyük fel, hogy valamely H halmazra $|\mathcal{P}(H)| \not> |H|$, azaz a trichotómia miatt $|H| \geq |\mathcal{P}(H)|$. Mivel létezik H-ból $\mathcal{P}(H)$-ba injekció (H tetszőleges h elemének a $\{h\}$ részhalmazt feleltetjük meg), ezért $|H| \leq |\mathcal{P}(H)|$ teljesül. A Cantor-Bernstein tétel szerint ebből $|H| = |\mathcal{P}(H)|$ következik.

Létezik tehát egy $f : H \to \mathcal{P}(H)$ bijekció. Legyen $A := \{h \in H : h \notin f(h)\}$, vagyis azon H-beli elemek halmaza, amiket a nekik megfelelő részhalmaz nem tartalmaz. Világos, hogy A a H halmaz egy jól meghatározott részhalmaza, és így az f bijektív volta miatt létezik egy olyan $a \in H$ elem, amire $A = f(a)$. Két eset lehetséges. Az a elem vagy A-ban van, vagy nem.

Ha $a \in A$, akkor A definíciója miatt $a \notin f(a) = A$, ami ellentmondás. Ha pedig $a \notin A$, akkor a azért nem eleme az A halmaznak, mert $a \notin f(a)$ nem teljesül, tehát $a \in f(a) = A$, ami szintén nem lehetséges. Az ellentmondás az indirekt feltevés hamis voltát bizonyítja, ez pedig Cantor tételét igazolja. □

A Cantor tételnek egy következménye, hogy nem létezik a számosságok között legnagyobb, azaz minden halmaznál van nagyobb számosságú halmaz (például a hatványhalmaza). Innen adódik, hogy nem létezhet olyan halmaz sem, aminek minden halmaz eleme, hiszen ennél a halmaznál nem volna nagyobb számosságú halmaz. Ugyanennek a ténynek egy ravaszabb megfogalmazása a Russel paradoxon. Álljon az R halmaz mindazon halmazokból, amik nem tartalmazzák önmagukat elemként: $R := \{A : A \notin A\}$. Kérdés, hogy vajon R eleme-e R-nek. Ha igen, akkor $R \notin R$, ha nem, akkor pedig R definíciója szerint nem teljesül, hogy $R \notin R$, azaz $R \in R$. Ejnye.

Bertrand Russel a paradoxont 1901 körül vette észre (éppen a fenti Cantor tétel kapcsán), és a matematikusoknak jópár évnyi fejtörésébe került, míg sikerült tisztázni a látszólagos ellentmondást. Russel eredménye számos formában lett közismert. Ezek egyike a borbélyparadoxon: tegyük fel, hogy egy városban egyetlen borbély van, és igaz, hogy pontosan azokat a férfiakat borotválja ez a borbély, akik maguk nem borotválkoznak. Borotválkozik-e a borbély, vagy sem? (Nem az a megfejtés, ami a következő feladványé. Hazamegy a favágó, és így szól a fiához: „*Te az én fiam vagy, de én nem vagyok az apád.*”. Na, hogy lehet ez, ha a favágó igazat mond?)

A paradoxont a halmazelmélet axiomatikus megalapozása oldotta meg. Ahogyan a világ összes halmaza nem lehet egyetlen halmaz eleme, úgy a paradoxonban definiált halmazok osztálya (azaz R) sem alkot halmazt. A halmaz a matematikában alapfogalom, nem definiáljuk, de nem igaz az az intuitív kép, hogy minden, amiről beszélni tudunk, az egyúttal halmaz is.

Tétel: $|(0,1) \times (0,1)| = 2^{\aleph_0}$, azaz a nyílt egységnégyzetnek kontinuum sok pontja van. Más szóval kontinuum sok kontinuum méretű halmaz uniója is (csak) kontinuum számosságú.

Köv.: Megszámlálhatóan sok kontinuum méretű halmaz uniója kontinuum számosságú. Kontinuum és megszámlálható halmaz uniója kontinuum.

Biz.: Világos, hogy $|(0,1)| = |(0,1) \times \frac{1}{2}|$, és $(0,1) \times \frac{1}{2} \subseteq (0,1) \times (0,1)$, ezért $|(0,1)| \leq |(0,1) \times (0,1)|$. A Cantor-Bernstein tétel szerint tehát elegendő egy $f : (0,1) \times (0,1) \to (0,1)$ injekciót adni. Legyen tehát $(x,y) \in (0,1) \times (0,1)$ tetszőleges. Legyenek mondjuk $x = 0,x_1x_2x_3\ldots$ és $y = 0,y_1y_2y_3\ldots$ a tízes számrendszerbeli alakok. Legyen $f(x,y) := 0,x_1y_1x_2y_2\ldots$. Világos, hogy $f(x,y)$ egy jól meghatározott $(0,1)$-beli szám (hiszen nem lehet, hogy valahonnan kezdve csupa 9-est tartalmaz). Az is világos, hogy ha $f(x,y)$ adott, akkor abból x és y meghatározható, vagyis f injektív[4]. Nekünk pedig éppen erre van szükségünk. □

Köv.: Az $\mathbb{R}$ és $\mathbb{C}$ egyaránt kontinuum számosságú halmazok.

Biz.: $\mathbb{R}$ előáll megszámlálható sok $(0,1)$ intervallummal azonos számosságú halmaz egyesítéseként. $\mathbb{C}$-nek annyi pontja van, mint az $\mathbb{R}^2$ síknak, és $\mathbb{R}^2$ előáll kontinuum sok egyenes uniójaként. □

Igazán szuper, hogy a kontinuum több, mint megszámlálható, de vajon van-e olyan halmaz, aminek a számossága szigorúan e két számosság közé esik? A kérdés jogos és érdekes, Cantor vette fel először. Kerestek ilyen halmazt, de senki nem talált. Próbálták hát bebizonyítani, hogy nem létezhet ilyen, ám ez sem járt sikerrel. 1900-ban Párizsban a nemzetközi matematikai kongresszuson David Hilbert, az akkori idők egyik legbefolyásosabb matematikusa tartott előadást arról, hogy mik az akkori matematika előtt álló legfontosabb problémák. Itt 10 probémát ismertetett, később a lista 23-re bővült. Olyan problémák szerepeltek a listán, mint a mindmáig megoldatlan Riemann sejtés és Goldbach sejtés. Hilbert legelső problémája pedig éppen ez a kérdés volt. Azaz, igazoljuk az alábbiakat.

Kontinuum hipotézis: Nem létezik olyan H halmaz, amire $\aleph_0 < |H| < 2^{\aleph_0}$ teljesül.

A fenti állítás általánosan is megfogalmazható.

Általánosított kontinuum hipotézis: Ha X egy végtelen halmaz, akkor nem létezik olyan H halmaz, amire $|X| < |H| < |\mathcal{P}(X)|$ teljesül.

Igaz vagy sem a kontinuum hipotézis? Ha tudjuk, akkor miért nem tétel? Ha nem tudjuk, akkor miért nem sejtés? Nos, Kurt Gödel és Paul Cohen egy-egy eredménye együtt adja meg az egészen váratlan választ. Gödel azt igazolta, hogy a halmazelmélet szokásos axiómáiból (akár a kiválasztási axiómát is beleértve) nem lehet a kontinuum hipotézist cáfolni, így semmiképp sem várható, hogy valaki egy megszámlálható és kontinuum közötti halmazt konstruál. Cohen eredménye pedig azt mutatja, hogy a kontinuum hipotézis a szokásos axiómarendszerben nem bizonyítható. Ez azt jelenti, hogy a kontinuum hipotézis eldönthetetlen a halmazelméleten belül: akár a kontinuumhipotézist, akár annak cáfolatát (de csak az egyiket) felvesszük az axiómák közé, akkor ettől nem kerül ellentmondás a halmazelmélet axiómarendszerébe. Más szavakkal: a kontinuumhipotézis éppúgy logikailag független ZFC-től (azaz a kiválasztási axiómával kiegészített Zermelo-Fraenkel axiómarendszertől), mint ahogyan a kiválasztási axióma volt logikailag független a ZF-től vagy ahogyan a párhuzamossági axióma független a geometria maradék axiómáitól.

[4] Érdemes meggondolni, hogy f miért is nem bijekció. (Ha ugyanis az volna, nem lett volna szükség a Cantor-Bernstein tételre a bizonyításban)