A számítástudomány alapjai
A BME I. éves villamosmérnök-hallgatói számára

Fleiner Tamás

Tartalomjegyzék

Bevezető

Jelen tankönyv a BME-n villamosmérnök-hallgatóknak oktatott, „A számítástudomány alapjai" című (VISZA 105 fedőnevű) tárgyhoz tartozó jegyzet, de hasznosan forgathatják a Bevezetés a Számítástudományba (VISZA 103 és VISZA 110) előadást hallgató mérnök-informatikusok és a Kombinatorika és Gráfelmélet (VIMA 0173 és VIMA 0175) tárgy matematikus hallgatói is. A feldolgozott anyag nagyrészt lefedi a tanórákon leadott (és számonkéréseken elvárt) ismereteket, helyenként túl is mutat az előadáson elhangzottakon, így olyan részeket is tartalmaz, amelyek ismeretét nem követeljük meg a vizsgán. Mivel a villamosmérnök tananyag éppen átalakulóban van, ezért bizonyos témakörök egyelőre hiányoznak, ám ahogyan a változások előrehaladnak, úgy kerülnek azok is kidolgozásra.

A vizsgára történő felkészítésen túl a jegyzetnek célja egyúttal az diszkrét matematikára fogékony hallgatók érdeklődésének felkeltése is. Az egy-egy témakör iránt komolyabban érdeklődő olvasókat célozzák azok a megjegyzések, amelyek mélyebb összefüggésekre mutatnak rá. Ne felejtsük el azonban, hogy ezek csupán a kiegészítő ismeretek: ahhoz, hogy egy adott anyagrészben valaki ténylegesen elmélyülhessen, a valódi szakirodalmat (is) érdemes tanulmányoznia. A jegyzet összeállításakor az is cél volt, hogy ne legyen túl száraz az anyag. A jegyzet ezért tartalmaz a tananyagot kiegészítő, ill. ahhoz kapcsolódó, érdekesnek ítélt információmorzsákat is. Az így (pl. **Megjegyzés** vagy **Történelem** címszavak után, vagy apró betűvel szedetten) közölt ismereteket a (BME) vizsgán tehát nem követeljük meg: az az általános irányelv, hogy az ilyen részeket még a jeles osztályzatért sem kötelező ismerni. Talán nem túl kockázatos azt kijelenteni, hogy a fennmaradó részek beható ismerete elegendő az adott témakörben a jeles osztályzathoz. A spektrum másik végének elérésére 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, hogy nem érti, miről beszél. Más szóval: a legalább elégséges osztályzatnak feltétele a törzsanyaghoz tartozó fogalmak, állítások pontos ismerete, vagyis az, 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 egyetlen egyet sem kell tudnia. Azonban aki ennek alap-

ján 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 (értsük: elengedhetetlen), hogy egyetlen témakörben se lehessen zavarba hozni a vizsgázót, mint egy-egy bizonyítás részletes ismerete. Akinek „sajnos" nem jut ideje a ferdetest obskurus definícióját megtanulni, de hatosra tudja a Menger tételt, az éppúgy megbukik, mint az, aki semmit sem tud a prímszám 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. Az az irányelv, hogy zh-k által le nem fedett anyagrészből minden vizsgázó kap kérdést. A vizsgáztató személye a helyszínen dől el, az esetek többségében valamelyik előadó vagy gyakorlatvezető előtt kell számot adni a tudásról.

Hogyan is jött létre a jelen jegyzet? A munka még 2004 tavaszán kezdődött egy segédlet megírásával, azóta hízik az anyag. Félév végén az előadáson elhangzottaknak megfelelően igyekeztem igazítani a tartalmon, és próbáltam folyamatosan gyomlálni a jelentős számban felbukkanó hibákat is. (Volt, van, lesz is belőlük bőven.) Ebben a harcban múlhatatlan érdemeket szereztek azok a hallgatók (és kollégák, különösen Tóth Géza, az anyag szakmai lektora), akik jelezték, ha elírást vagy hibát találtak. Munkájukat ezúton is köszönöm: ennek révén jegyzet használhatósága jelentősen javult és reményeim szerint számos későbbi hallgató felkészülése válik könnyebbé. Ebből a munkából természetesen én is kiveszem a részemet: minden átdolgozáskor újabb elírásokat és tévedéseket illesztek az anyagba az egyensúly megőrzése érdekében. Álljon azért itt egy névsor azokról, akik megjegyzéseikkel, javaslataikkal érdemben részt vettek a jegyzet javításában:

Baranyai Balázs, Benei Viktor, Bui Duy Hai, Csöndes László, Erdős Csanád, Fleiner Balázs, Hidasi Péter, Joó Ádám, Keresztes László, Ketipisz Vangelisz, Kovács Ákos, Molnár Gergely, Mucsi Dénes, Nagy Gábor, Nagy-Győr Ádám, Pereszlényi Attila, Pintér Olivér, Rádi Attila, Simon Károly, Simon Tamás, Sweidan Omar, Szabó Andor, Szabó Bálint, Szárnyas Gábor, Szebedy Bence, Szedelényi János, Szelei Tamás, Tarnay Kálmán, Tauber Ádám, Tóth Zoltán, Vandra Ákos, Varga Dániel, Varga Judit, Velinszky László, Virág Dániel, Viszkei György, Vőneki Balazs, Wiener Gábor, WolframAlpha, Zsolnay Károly.

Valószínűleg minden erőfeszítés ellenére is számos hiba maradt a most közreadott jegyzetben. Természetesen minden ilyen hiányosságért egyedül az enyém a felelősség.

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.

Minden olvasónak sikeres felkészülést és eredményes vizsgázást kívánok.

Budapest, 2013. június 30.

Fleiner Tamás

A Számítástudomány Alapjai vizsgatematika a 2012/2013-as tanévben

1. Leszámlálási alapfogalmak: permutációk, variációk és kombinációk (ismétlés nélkül és ismétléssel); binomiális együtthatók közti egyszerű összefüggések, a binomiális tétel, skatulya-elv, szita-formula.

2. Alapvető adatstruktúrák: tömb, láncolt lista, bináris fa. Lineáris és bináris keresés, ezek lépésszáma, minimumkeresés, beszúrási feladat, rendezési feladat. Buborék-, kiválasztásos, beszúrásos, összefésüléses és gyorsrendezés, alsó korlát, lépésszám-becslések.

3. Ládarendezés, bináris keresőfák. Keresés, beszúrás, törlés, minimumkiválasztás, pre-, in- és posztorder bináris keresőfában, rendezés bináris keresőfával. Kupac, kupacos rendezés.

4. Gráfelméleti alapfogalmak: pont, él, fokszám, szomszédossági mátrix, szomszédossági lista, éllista. Egyszerű gráf, részgráf, feszített részgráf, izomorfia, élsorozat, séta, út, kör, összefüggő gráf, komponens. Gráfok fokszámösszege, fák egyszerűbb tulajdonságai.

5. Cayley tétele fák számáról, Prüfer kód. Minimális költségű feszítőfa, Kruskal algoritmus, normál fák.

6. Euler-séta és körséta, létezésének szükséges és elégséges feltétele. Hamilton-kör és út; szükséges, illetve elégséges feltételek Hamilton-kör létezésére: Dirac és Ore tételei.

7. Legrövidebb utakat kereső algoritmusok (BFS, Dijkstra, Ford, Floyd). Legszélesebb utak irányított és irányítatlan gráfban.

8. Hálózati folyamok: hálózat, folyam, folyamnagyság (folyamérték), *st*-vágás, vágás kapacitása. Ford-Fulkerson tétel, javító utas algoritmus. Egészértékűségi lemma, Edmonds-Karp tétel (biz. nélkül).

9. Többtermelős, többfogyasztós hálózatok, csúcskapacitások és irányítatlan élek kezelése. Él- és pontidegen utak. Menger négy tétele, gráfok többszörös összefüggősége, kapcsolata a Menger tételekkel.

10. Páros gráfok, ekvivalens definíció. Párosítások, Hall, Frobenius és Kőnig tételei, alternáló utas algoritmus maximális párosítás keresésére. Lefogó és független csúcsok ill. élek, Gallai két tétele. Tutte tétele párosításokról (csak a triviális irányban bizonyítva).

11. Pont- és élszínezés, kromatikus szám, klikkszám, alsó és felső korlátok a kromatikus és élkromatikus számra, Brooks tétel (biz. nélkül), Myczielski-konstrukció, Vizing tétel (biz. nélkül).

12. Síkbarajzolhatóság, gömbre rajzolhatóság. Az Euler-féle poliédertétel és következményei: egyszerű, síkbarajzolható gráfok élszáma és minimális fokszáma. Kuratowski gráfok, Kuratowski tétele (csak könnyű irányban biz.), Fáry-Wagner tétel (biz. nélkül).

13. Dualitás, tulajdonságai. Elvágó él, soros élek, vágás. Gyenge izomorfia, absztrakt dualitás, Whitney három tétele (biz. nélkül), síkgráfok kromatikus száma, ötszíntétel.

14. Mélységi keresés és alkalmazásai (élek osztályozása, irányított kör létezésének eldöntése), alapkörrendszer, alap vágásrendszer. Aciklikus irányított gráfok jellemzése, topologikus sorrend, PERT-módszer, kritikus utak és tevékenységek.

15. Algoritmusok bonyolultsága, döntési problémák. $P, NP, co-NP$ bonyolultsági osztályok fogalma, feltételezett viszonyuk, polinomiális visszavezethetőség, NP-teljesség, Cook-Levin tétel (biz. nélkül), nevezetes NP-teljes problémák: SAT, HAM, 3-SZÍN, k-SZÍN, MAXFTN, MAXKLIKK, HAMÚT.

16. Oszthatóság, legnagyobb közös osztó, legkisebb közös többszörös, euklideszi algoritmus, prímek és felbonthatatlan számok, a számelmélet alaptétele, osztók száma, nevezetes tételek prímszámokról: prímek száma, prímek közti hézag mérete és a prímszámtétel (biz. nélkül).

17. Kongruencia fogalma, műveletek kongruenciákkal. Teljes és redukált maradékrendszer, az Euler-féle φ-függvény, Euler-Fermat tétel és kis Fermat tétel. Lineáris kongruenciák megoldhatósága és megoldása. Lineáris diofantikus egyenletek megoldása.

18. 2-változós művelet, félcsoport, csoport, példák számokon és nem számokon. Csoport rendje, csoportok izomorfiája, részcsoport, generált részcsoport, elem rendje, ciklikus csoport, diédercsoport.

19. Mellékosztály, Lagrange tétele, elem rendjére vonatkozó következménye. Gyűrűk. 0, 1, ellentett fogalma, 0-val szorzás gyűrűben. Kommutatív, egységelemesgyűrű.Példák gyűrűkre számokon és polinomokkal. Ferdetest, test fogalma, példák számokon, polinomok hányadosteste. Polinomok maradékos osztása példán szemléltetve.

20. Számelméleti algoritmusok: alapműveletek, (modulo m) hatványozás és az euklideszi algoritmus. Prímtesztelés. Nyilvános kulcsú titkosírások, digitális aláírás. Az RSA titkosítási módszer.

1. fejezet

Alapismeretek

1.1. Komplex számok

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

Az eddigi számfogalmakban közös tehát, hogy mindegyik alkalmas arra, hogy *megmérjen* valamit, azaz a számokon van egy *természetes rendezés*, melynek segítségével bármely két, különböző számról egyértelműen el lehet dönteni, melyik a nagyobb. A számfogalmak bevezetésére alkalmas motiváció, hogy mérhető dolgokat tudjak megmérni. A számokon értelmezett műveletek (összeadás, kivonás, szorzás, osztás, hatványozás, gyökvonás, logaritmus, szögfüggvények, stb) mindegyikéről elmondható, hogy arra 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. (Természetesen a komplex számoknak is tulajdonítható valamiféle „jelentés", azonban erre ebben a jegyzetben nem áll módunk részletesen kitérni.) A motiváció itt sokkal inkább az, hogy bizonyos műveletek nem voltak elvégezhetők a valós számokon, és valamilyen rejtélyes okból szeretnénk pl. a $\sqrt{-1}$-nek értelmet tulajdonítani.

Lássuk mindezt a gyakorlatban!

1.1. Definíció *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 $\overline{z} := a - bi$.

1.2. 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.*

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

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

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

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

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

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

Bizonyítás. 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. □

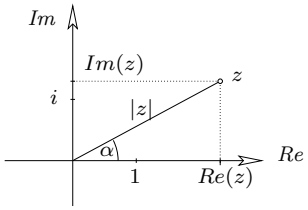
Láttuk, hogy a komplex számok egyértelműen jellemezhetők két valós „koordinátával", akárcsak a síkbeli koordinátarendszer pontjai. Természetesen adódik tehát egy kölcsönösen egyértelmű megfeleltetés a komplex számok és a (koordinátarendszerrel ellátott) sík pontjai között: a $z = a + bi$ komplex számnak 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.

1.4. 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 $|z + w| \leq |z| + |w|$.



Bizonyítás. (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 origó, 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.

1.5. 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.*

Bizonyítás. $zw = |z|(\cos\alpha + i\sin\alpha)|w|(\cos\beta + i\sin\beta) = |z||w|(\cos\alpha\cos\beta - \sin\alpha\sin\beta + i(\cos\alpha\sin\beta + \sin\alpha\cos\beta)) = |z||w|(\cos(\alpha+\beta) + i\sin(\alpha+\beta))$ 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 találhatók.

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

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

1.6. 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.

Bizonyítás. (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.

1.7. 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*

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

Bizonyítás. 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 rendezhetők. 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 állíthatók, 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 alkot, ami annyiban „ jobb" a valós számtestnél, hogy ebben minden polinomnak van gyöke, más szóval, hogy algebrailag zárt. (Testekről később lesz szó.) Erről szól az algebra alaptétele:

1.8. 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.*□

Az 1.8. Tétel következménye, hogy ha $p(x)$ valós együtthatós, akkor találunk egy α gyökét, ami vagy valós (és kiemelhetjük az $(x-\alpha)$ 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.

1.2. Kombinatorika

1.2.1. Elemi leszámlálások

1.9. Definíció *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.*

1.10. 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.

1.11. Definíció *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.

1.12. Definíció *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.*

1.13. 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 $V_{ism}(n,k) = n^k$.

1.14. Definíció *Legyen $n \in \mathbb{N}$. Ekkor n elem egy* permutációja *az n db, egymástól megkülönböztethető elem egy sorbarendezését jelenti. Formálisan az $\{1,2,\ldots,n\}$ elemek egy permutációján egy $\sigma : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ bijekciót (azaz kölcsönösen egyértelmű megfeleltetést értünk.*

1.15. Megjegyzés *Egy permutációt tehát megadhatunk úgy is, mint a σ leképezést, tehát 5 elemnek egy konkrét permutációja az a σ, amire $\sigma(1) = 3, \sigma(2) = 4, \sigma 3 = 5, \sigma(4) = 2, \sigma(5) = 1$ és $\sigma(6) = 6$. Ugyanezt a permutációt megadhatjuk egy táblázattal, amiben oszloponként tüntetjük fel hogy melyik elemet hova viszi a függvény:*
$\begin{array}{|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 3 & 4 & 5 & 2 & 1 & 6 \\ \hline \end{array}$*, de σ megadható úgy is, hogy megkeressük a ciklusait, azaz megvizsgáljuk, hogy egy elemet hova vihet el az iterált leképezés, és az így kapott ciklusokat zárójelek közé téve írjuk fel (az egy hosszú ciklusokat (azaz fix pontotkat) nem szokás kiírni): $\sigma = (1,3,5)(2,4)(6) = (1,3,5)(2,4)$. Később hasznos lesz, ha egy permutációra többféleképp tudunk gondolni.*

1.16. 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 $\frac{n!}{0!} = n!$.

1.17. Definíció *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.*

1.18. Példa *Ha tudjuk, hogy egy héten minden nap öt óránk van az általános iskolában, és ismerjük az egyes tárgyak heti óraszámait (legyenek ezek $k_1, k_2, \ldots, k_l$, amelyekre 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.)*

1.19. 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.

1.20. 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.

1.21. Definíció *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.*

1.22. Példa *Kézenfekvő példa a lottóhúzások lehetséges kimeneteleinek száma:* 90 *lehetséges számból az* 5 *nyerőszámot $C(90, 5)$-féleképp lehet kiválasztani, 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 $C(n, k) = \frac{V(n,k)}{k!} = \frac{n!}{(n-k)! \cdot k!}$.

1.23. 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, ráadásul 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 $k_2 = n - k$.*

1.24. Definíció *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. Ha* $k > n$, *akkor az* $\binom{n}{k}$ *binomiális együtthatót* 0*-nak definiáljuk.*

1.25. 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.*
4. Az előző megfigyelés általánosítása, hogy $\sum_{k=0}^{\infty}\binom{r}{k}\binom{s}{n-k} = \binom{r+s}{n}$*, hisz ha az* $r+s$ *elemet egy r és egy s méretű részre osztjuk, akkor n-t ebből úgy választunk ki, hogy valamilyen k-ra az s-ből választunk k-t és az r-ből pedig* $(n-k)$*-t.*

1.26. Definíció *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 megfeleltethetők 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* $C_{ism}(n,k)$.

1.27. 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.*

1.28. Tétel $C_{ism}(n,k) = \binom{n+k-1}{k}$

Bizonyítás. 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 $C_{ism}(n,k) = \binom{n+k-1}{k}$. □

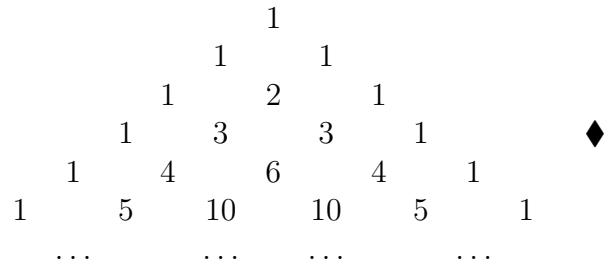
A binomiális együtthatókkal kapcsolatos a binomiális tétel.

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

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

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

Megjegyzés: 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 találhatók 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.



1.2.2. A szita-formula és a skatulya-elv

Elemi leszámlálási feladatokban sokszor nagyon hasznos a szita-formula.

1.31. Tétel (A szita-formula) *Ha $A_1, A_2, \ldots, A_n$ véges halmazok, akkor*

$$\left| \bigcup_{i\in\{1,2,\ldots,n\}} A_i \right| = \sum_{\emptyset\neq I\subseteq\{1,2,\ldots n\}} (-1)^{|I|+1} \cdot \left| \bigcap_{i\in I} A_i \right| \tag{1.1}$$

Szavakban: az unió elemszámát úgy kapjuk, hogy A_i halmazok elemszámainak összegéből levonjuk a páronkénti metszetek elemszámait, ehhez hozzáadjuk a hármas metszetek elemszámait, levonjuk a 4-es metszetek méretét, sít. A sztenderd példa, hogy 1 és 1000 között hány olyan szám van, ami a 30-hoz nem relatív prím. Mivel egy szám pontosan akkor nem relatív prím a 30-hoz, ha a $2, 3$ vagy 5 prímek valamelyikével osztható, ezért az 1 és 1000 közötti számok közül a 2-vel, 3-mal ill. 5-tel oszthatók számok halmazának uniójának elemszámát kell meghatároznunk. Ha vesszük a az 500 páros, 333 db 3-mal osztható és 200 db 5-tel osztható számot, akkor minden olyan számot kétszer számoltunk meg, ami két prímmel is osztható a $2, 3, 5$ közül. Ha tehát levonjuk a 166 db 6-tal, 100 db 10-zel ill. 66 db 15-tel osztható számot, akkor egyedül a 33 db 30-cal osztható számmal van csak baj, amelyeket 3-szor számoltunk meg és 3-szor vontunk le, tehát ezeket meg hozzá kell adni a végeredményhez, ami ilyenformán $(500 + 333 + 200 - 166 - 100 - 66 + 33)$-nak adódik. Ha azonban megértjük rendesen miről van szó, akkor a szita-formula bizonyítása bár absztrakt, de jóval rövidebb.

A szita-formula bizonyítása. Tekintsük az $A_1 \cup A_2 \cup \ldots \cup A_n$ halmazt, és legyen x ennek egy tetszőleges eleme. A szita-formula igazolásához mindössze azt kell megmutatnunk, hogy x hozzájárulása ugyanannyi az 1.1 formula baloldalához, mint a jobboldalhoz. A baloldal egyszerű: x-et pontosan egyszer számoltuk meg. Azt kell tehát igazolnunk, hogy x-et a jobboldalon összességében egyszer vesszük figyelembe. Tegyük fel tehát, hogy x éppen k db A_i halmaznak eleme. Világos, hogy éppen $\binom{k}{t}$-féleképp lehet az A_i-k közül t különböző x-t tartalmazó halmazt kiválasztani. Ezért x hozzájárulása a jobboldalhoz éppen

$$\sum_{i=1}^{k}(-1)^{i+1}\binom{k}{i} = 1 + \sum_{i=0}^{k}(-1)^{i+1}\binom{k}{i} = 1 - \sum_{i=0}^{k}(-1)^{i}\binom{k}{i} = 1 - (1-1)^k = 1 - 0 = 1\ ,$$

amint azt állítottuk. (A harmadik egyenlőség a binomiális tétel miatt igaz.) □

1.32. Példa *A szita-formulával meghatározhatjuk azon permutációk számát, amelyek olyan sorrendnek felelnek meg, ahol egyik elem sem ott áll, ahol az eredeti sorrendben állt. Legyen ugyanis a permutálandó elemek n száma rögzített, és jelentse A_i azon permutációit az n elemnek, amelyek az i-dik elemet a helyén hagyják. Világos, hogy $|A_i| = (n-1)!$,*

hisz az i-diktől különböző $n-1$ elem egy permutációjáról van szó. Sőt, ha k különböző A_i halmaz metszetét tekintjük, akkor ez éppen azokat a permutációkat tartalmazza, ahol a k adott elem a helyén van, azaz $n-k$ elemet permutálhatunk tetszőlegesen, így a k-as metszet mérete pontosan $(n-k)!$-nak adódik.

Ezek után úgy határozzuk meg a keresett permutációk számát, hogy leszámláljuk a komplementer halmazt, azaz mindazon permutációkat, amelyek legalább egy elemet helyben hagynak, más szóval meghatározzuk az $\bigcup_{i=1}^{n} A_i$ halmaz méretét. A keresett mennyiség tehát

$$n! - \left|\bigcup_{i=1}^{n} A_i\right| = n! - \sum_{I\subseteq\{1,2,\ldots,n\}} (-1)^{|I|+1} \left|\bigcap_{i\in I} A_i\right| = n! - \sum_{k=1}^{n}(-1)^{k+1} \sum_{\emptyset\neq I\subseteq\{1,2,\ldots,n\},|I|=k} \left|\bigcap_{i\in I} A_i\right| =$$

$$= n! + \sum_{k=1}^{n}(-1)^k \binom{n}{k}(n-k)! = n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! + \ldots =$$

$$= n! \cdot \left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots\right) \to n! \cdot \frac{1}{e}$$

Amit kaptunk, azt szokták néha úgy fogalmazni, hogy ha a színházi ruhatárban mindenki véletlenszerűen kap vissza egy kabátot, akkor kb $\frac{1}{e}$ a valószínűsége annak, hogy senki sem a saját ruháját kapja. Más szavakkal, ha minden villamosmérnökhallgató mikulás előtt kiúzza egy másik hallgató nevét a kalapból, akkor több, mint 60% valószínűséggel legalább egyvalaki saját magát lepi meg.

Valamiért a skatulya elv is ebbe a témakörbe tartozik, lássuk hát azt is. A skatulya-elvet általában csak körülírni szokták, valahogy úgy, hogy ha n dobozba több, mint n tárgyat helyezünk, akkor lesz olyan doboz, amiben 1-nél több tárgy van. A szerzőnek sajnos épp a már korábban emlegetett definíció-tétel-bizonyítás a vesszőparipája, úgyhogy következzen az egyesek számára hajmeresztő formalizmus.

1.33. Tétel (Skatulya-elv) *Ha $f : H \to K$ véges halmazok között egy leképezés és $|K| < |H|$, akkor létezik H-nak két egymástól különböző h és h' eleme úgy, hogy $f(h) = f(h')$ teljesül.*

Bizonyítás. Indirekt: ha f H bármely két eleméhez különböző K-beli elemeket rendel, akkor K-nak legalább annyi eleme van, mint H-nak, ellentmondás. □

1.34. Példa *(1) Ha minden villamosmérnökhallgató egy-egy 3-jegyű számzárral zárná a biciklijét, akkor bizonyosan lenne köztük két olyan, akik egymás bicaját használhatnák a saját kódjukkal.*
(Bizonyítás: több, mint 1000 *hallgató mindegyikéhez* 1000 *lehetséges számzárkód valamelyike tartozik.)*

(2) Ha $a_1, a_2, \ldots, a_{100}$ egész számok, akkor kiválasztható közülük néhány úgy, hogy összegük 100-zal osztható legyen.
(Bizonyítás: Tekintsük a $b_i := a_1 + a_2 + \ldots + a_i$ számokat. Ha valamelyik b_i a 100 többszöröse, kész vagyunk. Ha nem, akkor a $b_1, b_2, \ldots, b_{100}$ számok közül a skatulya-elv miatt lesz két olyan, ami ugyanarra a két jegyre végződik, mondjuk b_i és b_j, ahol $i < j$. Ám ekkor a $b_j - b_i = a_{i+1} + a_{i+2} + \ldots + a_j$ szám 100-zal osztható.)

A skatulya-elv alkalmazásával egészen komoly tételeket is bizonyíthatunk. Itt van mindjárt egy példa.

1.35. Tétel (Erdős-Szekeres tétel) *Bármely $k, n \in \mathbb{N}$ esetén tetszőleges $nk+1$ hosszú számsorozatban található n-nél hosszabb növekvő vagy k-nál hosszabb csökkenő részsorozat.*

Bizonyítás. Indirekt bizonyítunk, tegyük fel, hogy valamely n és k esetén van olyan $nk+1$ tagú sorozat, aminek se $n+1$ tagú növekvő, se $k+1$ tagú csökkenő részsorozata sincs. E sorozat x eleméhez rendeljünk hozzá azt az $(n(x), c(x))$ számpárt, ahol $n(x)$ a leghosszabb x-szel kezdődő monoton növekedő részsorozat hosszát, míg $c(x)$ a leghosszabb x-szel kezdődő monoton csökkenő részsorozat hosszát jelenti. Világos, hogy ha x és y a sorozatunk különböző elemei, (mondjuk y az x-t követi), akkor $x \leq y$ esetén $n(x) > n(y)$, míg ha $x \geq y$, akkor $c(x) > c(y)$ teljesül. Ez azt jelenti, hogy a sorozat különböző elemeihez különböző számpárokat rendelünk. Mivel $n(x) \in \{1, 2, \ldots, n\}$ és $c(x) \in \{1, 2, \ldots, k\}$, ezért a sorozat elemeihez rendelt számpárok nk-félék lehetnek. Mivel $nk+1$ taghoz rendeltünk számpárt, ezért két különöbző taghoz ugyanazt a párt kellett rendelnünk, ami lehetetlen. Az ellentmondás mutatja az indirekt feltevés helytelen voltát, ezzel pedig igazoltuk a tételt. □

Az Erdős-Szekeres tételre mutatunk egy másik igen elegáns, a skatulya-elvet nem használó bizonyítást is.

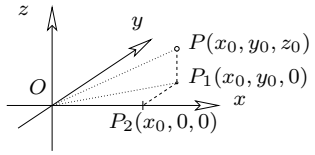
2. bizonyítás:. Legyen S_0 az $(a_1, a_2, \ldots, a_{nk+1})$ sorozat. Azt mondjuk, hogy egy S sorozat x eleme *érdekes*, ha az S sorozat x utáni elemei közül egyik sem kisebb x-nél. Vegyük észre, hogy egy sorozat érdekes elemei a sorozat monoton növekedő részsorozatát alkotják. Az S_0 sorozatból kiindulva definiáljuk az $S_1, S_2, \ldots$ részsorozatokat úgy, hogy S_{i+1} az a sorozat, amit úgy kapunk S_i-ből, hogy elhagyjuk S_i érdekes elemeit. Ha valamelyik S_i-nek több, mint n érdekes eleme van, akkor ezek az elemek egy legalább $n+1$ hosszúságú növekvő részsorozatot alkotnak az eredeti S_0 sorozatban, és az tétel állítása teljesül. Ha ez nem történik meg, akkor viszont mindig csak legfeljebb n elemet hagyunk el, és így az S_k sorozat sem üres. Legyen tehát x_1 az S_k egy eleme. Mivel x_1 nem érdekes S_{k-1}-ben, ezért van S_{k-1}-ben x_1 után egy nála kisebb x_2 elem. Ám x_2 sem érdekes S_{k-2}-ben, muszáj tehát S_{k-2}-ben x_2-t egy nála kisebb x_3 elemnek követnie. Az x_3-ból kapjuk az $x_4, x_5, \ldots$ elemeket, az utolsó elem x_{k+1} lesz S_0-ból. Mivel $x_0, x_1, x_2, \ldots, x_{k+1}$ az S_0 egy monoton csökkenő részsorozata, a tételt igazoltuk. □

1.3. Koordinátageometria

Tudjuk, hogy a háromdimenziós tér pontjai egyértelműen jellemezhetők egy valós számhármassal, már persze, amennyiben előzetesen rögzítettünk egy derékszögű koordinátarendszert. Természetes kérdés, hogy hogyan jellemezhetők különféle térbeli alakzatok, illetve azok metszetei. Térbeli alakzatokon most a pontot, az egyenest és a síkot értjük.

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

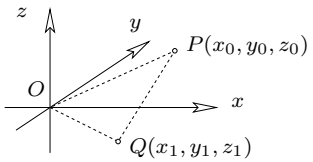
Bizonyítás. Legyen $P_1(x_0, y_0, 0)$ a P vetülete az xy síkra, és legyen $P_2(x_0, 0, 0)$ a P_1 vetülete az x tengelyre. Világos, hogy OP_2P_1 és OP_1P derékszögű háromszögek, ezért Pitagorasz tétele szerint $|OP_1|^2 = |OP_2|^2 + |P_2P_1|^2 = x_0^2 + y_0^2$, ill. $|OP|^2 = |OP_1|^2 + |P_1P|^2 = x_0^2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



A lemma segítségével jellemezhetjük két vektor merőlegességét.

1.37. 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 $OP \perp OQ \iff (x_0x_1 + y_0y_1 + z_0z_1 = 0)$.*

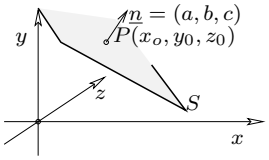
Bizonyítás. OP és OQ pontosan akkor merőlegesek, ha az $OPQ\triangle$ O-nál levő szöge $\frac{\pi}{2}$, ami Pitagorasz tétele szerint pontosan akkor teljesül, ha $|OP|^2 + |OQ|^2 = |PQ|^2$. Beírva a megfelelő koordinátákat, az előző lemma alapján ez pontosan azt jelenti, hogy $x_0^2+y_0^2+z_0^2+x_1^2+y_1^2+z_1^2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



1.38. Definíció *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.)*

1.39. 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.*

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



A fenti tétel mutatja az alábbi definíció érvényességét.

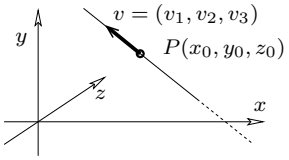
1.40. Definíció *Az* $\underline{n} = (a,b,c)$ *normálvektorú* $P(x_0,y_0,z_0)$ *ponton átmenő* sík normálvektoros egyenlete $ax+by+cz = konst$, *ahol* $konst = ax_0+by_0+cz_0$.

1.41. Definíció *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.

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

$$\begin{aligned} x &= x_0 + \lambda v_1 \\ y &= y_0 + \lambda v_2 \\ z &= z_0 + \lambda v_3 \ . \end{aligned} \tag{1.2}$$



1.43. Definíció *A* (1.2) *feltételrendszert az* e egyenes paraméteres egyenletrendszerének *nevezzük.*

Vizsgáljuk meg a (1.2) egyenletrendszert. Ha az irányvektor egyik koordinátasíkkal sem párhuzamos, azaz $v_1v_2v_3 \neq 0$, 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. fejezet

Lineáris algebra

2.1. Vektorterek

2.1. Definíció *A V halmazt* $\mathbb{R}$ feletti vektortér*nek mondjuk (és* $\mathbb{R}$ *elemeit* skalároknak *nevezzük), 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) $1u=u$

2.2. Megjegyzés *Az (ö4) feltételben szereplő* $-u$ *vektort az* u *vektor* ellentettjének *hívjuk.*

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

2.4. 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.

2.5. 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) $\lambda v = \mathbf{0} \Rightarrow (\lambda = 0$ vagy $v = \mathbf{0})$ azonosságok.

Bizonyítás. (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: $\mathbf{0} = \frac{1}{\lambda}\mathbf{0} = \frac{1}{\lambda}(\lambda v) = (\frac{1}{\lambda}\lambda)v = 1v = v$. □

2.6. Megjegyzés *A 2.5. Tétel (3) és (4) részének 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.*

2.7. Definíció *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.*

2.8. 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, amelyeknek a kitevője prímhatvány (és persze legfeljebb* 10*-edfokúak). Ebből az altérből egy polinom pl a* $p(x) = 24x^2 - x^3 + 4x^7$*.*

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

Bizonyítás. 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. □

2.10. 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.*

Bizonyítás. 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 $u \in \bigcap_{\alpha\in I} U_\alpha$. □

2.11. Definíció *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* $\sum_{i=1}^n \lambda_i v_i$ *lineáris kombináció* triviális*, ha* $\forall \lambda_i = 0$*.*

2.12. Definíció *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, amelyeket 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.

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

Bizonyítás. 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 $v + w \in \langle U \rangle$. □

2.14. Definíció *A $v_1, v_2, \ldots, v_n$ vektorrendszer* (lineárisan) független*, ha csak a triviális lineáris kombinációjuk állítja elő a $\mathbf{0}$-t, azaz, ha $\sum_{i=1}^{n} \lambda_i v_i = \mathbf{0} \Rightarrow \forall \lambda_i = 0$. A fenti rendszer* (lineárisan) összefüggő*, ha nem lineárisan független, azaz, ha a $\mathbf{0}$ előáll nemtriviális lineáris kombinációként is: $\sum_{i=1}^{n} \lambda_i v_i = \mathbf{0}$, és $\lambda_i \neq 0$ valamely i-re.*

2.15. Megjegyzések

1. *A 2.14. Definícióhoz 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, amelyekben minden lineárisan független halmaz véges. (Más szóval: a számunkra érdekes vektorterek bármely végtelen halmaza lineárisan összefüggő.)*

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

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

2.16. 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.*

Bizonyítás. 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 lineárisan független, akkor a $\mathbf{0}$ előáll nemtriviális lineáris kombinációként, pl. $\mathbf{0} = \sum_{i=1}^{n} \lambda_i v_i$ alakban, ahol (mondjuk) $\lambda_k \neq 0$. Ekkor átrendezéssel $\lambda_k v_k = \sum_{i \neq k} -\lambda_i v_i$, ahonnan $v_k = \frac{1}{\lambda_k} \sum_{i \neq k} -\lambda_i v_i = \sum_{i \neq k} -\frac{\lambda_i}{\lambda_k} v_i$ adódik, ami épp v_k előállítása a maradék vektorok lineáris kombinációjaként. □

2.17. Definíció *A $\{b_1, b_2, \ldots, b_n\}$ vektorrendszer a V vektortér* bázisa, *ha lineáris független és egyúttal V generátorrendszere.*

2.18. 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 lineáris kombinációjaként.*

Bizonyítás. 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. □

2.19. Definíció *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.*

2.20. 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. $[\lambda u]_B = \lambda \cdot [u]_B$.*

2.21. Definíció *A V vektortér* dimenziója *a V egy tetszőleges B bázisának elemszáma.*

2.22. Tétel (Kicserélési tétel) *Ha $F = \{f_1, f_2, \ldots, f_n\} \subseteq V$ független 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.*

Bizonyítás. Indirekt bizonyítunk, azaz feltesszük, hogy valamelyik f_i-hez nem létezik g_j. Rögzítsük ezt az f_i-t, és vizsgáljuk meg, mit jelent az, hogy $F \setminus \{f_i\} \cup \{g_j\}$ nem lineárisan független. Mivel $F \setminus \{f_i\}$ lineárisan független, ezért ha $F \setminus \{f_i\} \cup \{g_j\}$ egy nemtriviális lineáris kombinációja $\mathbf{0}$-t ad, akkor g_j együtthatója nemnulla, azaz g_j előállítható az $F \setminus \{f_i\}$-beli vektorok lineáris kombinációjaként. Ez minden g_j vektorra igaz, tehát $g_1, g_2, \ldots g_k \in \langle F \setminus \{f_i\}\rangle$. 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 $f_i \in \langle g_1, g_2, \ldots g_k\rangle \subset \langle F \setminus \{f_i\}\rangle$, 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. □

2.23. Következmény *Ha $f_1, f_2, \ldots f_n$ lineárisan függetlenek és a $g_1, g_2, \ldots g_k$ vektorok generálják V-t, akkor $n \leq k$.*

Bizonyítás. A kicserélési tétel által biztosított módon (tehát a függetlenség megtartásával) cseréljük ki sorban az $f_1, f_2, \ldots, f_n$ 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 $\mathbf{0}$-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. □

2.24. Következmény *Vektortér bármely két bázisa azonos elemszámú. A dimenzió fogalma jóldefiniált.*

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

2.25. Megjegyzés *Jegyezzük meg, hogy a fent kimondott állítások olyan vektorterekre vonatkoznak, amelyek* 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.)*

2.26. Tétel *Ha $F \subseteq V$ független 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.*

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

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

2.27. Állítás *(1)* $U \leq V \Rightarrow \dim U \leq \dim V$.

(2) Az alábbi 5 állítás ekvivalens. (a) $\dim V = n$ $\iff$ *(b)* $\exists n$*-elemű független, és minden* n*-elemű független bázis* $\iff$ *(c)* $\exists n$*-elemű generátorrendszer, és minden* n*-elemű generátorrendszer bázis* $\iff$ *(d)* $\exists n$*-elemű független, és bármely* $(n+1)$ *vektor összefüggő* $\iff$ *(e)* $\exists n$*-elemű generátorrendszer, és* $\nexists(n-1)$ *elemű generátorrendesz.*

Bizonyítás. (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 független generátorrendszer. Létezik tehát n-elemű független. 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 független.

(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 összefüggő.

(e) ⇒ (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. □

2.2. 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.

2.28. Definíció *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, amelyek megkaphatók 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
$\begin{array}{l}\alpha_{1,1}x_1+\alpha_{1,2}x_2+\ldots+\alpha_{1,n}x_n=b_1\\ \alpha_{2,1}x_1+\alpha_{2,2}x_2+\ldots+\alpha_{2,n}x_n=b_2\\ \vdots\\ \alpha_{k,1}x_1+\alpha_{k,2}x_2+\ldots+\alpha_{k,n}x_n=b_k\end{array}$	$\left(\begin{array}{cccc\|c}\alpha_{1,1}&\alpha_{1,2}&\ldots&\alpha_{1,n}&b_1\\ \alpha_{2,1}&\alpha_{2,2}&\ldots&\alpha_{2,n}&b_2\\ \vdots&\vdots&&\vdots&\vdots\\ \alpha_{k,1}&\alpha_{k,2}&\ldots&\alpha_{k,n}&b_k\end{array}\right)$	$\left(\begin{array}{c\|c\|c\|c\|c\|c}0&1\ldots&&&&\\ \hline &0&1\ldots&&&\\ \hline &&0&1\ldots&&\\ \hline &&&0&1\ldots&\\ \hline &&&&0\ldots0&\vdots\\ &&&&\ddots&\\ &&&&0\ldots0&\end{array}\right)$

2.29. Definíció *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.*

2.30. Definíció *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.

2.31. Definíció *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.*

2.32. 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.*

2.33. 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* $v = 7$*.*

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

2.34. Következmény *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, amelyek 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.

2.35. Definíció *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.

2.36. 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.*

Bizonyítás. 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. □

2.37. Állítás *Elemi sorekvivalens átalakítás során a lineáris egyenletrendszer megoldásainak halmaza nem változik.*

Bizonyítás. 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. □

2.38. Tétel *Elemi sorekvivalens átalakításokkal tetszőleges kibővített együtthatómátrix lépcsős alakra hozható.*

Bizonyítás. 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-eliminálunk 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.

Azért ha írásban kell a Gauss-eliminációt végrehajtani, akkor jobban járunk, ha a fenti bizonyításbeli rekurzióval próbálkozás helyett inkább akkurátusan kiírjuk az elhagyandó sorokat és oszlopokat.

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.

2.39. 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.*

2.40. 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.*

Bizonyítás. 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. □

2.41. Következmény *(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.

Bizonyítás. (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.

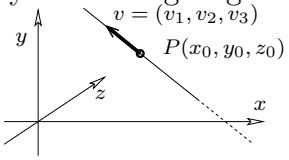
Világos, hogy egy homogén lineáris egyenletrendszer kibővített együtthatómátrixában sosem keletkezhet tilos sor az elemi sorekvivalens átalakítások hatására, hisz a jobboldal mindvégig 0 lesz. Csakugyan: minden homogén lineáris egyenletrendszernek létezik megoldása, mégpedig az ú.n. *triviális megoldás*, ami minden ismeretlennek 0 értéket ad. A nemtriviális megoldás létezésének elégséges feltételét adja a következő tétel.

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

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

2.2.1. Egy koordinátageometriai alkalmazás

Láttuk, hogy egy e egyenes pontjait jellemzi a e egyenes 1.2 paraméteres egyenletrendszere, amit az e egy $p = (x_0, y_0, z_0)$ pontjából és az e egy nemnulla $\underline{v} = (v_1, v_2, v_3)$ irányvektora segítségével írtunk fel.



Emlékeztetőül: az e egyenest pontosan azok az (x, y, z) koordinátájú pontok alkotják, amelyek előállnak $(x, y, z) = (x_0, y_0, z_0) + \lambda(v_1, v_2, v_3)$ alakban valamely $\lambda \in \mathbb{R}$ esetén, azaz a koordináták kielégítik az 1.2 rendszerrel ekvivalens, 3 egyenletből álló, 4 ismeretlent (x, y, z, λ) tartalmazó

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

egyenletrendszert.

A 2.1 egyenletrendszer kibővített együtthatómátrixa redukált lépcsős alakú, és az x, y és z-nek megfelelő oszlpokban vannak a vezéregyesek:

$$\left(\begin{array}{cccc|c} x & y & z & \lambda & \\ 1 & 0 & 0 & v_1 & x_0 \\ 0 & 1 & 0 & v_2 & y_0 \\ 0 & 0 & 1 & v_3 & z_0 \end{array}\right) \rightarrow \left(\begin{array}{cccc|c} \lambda & x & y & z & \\ v_1 & 1 & 0 & 0 & x_0 \\ v_2 & 0 & 1 & 0 & y_0 \\ v_3 & 0 & 0 & 1 & z_0 \end{array}\right)$$

Megtehető azonban, hogy a kibővített együtthatómátrix oszlopait nem x, y, z, λ sorrendben írjuk fel, és ekkor elvégezhető lesz a Gauss-elimináció úgy, hogy a λ ne szabad paraméter legyen, hanem az oszlopában vezéregyes álljon, és persze ekkor ennek a vezéregyesnek a sorában lesz még más nemnulla is. Minthogy mi csak x, y, z-re akarjuk

megoldani az egyenletrendszert, az az egyenlőség, ami a λ vezéregyesének sorához tartozik, egyszerűen elhagyható. Marad tehát 2 egyenlet, mindegyikben csak x, y, z a változók, és megoldásai pontosan az e egyenes pontjainak (x, y, z) koordinátái lesznek.

Láttuk tehát, hogy a síkot egyetlen egyenlet, míg az egyenes pontjait két egyenlet írta le. Világos az is, hogy a „pont egyenlete" voltaképpen egy három egyenletből álló lineáris egyenletrendszer: a $p = (x_0, y_0, z{+}0)$ ponthoz az $x = x_0, y = y_0, z = z_0$ egyenletrendszer tartozik. Ha pedig a fent leírt halmazok (pont, egyenes, sík) közül néhánynak a közös pontjait kell meghatároznunk, akkor az eljárás az lehet, hogy mindegyik ponthalmaznak felírjuk az egyenlet(rendszer)ét, ezeket egy közös egyenletrendszernek tekintve, azt Gauss-eliminációval megoldjuk. Ha nincs megoldás, akkor a metszet értelemszerűen üres, egyébként a redukált lépcsős alakban szereplő egyenletek számától függően a megoldás egy pont, egy egyenes vagy éppen egy sík lesz.

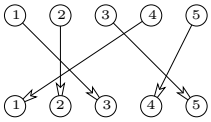
2.3. Permutációk, determinánsok

2.3.1. Permutációk, inverziószám

2.43. Definíció *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.*

2.44. 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.)

2.45. Definíció *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.*

2.46. 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.*

A fenti 2.46. Megfigyelés úgy is megfogalmazható, hogy $I(\sigma)$ 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.

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

Bizonyítás. 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 $I(\sigma) = I(\sigma^{-1})$. □

2.3.2. 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, amelyek 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.

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.

2.48. Példa *Az alábbi* 3×3 *méretű mátrix determinánsa például* $|A| = (-1)^0 \cdot aei + (-1)^1 \cdot afh + (-1)^1 \cdot bdi + (-1)^2 \cdot bfg + (-1)^2 \cdot cdh + (-1)^3 \cdot ceg$.

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

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 $(A^T)_i^j = A_j^i$.) A négyzetes A mátrix *főátlója* a bal felső sarkot és a jobb alsó sarkot összekötő átló mentén elhelyezkedő mátrixelemek halmaza. A négyzetes A mátrix *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.

2.49. 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.*

Bizonyítás. (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, amelyek tartalmaznak a főátló alól elemet, nem érdekesek, hiszen értékük 0. Igy csak azokat kell összegeznünk a megfelelő előjellel, amelyeknek 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. □

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.

2.50. 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 aldeterminánsnak 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.

2.51. Tétel (Kifejtési tétel) *Ha A $n \times n$-es mátrix és i rögzített, akkor*

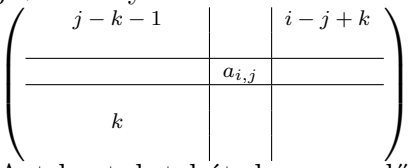
(1) $\det(A) = \sum_{j=1}^{n} a_{i,j} \cdot A_{i,j}$ *(*az i-dik sor szerinti kifejtés*). Rögzített j-re* $\det(A) = \sum_{i=1}^{n} a_{i,j} \cdot A_{i,j}$ *(*a j-dik oszlop szerinti kifejtés*), ill.*

(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*).*

Bizonyítás. (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, amelyek az $A_{i,j}$ előjeles aldeterminánsban 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.

2.4. Mátrixok

2.4.1. Mátrixműveletek, térbeli vektorok szorzása

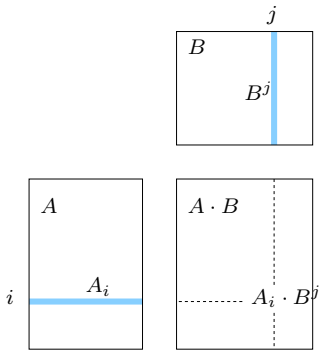
A determinánsok tárgyalása után érdemes a mátrixok között műveleteket bevezetni.

2.52. Definíció *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 $(A+B)_i^j = A_i^j + B_i^j$.*

2.53. 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.

2.54. Definíció *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.*



2.55. 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:* $(A \cdot B)^i = B^i_1 \cdot A^1 + B^i_2 \cdot A^2 + \ldots \square$

A továbbiakban többször lesz szükség a 2.55. Megfigyelésre.

2.56. 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.

2.57. 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 $x = (x_1, x_2, \ldots, x_n)^T$ 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.

2.58. Tétel (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.

2.59. Definíció *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.*

2.60. 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. □

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

2.62. 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).*

Bizonyítás. (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. □

2.63. 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.*

2.4.2. Mátrix inverze

2.64. Definíció *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 $A \cdot J = I_n$.*

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

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

2.66. Következmény *Ha egy mátrixnak van jobb és balinverze is, akkor azok egyértelműek.*□

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

2.68. Következmény *Az A mátrixnak pontosan akkor van jobbinverze, ha A-nak létezik balinverze.*

A bizonyításhoz egy segédtételre van szükség.

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

Bizonyítás. 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 2.68. Következmény bizonyítása a 2.67. 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 2.67. Tétel miatt azzal ekvivalens, hogy A^T-nak létezik egy X jobbinverze, ami a 2.69. Lemma szerint éppen azt jelenti, hogy X^T az A balinverze. □

2.70. 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.*

Bizonyítás. 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 lineáris függetlenségét, 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 2.67. 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. □

2.71. 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.*

2.72. Következmény *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* $B = A^{-1}$.□

2.4.3. 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.

2.73. Definíció *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.)*

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

Bizonyítás. Mivel négyzetes mátrix determinánsa megegyezik a transzponáltjának determinánsával, ezért az A-beli legnagyobb nemnulla aldeterminánsz az A^T-beli legnagyobb nemnulla aldeterminánsz transzponáltja lesz, ezért méretük megegyezik. □

2.75. 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 összefüggők, 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.*

2.76. Tétel *Tetszőleges A mátrixra* $s(A) = d(A)$.

A bizonyítás előtt rámutatunk egy fontos következményre.

2.77. Következmény *Tetszőleges A mátrixra $o(A) = d(A) = s(A)$.*

Bizonyítás. 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. □

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

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

A tétel bizonyításához az alábbi segédtételt használjuk.

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

Bizonyítás. 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. □

A 2.76. 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. □

2.4.4. Lineáris egyenletrendszerek tárgyalása mátrixokkal

2.80. 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) $b \in \langle A^1, \dots, A^n\rangle$ (és $A^1, \dots A^n$ lineárisan független vektorok).

(5) $\langle A^1, \dots, A^n\rangle = \langle b, A^1, \dots, A^n\rangle$ (és $A^1, \dots A^n$ lineárisan független vektorok).

(6) $\dim(\langle A^1, \dots, A^n\rangle) = \dim(\langle b, A^1, \dots, A^n\rangle)(= n)$.

(7) $r(A) = r(A|b)(= n)$.

Bizonyítás. (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 $A^1, \dots, A^n$ 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. □

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

Bizonyítás. 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 $|A| \neq 0$. □

2.5. Lineáris leképezések

2.82. Definíció *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 művelettartó leképezést nevezzük.*

Könnyen látható, hogy az (1,2) tulajdonságok helyett megkívánhatnánk az alábbi tulajdonságot:

(3) $\mathcal{A}(\lambda u + \mu v) = \lambda \mathcal{A}(u) + \mu \mathcal{A}(v) \quad \forall u, v \in V, \forall \lambda, \mu \in \mathbb{R}$. Ha ugyanis $\mathcal{A}$ lineáris, akkor $\mathcal{A}(\lambda u + \mu v) = \mathcal{A}(\lambda u) + \mathcal{A}(\mu v) = \lambda \mathcal{A}(u) + \mu \mathcal{A}(v)$. Másrészt ha (3) fenáll, akkor $\lambda = \mu = 1$ esetén (1), míg $\mu = 0$ helyettesítéssel (2) következik.

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.

2.83. 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.*□

2.84. Példa *(1) A síkvektorokon az x tengelyre vetítés,*

(2) a síkvektorokon az origó körüli (nyújtva)forgatás,

(3) a síkvektoroknak egy origón átmenő egyenesre tükrözése,

(4) a 2×2-es mátrixokhoz 2×3-as mátrixok hozzárendelése $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} b & 0 & 2c-a \\ d & d & 3d \end{pmatrix}$ *szerint,*

(5) A polinomok vektorterén a deriválás, azaz $p(x) \mapsto p'(x)$. A művelettartás a deriválás azonosságai miatt igaz: $(p+q)'(x) = p'(x) + q'(x)$, ill. $(\lambda p)'(x) = \lambda p'(x)$.

2.85. 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 $\mathcal{A}(u_i) = v_i \quad \forall i$.*

2.86. 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.*

Bizonyítás. Tegyük fel, hogy létezik a kívánt lineáris leképezés, megmutatjuk, hogy egyértelmű. Legyen ugyanis $u \in U$ tetszőleges vektor. Ekkor u egyértelműen áll elő az U

adott bázisának lineáris kombinációjaként, mondjuk $u = \sum_{i=1}^n \lambda_i u_i$ alakban. Ekkor $\mathcal{A}$ feltételezett linearitása miatt $\mathcal{A}(u) = \mathcal{A}(\sum_{i=1}^n \lambda_i u_i) = \sum_{i=1}^n \lambda_i \mathcal{A}(u_i) = \sum_{i=1}^n \lambda_i v_i$, tehát (ha $\mathcal{A}$ valóban létezik, akkor) $\mathcal{A}(u)$ egyértelműen meghatározott.

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

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

(a fenti negyedik ill. az alábbi harmadik egyenlőségnél használjuk, hogy $\mathcal{A}$-t hogyan definiáltuk a bázis lineáris kombinációin) ill.

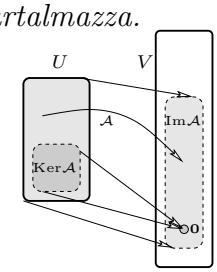
$$\mathcal{A}(\lambda\ u) = \mathcal{A}(\lambda \sum_{i=1}^n \lambda_i u_i) = \mathcal{A}(\sum_{i=1}^n \lambda\lambda_i u_i) = \sum_{i=1}^n \lambda\lambda_i v_i = \lambda \sum_{i=1}^n \lambda_i v_i = \lambda \mathcal{A}(u) \ .$$

□

2.87. Definíció *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, amelyek a V tér nullvektorába képződnek, a képtér pedig a V tér mindazon elemeinek halmaza, amelyek előállnak valamely U-beli vektor képeként. (Ld. az ábrát.)

2.88. 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.

2.89. 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.*

Bizonyítás. 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. □

2.90. Tétel (Dimenziótétel) *Ha* $\mathcal{A} : U \to V$ *lineáris leképezés, akkor* $\dim \mathrm{Ker}\mathcal{A} + \dim \mathrm{Im}\mathcal{A} = \dim U$*.*

Bizonyítás. 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. □

2.91. Definíció *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:* $U \cong V$*.*

2.92. Állítás *(1) Az* $\mathcal{A} : U \to V$ *lineáris leképezés (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* $\dim U = \dim V \iff U \cong V$*.*

Bizonyítás. (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 $U \cong V$. □

2.5.1. Lineáris leképezések mátrixai

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

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

Nézzük meg, hogyan kaphatjuk meg a leképezés mátrixának ismeretében egy u vektor koordinátavektorából az $\mathcal{A}(u)$ vektor koordinátavektorát. (Értelemszerűen a B_1 ill. B_2 bázisban felírt koordinátavektorokról beszélünk.) Meg kell határoznunk tehát, hogy egy $u = \sum_{i=1}^{n} \mu_i u_i$ vektor képét hogyan írhatjuk fel a $v_1, \ldots v_m$ bázisban. Hát lássuk:
$\mathcal{A}(u) = \mathcal{A}(\sum_{i=1}^{n} \mu_i u_i) = \sum_{i=1}^{n} \mu_i A(u_i) = \sum_{i=1}^{n} \mu_i (\sum_{j=1}^{m} \lambda_j^i v_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} \mu_i (\lambda_j^i v_j) = \sum_{j=1}^{m} \sum_{i=1}^{n} \mu_i \lambda_j^i v_j = \sum_{j=1}^{m} v_j \sum_{i=1}^{n} \mu_i \lambda_j^i = \sum_{j=1}^{m} (\sum_{i=1}^{n} \mu_i \lambda_j^i) v_j$, tehát a keresett koordinátavektor egy olyan, m-elemű oszlopvektor, aminek j-dik koordinátája $\sum_{i=1}^{n} \mu_i \lambda_j^i$. Ha jól megfigyeljük, éppen azt kaptuk, hogy a leképezés mátrixával való szorzás megadja a leképezést a koordinátavektorokon. Ezt írja le az alábbi tétel.

2.94. 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.)*

2.95. 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.

2.96. Definíció *$\mathcal{A}, \mathcal{B} \in \mathrm{Hom}(U,V)$ 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.*

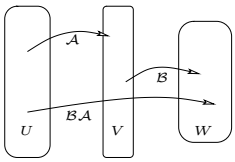
2.97. Megfigyelés *Ha $\mathcal{A}, \mathcal{B} \in \mathrm{Hom}(U,V)$ és $\lambda \in \mathbb{R}$, akkor $\mathcal{A}+\mathcal{B}, \lambda\mathcal{A} \in \mathrm{Hom}(U,V)$, azaz lineáris leképezések összege és skalárszorosa is lineáris leképezés. E műveletekkel* $\mathrm{Hom}(U,V)$ *szintén valós vektortér, 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.)*

Bizonyítás. $(\mathcal{A}+\mathcal{B})(u+v) = \mathcal{A}(u+v)+\mathcal{B}(u+v) = \mathcal{A}(u)+\mathcal{A}(v)+\mathcal{B}(u)+\mathcal{B}(v) = (\mathcal{A}(u)+\mathcal{B}(u))+(\mathcal{A}(v)+\mathcal{B}(v)) = (\mathcal{A}+\mathcal{B})(u)+(\mathcal{A}+\mathcal{B})(v)$, 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 leképezéxmátrix 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. □

A fentieken túl értelmezhető lineáris leképezések szorzata is.

2.98. Definíció *$\mathcal{A} \in \mathrm{Hom}(U,V)$, $\mathcal{B} \in \mathrm{Hom}(V,W)$ 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.))*



2.99. 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.*

Bizonyítás. 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. $(\mathcal{BA})(\lambda u) = \mathcal{B}(\mathcal{A}(\lambda u)) = \mathcal{B}(\lambda\mathcal{A}(u)) = \lambda\mathcal{B}(\mathcal{A}(u)) = \lambda(\mathcal{BA})(u)$. □

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.

2.100. 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 $[\mathcal{B}\mathcal{A}]_{B_3}^{B_1} = [\mathcal{B}]_{B_3}^{B_2} \cdot [\mathcal{A}]_{B_2}^{B_1}$, azaz lineáris leképezések szorzatának mátrixa azonos a leképezések mátrixainak szorzatával (egyező bázisok esetén).* □

2.101. Következmény *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).*

Bizonyítás. 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. □

2.5.2. 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 $\mathrm{Ker}\mathcal{A}$ 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.

2.102. Definíció *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.

2.103. Definíció *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.

2.104. 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.

2.105. Tétel *(1) Lineáris transzformáció minden sajátvektora pontosan egy sajátértékhez tartozik.*

(2) Bármely λ sajátértékhez tartozó sajátaltér a V vektortér altere.

Bizonyítás. (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.

2.106. Definíció *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.*

2.107. 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.

Bizonyítás. (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.

2.108. 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:

$$\left(\begin{array}{ccc|c} 0 & 0 & -3 & 0 \\ 0 & 0 & 5 & 0 \\ 1 & 1 & -2 & 0 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 1 & -2 & 0 \\ 0 & 0 & -3 & 0 \\ 0 & 0 & 5 & 0 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 1 & -2 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 5 & 0 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 1 & -2 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

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.*

2.109. Tétel (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.)* $\square$

3. fejezet

Gráfok

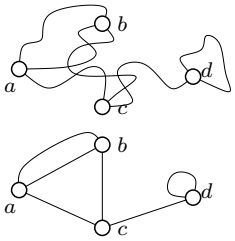
3.1. A gráfelmélet alapjai

A diszkrét matematikában az egyik legfontosabb fogalom a gráf. A legváratlanabb szituációkban bizonyul nagyon jól használhatónak és számos gyakorlati alkalmazáshoz kapcsolódó modell alapvető összetevője.

3.1. Definíció *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 $G = (V, E)$. A G egyszerű gráf* véges*, ha V véges halmaz.*

3.2. Definíció *A G gráf egy* diagramja *a G egy olyan lerajzolása, amiben a csúcsoknak (síkbeli) pontok felelnek meg, éleknek pedig olyan síkgörbék, amelyek 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.* Hurokél *az olyan él, aminek két végpontja megegyezik. A $G = (V, E)$ pár* gráf*, ha $V \neq \emptyset$, E élhalmaz V-n, és párhuzamos és hurokél is megengedett.*

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



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

3.4. Megjegyzések *1. Gráf diagramjának a definíciójában görbe helyett szerencsésebb töröttvonalról beszelni, ugyanis egy görbe egészen váratlan módon is tud viselkedni. Például egy egységnégyzet minden belső pontján áthalad.*

2. A párhuzamos éleket precízen egy kicsit körülményes definiálni. Az egyik lehetőseg hogy $E(G)$-t „multihalmaznak" tekintjük (egy él többszörös multiplicitással lehet eleme), de járható út az is, ha 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. A hurokél definíciójához is módosítani kellene az él definícióját, de (kivételesen) itt sem az absztrakt formalizmus a cél.

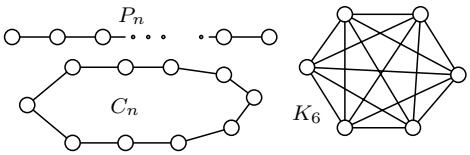
3.5. Definíció *A G gráf* szomszédossági mátrixa *az a $V(G) \times V(G)$ méretű mátrix, aminek (u, v) pozícióján az u és v közti élek száma áll ($u = v$ esetén a hurokélek számának kétszerese). A G gráf* véges, *ha $V(G)$ és $E(G)$ is véges halmazok.*

3.6. Definíció *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-)reguláris*nak mondjuk, ha minden pontjának ugyanannyi (r) a foka: $\Delta(G) = \delta(G)(= r)$.*

3.7. 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.*

Bizonyítás. Ha G-nek nincs éle, akkor a fokszámösszeg is és az élszám (kétszerese) is 0. Építsük fel G-t úgy, hogy egyenként húzzuk be G éleit. 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. □

3.8. Definíció 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*:*
$V(P_n) = V(C_n) = \{v_1, \ldots, v_n\}$*,* $E(P_n) = \{v_i v_{i+1} : 1 \leq i < n\}$*,* $E(C_n) = E(P_n) \cup \{v_1 v_n\}$*. (ld. az ábrát)*



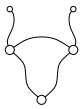
Megfigyelés:
$K_2 = P_2, K_3 = C_3$ ♦

3.9. Definíció $D = (V, A)$ 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.)*

3.10. Definíció *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* $uv \in E(G) \iff \varphi_V(u)\varphi_V(v) = \varphi_E(uv)$*. (Olyan kölcsönösen egyértértelmű megfelelés a pontok között, úgy, amelyre tetszőleges* $u, v \in V(G_1)$ *esetén* u*-ból pontosan annyi él vezet* v*-be* G_1*-ben, mint a* $\varphi(u)$*-ból* $\varphi(v)$*-be* G_2*-ben.)*

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

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


a bika

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

3.14. Definíció *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) különbözők.*

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

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

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

3.17. Definíció *$u, v \in V(G)$-re $u \sim v$, ha létezik u és v között séta.*

3.18. 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.*□

3.19. Definíció *A G gráf* komponense *$a \sim$ ekvivalenciareláció ekvivalenciaosztálya.*

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

3.20. 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 $u \in K$, $v \in V(G) \setminus K$.*□

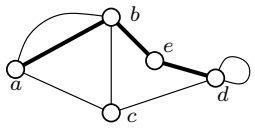
3.21. Következmény *Minden gráf egyértelműen bontható komponensekre.*□

3.22. Definíció *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 $E_v := \{e \in E : v$ végpontja e-nek$\}$. $G - v := (V \setminus \{v\}, E \setminus E_v)$ a v pont törlésével keletkező gráf. $E_{V'} := \{e \in E : e$-nek van V'-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.*

3.23. Definíció *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.*

Részgráfjot úgy kapunk, hogy a csúcsok mellett élek törlése is megengedett.

3.24. Definíció *A H gráf a G* részgráfja*, ha $H = (G - V') - E'$ alkalmas $V' \subseteq V(G)$ és $E' \subseteq E(G)$-re.*



Az 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.

3.25. Megjegyzés *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. Fák

3.2.1. Fák alaptulajdonságai

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

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

Bizonyítás. 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 összefüggő, 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 összefüggő. □

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

Bizonyítás. Indirekt. Ha G-ben van egy k pontú kör, akkor e kör k élének behúzása után $n-k$ izolált pontot és egy kört, azaz $n-k+1$ komponenst kapunk. Az eztán behúzott, további $n-1-k$ él mindengyike legfeljebb 1-gyel csökkenti a komponensek számát, végül tehát legalább $n-k+1-(n-1-k)=2$ komponens adódik, más szóval G nem lesz összefüggő. Ellentmondás. □

A 3.27. és 3.27. tételekből következik, hogy véges irányítatlan G gráf esetén az alábbi három tulajdonság közül bármely kettő teljesülése maga után vonja a harmadikat, azaz a fa definíciójához bármely kettőt használhatjuk.

1. G összefüggő
2. G körmentes
3. $|E(G) = |V(G)| - 1$, azaz G-nek eggyel kevesebb éle van, mint csúcsa.

Hasznos tulajdonság az alábbi is.

3.29. Állítás *Ha uv az F fa éle, akkor $F - uv$-nek két komponense lesz, melyek közül egyik az u, a másik a v csúcsot tartalmazza.*

Ha a és b az F fa csúcsai, akkor F-ben pontosan egy ab-út található.

Bizonyítás. Az uv él törlése után F-nek a 3.27. Tétel miatt pontosan $n-2$ éle lesz. Ha tehát a 3.27. tétel bizonyításában leírt módon építjük fel F-t élek egyenkénti behúzásával, akkor a végső gráfnak $n-(n-2)=2$ komponenese lesz, és világos, hogy a törölt él két végpontja különböző komponensbe kerülnek.

Az állítás második része abból következik, hogy mivel F összefüggő, ezért van F-ben (legalább egy) ab-út. Ha azonban P és P' különböző ab-utak lennének, akkor van olyan $e = uv$ él, ami a két út közül pontosan az egyikhez (mondjuk a P-hez) tartozik. Tegyük fel, hogy P-n végighaladva az a, u, v, b csúcsokat ebben a sorrendben érintjük. Világos, hogy $F - e$-ben u-ból eljuthatunk a-ba, a P' út a-ból b-be vezet $F - e$-ben, végül P-n el lehet jutni b-ből v-be. Márpedig ez ellentmond az első részben igazoltaknak, miszerint $F - e$-ben u és v különböző komponensbe tartoznak. □

3.30. Következmény *Minden véges, összefüggő 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.)*

Bizonyítás. Hagyjunk el éleket, míg a gráf összefüggő marad. Mindaddig, amíg a gráf tartalmaz kört, el tudjuk hagyni a kör egy élét, mert ezáltal a gráf összefüggő marad. Végül tehát egy körmentes, összefüggő F részgráfját kapjuk G-nek. Ez az F feszítőfa lesz, hisz G-ből egyáltalán nem hagytunk el pontot. □

3.31. Állítás *Legyen F egy fa, és húzzunk be F-be két nem szomszédos pont közé egy új e élt. Ekkor a kapott $F + e$ gráfnak pontosan egy köre van.*

Bizonyítás. Világos, hogy az $F + e$ gráf összefüggő, de nem fa, ezért tartalmaz kör. Ráadásul $F + e$ minden köre tartalmazza e-t, és persze e-n kívül egy olyan F-beli utat, ami e két végpontját köti össze. A 3.29. Állítás miatt viszont e két végpontja között pontosan egy út halad F-ben, ezért $F + e$-nek pontosan egy köre van. □

3.32. Definíció *Ha F a G gráf feszítőfája és e a G-nek egy F-ben nem szereplő éle, akkor az $F + e$ gráfnak a 3.31. Állítás szerint egyértelmű körét az e* él F-hez tartozó alapkörének *nevezzük.*

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

3.34. Tétel *Minden legalább 2 pontú F fának legalább két levele van.*

Bizonyítás. Tekintsünk F egy leghosszabb útját, mondjuk P-t! A P út egyik végpontjából sem indulhat további él: ha az ugyanis egy P-n kívüli pontba futna, akkor P nem lenne leghosszabb, ha pedig P egy pontjába, akkor a gráf nem lenne körmentes. □

3.2.2. Cayley tétele

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

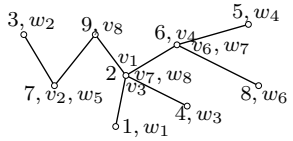
Számozott csúcsokon (izomorf fákat többször megszámolva) $n =$ 1-re 1, $n =$ 2-re 1, $n =$ 3-ra 3, $n =$ 4-re 16 ($4 \times K_{1,3}$ és $12 \times P_4$), $n =$ 5-re 125 ($60 \times$ 2-levelű, $60 \times$ 3-levelű, $5 \times$ 4-levelű), $n =$ 6-ra sok.

3.35. Tétel (Cayley tétele) *Az $\{1, 2, \ldots, n\}$ ponthalmazon n^{n-2} különböző fa adható meg.*

Bizonyítás. Az ún. Prüfer-kód segítségével bizonyítunk. Részfák egy $F = F_1 > F_2 > \ldots > F_{n-1}$ sorozatát konstruáljuk az alábbiak szerint. Legyen $i \in \{1, 2, \ldots, n-1\}$-re w_i az F_i legkisebb sorszámú levele, v_i pedig w_i F_i-beli szomszédja. Legyen továbbá $F_{i+1} := F_i - w_i$. (Az aktuális F_i fának a legkisebb w_i levelét hagyjuk el, ami v_i-hez csatlakozik.)

3.36. Megfigyelés *$V(F_n) = \{n\}$, azaz $v_{n-1} = n$.*

Bizonyítás. Az n csúcsot sosem hagytuk el, hisz mindig legl. 2 levél volt. □



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

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

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

A 3.37. Megfigyelés bizonyítása. Láttuk, hogy $V(F_{n-1}) = \{n\}$, ezért a $v = n$ pont éppen annyiszor szerepel a $v_1, v_2, \ldots, v_{n-1}$ pontok között, ahányszor egy-egy szomszédja törlésre került, azaz $d(n)$-szer. Mivel $v_{n-1} = n$, ezért a Prüfer-kódban $d(n) - 1$-szer szerepel az n.

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

3.38. Következmény *Az F fa levelei pontosan F-nek a Prüfer-kódban nem szereplő csúcsai.*

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

3.39. Következmény *w_1 a legkisebb olyan természetes szám, ami nem szerepel a $v_1, v_2, \ldots, v_{n-1}$ sorozatban.*□

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

Azt kell még igazolni, hogy egy tetszőleges $(v_1, v_2, \ldots, v_{n-2})$ sorozatból a fenti módszer szerint konstruált F gráf olyan fa, aminek Prüfer-kódja éppen $(v_1, v_2, \ldots, v_{n-2})$.

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

3.40. Megfigyelés *(1) $w_1, w_2, \ldots, w_{n-1}, n$ különbözők. (Hisz w_j választásakor w_i tiltott ha $i < j$.)*
(2) $v_k \notin \{w_1, w_2, \ldots, w_k\}$ (w_i választásakor $i \leq k$-ra $w_i \neq v_k$) , így $v_k \in \{w_{k+1}, w_{k+2}, \ldots, w_{n-1}, n\}$.□

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

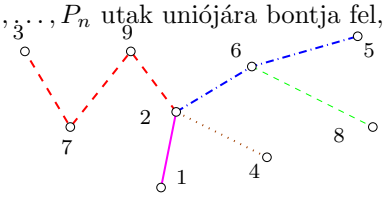
$$L(F'_{k+1}) = \{w_{k+1}, \ldots, w_{n-1}, n\} \setminus \{v_{k+1}, \ldots, v_{n-1}\} = \{1, 2, \ldots, n\} \setminus (\{w_1, w_2, \ldots, w_k\} \cup \{v_{k+1}, \ldots, v_{n-1}\}) .$$

Világos, hogy $L(F'_k) = (L(F'_{k+1}) \setminus \{v_k\}) \cup \{w_k\} = \{1, 2, \ldots, n\} \setminus (\{w_1, w_2, \ldots, w_{k-1}\} \cup \{v_k, v_{k+1}, \ldots, v_{n-1}\})$, és az F_k Prüfer-kódjára vonatkozó megfigyelés szerint w_k-t éppen e halmaz legkisebb eleme. □

3.41. 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 valamivel közvetlenebbül látszik a kölcsönösen egyértelmű megfeleltetés a fák és az azokat leíró ismétléses variációk között, továbbá, hogy a fa rekonstrukciója a kód alapján valamivel egyszerűbb.

Cayley tételének unortodox bizonyítása. 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 egyértelmű 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 különbözők.



$P_1 = \{1\}$, $P_2 = \{\mathbf{1}, 2\}$, $P_3 = \{\mathbf{2}, \mathbf{9}, \mathbf{7}, 3\}$
$P_4 = \{\mathbf{2}, 4\}$, $P_5 = \{\mathbf{2}, \mathbf{6}, 5\}$, $P_6 = \{6\}$
$P_7 = \{7\}$, $P_8 = \{\mathbf{6}, 8\}$, $P_9 = \{9\}$
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 ráádásul $n-1$ számból áll, hiszen minden P_i út kódja megegyezik P_i éleinek számával, tehát az F fa Refürp-kódja is épp olyan hosszú, mint ahány éle van F-nek.

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

Azt kell csupán igazolni, hogy ha $1 = r(1), r(2), r(3), \ldots, r(n-1)$ 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. (Ha P_3 egypontú, akkor itt P_3 helyett az első, nem egypontú P_i útról van szó, hiszen annak a kódja kezdődik $r(i+1)$-gyel.) 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 $P_2, P_3, \dots P_{i+1}$ utak valamelyikének kódjában már szerepelt korábban. Ezért $s+1$ olyan szám, amire

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

teljesül. Világos, hogy ha $s+1$-re a 3.1 reláció fennáll, akkor $r(s+1)$ nem lehet benne P_{i+1} kódjában, tehát $s+1$ a legkisebb olyan szám, ami teljesíti a 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 rekonstruálhatók, 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 $r(1), r(2), r(3), \dots, r(n-1)$. □

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 $i+1 \leq n-1$ 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.

3.42. 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. Kruskal algoritmusa

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

Formálisan: Adott $G = (V, E)$ lehetséges utak összefüggő gráfja és a $k : E \to \mathbb{R}_+$ költségfv. Egy $F \subseteq E$ élhalmaz *költsége* $k(F) := \sum_{f \in F} k(f)$. Feladat: keressünk egy olyan $F \subseteq E$ élhamazt, amire (V, F) fa, és ezen belül $k(F)$ minimális. Az ilyen (V, F) fát *minimális költségű feszítőfának* nevezzük. Az alábbiakban mutatunk egy, a feladatot megoldó algoritmust. Akárcsak a későbbiekben, az algoritmust az input, output és a működés pontos leírásával adjuk meg.

Kruskal algoritmusa:
Input: $G = (V, E)$ összefüggő gráf, $k : E \to \mathbb{R}_+$ költségfv.
Output: A G gráf egy $F = F_m$ min. ktg-ű feszítőfája.
Az algoritmus működése:

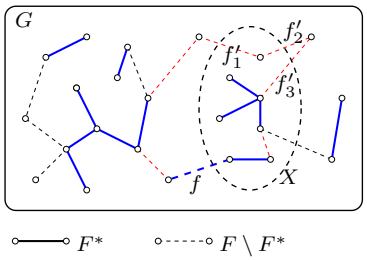
Legyen $E = \{e_1, e_2, \ldots, e_m\}$, növekvő költség szerint sorbarendezve (azaz $k(e_1) \leq k(e_2) \leq \ldots \leq k(e_m)$) és legyen $F_0 := \emptyset$. Sorban minden e_i-ről eldöntjük, hogy bevesszük-e az F_i élhalmazba: ha F_{i-1} az e_i él hozzávételével körmentes marad, akkor $F_i := F_{i-1}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

Kruskal fenti algoritmusát hívják néha *mohó algoritmusnak* is, mert a feszítőfát mohó módon építjük: csak azzal törődünk, hogy mindig a legolcsóbbat válasszuk, már persze amennyiben ez a választás nem értelmetlen. A továbbiakban igazoljuk a Kruskal algoritmus helyességét, vagyis azt, hogy ez a „rövidlátó" hozzáállás (legalábbis ebben az esetben) a lehető legjobb eredményre vezet.

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

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

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



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

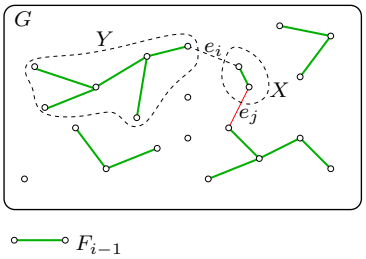
3.45. Tétel *A Kruskal algoritmus konstruálta (V, F) a G gráf egy minimális költségű feszítőfája.*

Bizonyítás. Az F felépítésekor sosem hoztunk létre kört, ezért F körmentes. A (V, F) gráfba bármely $e_j \in E \setminus F$-beli élt behúzva kört kapunk, hiszen e_j-t már az F_{j-1}-be behúzva is kör keletkezett. Eszerint tetszőleges e_j él végpontjai (V, F)-nek ugyanabban

a komponensében vannak. Mivel G összefüggő, ezért (V, F) is összefüggő, tehát a Kruskal algoritmus csakugyan feszítőfát konstruál.

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

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



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

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

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

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

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

Bemutatjuk a Kruskal algoritmusnak egy másik, gyakorlati alkalmazását is, ami többek között a Jelek és rendszerek tárgyhoz kapcsolódik. Tekintsünk egy villamos hálózatot, amely kizárólag kétpólusú áramköri elemeket tartalmaz (azaz feszültségforrást, áramforrást, ellenállást, esetleg tekercset vagy kondenzátort). Egy ilyen hálózathoz tartozik egy gráf, amelyben az élek az egyes áramköri elemeknek felelnek meg. „Visszafelé” is működik a kapcsolat, azaz tetszőleges véges irányított gráf éleihez tetszés szerinti áramköri elemeket rendelve egy hálózatot kapunk. Ha egy ilyen hálózatot csakugyan megépítenénk, akkor azt, hogy abban mi történik, azt különféle fizikai törvények, mint

például a Kirchhoff-féle hurok- és csomóponti törvények ill. az Ohm törvény írják le. Egy hálózatot akkor nevezünk *egyértelműen megoldhatónak*, ha ezekből a törvényekből a hálózat bármely élén meghatározható az ott folyó áramerősség és bármely két csúcs között a potenciálkülönbség.

Az egyértelmű megoldhatóságnak például szükséges feltétele, hogy a gráfban ne legyen olyan kör, aminek a mentén kizárólag feszültségforrások vannak. Ebben az esetben ugyanis ha az feszültségforrások feszültségeinak előjeles összege a kör mentén nem nulla, akkor sérül a huroktörvény, ezért nem képes az összes feszültségforrás egyszerre megfelelően működni, tehát egyáltalán nem lenne megoldható a hálózat.

Abban az esetben viszont, ha egy csupa feszültségforrást tartalmazó kör mentén a feszültségkülönbségek előjeles összege nulla lenne, akkor éppenséggel lehetséges, hogy megoldható a hálózat, ám a megoldás nem egyértelmű: egy tetszőleges megoldásból kiindulva és a kör mentén tetszőleges áramot még körbeküldve egy másik, különböző megoldást kapunk.

Hasonló a helyzet az áramforrásokkal. Ha néhány áramforrás elhagyásától a gráfunk komponenseinek száma megnő (más szóval a hálózat szétesik), azaz, ha az áramforrások alkotta élekből található vágás a gráfban (ld. a 3.134. Definíciót), akkor szintén nem lehet a hálózat egyértelműen megoldható. Tegyük fel ugyanis, hogy a hálózat diszjunkt X és Y ponthalmazai között futó minden él áramforrás. Ha most mindezen éleken az áramok előjeles összege nem nulla, akkor a nem létezhet megoldás, hisz sérül a csomóponti törvény. Ha pedig nulla az aramok előjeles összege, akkor még ha van is megoldás, nem lehet egyértelmű, mert az X és Y közti potenciálkülönbség bármi lehet.

A fentieket úgy fogalmazhatjuk, hogy az egyértelmű megoldhatóságnak szükséges feltétele, hogy a feszültségforrásoknak megfelelő élek körmentes, az áramforrásoknak megfelelők pedig vágásmentes élhalmazt alkossanak a hálózatot leíró G gráfban. Kiderül, hogy ennek a feltételnek a teljesülése egyúttal elégséges is az egyértelmű megoldhatósághoz. Azt mondhatjuk tehát, hogy a hálózat pontosan akkor egyértelmű megoldható, ha található benne az alább definiált normális fa.

3.47. Definíció *Tegyük fel, hogy egy összefüggő G gráf éleit 5 lehteséges kategóriába soroltuk: minden egyes él vagy feszültségforrás, vagy áramforrás, vagy ellenállás, vagy kondenzátor vagy pedig tekercs (és pontosan az egyik). A G gráf F feszítőfáját ekkor a G* normális fájának *nevezzük, ha F tartalmaz minden feszültségforrást és nem tartalmaz egyetlen áramforrást sem, továbbá az ilyen tulajdonságú feszítőfák között F olyan, ami a lehető legtöbb kondenzátort és a lehető legkevesebb tekercset tartalmazza.*

A definícióban a tekercs-kondenzátor feltétel jelentősége az, hogy a hálózatot leíró differenciálegyenletrendszer rendje nem más, mint a normális fában található tekercsek és a komplementerében található kondenzátorok számának összege. Az alábbi alkalmazás mutatja, hogyan lehet normális fát keresésni a Kruskal algoritmus segítségéel.

3.48. Alkalmazás *Tegyük fel, hogy G egy kizárólag kétpólusú áramköri elemeket tartalmazó hálózathoz tartozó gráf. Legyen a feszültségforrások költsége* 1*, a kondenzátoroké* 2*, az ellenállásoké* 3*, a tekercseké* 4*, végül az áramforrásoké pedig* 5*. Legyen továbbá F a G egy minimális költségű feszítőfája (amit például a Kruskal algoritmus szolgáltat). Ekkor ha F tartalmaz minden feszültségforrást de nem tartalmaz egyetlen áramforrást sem, akkor F normális fa. Ha azonban F tartalmaz áramforrást vagy F-en kívül van feszültségforrás, akkor G-nek nincs normális fája, és a hálózat nem oldható meg egyértelműen.*

3.3. Euler és Hamilton bejárások

3.3.1. Gráfok éleinek bejárása

3.49. Definíció *A $G = (V, E)$ gráf* Euler-sétája (Euler-körsétája) *a G gráf egy olyan (kör)sétája, amely G minden élét (pontosan egyszer) tartalmazza.*

Bevett elnevezés az Euler-séta és Euler-körséta helyett az Euler-út ill. Euler-kör, még ha nem út ill. kör is az, amiről beszélünk. Voltaképpen a G gráf éleinek olyan bejárásáról van szó, melyben minden élt pontosan egyszer érintünk. Ez a rejtvényújságokban szokásos, „rajzoljuk le egy vonallal, a ceruza felemelése nélkül" típusú fejtörő absztrakt változata: ha a lerajzolandó ábrát egy (síkbarajzolt) gráf diagramjának tekintjük, melynek csúcsai az ábra csomópontjai, élei pedig a csomópontok között futó ívek, akkor pontosan abban az esetben oldható meg a feladvány, ha létezik az említett gráfnak Euler-sétája.

A gráfelmélet születését a „Königsbergi hidak problémájának" megoldásához szokás kötni. Történt ugyanis, hogy 1736-ban Leonard Euler megválaszolta városa, a porosz Königsberg polgárait izgalomban tartó kérdést, miszerint miért nem sikerül száraz lábbal olyan sétát tenniük, melyben a Pregolia folyó hét hídjának mindegyikén pontosan egyszer haladnak át, és mindeközben vízijárművet nem vesznek igénybe.

Euler megfigyelte, hogy az egyes szárazföldeket csúcsoknak, a hidakat pedig közöttük futó éleknek tekintve éppen egy minden élt pontosan egyszer tartalmazó élsorozat létezése a kérdés. A konkrét esetben pedig nem teljesül az alább következő szükséges feltétel.

3.50. Állítás *Ha a véges G gráfnak létezik Euler-körsétája, akkor G minden csúcsának páros a fokszáma. Ha G-ben létezik Euler-séta, akkor G-nek* 0 *vagy* 2 *páratlan fokú csúcsa van.*

3.51. Megjegyzés *Jegyezzük meg, hogy Königsberg mai neve Kalinyingrád, és a Kalinyingrádi Orosz Exklávé székhelye. Az exklávé annyit tesz, mint Oroszország olyan összefüggő komponense, ami nem tartalmazza Moszkvát. Szomszédai Litvánia és Lengyelország, így 2004 óta az EU veszi körül Oroszország egy részét. Kalinyingrád stratégiai jelentősége abból fakad, hogy ez az Orosz Föderáció egyetlen fagymentes balti tengeri kikötője, a szovjet balti flotta korábbi állomáshelye.*

Königsberg tehát a gráfelmélet bölcsőjének tekinthető. A matematika szempontjából azonban nemcsak emiatt fontos, hiszen szülötte volt a számelmélész Christian Goldbach (akinek sejtésére később térünk

ki), a geométer David Hilbert de a számelmélettől a Fourier-analízisig számos területet művelő Rudolf Lipschitz és még sokan mások is. A város a korabeli szellemi életnek szintén az egyik központja volt: innen származik például a filozófus Immanuel Kant és a fizikus Gustav Kirchhoff, utóbbiról szintén szó lesz nemsokára.

Eulerről egy érdekes tény még, hogy ha a ma kombinatorikával foglalkozó matematikusoknál megvizsgáljuk ki volt a doktori témavezetőjének a doktori témavezetőjének a ... stb, akkor az esetek jelentős részében Leonard Eulerig jutunk: a jelen jegyzet szerzője is az ő köbükunokája. A hidakra visszatérve említést érdemel még, hogy a jelenlegi hidak közül már csak kettő emlékeztet a korabeliekre. Egy hidat a németek 1935-ben építették újjá, míg kettőt a Brit hadsereg bombázott le a történelmi városközpont megsemmisítésekor, 1944 augusztusában. Később, a szovjet időkben további két hidat váltottak ki újakkal.

A 3.50. Állítás bizonyítása. A séta éleit az azokon való áthaladás szerint irányítva minden v csúcs befoka (azaz a v-be befutó élek száma) azonos lesz v kifokával (azaz a v-ből kiinduló élek számával), kivéve esetleg az első és utolsó csúcsot. A v csúcs fokszáma pedig a kifoka és befoka összege, tehát ha ezek egyenlők, akkor $d(v)$ feltétlenül páros. □

Az iménti szükséges feltételnek az értelmes megfordítása is igaz.

3.52. Tétel *Ha a $G = (V, E)$ gráf véges és összefüggő, akkor*

1. G-nek pontosan akkor van Euler-körsétája, ha G minden csúcsa páros fokú, ill.

2. G-nek pontosan akkor van Euler-sétája, ha G-nek 0 vagy 2 páratlan fokú csúcsa van.

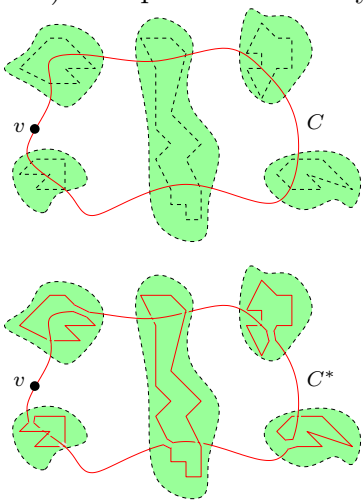
3.53. Megjegyzések *1. A 3.52. Tétel 2. részéről érdemes végiggondolni, mi van akkor, ha a G gráfnak pontosan egy páratlan fokú csúcsa van.*
2. Az egyik első gráfelmélettel foglalkozó könyvben a tétel első része így szerepel: Egy véges G gráfnak akkor és csak akkor van Euler-körsétája, ha G összefüggő és minden foka páros. Tanulságos meggondolni, miért is nem igaz ez az állítás.

Bizonyítás. A 3.52. Tétel bizonyítása 1.: A szükségesség a fenti megfigyelésből következik. Az elégségességet G élszáma szerinti indukcióval bizonyítjuk. 0 élű gráfokra a tétel nyilvánvalóan igaz. Tegyük fel, hogy m-nél kevesebb élű gráfokra a tételt már bebizonyítottuk, és legyen G-nek m éle.

G-ben létezik egy C kör, mert minden fokszám legalább kettő: ha elindulunk G egy tetszőleges csúcsából, és mindig csatlakozó éleken lépünk tovább, akkor egyszer egy korábban érintett v csúcsba kell jutnunk, hisz elsőfokú pont híján sosem akadhatunk el. A v csúcs két érintése között pedig éppen egy kört jártunk be.

Tekintsük a $G' = G - C$ gráfot, mely C éleinek törlésével keletkezik G-ből. G' minden egyes komponense véges, összefüggő, m-nél kevesebb élt tartalmaz, és minden fokszáma páros, ezért az indukciós feltevés miatt minden komponensnek van Euler-körsétája. A G gráf C^* Euler-körsétáját úgy kapjuk, hogy a C kör v csúcsából indulva C élein haladunk végig, azonban mikor egy nemtriviális komponensbe érkezünk, akkor az adott komponens Euler-körsétája szerint haladunk tovább, majd miután azzal végeztünk, folytatjuk a C kör bejárását. (Itt felhasználtuk, hogy ha egy komponensnek van Euler-körsétája, akkor

van olyan Euler-körsétája is, aminek kezdő- (és így végpontja) a komponens egy adott csúcsa.) A kapott élsorozat nyilván G Euler-körsétája lesz.

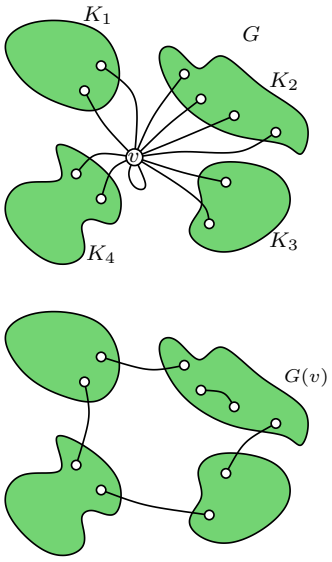


2.: Ha G minden csúcsának foka ps, akkor 1. miatt létezik Euler-körséta, ami egyúttal Euler-séta is. Egyébként húzzunk be G ptn fokú csúcsai között egy új e^* élt. (Ha már volt él e két csúcs között, akkor húzzunk be egy ezzel párhuzamosat.) 1. miatt a keletkező G' gráfnak létezik Euler-körsétája, feltehetjük, hogy ennek e^* az utolsó éle. Az e^* él Euler-körsétából való törlésekor pedig éppen G egy Euler-sétáját kapjuk.

Megadunk a 3.52. Tétel első részének az elégségességére egy másik lehetséges bizonyítást.

Második bizonyítás a 3.52. Tétel első részére. A G gráf csúcsainak számára vonatkozó teljes indukcióval bizonyítunk. Ha G-nek egyetlen csúcsa van, akkor G-nek csak hurokélei lehetnek; ezek pedig tetszőleges sorrendben felsorolva egy Euler-körsétát alkotnak. Tegyük fel tehát, hogy az $n-1$ csúcsú gráfokra már tudjuk az állítást, és legyen G-nek n csúcsa, ezek egyike legyen v. Legyenek $K_1, K_2, \dots K_s$ a $G-v$ gráf komponensei. Állítjuk, hogy v-ből legalább két él vezet mindegyik K_i-be. Mivel G összefüggő, ezért v és K_i közt van él. Ha tekintjük a v és K_i által feszített $G[K_i+v]$ részgráfot, akkor ez minden K_i-beli végponttal rendelkező élt tartalmaz, ezért $G[K_i+v]$ minden K_i-beli pontjának fokszáma páros. A $G[K_i+v]$ gráf fokszámösszege azonban csak úgy lehet páros, ha v foka is páros, ami eszerint legalább 2.

Azt kaptuk tehát, hogy v-ből $G-v$ minden komponensébe legalább két él vezet. Most végezzük el a következő átalakításokat. Hagyjuk el a v-re illeszkedő hurokéleket. Rendezzük párokba a v-ből induló (nem hurok)éleket, és ha vu, vw egy ilyen élpár, akkor helyettesítsünk azokat egy uw éllel. Arra kell azonban ügyelnünk, hogy az élek párosítását úgy végezzük el, hogy minden K_i-re legyen olyan vu, vw élpár, hogy u a K_i, w pedig a K_{i+1} pontja (ahol $K_{s+1} = K_1$). Hagyjuk el ezután a v csúcsot. A keletkező $G(v)$ gráf összefüggő lesz (hisz a K_i komponenseken „körbe" lehet menni. Ráadásul $G(v)$-nek $n-1$ csúcsa van, és $G(v)$-ben minden csúcs foka megegyezik az adott csúcs G-beli fokával, tehát páros. Az indukciós feltevés szerint tehát létezik $G(v)$-nek Euler körsétája. Ebből úgy kapjuk meg G egy Euler körsétáját, hogy minden alkalommal, amikor $G(v)$ egy újonnan bevezetett élén haladunk végig, olyankor e helyett a megfelelő két élt járjuk be, és áthaladunk v-n, majd a körséta végére biggyesztjük a v-beli hurokélek bejárását. Ez pedig azt jelenti, hogy G-nek létezik Euler körsétája, azaz igazoltuk az indukciós lépést.



□

A fenti tétel bár irányítatlan gráfokról szólt, irányított gráfokra is hasonló eredmény mondható ki. Az Euler-séta ill. körséta irányított változata a definíció értelemszerű módosításával kapható meg, és a páros fokszámokra vonatkozó állítás irányított az alábbiak szerint módosul.

3.54. Állítás *Ha a véges, irányított G gráfnak létezik Euler-körsétája, akkor G minden csúcsának ugyanannyi a befoka mint a kifoka, azaz tetszőleges v csúcsra igaz, hogy a v-be befutó élek száma megegyezik a v-ből kiinduló élek számával. Ha Euler-sétája van G-nek, akkor lehet két kivételes csúcs: az egyikben a befok egyel több a kifoknál, a másiknál a kifok nagyobb a befoknál eggyel.*

A bizonyítás az irányítatlan bizonyítás értelemszerű módosítása. A 3.54. Állítás alábbi megfordítása szintén teljesül.

3.55. Tétel *Ha a $G = (V, E)$ irányított gráf véges és irányítatlan értelemben összefüggő, akkor*

1. G-nek pontosan akkor van Euler-körsétája, ha G minden csúcsába ugyanannyi él fut be, mint ahány onnan kilép, ill.

2. G-nek pontosan akkor van Euler-sétája, ha G-be behúzható legfeljebb egy irányított él úgy, hogy a kapott gráf rendelkezzen az 1. pontban megfogalmazott tulajdonsággal.

Bármelyik fent közölt bizonyítás értelemszerű módosítása igazolja a fenti tételt. Ez az irányított változat később a Menger tételnél lesz hasznunkra. Jegyezzük meg azt is, hogy sem az irányítatlan, sem pedig az irányított változatnál nem kellett feltenni a szóbanforgó gráf egyszerűségét: az elmondott bizonyítások működnek párhuzamos és hurokélek megléte esetén is. (A második bizonyítás lényegesen támaszkodott is erre.)

E szakasz végén egy jól ismert feladat kapcsán mutatunk példát az Euler-bejárások egy kevéssé ismert alkalmazására. Erdős Pál, az egyik legnagyobb hatású magyar matematikus számos mondásáról volt közismert, ezek egyike szerint valahol odafenn, a „legfőbb fasisztánál” (ami ebben a nyelvezetben a teremtő megnevezése) ott van a „Könyv”, amiben a világ minden tételére megtalálható a létező legelegánsabb bizonyítás. Igen ritkán, egy-egy frappáns bizonyítás megtalálásakor mi is bepillanthatunk ebbe a „Könyvbe”. (Erdős elmélete nyitott volt az ateisták felé is, hisz —mint azt egyszer kifejtette— nem szükséges hinni a legfőbb fasisztában ahhoz, hogy meg legyünk győződve a „Könyv” létezéséről.) Erdős 1996-os halála után nem sokkal ki is adták a Proofs from THE BOOK c. kötetet, ami számos olyan bizonyítást tartalmazott, amielyekről a szerzők szerint maga Erdős is elismerte volna, hogy a „Könyvből” valók. Nos, ebben a kötetben szerepel az alábbi állítás.

3.56. Alkalmazás *Ha egy T téglalap kiparkettázható a $T_1, T_2, \ldots, T_n$ téglalapokkal úgy, hogy minden T_i téglalapnak van egész hosszúságú oldala, akkor T-nek is van egész hosszúságú oldala.*

A kötet számos bizonyítást közöl (némileg ellentmondva Erdős koncepciójának). Az alább közölt, az ott szereplőnél valamivel egyszerűbb gondolatmenet Fleiner Balázstól származik.

Bizonyítás. Feltehetjük, hogy a T téglalap egyik csúcsa a koordinátarendszer origója és T oldalai párhuzamosak a koordinátatengelyekkel. Tekintsük a kiparkettázott T téglalapot és válasszuk ki minden T_i téglalapnak két egész hosszúságú, párhuzamos oldalát. (Ha valamelyik T_i-nek mind a négy oldala egész hosszúságú, akkor tetszőlegesen választunk a két lehetőség közül.) Legyen G az a gráf, aminek csúcsai a T_i téglalapok csúcsai, és minden T_i-nek pontosan két él fog megfelelni, mégpedig azok, amelyeket a kiválasztott egész oldalak meghatároznak. (Tehát G-ben lehetnek párhuzamos élek is.)

Vegyük észre, hogy G minden csúcsának 2 vagy 4 a fokszáma, kivéve a T téglalap A, B, C, D csúcsainak megfelelő négy elsőfokú csúcsot. Húzzuk be G-be az AB és CD éleket. Az így kapott G' gráf minden csúcsának páros lesz a fokszáma, ezért G'-nek az A-t tartalmazó komponensének lesz Euler-körsétája. Hagyjuk el a körsétából az AB élt, ekkor egy A-ból B-be vezető séta marad. Ha ez a séta tartalmazza a CD élt, akkor hagyjuk el azt is: ezáltal az AB séta ugyan két sétára esik szét, de mindkét séta végpontjai a T téglalap csúcsai lesznek.

Így vagy úgy, de találunk olyan G-beli sétát, ami a T téglalap két csúcsát köti össze. Mivel egy ilyen sétában mindig vízszintesen vagy függőlegesen lépünk és mindig egész távolságot, ezért T e két csúcsának koordinátái egész számban különböznek egymástól, tehát van a T téglalapnak egész hosszúságú oldala.□

Éredekes összevetni a fenti bizonyítást az alábbi, gráfelméletet egyáltalán nem használó megoldással.

A 3.56. Tétel második bizonyítása. Ismét feltesszük, hogy a T téglalap oldalai vízszintesek és függőlegesek a koordinátarendszerben. Fessük a síkot pepitára, azaz tekintsük a síknak egy $\frac{1}{2} \times \frac{1}{2}$ méretű négyzetekkel való parkettázását, és fessük ki a kis négyzeteket sakktáblaszerűen feketére és fehérre. Nem nehéz belátni, hogy egy vízszintes és függőleges oldalakkal rendelkező T' téglalapnak pontosan akkor van egész hosszúságú oldala, ha bárhogyan is toljuk el T'-t a síkon, T' területének pontosan a fele lesz fehér és pontosan a fele fekete.

Ha tehát T bármely eltoltját kiparkettáztuk a T_i téglalapokkal, akkor a megfigyelésünk miatt minden T_i-nek pontosan a fele lesz feketére festve. Ez tehát a kiparkettázott T-re is igaz, így a fenti megfigyelés miatt T-nek is van egész hosszúságú oldala, és nekünk pontosan ezt kellett igazolnunk. □

A fenti bizonyításhoz nem szükséges a T téglalap összes eltoltjáról belátni azt, hogy a pepitaszínezés a felét festi feketére, elegendő mindössze azt az eltoltat vizsgálni, amelynek (mondjuk) bal alsó csúcsa rácspont.

Bár a második megoldás legalább olyan elegáns, mint az elsőnek közölt, arra még úgy sem könnyű rájönni, ha az ember kifejezetten az ilyen feladatoknál szokásos színezéses invariánst keresi. Ami viszont az igazán izgalmas a dologban, hogy egymástól látszólag egészen távoli módszerek képesek ugyanannak a jelenségnek az okára rávilágítani.

3.3.2. Gráfok csúcsainak bejárása

Ha élek helyett csúcsokról beszélünk, akkor egy másik fontos fogalomhoz jutunk.

3.57. Definíció *A G gráf* Hamilton-köre (Hamilton-útja) *a G olyan köre (útja), mely G minden csúcsát tartalmazza.*

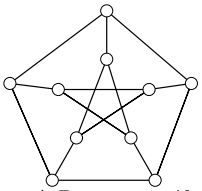
Mivel egy körben (útban) szereplő minden csúcs különböző, ezért a Hamilton-kör (Hamilton-út) a G gráf olyan bejárása, mely G minden csúcsát *pontosan* egyszer érinti.

3.58. Állítás *Ha a véges G gráfban létezik Hamilton-kör (ill. Hamilton-út), akkor G-nek k tetszőleges pontját törölve, a keletkező gráfnak legfeljebb k (ill. $k+1$) komponense van.*

Bizonyítás. Ha a G gráf maga egy Hamilton-kör (Hamilton-út), akkor az állítás világos. Ha G-nek további élei is vannak, akkor a pontok törlése után keletkező komponensek száma csak csökkenhet. □

A fenti állítás szereplő feltétel szükséges, ám nem elégséges. A Petersen-gráfnak nincs Hamilton-köre, noha teljesíti a feltételt. Ha volna Hamilton-köre, akkor 3 színnel színezhetnénk az éleit úgy, hogy az azonos színű élek páronként diszjunktak legyenek. (A Hamilton-kör 10 élére kell 2 szín, a kimaradó élek pedig diszjunktak, mivel a Petersen-gráf 3-reguláris.) Márpedig a külső ötszög és a hozzá csatlakozó élek 3-színezése (a szimmetria miatt) lényegében egyértelmű, és ez nem terjeszthető ki globális 3-színezéssé.

Ha a Petersen-gráf külső köréből a, belső köréből pedig b csúcsot hagyunk el, akkor a külső ill. belső körön keletkező komponensek száma legfeljebb a ill. b, vagyis a gráfnak nem keletkezhet összességében $a+b$-nél több komponense.



A Petersen-gráf

Vannak azonban jól használható, elégséges feltételek is Hamilton-kör létezésére.

3.59. Tétel (Dirac tétele) *Ha az n pontú ($n \geq 3$), egyszerű G gráf minden pontjának foka legalább $\frac{n}{2}$, akkor G-nek van Hamilton-köre.*

3.60. Tétel (Ore tétele) *Ha az n pontú ($n \geq 3$), egyszerű G gráf olyan, hogy $uv \notin E(G)$ esetén $d(u) + d(v) \geq n$ (azaz összekötetlen csúcsok fokszámösszege legalább n), akkor G-nek létezik Hamilton-köre.*

Ha egy gráfra teljesül a Dirac feltétel, akkor teljesül rá az Ore is. Ezért a Dirac tétel következik az Ore tételből.

3.61. Tétel (Pósa tétele:) *Ha az n pontú ($n \geq 3$), egyszerű G gráf fokszámai $d_1 \leq d_2 \leq \ldots \leq d_n$, és minden $k < \frac{n}{2}$ esetén $d_k \geq k+1$, akkor G-nek létezik Hamilton-köre.*

3.62. Állítás *Ha egy gráfra teljesül az Ore feltétel, akkor teljesül rá a Pósa is. Ezért az Ore tétel következik a Pósa tételből.*

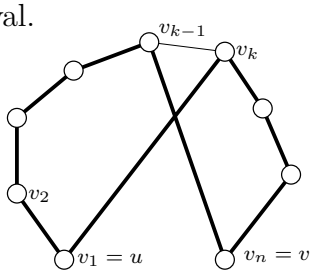
Bizonyítás. Indirekt bizonyítunk: tegyük fel, hogy teljesül az Ore feltétel, de a Pósa feltétel nem. Legyen $d_k \leq k$ valamely $1 \leq k < \frac{n}{2}$-re, és legyen U a k legkisebb fokú pont halmaza. Bármely U-beli pont fokszáma legfeljebb k, így bármely két U-beli pont fokszámösszege kisebb, mint n, ezért az Ore feltétel miatt U teljes gráfot feszít. Minden U-beli pontból tehát $k-1$ él indul U-beli ponthoz, ezért legfeljebb 1 él indulhat U-n kívülre. $k < \frac{n}{2}$ miatt létezik tehát $V(G) \setminus U$-nak olyan v pontja, mely U egyetlen pontjával sincs összekötve. Ekkor tetszőleges $u \in U$ csúcsra u és v fokszámösszege legfeljebb $k + (n-k-1) = n-1$, ami ellentmond az Ore feltételnek. □

3.63. Tétel (Chvátal tétele) *Legyen G n pontú ($n \geq 3$), egyszerű gráf, melynek fokszámai $d_1 \leq d_2 \leq \ldots \leq d_n$. Tegyük fel, hogy minden olyan $k < \frac{n}{2}$-re, melyre $d_k \leq k$ teljesül, fennáll a $d_{n-k} \geq n-k$ egyenlőtlenség. Ekkor G-nek létezik Hamilton-köre.*

Másrészt, ha egy $d_1 \leq d_2 \leq \ldots \leq d_n$ sorozatra nem teljesül az előző feltétel, akkor van olyan G' gráf, aminek nincs Hamilton-köre, és fokszámainak $d'_1 \leq d'_2 \leq \ldots \leq d'_n$ sorozatára $d_i \leq d'_i$ $\forall i = 1, 2, \ldots, n$ áll fenn.

Könnyen látható, hogy ha egy gráfra teljesül a Pósa feltétel, akkor teljesül rá a Chvátal is. Ezért a Pósa tétel következik az Chvátal tételből.

A 3.60. Tétel bizonyítása. Legyen G egy ellenpélda a tételre. Mivel új élek behúzása nem rontja el az Ore-tulajdonságot, feltehetjük, hogy G-ben bármely új él behúzása létrehoz egy Hamilton-kört, azaz G bármely két összekötetlen pontja között vezet Hamilton-út. Ha tehát u és v nem szomszédosak, akkor létezik egy P Hamilton-út u-ból v-be, feltehetjük, hogy ez az út az $u = v_1, v_2, v_3, \ldots, v_n = v$ sorrendben tartalmazza G csúcsait. Ha most $v_1 v_k$ a G gráf éle, akkor $v_{k-1} v_n$ nem lehet G éle, mert $v_1, v_2, \ldots, v_{k-1}, v_n, v_{n-1}, v_{n-2}, \ldots, v_k, v_1$ egy Hamilton-kör lenne, ellentétben G választásával.



Ha tehát v_1 szomszédai a $v_{i_1}, v_{i_2}, \ldots, v_{i_m}$ csúcsok, akkor v_n-nek nem lehet szomszédja a $v_{i_1-1}, v_{i_2-1}, \ldots, v_{i_m-1}$ csúcsok egyike sem, azaz v_n szomszédainak száma legfeljebb $n-1-m$ lesz, vagyis $d(v_1) + d(v_n) \leq m + n - 1 - m = n - 1 < n$, ellentmondás. □

A 3.63. Tétel bizonyítása. Feltehetjük, hogy G csúcsai az $1, 2, \ldots n$ pontok, és $d(1) \leq d(2) \leq \ldots \leq d(n)$. Indirekt bizonyítunk, legyen G egy ellenpélda a tételre. Mivel új élek behúzása nem rontja el a Chvátal-tulajdonságot, feltehetjük, hogy G-ben bármely új él behúzása létrehoz egy Hamilton-kört, azaz G bármely két összekötetlen pontja között

vezet Hamilton-út. Ha tehát k és l nem szomszédosak, akkor az P_{kl} Hamilton-úton a k szomszédait megelőző pontok V_{kl} halmazából nem futhat él l-be, mert akkor lenne G-ben Hamilton-kör. Ezért (figyelembe véve, hogy $k \in V_{kl}$) $d(k)+d(l) \leq d(k)+(n-1)-d(k) = n-1$ teljesül. (Ez idáig az Ore tétel bizonyítása.)

Válasszuk most a nem szomszédos k, l pontokat úgy, hogy $d(k) + d(l)$ maximális legyen. Feltehető, hogy $k < l$. (Világos, hogy $d(k) \leq \frac{1}{2}(d(k) + d(l)) \leq \frac{n-1}{2} < \frac{n}{2}$.) Mivel nem V_{kl} pontjait választottuk k helyett, ezért $d(i) \leq d(k)$ áll minden $i \in V_{kl}$-re. Eszerint $d(d(k)) \leq d(k)$, így a Chvátal feltétel miatt $d(n - d(k)) \geq n - d(k)$ áll, vagyis G-nek legalább $d(k) + 1$ olyan pontja van, mely legalább $n - d(k)$-fokú. $d(k) < \frac{n}{2}$ miatt van tehát e pontok között egy l', mely nem szomszédja k-nak, de ekkor $d(k) + d(l') \geq d(k) + n - d(k) = n > d(k) + d(l)$, ellentmondásban l választásával.

A tétel másik részéhez, ha csak a fokszámsorozat alapján kell megmondani, van-e biztosan Hamilton-kör a gráfban, akkor nem állíthatunk erősebbet a Chvátal tételnél. Tetszőleges $n \in \mathbb{N}$-re és tetszőleges $k < \frac{n}{2}$-re létezik ugyanis olyan n pontú, egyszerű gráf, melynek nincs Hamilton-köre, de k db k-adfokú, $(n - 2k)$ db $(n - k - 1)$-edfokú és k db $(n-1)$-edfokú pontja van. (Az innen adódó fokszámsorozat csak k-ra sérti meg a Chvátal feltételt. Bármely fokszám megnövelésével pedig teljesül a Chvátal feltétel.) Legyenek ugyanis az A, B, C ponthalmazok rendre k, k ill. $n-2k$ pontúak, húzzuk be C-n belül az összes élt, továbbá kössük össze B minden pontját az összes többi ponttal. A fokszámok a fentiek lesznek, de B elhagyásával $k + 1$ komponens keletkezik, nem található tehát a gráfban Hamilton-kör.

3.4. Gráfbejárások

Egy G gráf egy *bejárásán* a G csúcsainak valamilyen sorrendben történő végiglátogatását értjük. Az általános szabály, hogy minden v csúcsot lehetőleg úgy látogassunk meg először, hogy egy korábban már meglátogatott u csúcsból érkezzünk egy uv él mentén. (Azaz nem „húzhatunk elő a kalapból" új csúcsot mindaddig, míg korábban elért csúcsból tudunk bejáratlan csúcsba lépni.) A cél (értelemszerűen) a gráf összes csúcsának végiglátogatása. A fentiek alapján minden bejáráshoz tartozik egy *elérési sorrend*, azaz G csúcsainak egy sorrendje, aszerint hogy mikor láttuk *először* az adott csúcsot és egy *befejezési sorrend* is, ami azt írja le, hogy mikor foglalkoztunk utoljára az adott csúccsal. A bejárás során egy csúcsot vagy egy már korábban bejárt csúcsból odavezető él mentén értünk el, vagy csak úgy, a kalapból húztuk elő, mint ahogyan pl. azt a legelsőnek bejárt csúccsal tettük. Az előbbi típusú csúcsok mindegyikéhez egyértelműen tartozik egy (irányított) odavezető él, ami mentén először jutottunk el az adott csúcsba. Ezek az élek egy (irányítatlan értelemben) körmentes gráfot alkotnak, hiszen minden pontba legfeljebb egy ilyen él fut be, és egy él mindig korábban elért csúcsból vezet egy később elért csúcsba. Ezen élek tehát egy erdőt alkotnak. Ezt az erdőt (helytelenül) *bejárási*

fának nevezzük. A bejárási fa komponensei tehát olyan irányított fák, melyek élei a gyökértől kifelé vannak irányítva. A bejárás ismeretében G tetszőleges uv éle az alábbi 4 típus valamelyikéhez tartozik. Az uv élt *faélnek* mondjuk, ha uv a bejárási fa éle. Ha a bejárási fában u-ból v-be irányított út vezet (azaz u a v őse), akkor uv *előreél*. Ha v-ből u-ba vezet út a bejárási fában (azaz u a v leszármazottja), akkor uv *visszaél*. Végül pedig, ha u és v között nincs irányított út a fában (azaz u-nak és v-nek közös őse van vagy u és v a bejárási fa különböző komponenseibe esnek), akkor uv *keresztél*.

A fent elmondottak érvényesek irányított és irányítatlan gráfokra is, utóbbiban az előreél és a visszaél ugyanazt jelenti. A továbbiakban irányított gráfokkal foglalkozunk, ugyanis az irányítatlan gráfokra kimondható állítások innen egyszerűen megkaphatók, ha egy irányítatlan gráf minden élét egy oda-vissza mutató élpárral helyettesítjük. Két alapvetően fontos bejárási stratégiát fogunk közelebbről megvizsgálni. A mélységi bejárásnál mindig a legkésőbb bejárt csúcsból szeretnénk új csúcsba továbblépni, a szélességi bejárásban pedig a lehető legkorábban elért csúcsból próbáljuk megtenni ugyanezt.

A különféle szabályok szerint végrehajtott gráfbejárások számos esetben bizonyulnak hasznos eszköznek, például legrövidebb utak keresésénél, összefüggőség eldöntésénél vagy a komponensek meghatározásánál.

3.4.1. Legrövidebb utak

Értelmezhető egy gráf csúcsai között a távolság fogalma, ami különösen hasznos lehet gyakorlati alkalmazásokban.

3.64. Definíció *Ha u és v a G gráf csúcsai, akkor az u és v G-beli* távolsága *a legrövidebb u-ból v-be vezető G-beli út élszáma.*

A fenti definícióban nem határoztuk meg, hogy G irányított vagy irányítatlan. Utóbbi esetben, amikoris persze irányított utat kell a definícióban érteni, az a furcsaság is előfordulhat, hogy az u és v távolsága nem egyezik meg v és u távolságával, még csak az sem biztos, hogy mindkettő létezik. Annak ellenére, hogy a távolságfüggvény nem szimmetrikus, igaz rá az alábbi tulajdonság.

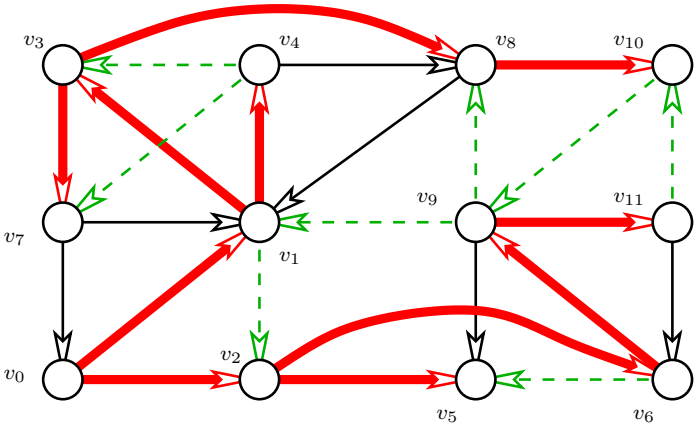
3.65. Megfigyelés *Ha a G gráfban P egy legrövidebb uv-út, és P' a P egy részútja (mondjuk x-ből y-ba), akkor P' a G egy legrövidebb xy-útja.*

Bizonyítás. Indirekt bizonyítunk. Ha lenne G-ben egy P'-nél kevesebb élt használó P'' út x-ből y-ba, akkor P-ben P'-t P''-vel helyettesítve a G egy P-nél kevesebb élből álló uv sétáját kapnánk. Márpedig a legrövidebb G-beli uv-út ennél a sétánál nem használhatna több élt, jóllehet P többet használ. Az ellentmondás a megfigyelést bizonyítja. □

Gyakran felmerülő probléma, hogy adott gráfban határozzuk meg két adott csúcs távolságát. Egy erre a célra is használható hatékony eljárás, a szélességi bejárás ismertetése a célunk.

A szélességi bejárás

A *szélességi bejárás* (angolul „breadth first search”, röviden BFS) a következő stratégia szerint történik. Kiindulunk egy v_0 gyökérből, és bejárjuk v_0 bejáratlan (ki-)szomszédait (azaz a v_0-ból irányított élen elérhető csúcsokat). Legyenek ezek a csúcsok $v_1, v_2, \ldots, v_k$. Ha már nem tudjuk v_0 több szomszédját bejárni, akkor bejárjuk v_1 *bejáratlan* szomszédait. Legyenek ezek $v_{k+1}, v_{k+2}, \ldots, v_{k+l}$. Ezután bejárjuk v_2 bejáratlan szomszédait, mint soron következő csúcsokat. Általában, ha már $v_0, v_1, \ldots v_{i-1}$ pont szomszédait bejártuk, és ezáltal a bejárt pontok halmaza $v_0, v_1, v_2, \ldots, v_p$, akkor bejárjuk v_i még bejáratlan szomszédait, és ezeket a bejárási sorrend végére biggyesztjük: $v_{p+1}, v_{p+2}, \ldots$. Ha már nem tudunk így több pontot bejárni, de még van bejáratlan pont, akkor választunk egy új gyökeret, és onnan kiindulva folytatjuk a fenti eljárást. (Az ábrán a faéleket vastag, a keresztéleket szaggatott, a visszaéleket pedig folytonossal nyíllal jelöltük.)



A G gráf éleinek a szélességi bejárás utáni osztályozásakor nem kaphatunk előreélt, hisz ha v_iv_j él $i < j$ esetén, akkor vagy még v_i szomszédainak megvizsgálása előtt eljutottunk v_j-be, (ekkor v_j nem leszármazottja v_i-nek), vagy legkésőbb v_i vizsgálatakor jártuk be v_j, amikoris v_iv_j faél.

A szélességi bejárással kapott *szélességi fa* (ami persze csak erdő) fontos tulajdonsága, hogy abban minden v_0-ból v_i-be vezető út egy legrövidebb (azaz lehető legkevesebb élből álló) v_0v_i-útja az *eredeti* G gráfnak. (Ezért a szélességi fát a legrövidebb utak fájának is szokták nevezni.) Ennél egy kicsit több is igaz.

3.66. Tétel *Ha a szélességi bejárásban kapott szélességi fában v_i-ből v_j-be irányított út vezet, akkor ez az út egyben a G gráf (egyik) legrövidebb uv-útja is.*

Bizonyítás. Elegendő bebizonyítani, hogy minden v_j-re a szélességi fa v_0v_j-útja a G gráf egy legrövidebb v_0v_j-útja, hisz ha v_i rajta van ezen az úton, akkor a legrövidebb utakra vonatkozó megfigyelés miatt a szélességi fa v_iv_j-útja is legrövidebb G-ben.

Jelölje V_t a G gráf v_0-tól t távolságra levő csúcsainak halmazát. (Világos, hogy $V_0 = \{v_0\}$, V_1 pedig v_0 (ki)szomszédainak halmaza.) Elegendő azt igazolnunk, hogy ha $v_i \in V_t$ és v_iv_j a szélességi fa éle, akkor $v_j \in V_{t+1}$, azaz a szélességi fa minden éle mentén egységnyit távolodunk a gyökértől (a G-ben mért távolság szerint). Hogyan működik

a szélességi bejárás? Először v_0-t járjuk be, majd a V_1-t alkotó szomszédait, és ennek során minden faél V_0-ból V_1-be vezet. Ezt követik a V_1-beli pontok eddig be nem járt szomszédai, azaz pontosan azok a pontok, amelyek V_2-t alkotják. Ennek során mindig V_1-ből V_2-be futó éleket veszünk a szélességi fába. Ezek után jönnek a V_2-beli pontok eddig be nem járt szomszédai, azaz a V_3-beli csúcsok, és így tovább. □

Ha tehát egy G gráfban szeretnénk egy adott u csúcsból egy másik v csúcsba megtalálni a legrövidebb utat, akkor nem kell mást tennünk, mint u-ból végrehajtani egy szélességi bejárást, és a kapott szélességi fában megkeresni az u gyökérből v be az utat. Az eljárás lépésszáma lényegében a szélességi bejárás lépésszámával egyezik meg, amit az alábbiak szerint lehet becsülni.

3.67. Tétel *A szélességi bejárás lépésszáma $O(n+m)$, azaz létezik egy c konstans úgy, hogy a szélességi bejárás legfeljebb $c(n+m)$ lépést használ, ahol n és m a G gráf csúcsai ill. élei számát jelöli.*

Bizonyítás. Vegyük észre, hogy a szélességi bejárás minden lépése a G gráfnak vagy egy éléhez, vagy egy csúcsához köthető. A v_i csúcshoz kötjük azt a lépést, amikor a v_i-t először elérjük, illetve azt, amikor észrevesszük, hogy a v_i csúcsból már nem vezet bejáratlan pontba él (azaz amikor v_i-ből továbblépünk v_{i+1}-be). Az $e = v_iv_j$ élhez kötjük azt a lépést, amikor v_i-ből megvizsgáljuk, hogy v_j-t már bejártuk-e. Minden csúcshoz ill. élhez legfeljebb 2 lépést kötöttünk, ezzel az állítást igazoltuk. □

A szélességi bejárás segítségével tehát nemcsak hatékonyan tudjuk megkeresni a gráfbeli távolságokat egy gyökérpontból, hanem gyorsan el tudjuk dönteni azt is, összefüggő-e az inputként kapott irányítatlan gráf, ill. ha nem az, akkor meg tudjuk találni a komponenseit. (Az input G komponenseit pontosan azok a pontok alkotják, amelyek két „kalapból előhúzott" pont között értünk el, a másodiknak előhúzott pontot nem beleértve.)

Általános távolságfüggvények gráfokon

Egy gráf két csúcsa közötti legrövidebb út meghatározása gyakorlati problémaként pl. úgy merülhet fel, hogy egy ország úthálózata alkotta gráfon keresünk két pont között egy leggyorsabb útvonalat. Adott tehát egy gráf, aminek csúcsai a közlekedési csomópontok, élei az egyes útszakaszok, és két kijelölt csúcs. Természetesen ilyenkor nagyon nem mindegy, hogy egy-egy gráfél (azaz útszakasz) milyen hosszú, milyen sebességkorlátozas érvényes ill. az adott napszakban mennyire lehet haladni az adott szakaszon. Szükségünk van tehát erre vonatkozóan még további információra. Az alábbiakban ezt igyekszünk formalizálni.

3.68. Definíció *Legyen $G = (V, E)$ irányított gráf, és legyen $l : E \to \mathbb{R}$ egy* hosszfüggvény *G élein. Az e él* hossza *alatt az $l(e)$ számot értjük, de beszélhetünk ekkor a G gráf*

egy P útjának $l(P)$ hosszáról is az $l(P) := \sum_{e \in E(P)} l(e)$ definíció alapján. Ennek alapján értelmezhető a G gráf tetszőleges u és v pontjának távolsága, azaz a legrövidebb u-ból v-be vezető út hossza: $dist(u, v) := \min\{l(P) : P$ a G gráf u-ból v-be vezető útja$\}$ (ha nem vezet u-ból v-be (irányított) út G-ben, akkor $dist(u, v) := \infty$). Jegyezzük meg, hogy általában itt sem igaz, hogy $dist(u, v) = dist(v, u)$, jóllehet irányítatlan gráfokra ez is teljesül.

Bár a gráf pontjai közti *dist* távolságfüggvény jóldefiniált, mégis, a fenti távolságfogalom bizonyos esetekben ellentmond az intuíciónak. Azt várhatnánk ugyanis, hogy a két pont közötti legrövidebb út egyben legrövidebb *élsorozat* is: nincs értelme egy pontot többször érinteni, ha u-ból v-be szeretnénk eljutni. Ez azonban nincs így. Ha G-ben van *negatív kör*, azaz olyan irányított kör, melyben az élek összhossza negatív, akkor e kör két pontja között tetszőlegesen rövid (negatív összhosszú) élsorozat is létezik: egyszerűen kellően sokszor körbe kell menni a körön. Negatív kör jelenléte esetén az a korábbi megfigyelésünk sem igaz, hogy legrövidebb út részútja is legrövidebb (az adott csúcsok között).

Ha ellenben nincs a gráfban ilyen csúfság még az esetleges negatív élhosszok ellenére sem, (azaz ha a távolságfüggvény *konzervatív*), akkor könnyen látható, hogy minden legrövidebb út egyúttal legrövidebb élsorozat is és legrövidebb út részútja is legrövidebb. Azt is eláruljuk, hogy nem konzervatív távolságfüggvényt is megengedve a legrövidebb út probléma bizonyíthatóan nehéz (pontosabban NP-teljes) lesz. Ezért a továbbiakban konzervatív gráfokkal fogunk foglalkozni. Könnyen látható, hogy egy irányítatlan gráf pontosan akkor konzervatív, ha nincs negatív hosszúságú éle. A nemnegatív élhosszfügvény azonban az irányított gráfok esetén is fontos speciális eset, pl a gyakorlati útvonaltervezési alkalmazás is ilyen. Láttuk, hogy a BFS algoritmus jól működik, ha egy út hosszát az élszámával definiáljuk, azaz ha a távolságfüggvény az azonosan 1 függvény. A BFS algoritmust fogjuk nemnegatív élhosszokra általánosítani: egy újabb bejárási algoritmust írunk le, ahol –ellentétben az eddigi szabállyal, amikoris mindig a legkorábban elért pontból szerettük volna felfedezni a következőnek elértet– az éppen elérendő pontot mindig úgy választjuk, hogy az eddig elérteken keresztül a lehető legközelebb legyen a gyökérhez.

Mielőtt azonban ezt megtennénk, leírjuk azt az általános eljárást, amit rutinként alkalmazni fogunk a távolságok meghatározására. Tegyük fel, hogy a $d : V \to \mathbb{R}$ függvény egy felső becslés a távolságokra, azaz $dist(u, x) \leq d(x)$ minden $x \in V$ esetén.(Némileg szerencsétlen a d jelölés, hiszen így jelöltük a fokszámfüggvényt is, de ez itt remélhetőleg nem fog félreértést okozni.) Ha xv irányított él, akkor a legrövidebb uv-útnál nem lehet rövidebb az sem, ha először u-ból x-be megyünk, majd onnan közvetlenül v-be:

$$dist(u, v) = min\{dist(u, w) + l(wv) : wv \in E\} \leq dist(u, x) + l(xv) \leq d(x) + l(xv).$$

Ha tehát

$$d(x) + l(xv) < d(v) \tag{3.2}$$

áll valamely x csúcsra, akkor $dist(u,v) \leq d(x) + l(xv)$ miatt az eddigi $d(v)$ felső becslés $d(x) + l(xv)$-re javítható. Ezt a változtatást nevezzük az $e = xv$ *él mentén történő javításnak*. Az is könnyen látható, hogy ha egy d felső becslés olyan, hogy egyetlen $e = xv$ él mentén sem lehet rajta javítani, akkor $d(v) = dist(u,v)$ minden v esetén.

A fenti megfigyelés segítségével hatékonyan tudunk legrövidebb utakat keresni.

Dijkstra algoritmusa

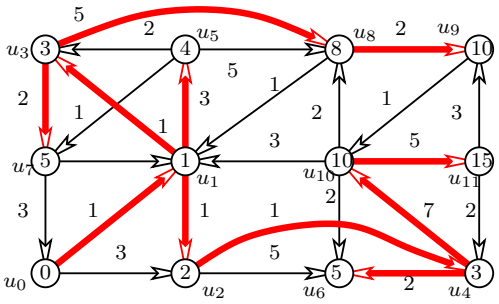
Input: Egy $G = (V,E)$ irányított gráf, egy $l : E \to \mathbb{R}_+$ nemnegatív hosszfüggvény és egy $u = u_0 \in V$ gyökérpont.

Output: a $dist(u,\cdot)$ függvény, azaz kiszámítjuk a $dist(u,v)$ távolságot G minden v csúcsára, meghatározunk egy legrövidebb uv utat, és nem mellesleg bejárjuk a G gráfot.

A fenti feladatot oldja meg Dijkstra algoritmusa, ami a BFS algoritmus általánosításának tekinthető abban az értelemben, hogy ha minden élhossz pozitív egész, akkor a Dijkstra algoritmus azt szimulálja, hogyan működne a BFS arra a gráfra, amit úgy kapunk a bemenetből, hogy minden élt egy olyan hosszú úttal helyettesítünk, amennyi az adott él hossza. (Természetesen a BFS lefuttatásával is megoldjuk a feladatot, a baj azonban ezzel az, hogy az input gráf hatalmasra tud növekedni, és ennek hatására a lépésszám elfogadhatatlanul nagy lesz. A Dijkstra algoritmus ettől még tekinthető a BFS-nek a megnövelt gráfon történő egyfajta gyors elvégzésének is.)

Működés: A $dist(u,\cdot)$ függvény egy d felső becsléséből indulunk ki: kezdetben $d(u_0) := 0$, ill. $d(v) := \infty$ minden további $u \neq v$ csúcsra. Legyen $U_0 := \{u_0\}$. Először elvégezzük a javítást az összes, u_0-ból induló élre. Legyen u_1 egyike azon pontoknak, amire a javítások után kapott d felső becslés minimális. Lépjünk u_1-be a minimumot meghatározó élen és legyen $U_1 := U_0 \cup \{u_1\}$. Világos, hogy $d(u_1) = dist(u,u_1)$ és u_1 az u-hoz legközelebbi csúcs. Az általános lépéshez tegyük fel, hogy már bejártuk az u-hoz legközelebbi i db pontot, ezek az $U_i = \{u_0, u_1, \ldots, u_i\}$ halmazt alkotják, és azt is tudjuk, hogy minden $x \in U_i$-re $d(x) = dist(u,x)$ teljesül. Végezzük most el a javításokat az u_i-ből induló összes U_i-t elhagyó élre. Legyen u_{i+1} egy olyan U_i-n kívüli csúcs, amire a javítások utáni $d(x)$ minimális. A minimumot megvalósító élen (vagy azok egyikén) lépjünk u_{i+1}-be és legyen $U_{i+1} := U_i \cup \{u_{i+1}\}$.

Könnyű látni, hogy $d(u_{i+1}) = dist(u,u_{i+1})$, továbbá, hogy U_{i+1} is az u-hoz legközelebbi pontok halmaza (itt kell használni, hogy nincsenek negatív hosszúságú élek), ezért U_{i+1} is rendelkezik azzal a tulajdonsággal hogy minden $x \in U_{i+1}$-re $d(x) = dist(u,x)$. Világos, hogy az U_i halmaz legfeljebb $(n-1)$-szeri hízlalása után már nem tudunk több javítást végezni, ezért az algoritmus véget ér: minden u-ból elérhető x pontra $d(x) = dist(u,x)$ lesz, az u-ból nem elérhető y pontokra pedig $d(y) = \infty$ áll.



Az algoritmus lépésszámának becsléséhez azt érdemes megfigyelni, hogy minden él mentén legfeljebb egyszer javítottunk, ami az élszám (m) konstansszorosa számú lépést jelent. Az algoritmus persze nem csak javításokat végez. A másik fajta lépés az aktuális u_{i+1} kiválasztása. Ez egy minimumválasztás, legfeljebb n becslés közül, ami legfeljebb n lépésben elvégezhető. A minimumválasztások száma az algoritmus futása során legfeljebb n, tehát erre a célra legfeljebb $konst \cdot n^2$ lépés kell. Mivel $m \leq n^2$, ezért a Dijkstra algoritmus futásideje n^2 konstansszorosával becsülhető. Alkalmas adatstruktúra-választással az algoritmus futásidejére $konst \cdot (n+m) \log n$ becslés kapható, ami javulás a $konst \cdot n^2$-hez képest, ha a gráfnak nincs túl sok éle. Ha a gráfnak sok éle van, akkor létezik olyan implementáció, ami $konst \cdot m$ lépést tesz.

Érdemes végiggondolni, hogy ha minden élhossz 1, akkor a Dijkstra algoritmus lényegében egy annyiban módosított szélességi keresés, hogy minden x csúcs bejárásakor feljegyezzük $d(x)$-t, vagyis azt, hogy x a szélességi fában milyen távol van a gyökértől.

Tanulságos meggondolni, hogy irányítatlan gráfon adott nemnegatív élhosszok esetén egy „mechanikus számítógép” segítségével egy mozdulattal meghatározhatók a gyökértől való távolságok. Feleljen meg minden pontnak egy (pontszerű) súly, és az u ill. v csúcsoknak megfelelő súlyokat kössük össze egy $l(u,v)$ hosszúságú zsinórral. Ha most ezt a rendszert felemeljük az u gráfcsúcsnak megfelelő súlyánál fogva, akkor minden v csúcsnak megfelelő súly éppen $dist(u,v)$ távolsággal lesz a felemelt, u-nak megfelelő súly alatt. A Dijkstra algoritmus (a megfelelő irányítatlan gráfon futtatva) ebben az esetben azt modellezi, hogy ha lassan emelni kezdjük a gyökércsúcsot, akkor milyen sorrendben emelkednek fel a további súlyok az asztalról, a bejárási fát az éppen megfeszülő zsinórok alkotják, és a $dist(u,\cdot)$ függvény pedig azt tartja nyilván, hogy egy-egy súly a felemelkedésekor mennyivel lesz a gyökér alatt.

Ford algoritmusa

Ford algoritmusának bemenete (inputja) egy irányított $G=(V,E)$ gráf, élein egy $l : E \to \mathbb{R}$ konzervatív hosszfüggvény, és egy $u \in V$ csúcs. Az algoritmus kimenete (outputja) a $dist(u,\cdot)$ függvény, azaz a $dist(u,v)$ távolságok meghatározása az összes $v \in V$ csúcsra.

Az algoritmus működése: legyen $E = \{e_1, e_2, \ldots\}$, és legyen $d(u) := 0$, ill. $d(v) := \infty$ a további $u \neq v \in V$ csúcsokra. Az algoritmus fázisokból áll. Egy fázis abból áll, hogy sorra megpróbálunk az $e_1, e_2, \ldots$ élek mentén javítani. Ha egy fázisban nem történt sikeres javítás, akkor az algoritmus véget ér, és a $dist(u,v) = d(v)$ áll minden v csúcsra.

Az algoritmusnak legfeljebb $n-1$ fázisa lesz, ahol n a G csúcsainak száma. Ugyanis

az első fázisban a $d(v) = dist(u, v)$ lesz minden olyan v-re, amire létezik a legrövidebb uv-utak között egyélű. A második fázisban a $d(v)$ értéke már azokra a v csúcsokra is helyesen lesz beállítva, amelyekre létezik a legrövidebb uv-utak között kétélű. Általában, az i-dik fázis végén a legfeljebb i élű legrövidebb úton elérhető v pontokra lesz a $dist(u, v)$ kiszámítva. Mivel egy útnak legfeljebb $n - 1$ éle lehet, ezért legkésőbb az $(n - 1)$-dik fázis végén az algoritmus véget ér.

A Ford algoritmus minden fázisában nagyjából élszámnyi lépést végzünk, ezért az egész algoritmus lépésszáma nm konstansszorosával becsülhető, ahol m a G élszáma.

A Ford algoritmus arra is alkalmas, hogy hatékonyan eldöntsük, létezik-e egy irányított G gráfban negatív kör, azaz, hogy egy adott távolságfüggvény csakugyan konzervatív-e. Ha ugyanis l konzervatív, akkor a Ford algoritmus (mint láttuk) legfeljebb $n - 1$ fázis után véget ér. Ha azonban nem konzervatív G súlyozása, akkor a negatív kör mentén mindig lehet javítani, vagyis sosem ér véget az algoritmus, így megéri még az n-dik fázist is.

Floyd algoritmusa

Konzervatív távolságfüggvények esetén Ford algoritmusával hatékonyan tudjuk meghatározni a gráf összes pontpárjának távolságát (minden gyökérből futtatunk egy Ford algoritmust, összesen $konst \cdot n^2 m$ lépéssel), de létezik erre a problémára hatékonyabb megközelítés is. Feltehetjük, hogy $v_1, v_2, \ldots, v_n$ a G gráf csúcsai. Jelölje $d^{(k)}(i, j)$ a v_i-ből v_j-be vezető legrövidebb olyan út hosszát, aminek csúcsai a $v_i, v_j, v_1, v_2, \ldots, v_k$ halmazból kerülnek ki. Világos, hogy $d^{(0)}(i, j) = l(v_i, v_j)$. Mivel a $d^{(k+1)}(i, j)$-t meghatározó út vagy nem használja a v_k pontot, vagy egy $v_i v_k$ és egy $v_k v_j$-útra bontható ezért $d^{(k+1)}(i, j) = \min\{d^{(k)}(i, j), d^{(k)}(i, k + 1) + d^{(k)}(k + 1, j)\}$ tehát $d^{(k)}$ ismeretében $d^{(k+1)}$ könnyen számítható. Tehát $dist(v_i, v_j) = d^{(n)}(i, j)$, és utóbbi függvényt $konst \cdot n^3$ lépésben ki tudjuk számítani, hiszen pontosan egyszer kell minden $d^{(k)}(i, j)$ értéket kiszámolni, ahol $i, j, k \in \{1, 2, \ldots, n\}$.

3.4.2. Legszélesebb utak

Ha egy gráf éleihez számokat rendelünk, az nem csak az adott él hosszát vagy költségét írhatja le. Elképzelhető olyan modell is, ahol egy élhalmazt nem a hozzájuk rendelt számok összege, hanem mondjuk azok minimuma jellemez. Képzeljük el, hogy egy számítógéphálózat egyik csúcsából egy másik csúcsába kell adatfolyamot küldenünk úgy, hogy az esetleges késleltetés nem okoz problémát, azonban az adatok csak egyetlen útvonalon utazhatnak, amelyen minél nagyobb sávszélesség elérése a cél. Ebben az esetben a számítógéphálózatot leíró gráf éleihez tartozó értékek az adott kapcsolat sávszélességének felelnek meg és egy út sávszélessége pedig az úton található élek sávszélességének minimuma lesz. Ez motiválja az alábbi definíciót.

3.69. Definíció *Legyen $G = (V, E)$ egy irányított vagy irányítatlan gráf, és legyen $w : E \to \mathbb{R}_+$ az egyes élek „szélességét" leíró függvény. Ha P a G egy útja, akkor w szélessége a P legkeskenyebb élének szélessége: $w(P) := \min\{w(e) : e \in E(P)\}$.*

A legrövidebb utak kereséséhez hasonlóan természetes probléma adott G gráf és w szélességfüggvény esetén, hogy G bármely két csúcsa között legszélesebb utat keressünk, ill., hogy egy G-beli gyökérpontból G bármely másik pontjába legszélesebb utat találjunk.

Az alábbi tétel szerint ha G irányítatlan, akkor nagyon gyorsan boldogulhatunk, mert G tetszőleges maximális össz-szélességű feszítőfája a G gráf bármely két csúcsa között egy maximális szélességű utat tartalmaz.

3.70. Tétel *Tegyük fel, hogy $G = (V, E)$ irányítatlan, összefüggő gráf és a $w : E \to \mathbb{R}_+$ szélességfüggvény olyan, hogy $w(e_1) \geq w(e_2) \geq \ldots \geq w(e_m)$, ahol $E = \{e_1, e_2, \ldots, e_m\}$. Ekkor a Kruskal algoritmust az $e_1, e_2, \ldots$ sorrendben lefuttatva a G olyan F feszítőfáját adja meg, ami G bármely két csúcsa között G egy legszélesebb útját tartalmazza.*

Bizonyítás. Indirekt bizonyítunk. Legyen F a Tételben leírt feszítőfa, és tegyük fel, hogy P olyan uv-út G-ben, ami szélesebb az u-t és v-t F-ben összekötő P' útnál. A P' út szélességét meghatározó e' él szélessége tehát kisebb a P út bármely élének szélességénél. Hagyjuk el e'-t F-ből, miáltal F úgy esik két komponensre, hogy a u az egyik, v pedig a másik komponensbe kerül. Mivel P egy u-t és v-t összekötő út, a P-nek van legalább egy olyan (mondjuk e) éle, ami $F - e'$ két komponense között fut, és ezért persze e nem éle F-nek. Az indirekt feltevés miatt $w(e) > w(e')$, de ekkor a Kruskal algoritmus e-t e'-nél korábban ellenőrizte, tehát $F - e'$ egy részhalmazához próbálta hozzávenni. Mivel e-t még $F - e'$-höz hozzávéve sem kapunk kört, a Kruskal algoritmus futásakor az e élt be kellett volna vennünk az F élhalmazba, márpedig ez ellentmond annak, hogy e nem éle F-nek. Ez az ellentmondás pedig az indirekt feltevésünket cáfolja, tehát F a G gráf bármely csúcsa között egy legszélesebb utat tartalmaz. □

A fenti bizonyítás értelemszerű módosításával az is igazolható, hogy a 3.70. Tételben a Kruskal algoritmus helyett bármely más olyan algoritmust is használhattunk volna, ami egy legnagyobb össz-szélességű feszítőfát talál a G gráfban. Ha azonban a G gráf irányított, akkor a fenti eljárás nem működik. Kiderül azonban, hogy a Dijkstra algoritmus egy értelemszerű módosítása alkalmazható erre az esetre. Mivel az algoritmus kiterjesztése lényegesen általánosabb körülmények között is működik, ezért az alábbiakban általánosítjuk a legszélesebb utak keresésének problémáját, és erre az általánosított problémára mutatunk eljárást.

3.71. Definíció *Tegyük fel, hogy a G gráf útjain úgy értelmeztünk egy „jóság" nevű tulajdonságot. Ez a tulajdonság* rendezés, *ha bármely út legalább olyan jó mint önmaga, bármely két út összehasonlítható (azaz közülük az egyik legalább olyan „jó", mint a másik) és tranzitív, azaz ha P „jobb", mint Q és Q „jobb", mint R, akor P is „jobb" mint R.*

A „jóság" tulajdonságot akkor nevezzük monotonnak*, ha tetszőleges út részútja mindig legalább olyan „jó", mint maga az út. Végül a jóság tulajdonság* konzisztens*, ha tetszőleges út egy kezdőszakaszát egy, a kezdőszakasznál nem „rosszabb" úttal helyettesítve a kiindulási útnál nem kaphatunk kevésbé „jót".*

Vegyük észre, hogy ha egy út annál „ jobb" minél szélesebb, akkor ez a fajta „ jóság" tulajdonság monoton, konzisztens rendezés. Hasonlóan, ha egy utat akkor tekintünk „ jobbnak" egy másiknál, ha kevesebb élt tartalmaz (vagy általánosabban: ha adott nemnegatív hosszfügvény szerint rövidebb), akkor is egy monoton, konzisztens rendezést definiáltunk. Szükségünk lesz a következő segédtételre.

3.72. Lemma *Ha a „jóság" a G irányított gráf útjain egy monoton, konzisztens rendezés, és P egy „legjobb" uv-út G-ben (azaz nincs P-nél jobb uv-út), akkor P tetszőleges w pontjára G „legjobb" uw-útja legalább olyan „jó", mint P.*

Bizonyítás. A P út u-ból w-be vezető P' része a P út részútja, ezért a „ jóság" monotonitása miatt P' legalább olyan jó, mint P, és a „legjobb" uw-út nem lehet P'-nél „rosszabb". □

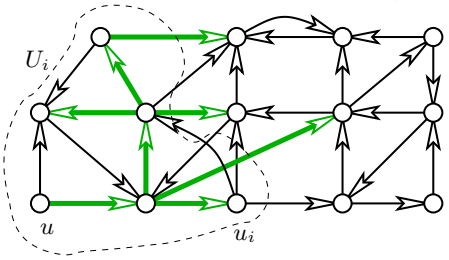
A legszélesebb utak irányított gráfban történő kereséséhez az a fő eredmény, hogy tetszőleges monoton, konzisztens rendezés esetén használható a Dijkstra algoritmus alábbi változata.

Dijkstra algoritmusa az utak monoton, konzisztens „ jóság" szerinti rendezésekor

Input: Egy n csúcsú $G = (V, E)$ irányított gráf, $u = u_0$ gyökérpont és egy monoton, konzisztens „ jóság" szerinti rendezés G útjain.

Output: G egy u gyökerű, u-ból kifelé irányított F részfája, amiben minden u-ból G-ben elérhető csúcs elérhető, mégpedig egy „ legjobb" G-beli uv-úton.

Működés: Legyen $U_0 = u_0$ és F_0 az u_0 pontot tartalmazó egypontú fa. Az algoritmus az i-dik lépésben elkészíti az F_i részfát és az $U_i = \{u_0, u_1, \ldots, u_i\}$ halmazt, az output pedig az $F = F_n$ részfa. A továbbiakban jelölje P_v^i az F_i fa uv-útját (feltéve, hogy v csúcsa F_i-nek). Az algoritmus futása során minden i-re igaz, hogy u-ból F_i-ben az U_i halmaz minden v csúcsa elérhető, továbbá, hogy U_{i-1}-en kívül F_i-nek csak levelei vannak.



Az algoritmus i-dik lépésében az F_{i-1} részfából úgy készíti el az F_i részfát, hogy a G gráf összes olyan $u_{i-1}v$ élen javítunk, amire $v \notin U_{i-1}$. A javítás abból áll, hogy ha

P_v^{i-1} nem „jobb” mint az az út, amit úgy kapunk, hogy a $P_{u_{i-1}}^{i-1}$ utat kiegészítjük az $u_{i-1}v$ éllel (mivel v az F_{i-1} levéle, ezért ez valóban út lesz), akkor töröljük F_{i-1}-nek a v-be vezető élét, és bevesszük F_i-be az $u_{i-1}v$ élt. (Speciálisan, ha v nem volt csúcsa az F_{i-1} fának, akkor F_i-be automatikusan bevesszük az $u_{i-1}v$ élt.) Az algoritmus i-dik lépésének második részében pedig tekintjük az U_{i-1}-ből kivezető P_v^i-utakat, ezen utak „legjobbika” vezessen u_i-be, és legyen $U_i := U_{i-1} \cup \{u_i\}$. Rendszerint azt is érdemes feljegyezni, hogy mennyire „jó” a $P_{u_i}^i$ út, mert ez lesz majd G legjobb uu_i-útjának „jósága” is, és bizonyos „jóságfogalmak” estén ebből tudjuk gyorsan meghatározni az épülő fában u_i leszármzottaiba vezető utak „jóságát”.

Az algoritmus helyességéhez csupán azt alábbi Lemmát kell igazolni.

3.73. Lemma *A fent leírt Dijkstra algoritmus végrehajtása után az alábbi tulajdonságok teljesülnek minden $i = 0, 1, \ldots n$ esetén.*

$$\begin{gathered}\textit{Az } F_{i+1} \textit{ fa tetszőleges } v \textit{ csúcsára } P_v^{i+1} \textit{ az egyik „legjobb” olyan } G\textit{-beli } uv\textit{-út,} \\ \textit{ami } v\textit{-n kívül kizárólag } U_i \textit{ csúcsait használja.} \qquad (3.3)\end{gathered}$$

$$\begin{gathered}\textit{Ha } v \in U_i \not\ni w\textit{, és } P \textit{ a } G \textit{ egy tetszőleges } uw\textit{-útja,} \\ \textit{akkor } P_v^i \textit{ legalább olyan „jó”, mint } P. \qquad (3.4)\end{gathered}$$

Tekintettel a $V(G) = U_{n-1}$ egyenlőségre, az algoritmus helyessége azonnal következik az output $F = F_n$ fa 3.3 tulajdonságából.

A 3.73. Lemma bizonyítása. Azt igazoljuk i szerinti indukcióval, hogy az F_i fára minden i esetén fennállnak a 3.3 és 3.4 tulajdonságok. A „jóság” monotonitása miatt az egypontú utak a legjobbak, ezért $i = 0$-ra teljesül a 3.4 tulajdonság. A 3.3 tulajdonság $i = 0$-ra közvetlenül adódik az F_1 definíciójából. Tegyük fel tehát, hogy 3.3 és 3.4 teljesülnek $(i-1)$-re, az indukciós lépésben pedig ugyanezt igazoljuk i-re.

Legyen tehát v az F_{i+1} fa egy pontja, és legyen P az egyik „legjobb” olyan uv-út, ami v-n kívül csak U_i csúcsait használja. Legyen $w \in U_i$ a P útnak a v-t megelőző csúcsa. és legyen P_w az P-ből v törlésével keletkező részút. A jóság monotonitása miatt P_w nem „rosszabb” P-nél és az $(i-1)$-re vonatkozó 3.3 tulajdonság miatt P_w^i nem „rosszabb” P_w-nél, tehát P-nél sem.

1. eset Ha v rajta van a P_w^i-úton, akkor P_v^i a P_w^i kezdőszelete, tehát a jóság monotonitása miatt nem „rosszabb” P_w^i-nél és P-nél sem. Ilyenformán P_v^i is egy „legjobb” olyan uv-út, ami v-n kívül csak U_i csúcsait használja. Mivel a P_v^{i+1} út nem lehet „rosszabb” P_v^i-nél, ezért ekkor a 3.3 teljesül i-re.

2. eset Ha azonban v nincs rajta a P_w^i úton, akkor legyen P' az az uv-út, amit úgy kapunk, hogy a P út w-ig tartó kezdőszeletét helyettesítjük P_w^i-vel. Figyeljük meg egyrészt, hogy az $(i-1)$-re vonatkozó 3.3 tulajdonság és a „jóság” konzisztenciája miatt P' nem „rosszabb” P-nél.

2.1 eset Ha a P' út tartalmazza az u_i csúcsot (ami az F_{i-1} fának levele), akkor $w = u_i$.

2.1.1 eset Ha most $v \notin U_i$, akkor az algoritmus i-dik lépésében az u_iv él menti javításnál az u_iv élt becseréltük F_i-be ezért $P' = P_v^i$, ami i-re igazolja a 3.3 tulajdonságot.

2.1.2 eset Ha pedig $v \in U_i$, akkor az $(i-1)$-re feltett 3.4 tulajdonság miatt a P_v^i út „jobb” a $P_{u_i}^i = P_w^i$ útnál, ami a P' út kezdőszelete lévén nem rosszabb P'-nél, tehát P-nél sem. Azt kaptuk tehát, hogy P_v^i ismét csak az egyik „legjobb” olyan uv-út, ami v-n kívül csak U_i csúcsait használja, tehát a 3.3 tulajdonság ekkor is teljesül.

2.2 eset Végül, ha a P' út nem tartalmazza az u_i csúcsot, akkor az algoritmusból adódóan P_v^{i+1} nem „rosszabb” P_v^i-nél, ami $(i-1)$-re érvényes 3.3 tulajdonság miatt nem rosszabb P'-nél, tehát P-nél sem. Ebben az esetben is teljesül tehát a 3.3 tulajdonság i-re.

Az indukciós lépés befejezéséhez a 3.4 tulajdonságot kell i-re igazolnunk. Tegyük fel, hogy $v \in U_i$ és $w \notin U_i$, valamint, hogy P a G egy tetszőleges uw-útja. Ha $v \neq u_i$, azaz $v \in U_{i-1}$, akkor az $(i-1)$-re feltett 3.4 tulajdonság miatt P_v^{i-1} nem rosszabb P-nél. Az algoritmusból adódóan pedig P_v^i nem rosszabb, mint P_v^{i-1}-nél, tehát P_v^i csakugyan legalább olyan jó, mint P.

Feltehetjük tehát, hogy $v = u_i$. Legyen x a P út utolsó U_i-beli csúcsa után következő csúcs és készítsük el a P' utat úgy, hogy a P út u-ból x-be vezető részét P_x^i-szel helyettesítjük. Mivel x-be vezet U_i-beli pontból él, ezért x benne van az F_i fában. Ráadásul P_x^i minden x előtti csúcsa U_i-beli, ezért P' valóban egy G-beli út lesz. Az $(i-1)$-re feltett 3.3 tulajdonság miatt P_x^i legalább olyan „jó", mint az amit helyettesítettünk vele P-ben, ezért a „jóság" konzisztenciája miatt P' legalább olyan „jó", mint P. Az algoritmus i-dik lépésében u_i-t úgy választottuk, hogy $P_{u_i}^i$ ne legyen „rosszabb" P_x^i-nél, ezért $P_{u_i}^i$ nem „rosszabb" P'-nél és így P-nél sem. Ez pedig a 3.4 tulajdonságot igazolja, és ezzel befejeztük az indukciós lépés bizonyítását. □

Miért kínlódtunk az általánosított Dijkstra algoritmus helyességének „jóságos" igazolásával ahelyett, hogy külön bizonyítottunk volna legrövidebb utakra és legszélesebbekre is? Két okból. Egyrészt példát mutattunk arra a fajta gondolkodásmódra, aminek elsajátítása a tárgy egyik célja, és talán haszna is azok számára, akik megértenek valamit belőle, és nem csak átmennek a vizsgán. Arról van ugyanis szó, hogy amint sikerült igazolni egy módszer helyességét, azonnal felmerül (egy matematikusban) a természetes kérdés: vajon melyek azok a legáltalánosabb feltételek, amelyek fennállása mellett még helyesen működik az algoritmus? Erre láttunk egyfajta választ a fenti gondolatmenetben. De innen mindjárt látszik a másik ok is. Az utak rövidsége ill. szélessége csupán két kiragadott példa volt monoton, konzisztens rendezésre. Az algoritmus ereje abban áll, hogy bármely ilyen szituációban helyesen működik, tehát ha pl egy gráf élein adott egy l hossz- és egy w szélességfüggvény, akkor egy P út „jóságát" definiálhatjuk éppenséggel úgy, hogy P akkor „jobb", mint P', ha $g(P) \geq g(P')$, ahol $g(P) := 63 \cdot w(P) - 37 \cdot l(P)$. Ez a „jóságfogalom" könnyen láthatóan monoton és konzisztens rendezés, tehát erre is működik az algoritmus. (Voltaképpen arról van szó, hogy a jóság szempontjából súlyozzuk az út szélességét és hosszát, a konkrét példában 63%-ban számít a szélesség, és 37%-ban a hossz.) Egy érdekes extrém eset, amikor a szélesség 100%-ban számít, és „infinitezimálisan" a hossz, vagyis egy P út akkor „jobb" P'-nél, ha P szélesebb P'-nél vagy ha P és P' egyforma szélesek, de P rövidebb. Ekkor a fenti algoritmus ú.n. legrövidebb legszélesebb utakat keres: a megtalált uv-út a létező legszélesebb uv-utak egyike, mégpedig az egyik legrövidebb lesz. Működik persze a dolog fordított prioritással is: az általánosított Dijkstra algoritmus tetszőleges u gyökérből (kezdőpontból) megtalálja a G olyan kifelé irányított „feszítőfáját", amely a gyökérpontból bármely más csúcsba egy legrövidebb utat tartalmaz, de ha több ilyen is van, akkor a legrövidebbek közül a legszélesebbek egyikét.

3.4.3. Mélységi bejárás, aciklikus gráfok, leghosszabb utak

A *mélységi bejárás* (amit az angol „depth first search" elnevezés rövidítéséből DFS-nek is neveznek) olyan bejárás, ahol egy v_0 gyökércsúcsból indulunk, és mindig a legutóbb elért v_i csúcsból egy még bejáratlan v_{i+1} csúcsba igyekszünk egy gráfél mentén továbblépni. Ha ez nem lehetséges, akkor a v_i-ből visszalépünk abba a v_j csúcsba, ahonnan v_i-t elértük, és v_j-ből próbálunk bejáratlan csúcsba lépni. Ha ez sem sikerül, innen is visszalépünk, sít. Ha visszajutottunk a v_0 csúcsba, és már innen sem tuduk új csúcsot elérni, de még nem jártunk be minden csúcsot, akkor egy újabb gyökeret választunk a bejáratlan csúcsok közül, és folytatjuk a bejárást. A mélységi bejárás bejárási fáját *mélységi fának* nevezzük (jóllehet ez például nem összefüggő, irányítatlan gráf esetén csak erdő).

Egy mélységi bejáráshoz tartozó *mélységi számozáson* a mélységi bejárás elérési sorrendjét értjük, azaz a fenti leírásban a v_i csúcs mélységi száma i. A bejárt G gráf éleit a bejárásoknál elmondottak szerint osztályozhatjuk. A mélységi bejárás sajátosságaiból az alábbi adódik az osztályozásra.

Legyen uv a gráf éle. Ha v mélységi száma nagyobb, mint u-é, akkor u eléréséig v-t nem értük el, így vissza sem léphettünk még v-ből amikor u-t elértük. Ezért amikor u-t befejezzük (vagyis amikor u-ból visszalépünk), akkor a mélységi bejárárás szabálya alapján v-t már el kellett érnünk, legrosszabb esetben a közvetlen uv élen. Tehát a mélységi fában v az u közvetlen vagy közvetett leszármazottja, vagyis uv faél vagy előreél.

A másik lehetőség az, ha az uv él olyan, hogy u mélységi száma nagyobb v-énél. Ekkor persze u-ból v-be nem vezethet irányított út a mélységi fában (azaz v nem lehet u leszármazottja), hiszen a faélek mentén a mélységi szám növekszik. Vagyis vagy u a v leszármazottja, amikoris az uv él visszaél, vagy u és v nem leszármazottai egymásnak, de ehhez v-ből még u elérése előtt vissza kellett lépnünk. Ekkor pedig az uv él keresztél.

A keresztélekkel kapcsolatos fontos megfigyelés, hogy irányítatlan gráf mélységi bejárása után a gráfban csak faélek és előreélek lesznek. Minden visszaél ugyanis egyben előreél is, keresztélek pedig azért nem adódnak, mert egy keresztél két végpontja nem leszármazottai egymásnak a mélységi fában, keresztél mindig később elért pontból vezet korábban elért pontba, de az irányítatlan gráfból képzett irányított gráfban minden él fordítottja is megtalálható.

3.74. Definíció *Egy G (irányított) gráfot* aciklikusnak *mondunk, ha G nem tartalmaz (irányított) kört.*

3.75. Tétel *Legyen G irányított gráf. Ekkor az alábbi négy állítás ekvivalens. (1) G aciklikus. (2) G egyetlen mélységi bejárásában sincs visszaél. (3) G valamely mélységi bejárásában nincs visszaél. (4) G csúcsai sorbarendezhetők úgy, hogy G minden éle egy a sorrendben későbbi csúcsba mutat.*

3.76. Definíció *A 3.75. Tétel (4) pontjában leírt sorrendet* topologikus sorrend*nek nevezzük.*

Bizonyítás. 1. $\Rightarrow$ 2.: Ha egy mélységi bejárásban találnánk egy uv visszaélt, akkor létezik egy vu-út csupa faélekből, ehhez az uv visszaélt hozzáadva egy kört kapnánk.

2. $\Rightarrow$ 3.: Triviális.

3. $\Rightarrow$ 4.: Tekintsük azt a mélységi bejárást, amiben nincs visszaél. Vegyük észre, hogy ennek során minden v csúcs esetén pontosan egyszer történt meg, hogy éppen v-ből próbáltunk bejáratlan csúcsot találni, de ilyen nem volt (és ezért vagy visszaléptünk v-ből az ősébe, vagy v gyökér volt, és új gyökeret kerestünk). E mélységi bejáráshoz tartozik tehát egy *befejezési sorrend* is, ami a csúcsokat olyan sorrendben sorolja fel, ahogyan a fenti szituáció előadódott. Könnyen látható, hogy ha uv faél, előreél vagy keresztél, akkor v megelőzi u-t a befejezési sorrendben. Ezért ha egy mélységi bejárás után a G

gráfban nincs visszaél akkor a megfordított befejezési sorrend pontosan olyan sorrendet ad, amilyet kerestünk.

4. $\Rightarrow$ 1.: Ha lenne irányított kör, akkor az feltétlenül tartalmazna olyan élt, ami egy, a sorrendben későbbi csúcsból mutat egy korábbiba. A feltétel szerint ilyen nincs, tehát G aciklikus. □

3.77. Megjegyzés *Megmutatható, hogy egy irányított gráf minden irányított köre egyértelműen előáll mint alapkörök szimmetrikus különbsége, azaz tetszőleges C körhöz egyértelműen létezik néhány alapkör úgy, hogy C élei pontosan azok, amelyeket az alapkörhalmazból páratlan sok tartalmaz. Ilyen tulajdonsággal rendelkező alapkörhalmazt úgy kaphatunk, hogy tekintjük egy mélységi fához tartozó visszaélek által meghatározott köröket.*

3.78. Tétel *Ha a G gráfnak n csúcsa és e éle van, akkor a mélységi bejárás lépésszáma lineáris, azaz létezik egy c konstans úgy, hogy a mélységi bejárás legfeljebb $c(n+e)$ lépést használ.*

Bizonyítás. A bizonyítás lényegében azonos a szélességi bejárásra vonatkozó hasonló állítás bizonyításával.
Vegyük észre, hogy a mélységi bejárás minden lépése a G gráfnak vagy egy éléhez, vagy egy csúcsához köthető. A v csúcshoz kötjük azt a lépést, amikor a v-t először elérjük, illetve azt, amikor észrevesszük, hogy a v csúcsból már nem vezet bejáratlan pontba él (azaz amikor v-ből visszalépünk v ősébe). Az $e = uv$ élhez kötjük azt a lépést, amikor u-ból megvizsgáljuk, hogy v-t bejártuk-e. Minden csúcshoz ill. élhez legfeljebb 2 lépést kötöttünk, ezzel az állítást igazoltuk.

Történelem: A DFS eredete
Gyerekkori olvasmányai vagy filmélménye alapján a legtöbb ember ismeri az ismeretlen labirintusból történő kijutásra szolgáló univerzális eljárást: válasszunk ki egy falat, és kövessük azt egészen addig, amíg ki nem jutunk. Kevesebben gondolkodnak már el azon, miért is működik ez a módszer. Azonban akik ezt megpróbálják, azok közül is sokan feladják, mert nem könnyű ezt bizonyítani. Ez azonban nem véletlen: a módszer ugyanis nem jó, általában nem működik, így a helyességét sem lehet bebizonyítani. Annak, hogy mégis elterjedt a köztudatban, valószínűleg két oka van. Egyrészt az, hogy egy egyszerű, könnyen megjegyezhető algoritmusról van szó, ami azt a megnyugtató érzést kelti a hiszékeny befogadóban, hogy valami hasznosat tanult, aminek segítségével a módszert nem ismerőkkel szemben igazi versenyelőnybe kerül egy mégoly valószínűtlen, ám felettébb kilátástalan helyzetben. A másik ok pedig az lehet, hogy a módszer sokszor valóban működik. A rejtvényekben található legtöbb labirintus ugyanis olyan, hogy abban nincsenek „falszigetek", azaz sehonnan sem lehet úgy visszajutni a kiindulási pontunkba úgy, hogy ne haladjunk végig kétszer ugyanazon a folyosón. Márpedig az ilyesfajta útvesztőkből mindig kijutunk folytonosan jobbratartva.

Ha elméletileg akarjuk megoldani a labirintusból menekülés problémáját, akkor érdemes a labirintust egy irányítatlan G gráfnak tekinteni, aminek élei a folyosóknak felelnek meg, csúcsai pedig a folyosók végpontjai. A szabadulási feladat pedig azt kívánja, hogy az általunk nem ismert G gráf egy adott u csúcsából kiindulva találjunk egy olyan sétát G-ben, ami G egy meghatározott, de általunk ismeretlen v csúcsába (a kijárathoz) vezet. Mivel nem ismerjük sem G-t, sem a séta végcélját, olyan sétát kell találnunk, ami G minden

u-ból elérhető csúcsába eljut. Más szóval az a cél, hogy bejárjuk a G gráf u-t tartalmazó komponensének minden csúcsát. Ha például a szélességi bejárással próbálkozunk, akkor az azért nem kielégítő módszer, mert ott az aktuális csúcsból kivezető élek ellenőrzése után, egy másik, esetleg egészen távoli csúcsban kell folytatni a munkát. Ha tehát a szélességi bejárás alapján egy sétát szeretnénk találni, amelyik G minden elérhető csúcsába eljut, akkor ahhoz állandóan nyilván kellene tartani a gráf már felfedezett részét, és a kapott séta hossza a G élei összhosszának tetszőlegesen sokszorosa lehetne. Azonban BFS-sel szemben szemben a DFS algoritmus természetes módon határoz meg egy bejárási sétát, hiszen egy csúcsból mindig egy másik, vele szomszédos csúcsba lépünk. Könnyen látható, hogy DFS algoritmusnak megfelelő G-beli séta olyan, ami a DFS fát oda-vissza végigjárja, és minden DFS fán kívüli élen is egyszer oda-vissza végigmegy.

Úgy tűnik, a DFS bejárás első leírása még jóval a gráfelmélet létezése előttről származik: az 1800-as években élt francia matematikus, Charles Pierre Trémaux mutatott rá, hogyan lehet egy kréta segítségével (amivel a folyosókra húzunk vonalakat) tetszőleges labirintusból véges idő alatt kijutni, ha ez egyáltalán lehetséges. Az általa leírt, a mélységi bejárást megvalósító szabály a következő. Kezdetben tetszőleges irányba indulunk, és ahogyan haladunk, krétánkkal mindvégig vonalat húzunk az érintett folyosón úgy, hogy egy folyosón sosem haladunk át harmadszor, tehát minden folyosón legfeljebb két vonal lesz. Döntési helyzet akkor áll elő, ha egy folyosó végére, egy kereszteződéshez érkezünk. Haladjunk innen tovább egy tetszőlegesen kiválasztott olyan folyosón, amin a lehető legkevesebb (de legfeljebb egy) vonal van. Ha ezt az eljárást követjük és a kijárat elérhető a labirintusban, akkor előbb-utóbb megtaláljuk azt, és amikor ez megtörténik, akkor a pontosan egyszer bejárt folyosók utat alkotnak a kiindulási pont és a kijárat között. Ha a kiindulási pontunkból nem érhető el kijárat, akkor előbb-utóbb olyan kereszteződéshez érünk, ahonnan minden folyosón már két vonal van. Ekkor a kiindulási pontban vagyunk, és a labirintus minden bejárható részét bejártuk. Ez a módszer tehát rendelkezik azzal a tulajdonsággal, hogy legfeljebb kétszer annyit kell gyalogolni, mint a labirintusbeli folyosók összhossza, sőt, még ennél is kevesebbet, mégpedig a kiindulási pont és a kijárat közti távolsággal.

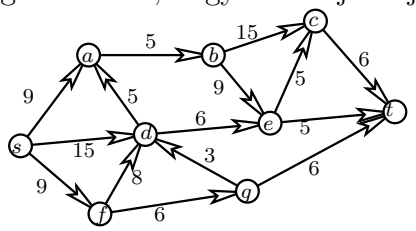
Persze itt sem úgy igaz minden, ahogy az ember elsőre gondolná. Érdemes megfigyelni, hogy a fenti eljárás ugyan nagyon szoros kapcsolatban van a mélységi bejárással, ám mégsem egészen arról van szó. Tanulságos meggondolni mi is a pontos különbség, és hogy hogyan kellene a Trémaux-szabályt megváltoztatni, hogy valóban a DFS szerint haladjunk. Ha ez sikerült, akkor azon lehet elmorfondírozni, hogy a két eljárás közül vajon melyik alkalmasabb a konkrét feladatra. ♦

A PERT-módszer: leghosszabb utak aciklikus gráfokban

A mélységi bejárás kapcsán előkerült aciklikus, irányított gráfok alkalmazására egy lehetséges példa a PERT-módszer (a név az angol „project evaluation and review technique" rövidítéséből származik). A probléma lényege egy összetett F feladat (project) optimális ütemezése. F részfeladatokból (tevékenységekből) áll, és F-t akkor tekintjük elvégzettnek, ha minden részfeladatát elvégeztük. A tevékenységek elvégzésére azonban bizonyos szabályok vonatkoznak. A szabályok mindegyike olyan alakú, hogy valamely v tevékenységet nem kezdhetünk hamarabb, mint egy másik u tevékenység megkezdése után $c(uv)$ idővel. (Pl. azért, mert v-t csak u befejezése után lehet elkezdeni, és u elvégzése éppen

$c(uv)$ ideig tart.) Definiálható tehát F-hez egy $P(F)$ irányított gráf, aminek csúcsai a tevékenységek. Minden szabálynak megfelel $P(F)$ egy súlyozott, irányított éle, a fenti szabálynak konkrétan az uv él felel meg, $c(uv)$ súllyal.

Világos, hogy az összetett feladat nem végezhető el, ha a $P(F)$ gráf irányított kört tartalmaz. (Valójában $P(F)$ tartalmazhat irányított kört, ha annak minden éle 0 súlyú. Ám ekkor az adott tevékenységeknek egy időben kell elkezdődniük, így a kört egy ponttal helyettesíthetjük, azaz az adott tevékenységeket egyetlen tevékenységnek tekintjük.) Feltehető tehát, hogy $P(F)$ aciklikus. Ha több forrása ill. nyelője van $P(F)$-nek, akkor érdemes $P(F)$-t kiegészíteni két csúccsal: az s csúcs fog a kiindulásnak megfelelni, minden más csúcsba fut s-ből egy-egy 0 súlyú él, ill. egy, az összetett feladat elvégzését reprezentáló t csúccsal, ahova minden egyéb csúcsból fut egy-egy él. Az ut él súlya az u tevékenység elvégzésének ideje, azaz az az idő, amennyit biztosan várni kell az u megkezdésétől, hogy F befejeződjék.



Egy PERT problémához tartozó gráf és élsúlyok

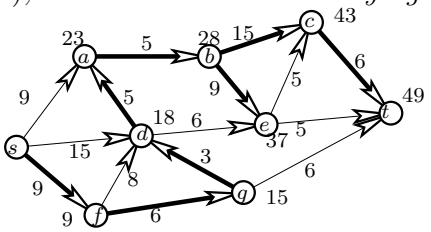
Az F feladat k *ütemezésése* abból áll, hogy az F minden tevékenységének úgy jelölünk ki egy-egy kezdési időpontot, hogy minden vonatkozó szabályt betartunk. Más szóval, $P(F)$ minden v csúcsához rendelünk egy $k(v)$ számot (v kezdési időpontját), úgy, hogy $k(s) = 0$, továbbá, hogy $P(F)$ minden uv élére $k(v) \geq k(u) + c(uv)$ teljesüljön. Az F feladat k ütemezés szerinti elvégzéséhez szükséges idő $k(t)$. Az F *optimális ütemezése* egy olyan k ütemezés, amire $k(t)$ minimális. Az F feladat $h(F)$ *hossza* az F végrehajtásához szükséges idő, azaz $h(F) = k(t)$, ahol k az F egy optimális ütemezése. Az u tevékenységet *kritikus tevékenységnek* nevezzük, ha u optimális ütemezés melletti kezdési időpontja nem függ az optimális ütemezéstől, azaz $k(u) = k'(u)$ bármely optimális k és k' ütemezésekre. (Úgy is mondhatjuk, hogy ha u-t nem kezdjük el „időben", akkor az egész F befejezése csúszik.)

A PERT-módszer célja az adott F feladahoz egy optimális ütemezés kiszámítása, $h(F)$ meghatározása, továbbá F kritikus tevékenységeinek meghatározása. A $P(F)$ gráf egy (irányított) útjának *súlya* az út által használt élek súlyának összege.

3.79. Tétel *A fentiek szerint megadott F feladat hossza megegyezik a $P(F)$ gráfban az irányított st-utak súlyának maximumával. Egy u tevékenység pontosan akkor kritikus, ha létezik u-n keresztül $P(F)$-ben $h(F)$ súlyú, irányíott st-út.*

A $P(F)$ gráf $h(F)$ súlyú, irányított st-útját a $P(F)$ kritikus útjának *nevezzük. A fenti tétel lényege éppen az, hogy a kritikus utak megtalálásával meghatározható mind*

$h(F)$, mind a kritikus tevékenységek halmaza.



Az előző PERT probléma optimális ütemezése és az azt meghatározó élek

Bizonyítás. Legyen $(s, u_1, u_2, \ldots, u_l, t)$ egy irányított st-út $P(F)$-ben, és legyen k az F egy optimális ütemezése. Ekkor definíció szerint

$$h(F) = k(t) \geq k(u_l) + c(u_l t) \geq k(u_{l-1}) + c(u_{l-1}u_l) + c(u_l t) \geq$$

$$\geq k(u_{l-2}) + c(u_{l-2}u_{l-1}) + c(u_{l-1}u_l) + c(u_l t) \geq \ldots \geq c(su_1) + \left(\sum_{i=1}^{l-1} c(u_i u_{i+1})\right) + c(u_l t) \ ,$$

azaz F hossza nem kevesebb, mint az irányított st-utak súlyának maximuma. A tétel első részének bizonyításához tehát elegendő egy k ütemezést és $P(F)$-ben egy $k(t)$ súlyú irányított st utat konstruálni.

Legyen $v_0 := s$, $k(v_0) := 0$ és legyen v_{i+1} a $G_{i+1} := G - \{v_0, v_1, \ldots, v_i\}$ gráfnak egy forrása. Ha már $k(v_1), k(v_2), \ldots, k(v_i)$-t meghatároztuk, legyen

$$k(v_{i+1}) := \max\{k(v_j) + c(v_j v_{i+1}) : v_j v_{i+1} \in E(P(F))\} \ ,$$

és jelöljük meg $P(F)$ mindazon $v_j v_{i+1}$ éleit, ahol a fenti maximum felvétetik. Világos, hogy az eljárás meghatározza $P(F)$ csúcsainak egy $v_0, v_1, \ldots$ sorrendjét és minden v_i-hez hozzárendel egy $k(v_i)$ számot. Mivel az eljárás során mindig forrást választottunk, ezért $P(F)$ minden $v_i v_j$ élére $i < j$ teljesül. A $k(v_j)$ definíciója alapján $k(v_j) \geq k(v_i) + c(v_i v_j)$ áll minden $v_i v_j$ élre, azaz k csakugyan egy ütemezés.

Minden $v_i \neq s$-hez van egy $v_j v_i$ megjelölt él, amire $j < i$. Ez azt jelenti, hogy minden v_i-be létezik s-ből irányított út megjelölt éleken. Létezik tehát egy csak megjelölt éleket használó $P = (s, v_{i_1}, v_{i_2}, \ldots, v_{i_l}, t)$ út is, amire

$$k(t) = c(v_{i_l} t) + k(v_{i_l}) = c(v_{i_l} t) + c(v_{i_{l-1}} v_{i_l}) + k(v_{i_{l-1}}) = \ldots = c(v_{i_l} t) + \sum_{j=l}^{1} c(v_{i_{j-1}} v_{i_j}) + c(s v_{i_1}) \ ,$$

□

azaz a P út súlya éppen $k(t)$. Ezzel a tétel első részét bebizonyítottuk. A bizonyítás azt is mutatja, hogy a P út minden csúcsa kritikus tevékenységnek felel meg.

A második részhez legyen Q a $P(F)$ azon csúcsainak halmaza, melyekből t elérhető megjelölt élekből álló, irányított úton. Világos, hogy minden $q \in Q$ csúcson keresztül

van megjelölt élekből álló, irányított st-út is, tehát minden Q-beli csúcs kritikus tevékenységnek felel meg.

Azt kell még látni, hogy ha egy v_l tevékenység nincs kritikus úton, akkor F nem kritikus. Válasszunek egy pozitív ε konstanst úgy, hogy $\varepsilon < c(v_iv_j)$ álljon minden *jelöletlen* v_iv_j élre (azaz v_i ε-nyi késése még nem okozza v_j késését). Válasszunk egy optimális k ütemezést, és késleltessük ε-nal minden, a v_l-ből jelölt élen elérhető tevékenység kezdési időpontját. Az ε választása miatt ez is ütemezés lesz, és mivel v_i nincs kritikus úton, ezért v_i-ből t nem érhető el. Vagyis az ütemezés optmiális marad, de v_i végrehajtása ε idővel elcsúszott.

A fenti bizonyítás egyben módszert is ad az F feladat hosszának, kritikus útjainak és kritikus tevékenységeinek megtalálására. Az algoritmus minden lépésben a maradék gráf egy forrását dolgozza fel. Hasznos látni, V pontjainak egy $v_1, v_2, \ldots$ sorrendje pontosan akkor lehet feldolgozási sorrend, ha a G gráf minden v_iv_j élére $i < j$ áll. Láttuk, hogy egy mélységi keresés során a csúcsok fordított befejezési sorrendje éppen ilyen lesz, persze, csak ha G valóban aciklikus. (Ha pedig a feladatkitűzéskor „csaltak", és volt G-ben irányított kör, akkor a mélységi keresés azt is felismeri a visszaél meglétéből.

Megjegyezzük, hogy a PERT módszer úgy is működik, ha egyszerre nem csak egy forrást dolgozunk fel, hanem (amennyiben több is van, akkor) tetszőleges számút: az első lépésben G forrásainak V_1 részhalmazát, aztán $G - V_1$ forrásainak V_2 részhalmazát, stb. A G gráf csúcsainak $V_1, V_2, \ldots$ halmazokra történő partícionlálását a G *emeletekre bontásának* is szokás nevezni. Ha tehát adott egy emeletekre bontás, akkor egy lépésben az aktuális emelet minden v forrására kiszámítjuk a $k(v)$ értéket, majd a következő emeletet dolgozzuk fel. A bizonyításban leírt algoritmus egy topologikus sorrendet, mint speciális emeletekre bontást használja: ebben minden emelet egypontú.

3.5. Hálózati folyamok és alkalmazásaik

A továbbiakban olyan irányított gráfokat vizsgálunk, amelyeknek minden éléhez tartozik egy, az adott élt valamilyen szempontból jellemző szám. Számos gyakorlati probléma vezet ilyen számozott élekkel rendelkező gráfokra, elég itt az imént tárgyalt legrövidebb utakra vagy a hamarosan felbukkanó) PERT problémára utalni. Mi itt most egy másik modellel foglalkozunk.

3.80. Definíció Hálózatnak *nevezünk egy olyan* (G, s, t, c) *négyest, amelyben* G *egy irányított gráf, aminek* s *és* t *különböző csúcsai, továbbá* G *minden* e *élét jellemzi egy nemnegatív* $c(e)$ *szám, az* e *él ú.n.* kapacitása. *(Nem követelmény, hogy a* G *aciklikus legyen: megengedünk irányított köröket is.)*

A G gráfot szemléletesen egy számítógéphálózat modelljének gondolhatjuk: G minden csúcsa egy-egy számítógép, és az s csúcsban található számítógépről szeretnénk információt küldeni a t csúcsbelibe. Az irányított élek a gépeket összekötő, kommunkikációs csatornáknak felelnek meg. Minden ilyen csatornán csak egy irányba küldhető információ, továbbá minden csatornának adott a maximális sávszélessége is. Egy más személet alapján egy csőhálózat modelljének tekinthető a hálózat, ahol s-ben tápláljuk a

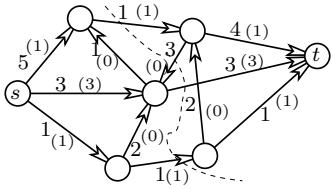
hálózatba a t-be szállítandó folyadékot. A csúcspontok közötti kapcsolatot reprezentáló élek itt egy-egy csőnek felelnek meg, aminek a $c(e)$ kapacitása azt fejezi ki, mennyi folyadékot lehet az adott csövön egységnyi idő alatt továbbítani. (A hasonlat annyiban sántít, hogy egy szokványos csövön bármerre lehet a folyadékot szállítani, míg a modellbeli irányított élek ezt csak egy irányba engedik meg. Azonban ha G minden irányított élének ellenkező irányítású párja is ugyanakkora kapacitású éle G-nek, akkor ez már valóban a kétirányú csőhálózat egy lehetséges modellje lesz. Ilyen értelemben tehát az irányított gráfmodell általánosabb a csőhálózatnál.) Természetes kérdés, hogy az adott kapacitáskorlátok mellett mennyi a hálózat átbocsátóképessége, azaz egységnyi idő alatt mennyi információ ill. folyadék juthat s-ből t-be.

A fenti bekezdésben az apró betű arra utal, hogy bár hasznos dolog szemléletes jelentést tulajdonítani a vizsgált hálozati modellnek, mindez nem elegendő a folyamok és az azt követő (Menger, párosítások) anyagrész elvárt szintű megértéséhez. Tapasztalatom szerint számos hallgató pusztán a szemléletes példa nagyjából ismeretével felvértezve vág neki a vizsgának, és nem képes definiálni az absztrakt fogalmakat (úgymint **hálózat, folyam, folyamnagyság,** st**-vágás** ill. **vágás kapacitása**). Tisztelettel szeretnék mindenkit lebeszélni az ilyesfajta próbálkozásról.

3.81. Definíció *A* (G, s, t, c) *hálózatban* folyamnak *mondunk egy olyan* f *függvényt, mely* G *minden éléhez egy számot rendel úgy, hogy*

1. $0 \leq f(e) \leq c(e)$ *teljesül* G *minden* e *élére, továbbá*
2. $\sum\{f(uv) : uv \in E(G)\} = \sum\{f(vu) : vu \in E(G)\}$ *áll* G *minden,* s*-től és* t*-től különböző* v *csúcsára.*

Az első *kapacitás-feltétel* azt fejezi ki, hogy a folyam minden élen legfeljebb kapacitásnyi lehet, a második, ú.n. *Kirchhoff-szabály* azt mondja ki, hogy minden, s-től és t-től különböző v csúcsra a befolyó folyam összmennyisége azonos a kifolyó összfolyammal, tehát egyetlen csúcsban sem keletkezik vagy tűnik el folyadék. A név egyúttal arra is utal, hogy a hálózati folyam fogalma az elektromos hálózatok elméletében is hasznos segédeszköz.



Hálózati folyam. A zárójelekben
az f folyam által felvett értékek állnak.
A folyamérték $m_f = 1 + 3 + 1 = 5$.
A szaggatott vonal 5 értékű st-vágást jelöl.
(A Ford-Fulkerson algoritmus másikat talál.)

3.82. Definíció *Az* f *folyam* m_f folyam nagysága *(ómagyarul: a folyam* értéke*) az a nettó folyammennyiség, ami* s*-ből kifolyik:*

$$m_f := \sum\{f(sv) : sv \in E(G)\} - \sum\{f(vs) : vs \in E(G)\} \ .$$

(Rendszerint nincs ok arra, hogy s*-be folyam érkezzen, hiszen onnan minél többet akarunk kijuttatni, de általában nem zárhatjuk ki ezt a lehetőséget sem. Az* s*-t elhagyó összfolyammennyiség kiszámításához tehát le kell vonni azt, ami* s*-be érkezik.)*

Az f folyam nagyságát máshogyan is kiszámíthatjuk.

3.83. Definíció *Legyen X a G csúcsainak egy s-t tartalmazó, de t-től diszjunkt részhalmaza. Az X és $V(G) \setminus X$ között futó éleinek halmazát a hálózat egy st-vágásának nevezzük. Az X által meghatározott st-vágás* kapacitása *az X-ből $V \setminus X$-be futó élek kapacitásösszege, azaz $\sum\{c(xv) : x \in X \not\ni v \in V(G)\}$.*

Szemlélet alapján világos, hogy az X által meghatározott st-vágás kapacitása felső korlát a lehetséges folyamnagyságra. Sőt, azt sem nehéz elhinni, hogy tetszőleges f folyam m_f folyam nagysága meghatározható úgy, hogy az X-ből $V(G) \setminus X$-be futó éleken haladó összfolyammennyiségből levonjuk a $V(G) \setminus X$-ből X-be továbbított folyammennyiséget. Ezt a két tényt bizonyítjuk az alábbiakban.

3.84. Állítás *Ha f a (G, s, t, c) hálózat egy folyama, és $s \in X \subseteq V(G) \setminus \{t\}$, akkor $m_f = \sum\{f(xv) : x \in X \not\ni v \in V(G)\} - \sum\{f(vx) : x \in X \not\ni v \in V(G)\}$, továbbá $m_f \leq \sum\{c(xv) : x \in X \not\ni v \in V(G)\}$.*

Bizonyítás. Felhasználva, hogy minden $s \neq x \in X$-re $\sum\{f(xv) : v \in V(G)\} - \sum\{f(vx) : v \in V(G)\} = 0$ és $0 \leq f(uv) \leq c(uv)$, kapjuk, hogy

$$m_f = \sum\{f(sv) : v \in V(G)\} - \sum\{f(vs) : v \in V(G)\} = \sum_{x \in X} \Big(\sum\{f(xv) : v \in V(G)\} - \sum\{f(vx) : v \in V(G)\} \Big) =$$

$$= \sum_{x \in X} \Big(\sum\{f(xv) : v \in V(G) \setminus X\} - \sum\{f(vx) : v \in V(G) \setminus X\} \Big) =$$

$$= \sum\{f(xv) : x \in X \not\ni v \in V(G)\} - \sum\{f(vx) : x \in X \not\ni v \in V(G)\} \leq \sum\{c(xv) : x \in X \not\ni v \in V(G)\}$$ □

Az st-vágás tehát egy kézenfekvő eszköz annak bizonyítására, hogy a folyamnagyság nem lehet nagyobb egy adott mennyiségnél. Valójában ennél jobb bizonyíték nem is kell: a maximális folyamnagyság pontosan megegyezik a minimális vágáskapacitással. Ezt mondja ki az alábbi „max-flow min-cut” (MFMC) tétel.

3.85. Tétel (Ford-Fulkerson tétel) *Ha (G, s, t, c) egy véges hálózat, akkor létezik egy f folyam és egy $s \in X \subseteq V(G) \setminus \{t\}$ részhalmaz úgy, hogy az m_f folyamnagyság azonos az X által definiált st-vágás kapacitásával.*

Bizonyítás. Először (a teljesség kedvéért) igazoljuk, hogy létezik maximális folyam, azaz olyan f folyam, melyre $m_f \geq m_{f'}$ minden f' folyamra. Nyilván az $X = \{s\}$ által meghatározott vágás véges kapacitása felső korlát a lehetséges folyamnagyságokra. A lehetséges folyamnagyságok x szuprémuma tehát véges. Azt kell megmutatni, hogy létezik x nagyságú folyam. A szuprémum definíciója miatt léteznek $f_1, f_2, \ldots$ folyamok, amelyekre $\lim_{n \to \infty} m_{f_n} = x$. Az f_n sorozatnak a G gráf minden e éléhez van olyan részsorozata, hogy a részsorozat az e élen konvergens. Véve a részsorozatok részsorozatait, az eredeti f_n sorozatnak olyan f_{n_i} részsorozatát kapjuk, melyre teljesül, hogy G minden e élére $f_{n_i}(e)$ konvergens. Jelölje $f(e)$ az $f_{n_i}(e)$ sorozat határértékét. Mivel $0 \leq f_{n_i}(e) \leq c(e)$, ezért a rendőr-elv (régebbi nevén csendőr-szabály) miatt $0 \leq f(e) \leq c(e)$, és a limeszként kapott f függvényre a Kirchhoff-feltétel teljesülése hasonlóan következik. Azt kaptuk tehát, hogy f valóban folyam. A folyamnagyság

definíciójából pedig az látszik, hogy $x = \lim m_{f_n} = \lim m_{f_{n_i}} = m_f$, tehát f csakugyan egy maximális nagyságú folyam.

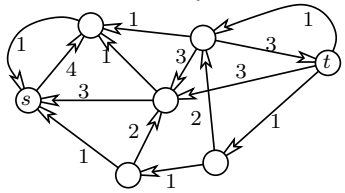
Legyen tehát f maximális nagyságú folyam. A célunk f segítségével egy m_f kapacitású vágás megtalálása. Bevezetjük a (G_f, s, t, c_f) hálózatot a $G_f = (V(G), E_f)$ segédgráfon, melyre $E_f := E_f^{elore} \cup E_f^{vissza}$, ahol

$$E_f^{elore} := \{uv : f(uv) < c(uv)\} \qquad E_f^{vissza} := \{vu : 0 < f(uv)\} .$$

G_f-nek tehát előre és visszaélei vannak: az előreélek G azon élei, amin még tovább növelhető a folyam, a visszaélek pedig G azon éleinek a fordítottjai, amelyeken a folyam pozitív, tehát csökkenthető. A G_f segédgráfon definiáljuk a

$$c_f(uv) := \begin{cases} c(uv) - f(uv) & \text{ha } uv \text{ előreél} \\ f(vu) & \text{ha } uv \text{ visszaél} \end{cases}$$

kapacitásokat. Ha tehát van egy P irányított út G_f-ben s-ből t-be (ú.n. javító út), akkor P előreélein ε-nal megnövelve f-t, P visszaéleinek megfordítottjain ε-nal csökkentve f-t egy, a Kirchhoff-szabályt teljesítő f'-t kapunk. Ha ε-t alkalmasan választjuk (nevezetesen ε a P út élein a c_f kapacitásfüggvény minimális értéke) akkor az eredeti kapacitásfeltételek is fennmaradnak, tehát f' folyam lesz, melynek nagysága $m_{f'} = m_f + \varepsilon > m_f$, ellentmondásban f maximalitásával.



Az előző példához tartozó (G_f, s, t, c_f) segédhálózat. (Nem tartalmaz javító utat.)

Legyen tehát X a G_f-ben s-ből elérhető pontok halmaza. A fentiek alapján $t \notin X$, azaz X csakugyan st-vágást határoz meg. Mivel X-ből nem lép ki G_f-nek éle, ezért minden X-ből $V(G) \setminus X$-be vezető uv élre $f(uv) = c(uv)$, és minden $V(G) \setminus X$-ből X-be lépő uv élen $f(uv) = 0$. Ha tehát az előző állítás felhasználásával számítjuk ki az m_f folyamnagyságot az X által definiált st-vágás segítségével, akkor $m_f = \sum\{f(xv) : x \in X \not\ni v \in V(G)\} - \sum\{f(vx) : x \in X \not\ni v \in V(G)\} = \sum\{c(xv) : x \in X \not\ni v \in V(G)\}$, ami éppen az X által meghatározott st-vágás kapacitása. □

Ha a c kapacitásfüggvény G minden élén egész értéket vesz fel, akkor a fenti bizonyítás egyben módszert is kínál a maximális folyam keresésére: kiindulunk az $f_0 \equiv 0$ folyamból, és elkészítjük az $f_0, f_1, f_2, \ldots$ folyamok sorozatát úgy, hogy $0 = m_{f_0} < m_{f_1} < m_{f_2} < \ldots$ egészek. Ha f_k-t már megtaláltuk, és f_k minden élen egész értéket vett fel, akkor a G_{f_k} segédgráfban keresünk egy P utat s-ből t-be, és f_{k+1}-t úgy kapjuk, hogy P mentén ε-nyi

folyamot vezetünk, ahol ε a P élei mentén a c_{f_k} kapacitásfüggvény minimális értéke. (Pontosabban P előreélein ε-nal növeljük, visszaéleinek fordítottjain ε-nal csökkentjük f_k-t.) Eztáltal az f_{k+1} folyam is minden élen egész lesz, hisz az ε meghatározásához bizonyos $c_{f_k}(e)$ (pozitív egész) kapacitások minimumát kellett képezni. Tehát $m_{f_k} < m_{f_{k+1}}$, és az $m_{f_{k+1}}$ folyamnagyság is egész. Mivel a maximális folyamnagyságot bármely vágáskapacitás felülről korlátozza, előbb-utóbb olyan f_l folyamot kapunk, amin már nem tudunk a fenti eljárással javítani. Ekkor tehát nincs a G_{f_l} segédgráfban st-út, létezik tehát m_{f_l} kapacitású vágás, tehát az f_l folyam minden élen egész és egyúttal maximális nagyságú is. Ezzel igazoltuk a Ford és Fulkerson alábbi tételét.

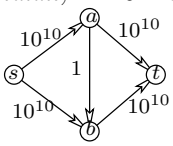
3.86. Tétel (Egészértékűségi (EgÉr) lemma) *Ha a (G, s, t, c) hálózatban minden e él $c(e)$ kapacitása egész szám, akkor létezik olyan maximális f folyam, hogy f a G gráf minden élén egész értéket vesz fel. Az ilyen folyamot* egészfolyamnak *nevezzük.*□

A fenti algoritmus akkor is véges eljárás, ha nem azt kötjük ki a kapacitásokról, hogy egészek, hanem csupán annyit, hogy racionálisak. Ekkor ugyanis minden egyes javításkor legalább a kapacitások közös nevezőjének reciprokával növeljük a folyam nagyságát, amit nem tehetünk meg végtelen sokszor. Ha azonban a c kapacitásfüggvény nem racionális, akkor még akár az is megtörténhet, hogy minden f_k-t tudjuk tovább javítani, ráadásul az m_{f_k} folyamnagyságok nem a maximális folyamnagysághoz, hanem egy annál kisebb számhoz konvergálnak. Egy másik kellemetlenség, hogy a fenti, növelő utas algoritmus sokszor sajnos nem elég hatékony. Az alábbi tétel mindkét problémára megoldást kínál.

3.87. Tétel (Edmonds-Karp tétel) *Ha a (G, s, t, c) hálózatban a maximális folyamot a javítóutas algoritmussal keressük, és mindig egy legkevesebb élből álló javító út mentén növelünk, akkor a maximális folyam meghatározásához szükséges lépésszám felülről becsülhető $|V(G)|$ polinomjával.*□

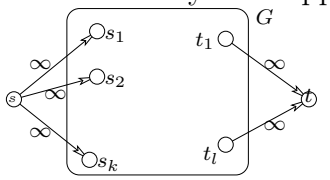
3.88. Megjegyzés *Az Edmonds-Karp tétel tehát azt biztosítja, hogy a legrövidebb javító utakon maximális mértékű javításokat végrehajtva gyorsan találjunk maximális folyamot.*

Ha eszetlenül próbálunk javítani, akkor indokolatlanul sok munkába kerülhet egy maximális folyam megtalálása: az ábrán látható hálózatban felváltva az sabt ill. sbat javító utakat választva mindig csak egységnyit tudunk emelni a folyamnagyságon, tehát az Edmonds-Karp algoritmus által két javítás után megtalált, $2 \cdot 10^{10}$ nagyságú maximális folyamot csillagászati számú lépés után találjuk csak meg.

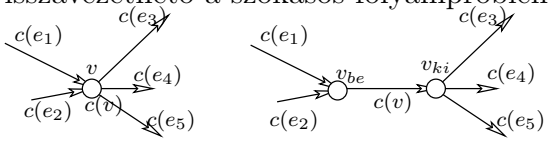


A folyamprobléma kiterjeszthető arra az esetre is, ha több forrásból több nyelőbe akarunk folyamot vezetni, de nincs megkötés arra, hogy melyik forrásból melyik nyelőbe érkezzék a folyam. Ha tehát $s_1, s_2, \ldots, s_k$ a források, $t_1, t_2, \ldots, t_l$ a nyelők, akkor bevezetünk egy-egy új s ill. t csúcsot, majd s-ből minden s_i-be ill. minden t_j-ből t-be vezetünk

egy ∞ kapacitású élt. (Ez így csalás. Egy hálózatban az élek kapacitása véges. A végtelen azonban itt annyit jelent, hogy olyan (véges) kapacitást adunk az adott élnek, hogy az ne legyen semminek se korlátja. Konkrétan: az ss_i él kapacitása legyen több, mint amennyi folyam az s_i-ből kifolyhat, és a t_jt él kapacitása pedig legyen több annál, mint amennyi folyam t_j-be érkezhet az odavezető éleken.) Ezzel a választással minen esetre az új hálózatbeli folyamok éppen a többtermelős, többfogyasztós folyamnak felelnek meg.



Értelmezhető az a folyamprobléma is, ahol nemcsak az éleknek, hanem a pontoknak is van kapacitásuk, ami felső korlát a ponton átfolyó folyammennyiségre. Ez a probléma is visszavezethető a szokásos folyamproblémára az alábbiak szerint.



Minden kapacitással rendelkező v csúcsból egy v_{be} és egy v_{ki} csúcsot képezünk: a v-be befutó éleket a v_{be} csúcsba vezetjük, a v-ből kiinduló élek pedig a v_{ki} csúcsból indulnak, továbbá bevezetünk egy $v_{be}v_{ki}$ élt a v csúcs kapacitásával. (Ezt az operációt a v pont *széthúzásának* nevezzük.) A pontszéthúzásokkal létrejövő hálózat folyamai a pontkapacitásos hálózat folyamainak felelnek meg, és viszont.

Lehetséges általánosítás még, hogy a hálózatban irányítatlan élek is vannak, amelyeken mindkét irányban folyhat folyam. Mint azt már a szakasz elején jeleztük, ekkor bevezetve két, ellentétesen irányított élt az irányítatlan él két végpontja között az elhagyott irányítatlan él kapacitásával, akkor a probléma ismételten visszavezethető hálózati folyamokra: minden hálózati folyamnak megfelel egy folyam az irányítatlan éleket tartalmazó gráfban, és minden, az irányítatlan éleket használó folyamnak megfelelnek folyamok a hálózatban. Ha azt szeretnénk, hogy kölcsönösen egyértelmű legyen a megfeleltetés, akkor azzal a megszorítással is élhetünk, hogy a konstruált hálózatban csak olyan folyamokat nézünk, amelyek rendelkeznek azzal a tulajdonsággal, hogy bármely irányítatlan élnek megfelelő két, oda-vissza irányított él közül legalább az egyiken 0 folyam folyik. A továbbiakban élni fogunk ezzel a feltevéssel.

Történelem: A folyammodell eredete

Ford és Fulkerson munkájának alapja az amerikai légierő számára 1955-ben készített, titkos Harris-Ross jelentés volt. Ebben a jelentésben az európai vasúti hálózatot egy 44 csúcsú, 105 élű gráffal modellezték. Az egyes csúcsok a vasúti igazgatóságoknak, az élek pedig az ezek között futó vasútvonalaknak feleltek meg. A CIA által szolgáltatott adatok alapján minden élhez egy tonnában mért kapacitást tudtak rendelni, és az így létrejött hálózatban kerestek maximális folyamot, ill. minimális vágást. A légierő érdeklődésének homlokterében természetesen a minimális vágás megtalálása állt: a hidegháború idején amerikai

szemmel valós veszélynek tűnt a Vörös Hadsereg nyugat-európai inváziója. Ennek megállítására a logisztika hatékony rombolása tűnt az egyetlen lehetőségnek. Azon túl, hogy a titkos jelentésben megtalálják a konkrét minimális vágást (érdekesség, hogy ez Lengyelországot kettévágja, majd a Csehszlovák-Szovjet, ill. Magyar-Román határ mentén halad), be is bizonyítják, hogy ennél jobb nincs, ugyanis mutatnak egy azonos nagyságú folyamot is a szovjet támaszpontokból Nyugat-Európába. A légicsapások tervezését elősegítendő, a jelentés egyúttal módszert is ad egy hálózat minimális vágásának meghatározására. Ross tábornok jól értette a hadsereg működését. A jelentésben hangsúlyozta: a javasolt új módszer nem forgatja fel fenekestül az eddigi rendszert, mert a számítógépet kezelő specialisták mellett továbbra is elengedhetetlen a jól képzett katonai szakértők munkája.

Ford és Fulkerson az absztrakt hálózati modellben kimondta és bebizonyította a maximális folyam – minimális vágás tételt, ami az ezután kialakuló kombinatorikus optimalizálás tudományának egyik alappillére lett, és ezáltal jelentős hatást gyakorolt számos más tudományterületre, pl. a gráfelméletre. A jelen jegyzetben a hálózati folyamokra támaszkodva fogjuk feldolgozni a következő két fejezetet (a Menger tételek ill. páros gráfok párosításainak áttekintését), amelyek bár jóval korábbi eredmények, tárgyalásuk a hálózatok ismeretében sokkal egységesebb. ♦

3.5.1. Menger tételei és gráfok többszörös összefüggősége

3.89. Definíció *A G irányított vagy irányítatlan gráf u ponjából v pontjába futó P és Q útjait* éldiszjunktaknak *vagy* élidegennek *(*pontdiszjunktaknak *vagy* pontidegennek*) nevezzük, ha $E(P) \cap E(Q) = \emptyset$ (ill. $V(P) \cap V(Q) = \{u, v\}$).*

Az éldiszjunkt (pontdiszjunkt) uv-utak maximális számát $\lambda(u, v)$-vel (ill. $\kappa(u, v)$-vel) jelöljük.

3.90. Definíció *Azt mondjuk hogy a G (irányított vagy irányítatlan) gráf U ponthalmaza (ill. F élhalmaza)* lefog *minden uv-utat, ha a $G - U$ (ill. $G - F$) gráfban nem létezik u-ból v-be (irányított) út.*

3.91. Tétel (Menger tételei) *1. Ha u és v a G irányított gráf különböző csúcsai, akkor az élidegen uv-utak ($\lambda_G(u, v)$-vel jelölt) maximális száma azonos az uv-utakat lefogó élek minimális számával.*

2. Ha u és v a G irányított gráf különböző, nem szomszédos csúcsai, akkor a pontidegen uv-utak ($\kappa_G(u, v)$-vel jelölt) maximális száma azonos az uv-utakat lefogó, u-tól és v-től különböző csúcsok minimális számával.

3. Ha u és v a G irányítatlan gráf különböző csúcsai, akkor az élidegen uv-utak ($\lambda_G(u, v)$-vel jelölt) maximális száma azonos az uv-utakat lefogó élek minimális számával.

4. Ha u és v a G irányítatlan gráf különböző, nem szomszédos csúcsai, akkor a pontidegen uv-utak ($\kappa_G(u, v)$-vel jelölt) maximális száma azonos az uv-utakat lefogó pontok minimális számával.

Bizonyítás. Világos, hogy a lefogó élek ill. pontok száma mind a négy esetben *legalább* annyi, mint a szóbanforgó utak száma, hisz a maximális számú út mindegyike egy-egy

különböző élt ill. pontot tartalmaz a lefogókból. A továbbiakban tehát mind a négy esetben bebizonyítjuk, hogy a lefogó elemek száma *legfeljebb* annyi, mint a pont- ill. éldiszjunkt utak maximális száma.

1. Definiáljuk a $(G, u, v, \mathbf{1})$ hálózatot. Ebben a hálózatban minden uv egészfolyam 0-t vagy 1-t rendel minden élhez. Legyen f ebben a hálózatban egy maximális nagyságú folyam, és legyen X olyan ponthalmaz, ami egy minimális uv-vágást határoz meg. Mivel minden él kapacitása egész, ezért az EgÉr lemma miatt feltehetjük, hogy f egészfolyam, és a nagysága mondjuk k. Ez itt azt jelenti, hogy G bármely élen vagy 0 vagy 1 mennyiségű folyam folyik. Az is igaz még, hogy az X ponthalmaz (ami u-t tartalmazza de v-t nem) olyan vágást határoz meg, aminek a kapacitása k. Ez itt azt jelenti, hogy X-ből pontosan k él lép ki. Világos, hogy ezt a k élt elhagyva nem tudunk az X halmazból $V \setminus X$-be eljutni, tehát ez a k él minden uv utat lefog, vagyis az uv-utakat lefogó élek minimális száma legfeljebb k. A továbbiakban tehát nincs más célunk, mint azt megmutatni, hogy létezik k éldiszjunkt uv-út G-ben.

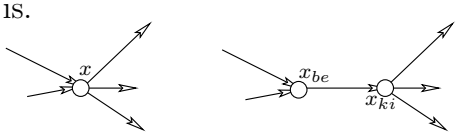
Az f maximális egészfolyamra gondolhatunk úgy, mint a javító utas algoritmus által szolgáltatott folyamra, hiszen egész kapacitások esetén az bizonyosan minden élen egész értéket vesz fel. Mivel minden él kapacitása egységnyi, ezért minden egyes javító út pontosan egy egységnyivel javította az aktuális folyamot, tehát a javító utas algoritmus pontosan k javító utat használt f konstrukciójában. Csábító gondolat, hogy ezzel készen is vagyunk, hiszen *„a k javító útnak az egységnyi kapacitások miatt muszáj éldiszjunktnak lennie, ezért máris megtaláltuk a keresett k éldiszjunkt uv-utat”.* Sajnos azonban ez a következtetés hibás, de szerencsére nem menthetetlenül. Ha mondjuk valami kozmikus szerencse folytán az f folyam konstrukciójában minden növelő út csak előreélekből állt, akkor helyes a következtetés. Ha azonban a növelő utakban visszaélek is szerepeltek, akkor még akár az a furcsaság is megtörténhet néhány növelés után, hogy a folyamban keletkezik egy minden mástól diszjunkt irányított kör, ahol pozitív mennyiségű folyam áramlik körbe, ám sem a körbe befelé, sem a körből kifelé nem folyik semmi. Amit az alábbiakban bebizonyítunk, az voltaképpen az, hogy tetszőleges f folyamhoz létezik olyan f' folyam, ami f-fel azonos nagyságú, minden élkapacitást legfeljebb annyira használ ki, mint f, ráadásul f' megkapható a növelő utas algoritmussal úgy, hogy mindig csak előreéleket használunk.

Tekintsük tehát a fent definiált, k nagyságú f folyamot, és legyen E' a G azon éleinek halmaza, amelyeken 1 egységnyi folyam folyik. A Kirchoff-szabály miatt minden u-tól és v-től különböző w csúcsra igaz, hogy E'-nek pontosan annyi éle mutat w-be, mint amennyi E'-beli él kilép w-ből. Abból pedig, hogy f nagysága k az következik, hogy u-ból k-val több E'-beli lép ki, mint amennyi u-ba érkezik, v-be pedig éppen k-val több éle érkezik E'-nek, mint amennyi kilép belőle. Tekintsük a $G^* = (V, E^*)$ gráfot, ahol az E^* élhalmazt úgy kapjuk, hogy E'-höz hozzáveszünk még k párhuzamos vu élt. A G^* gráf konstrukciója folytán G^* minden csúcsának megegyezik a kifoka és a befoka. Legyen K a G^*-nak az az irányítatlan értelemben vett komponense, ami az u csúcsot tartalmazza. A vu élek bevétele miatt K tartalmazni fogja persze a v csúcsot is. Az Euler-körsétákról szóló tétel irányított változata szerint K-nak létezik Euler-körsétája. Ha ebből a körsétából elhagyjuk az utólag bevett k párhuzamos vu élt, akkor a körséta k *éldiszjunkt* irányított uv sétára esik szét. Minden ilyen uv sétából (esetleges körök elhagyása után) kiválasztható egy-egy irányított uv-út.

Azt kaptuk tehát, hogy létezik k éldiszjunkt irányított uv-út és egyúttal k éllel lefog-

ható minden irányított uv-út G-ben. Ezért az éldiszjunkt irányított uv-utak maximális száma legalább annyi, mint az összes irányított uv utat lefogó élek minimális száma. A triviális max $\leq$ min egyenlőtlenséggel ezt egybevetve éppen a Menger tétel 1. része adódik.

2. Húzzunk szét minden u-tól és v-től különböző x pontot G-ben, azaz helyettesítsük x-t egy x_{be} és egy x_{ki} ponttal, vezessünk minden x-be futó élt egy, az x_{be} csúcsba érkező éllel, minden x-ből kiinduló élt egy, az x_{ki} csúcsból induló éllel, és húzzunk be egy $x_{be}x_{ki}$ élt is.

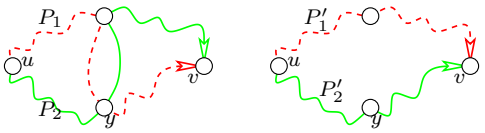


Ha ezt G minden $x \neq u, v$ csúcsára elvégezzük, akkor az így kapott G' gráfban k éldiszjunkt uv-út pontosan k pontdiszjunkt útnak felel meg G-ben, és viszont.

A már bebizonyított (első) Menger tétel szerint tehát létezik G'-nek $\kappa_G(u, v)$ éle, amelyek G' minden uv utját lefogják. Minden ilyen élnek kiválasztható egy-egy végpontja, aminek a G-beli megfelelője sem nem u, sem pedig v. (Itt használjuk ki, hogy u és v nem szomszédosak.) Világos, hogy ezáltal legfeljebb $\kappa_G(u, v)$ pontját jelöljük ki G-nek, ráadásul ezek a pontok a konstrukció folytán minden G-beli uv-utat lefognak.

3. Készítsük el a G' irányított gráfot úgy, hogy G minden élét oda és vissza is megirányítjuk! (G'-nek tehát kétszer annyi (hurokéltől különböző) éle lesz, mint G-nek.) Világos, hogy G'-ben létezik $\lambda_G(u, v)$ darab éldiszjunkt, irányított uv-út, hiszen G-ben van ennyi, és azok irányított változatai megteszik. Másfelől, ha G'-ben van k darab éldiszjunkt, irányított uv-út, akkor létezik k darab ilyen azzal a tulajdonsággal is, hogy ezen utak nem használnak ellentétesen irányított éleket.

Ha ugyanis egy $P_1 = (u \dots xy \dots v)$ út használja az xy élt, egy másik $P_2 = (u \dots yx \dots v)$ út pedig az yx élt, akkor a $P_1' = (u \dots x \dots v)$ illetve $P_2' = (u \dots y \dots v)$ utak ugyanazokat az éleket használják, mint P_1 és P_2, kivéve xy-t és yx-t.



Ha tehát minden olyan élre elvégezzük a fenti konstrukciót, amit két út oda-vissza használ akkor G'-ben kapunk k darab *irányított* uv-utat, amelyeknek a G-ben ugyanennyi (immár) éldiszjunkt, irányítatlan uv-út felel meg. Azt kaptuk tehát, hogy G'-ben az éldiszjunkt, irányított uv-utak maximális száma szintén $\lambda_G(u, v)$.

A már bizonyított első Menger tétel miatt létezik tehát G'-ben $\lambda_G(u, v)$ él, ami minden G'-beli uv-utat lefog. A konstrukció folytán ezen élek G-beli, irányítatlan megfelelői lefognak minden irányítatlan uv utat, ráadásul ez a G-beli élhalmaz is legfeljebb $\lambda_G(u, v)$ méretű.

4. Alkalmazzuk itt is a 3. rész bizonyításában használt konstrukciót: képezzük a G' gráfot a G éleinek oda-vissza irányításával. Világos, hogy az irányítatlan pontdisz-

junkt G-beli uv-utak kölcsönösen egyértelműen megfelelnek az irányított, pontdiszjunkt G'-beli uv-utaknak. Tehát G'-ben az irányított pontdiszjunkt utak maximális száma $\kappa_G(uv)$. A már bizonyított, második Menger tétel alapján létezik G'-nek $\kappa_G(u,v)$ pontja úgy, hogy azok minden irányított uv-utat lefognak. A konstrukció folytán ugyanezek a pontok lefognak G-ben is minden irányítatlan uv-utat, és nekünk éppen ezt kellett bizonyítanunk. □

A Menger tételek bizonyításának lényege, hogy kisebb-nagyobb átalakítások után az állítás közvetlenül adódik a hálózati folyamok MFMC tételéből, hiszen egy maximális diszjunkt útrendszer egy maximális nagyságú *egész*folyamból, a minimális lefogó halmaz pedig egy minimális kapacitású vágásból adódott. Ez a megfigyelés egy újabb előnyét mutatja a fenti bizonyításnak: amennyiben mi egy maximális pont- vagy éldiszjunkt útrendszerre illetve egy minimális, minden utat lefogó pont- vagy élhalmazra vagyunk kíváncsiak, akkor nem kell mást tenni, mint meghatározni az ismert módon egy maximális egészfolyamot illetve egy minimális vágást a gráfból képzett hálózatban.

Történelem: Menger és Kőnig
Menger 1927-ben publikálta a tételét, amely eredeti formájában az irányítatlan pontdiszjunkt változattal volt ekvivalens. Kőnig Dénes észrevette, hogy a tétel Menger által adott bizonyítása hibás, és egyúttal ki is javította az eredeti bizonyítást: a hiányzó láncszem a páros gráfokra vonatkozó (hamarosan sorra kerülő) $\nu = \tau$ egyenlőség volt. Kőnig levélben feltárta Mengernek a hibát, és azt is megírta neki, hogyan lehet kijavítani azt. Menger válaszában közölte, hogy tudott a dologról, és azt a készülő könyvében már kijavította, ám hogy hogyan, azt már nem árulta el. Az említett könyvben valóban egy helyes bizonyítás szerepel, de Menger egy szóval sem említi, hogy az eredeti bizonyítása hiányos. És természetesen Kőnig nevét is hiába keresnénk a szóban forgó résznél.

A Menger tétel Ford-Fulkerson alapú bizonyításához nem használtuk fel Kőnig tételét, ellentétben az eredeti bizonyítással, amihez szükség volt arra. Érdemes azonban látni e két tétel kapcsolatát is, ezért az a páros gráfokról szóló fejezetben levezetjük a Kőnig tételt Menger eredeti tételéből (És igen: a vizsgán azt is elfogadjuk az ott elsőnek közölt bizonyítás helyett.) ♦

3.92. Definíció *Az irányítatlan G gráfot* k-szorosan (pont)összefüggőnek *(röviden* k-összefüggőnek*) nevezzük, ha G-nek legalább $(k+1)$ pontja van, és G összefüggő marad, bárhogyan is hagyunk el belőle legfeljebb $k-1$ pontot. A maximális k-t, amire G k-összefüggő $\kappa(G)$ jelöli.*

3.93. Definíció *A G irányítatlan gráfot* k-szorosan élösszefüggőnek *(röviden* k-élösszefüggőnek*) nevezzük, ha G összefüggő marad, bárhogyan is hagyunk el belőle legfeljebb $k-1$ élt. A maximális k-t, amire G k-élösszefüggő $\lambda(G)$ jelöli.*

3.94. Tétel *Egy egyszerű, irányítatlan G gráf pontosan akkor k-összefüggő ha G-nek legalább $(k+1)$ pontja van, és G bármely két különböző pontja között létezik k pontidegen út. G pontosan akkor k-élösszefüggő, ha G bármely két, különböző pontja közt vezet k élidegen út.*

Bizonyítás. Az irányítatlan Menger tételekből könnyen adódik: ha bármely két pont között van k él- ill. pontdiszjunkt út, akkor G nem eshet szét k-nál kevesebb pont ill. él elhagyásával. Ha G k-élösszefüggő, akkor semelyik két pont közti utakat sem fogja le k-nál kevesebb él (azok elhagyásával ugyanis G szétesne), ezért Menger 3. tétele szerint tetszőleges két pont között létezik k élidegen út. Ezzel a tétel éldiszjunkt változatát igazoltuk.

A pontdiszjunt esethez tegyük fel indirekt, hogy G k-összefüggő, és u-ból v-be legfeljebb $k-1$ pontdiszjunkt út található. Ha u és v nem szomszédosak, akkor Menger 4. tétele miatt az uv-utak lefoghatók legfeljebb $k-1$ ponttal. Ezek elhagyásával G szétesne, de ez ellentmond G k-szoros összefüggőségének.

Ha $uv \in E(G)$, akkor az uv él törlése után keletkező G' gráf legfeljebb $k-2$ pontdiszjunkt uv utat tartalmaz, tehát Menger 4. tétele szerint létezik $k-2$ pontja, aminek elhagyásakor G' szétesik. A szétesett gráfban ismét összekötve az u és v pontokat egy legalább 3 pontú gráfot kapunk (hisz G-nek legalább $k+1$ pontja volt), mely az uv él törlésétől szétesik. De ekkor az uv él helyett u vagy v valamelyike is törölhető, hogy a gráf szétessen. Ismét azt kaptuk, hogy G legfeljebb $k-1$ alkalmas pont törlésével szétesik, ami a k-szoros összefüggőségnek mond ellent. □

3.95. Tétel (Menger) *Ha G legalább 3 pontú gráf akkor az alábbi állítások ekvivalensek.*

(1) G 2-összefüggő, (2) G bármely 2 pontján át vezet kör. Ha G-nek nincs izolált pontja, akkor a fentiekkel ekvivalens az is, hogy (3) G bármely 2 élén át vezet kör.

Bizonyítás. (1) $\Rightarrow$ (2). Ha G 2-összefüggő, akkor bármely u, v pontja között van két pontidegen út, amelyek együtt egy u-t és v-t tartalmazó kört alkotnak.
(2) $\Rightarrow$ (1). A kör tekinthető két pontidegen út uniójának, azaz bármely két pont között létezik legalább 2 pontidegen út, és az előző tétel szerint (figyelembevéve, hogy G legalább 3 pontú), azt jelenti, hogy G 2-összefüggő.
(3) $\Rightarrow$ (2). Ha u-n és v-n keresztül akarunk kört találni, akkor elegendő egy-egy u-ra és v-re illeszkedő élen keresztül kört találni, ami a (3) feltétel szerint létezik.
(1) $\Rightarrow$ (3) G úgy is 2-összefüggő marad, ha két élét felosztjuk egy-egy ponttal. (2) miatt létezik a felosztó pontokon keresztül kör, ami épp egy, a felosztott éleken keresztüli körnek felel meg. □

3.96. Tétel (Dirac tétele) *Ha G k-összefüggő, és $k \geq 2$, akkor G bármely k pontján keresztül található kör G-ben.*□

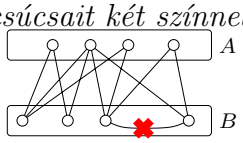
3.5.2. Páros gráfok, párosítások és gráfparaméterek

3.97. Definíció *A G gráf páros gráf, ha G két színnel kiszínezhető, azaz, ha $\chi(G) \leq 2$.*

3.98. Megjegyzés *A fenti definíció azzal ekvivalens, hogy a G gráf pontosan akkor páros, ha G csúcsai két diszjunkt halmazba oszthatók úgy, hogy G minden éle a két halmaz között fut, azaz mindkét halmazban van egy-egy csúcsa. (Ez egyébként a páros gráf szokásos definíciója.) Minden páros gráfnak van tehát két színosztálya, amelyek között az élei futnak. Azonban ez a két színosztály nem feltétlenül egyértelmű: pl az n pontból álló üres gráf csúcsainak tetszőleges két osztályra bontása teljesíti a feltételt. (Könnyen látható, hogy a két színnel való színezés pontosan akkor egyértelmű, ha a páros gráf összefüggő.)*

Ha hangsúlyozni akarjuk, hogy a szóbanforgó $G = (V, E)$ gráf *páros*, és egyúttal az A és B színosztályokat is meg szerenénk adni, akkor használhatjuk az egyébként elég szerencsétlen $G = (A, B; E)$ jelölést.

3.99. Megfigyelés *1. Minden páros hosszú kör páros gráf, t.i. felváltva ki lehet színezni a csúcsait két színnel.*



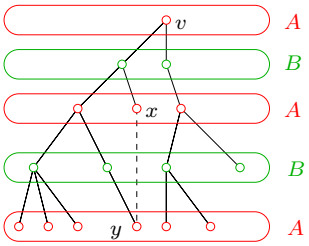
2. Páratlan körre ezt nem tehetjük meg, mert mikor körbeérünk, két azonos színű pont szomszédos lesz. A páratlan kör tehát nem páros gráf.
3. Ha egy gráf páros, akkor minden részgráfja is páros.
4. Páros gráf ezért nem tartalmazhat ptn kört. Megadjuk a páros gráfok egy ekvivalens jellemzését.

3.100. Tétel *A G véges gráf pontosan akkor páros, ha G nem tartalmaz páratlan kört (azaz, ha G minden köre páros).*

3.101. Következmény *Mivel a fában nincs kör (hát még ptn kör), ezért minden fa páros gráf.*

A 3.100. Tétel bizonyítása. Szükségesség: az előző megfigyelésből közvetlenül adódik.

Elégségesség: tegyük fel, hogy G nem tartalmaz páratlan kört. Azt kell megmutatni, hogy létezik alkalmas 2-színezés. Mivel élek csak a gráf komponensein belül futnak, ezért elegendő egy komponensen belül találni egy 2-színezést, azaz feltehető, hogy G összefüggő. Legyen F a G egy feszítőfája, és v pedig G egy tetszőleges pontja (F gyökere). Legyen A a v-től az F fán páros távolságra levő csúcsok, B pedig a v-től F-en páratlan hosszú úton elérhető csúcsok halmaza. (Pl. $v \in A$.) Világos, hogy F minden éle A és B között fut, de megmutatjuk, hogy ugyanez G-re is igaz. Innen az állítás következik, hisz ezáltal G pontjait két színosztályra tudtuk bontani.



Ha tehát futna G-nek egy xy éle (mondjuk) az A halmazon belül (B-re a bizonyítás szó szerint megegyezik), akkor létezne G-ben egy $xy \dots v \dots x$ páratlan hosszúságú körséta, melyet az iménti él, a v-t az x-szel ill. a v-t az y-nal összekötő F-beli utak határoznak meg. Ha ebből a körsétából levágjuk az F-beli vx-út és vy-út közös részét, amit a körséta duplán jár be, akkor a körsétából páros sok él marad ki, és maradék éle G-nek egy páratlan körét alkotják, ami ellentmondás. □

3.102. Definíció *A $G = (V, E)$ gráf éleinek M részhalmaza* független, *más szóval M* (részleges) párosítás, *ha az M-beli élek végpontjai különbözők, azaz G minden csúcsából legfeljebb egy M-beli él indul. Az M párosítás* teljes párosítás, *ha M G minden pontját* fedi, *azaz G minden csúcsára illeszkedik egy M-beli él.*

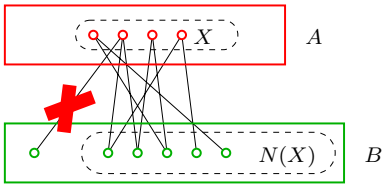
3.103. Példa *Egy tánciskolában tanuló fiúk ill. lányok halmazai alkossák a G páros gráf színosztályait. Fusson G-ben él két csúcs között, ha az adott fiú és lány hajlandó egymással táncolni. Ekkor G minden párosítása egy lehetséges táncpartner-választási szituációt ír le. Ebben a modellben a hatékony oktatás érdekében a tánctanár minél több élből álló párosítást szeretne találni, mely optimális esetben egy teljes párosítás.*

Egy másik lehetséges példa, ha a gráf csúcsai az egyetem termeinek ill. az ott folyó előadásoknak felelnek meg. Akkor van él egy teremnek és egy előadásnak megfelelő csúcs között, ha a terem alkalmas az adott előadás megtartására. Egy adott pillanatban az egyetemen folyó tevékenység egy párosítást indukál az előbb definiált segédgráfban.

3.104. Definíció *A $G = (V, E)$ gráf $X \subseteq V$ ponthalmaz szomszédainak halmazát $N(X)$ jelöli: $N(X) := \{v \in V : \exists x \in X,$ melyre $xv \in E\}$.*

3.105. Tétel (Frobenius tétele) *A $G = (A, B; E)$ véges, páros gráfnak pontosan akkor létezik teljes párosítása, ha $|A| = |B|$ és $|X| \leq |N(X)|$ minden $X \subseteq A$ ponthalmazra.*

3.106. Tétel (Hall tétele) *A $G = (A, B; E)$ véges, páros gráfnak pontosan akkor létezik A-t fedő párosítása, ha $|X| \leq |N(X)|$ minden $X \subseteq A$ ponthalmazra.*



A 3.106. Hall tételben szereplő feltételt szokás *Hall-feltételnek* hívni.

A 3.105. Frobenius tétel bizonyítása a 3.106. Hall tételéből. Világos, hogy ha van G-ben teljes párosítás, akkor egyrészt $|A| = |B|$ teljesül, továbbá a teljes párosítás egyúttal fedi az A színosztályt, tehát $|X| \leq |N(X)|$ teljesül minden $X \subseteq A$ ponthalmazra.

Most tegyük fel, hogy $|A| = |B|$ és teljesül a Hall-feltétel. A 3.106. Hall tétel miatt ekkor létezik G-ben egy A-t fedő M párosítás, és $|A| = |B|$ miatt az M párosítás B-t is fedi, tehát M teljes párosítás. □

Tehát a Frobenius tétel triviálisan következik a Hall tételből, így elég ez utóbbit igazolni, amit pedig a Kőnig tételből fogunk levezetni.

3.107. Definíció *Adott G gráf esetén $\nu(G)$ jelöli a G független élhalmazai közül a maximális méretét, azaz G maximális párosításának elemszámát.*

3.108. Definíció *A G gráf pontjainak U halmaza* lefogó ponthalmaz*, ha G minden élének van U-beli végpontja. A legkevesebb pontból álló lefogó ponthalmaz méretét $\tau(G)$ jelöli.*

3.109. Állítás *Ha G véges gráf, akkor $\nu(G) \leq \tau(G)$. (Itt G nem feltétlenül páros gráf.)*

Bizonyítás. Legyen M G-nek egy maximális ($\nu(G)$ élből álló) párosítása. Ha U egy minimális méretű lefogó ponthalmaz, akkor lefogja M minden élét is, ám U minden pontja legfeljebb egy párosításélt fog le. Tehát $\tau(G) = |U| \geq |M| = \nu(G)$. □

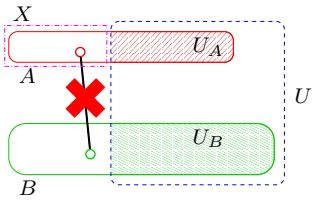
3.110. Tétel (Kőnig tétele) *Ha $G = (A, B; E)$ véges, páros gráf, akkor $\nu(G) = \tau(G)$.*

Történelem: Frobenius és Kőnig
Frobenius 1912-ben publikált egy determinánsokra vonatkozó eredményt, ami a gráfok nyelvén fogalmazva a páros gráfok teljes párosításának jellemzésével egyenértékű. Kőnig 1915-ben ettől az eredménytől függetlenül bizonyította a szóbanforgó tételét, amit aztán elküldött Frobeniusnak. Frobenius később megjelentetett egy elemi bizonyítást a saját tételére, majd ugyanitt úgy említette Kőniget, mint akinek az eredménye könnyen következik az övéből. Mindezen túl azt is megjegyezte, hogy „az a gráfelmélet masinéria, amin Kőnig bizonyítása alapszik nem sokat segít a determinánsok elméletében, hiszen Kőnig tétele egy meglehetősen speciális, nem sokat érő állítás. Minden, ami Kőnig eredményéből használható, megtalálható az ő saját, determinánsokról szóló tételében". Nos, az idő nem Frobeniust igazolta. ♦

A 3.106. Hall tétel bizonyítása. A szükségesség nyilvánvaló: ha létezik A-t fedő párosítás, akkor minden A-beli pontnak különböző párja van, tehát tetszőleges $X \subseteq A$ esetén az X-beli elemek B-beli párjai az $N(X)$ egy $|X|$ méretű részhalmazát alkotják.

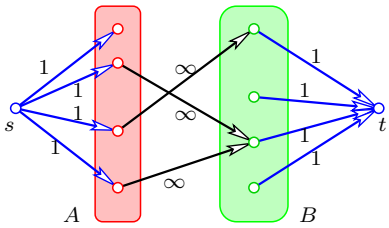
Az elégségességhez tegyük fel, hogy $|X| \leq |N(X)|$ minden $X \subseteq A$-ra. Azt kell igazolnunk, hogy $\nu(G) \geq |A|$. Legyen U minimális (azaz $\tau(G)$ méretű) lefogó ponthalmaz, és legyen $U_A := U \cap A$, $U_B := U \cap B$. Mivel U lefogja az $X := A \setminus U_A$-ból induló éleket, ezért $N(X) \subseteq U_B$, tehát $|N(X)| \leq |U_B|$. A Kőnig tétel ill. a Hall feltétel miatt

$$\nu(G) = \tau(G) = |U| = |U_A| + |U_B| \geq |U_A| + |N(X)| \geq |U_A| + |X| = |A| \ .$$



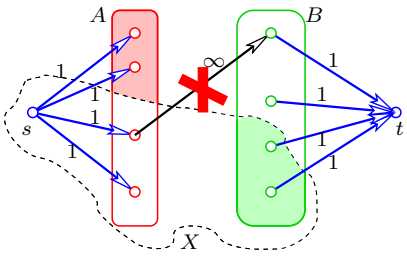
□

A 3.110. Kőnig tétel bizonyítása. Legyen G' az alábbi gráf. Irányítsuk G minden élét A-ból B-be, vegyünk fel egy új s és t pontot, vezessünk s-ből élt A minden pontjába, és vegyünk fel egy-egy élt B minden pontjából t-be. Adjunk minden élnek kapacitásokat: az s-ből induló ill. t-be érkező éleké legyen 1, az A-ból B-be futóké pedig legyen ∞ (pontosabban $|A|+1$). Tekintsük a (G', s, t, c) hálózatot, ahol c az imént definiált kapacitást jelenti.



Vegyük észre, hogy ha G-ben van egy k méretű párosítás, akkor létezik ebben a hálózatban k nagyságú egészfolyam: a párosításéleknek megfelelő éleken, az ezen élek A-beli végpontjaihoz vezető s-ből induló éleken, valamint a párosításélek B-beli végpontjaiból t-be vezető éleken legyen a folyam által felvett érték 1, minden egyéb élen 0. Az is könnyen látható, hogy a hálózatban minden egészfolyam úgy áll elő, hogy néhány, A-ból B-be vezető független élen a folyam 1 értéket vesz fel, ezeket az éleket s-ből tápláljuk, a kifolyó folyamot pedig t-be engedjük. A hálózatban tehát a maximális egészfolyam értéke $\nu(G)$, és az EgÉr lemma miatt a maximális folyamérték is ugyanennyi.

A Ford-Fulkerson tétel szerint létezik tehát egy $\nu(G)$ kapacitású vágás. Ha ezt a vágást az s-t tartalmazó X halmaz definiálja, akkor $X \cap A$-ból nem futhat G'-nek éle $B \setminus X$-be, hisz akkor a vágás kapacitása ∞ volna. (Pontosabban legalább $|A|+1$, de már az is több, mint $\nu(G)$, hisz A egy lefogó halmaz, ahonnan $\nu(G) \leq |A|$.) Ez azt jelenti, hogy $(A \setminus X) \cup (B \cap X)$ egy lefogó ponthalmaz, tehát $|A \setminus X| + |B \cap X| \geq \tau(G)$. A hálózat konstrukciójából adódóan az X által definiált vágás kapacitása $\nu(G) = |A \setminus X| + |B \cap X| \geq \tau(G)$. A Kőnig tétel előtt bizonyítottuk, hogy $\nu(G) \leq \tau(G)$ áll, ahonnan $\nu(G) = \tau(G)$ adódik.



□

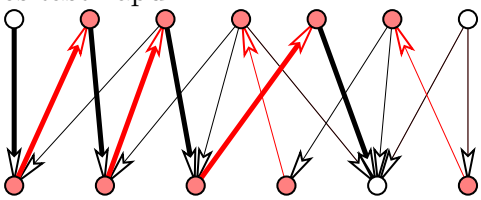
A 3.110. Kőnig tétel bizonyítása Menger tételével. Most hagyjuk meg a G gráfot irányítatlannak, de vegyük fel az s és t pontokat, vezessünk s és A minden pontja ill. t és B minden pontja között egy-egy élt. Világos, hogy ha létezik G-ben k független él, akkor ezek segítségével találunk k pontdiszjunkt st-utat a fent konstruált G' gráfban. Másfelől, ha ismerünk k pontdiszjunkt st-utat G'-ben, akkor az ezek által használt G-beli élek függetlenek. Tehát a G-ben a független élek maximális száma megegyezik G'-ben a pontdiszjunkt st-utak maximális számával: $\nu(G) = \kappa_{G'}(s,t)$.

Minthogy G'-ben s és t nem szomszédosak, alkalmazhatjuk Menger 4. tételét, amely szerint a pontdiszjunkt st-utak maximális száma ($\kappa_{G'}(s,t)$) megegyezik a minden st-utat lefogó, s-től és t-től különböző pontok minimális számával. Csupán azt kell észrevenni, hogy G csúcsainak egy U részhalmaza pontosan akkor fogja le G minden élét, ha ugyanez az U ponthalmaz G'-ben lefog minden st-utat. Tehát G-ben a lefogó pontok minimális száma megegyezik a G'-ben minden st-utat lefogó, s-től és t-től különböző pontok minimális számával: $\tau(G) = \kappa_{G'}(s,t) = \nu(G)$, ahol az utóbbi egyenlőséget a bizonyítás első részében láttuk be. □

Az alternáló utas algoritmus

A Kőnig tétel iménti bizonyításából hatékony algoritmust kaphatunk egy páros gráf maximális párosításának ill. minimális lefogó ponthalmazának megtalálására. Ha ugyanis a maximális folyamok meghatározására szolgáló javító utas módszert a Kőnig tétel bizonyításában leírt konstrukcióra alkalmazzuk, és eltekintünk az s-re ill. t-re illeszkedő élektől, akkor az alábbi eljárás adódik. Kiindulunk az üres párosításból, és azt javítgatjuk. Ha már találtunk egy M párosítást, akkor tekintjük az M-hez tartozó segédgráfot, azaz M éleit B-ből A-ba irányítjuk, G egyéb éleit pedig A-ból B-be.

Ha ebben a segédgráfban létezik egy P irányított út egy A-beli, az aktuális M párosítás által fedetlen pontból olyan B-beli pontba, melyet szintén nem fed a párosítás, akkor ezen az ú.n. *alternáló úton* az eddigi párosításéleket elhagyva, és P párosításon kívüli éleit bevéve (más szóval M helyett $M \Delta P$-t tekintve), egy eggyel nagyobb méretű párosítást kapunk.



Ha pedig nincs javító alternáló út, akkor M maximális párosítás, és könnyen található egy $|M|$ csúcsot tartalmazó lefogó ponthalmaz is.

Történelem: A magyar módszerről
Néha –helytelenül– a fent ismertetett eljárást nevezik *magyar módszernek*. Az „igazi" magyar módszer az amerikai Harold Kuhn találmánya. Történt ugyanis 1953-ban, hogy Kuhn éppen Kőnig Dénes könyvét lapozgatta, amikoris megakadt a szeme egy lábjegyzeten, mely Egerváry Jenő egy 1931-ből származó magyar nyelvű cikkére hivatkozik, mint a maximális párosításokról szóló $\nu = \tau$ tétel általánosítására. Kuhnt pedig éppen az a probléma érdekelte, hogy hogyan lehet egy páros gráfban nem maximális, hanem *maximális súlyú* párosítást találni. (A maximális párosítás a maximális súlyúnak speciális esete, amennyiben minden él súlya pontosan 1.) Nos, a nyom helyesnek bizonyult: Egerváry cikkében valóban erről volt szó. Ám ahhoz, hogy ez kiderüljön, pinduri kis elszántságra volt szükség: Kuhn egy magyar szótár és egy nyelvtankönyv segítségével két hét alatt lefordította magának a cikket. A módszer segítségével, a cikkben leírtak szerint meghatározta egy háromjegyű élsúlyokkal rendelkező, 24 csúcsú páros gráf egy maximális súlyú párosítását. A tény, hogy ehhez „mindössze" 3 órára volt szüksége, meggyőzte őt a módszer helyességéről. Magát az algoritmust tehát Kuhn írta le, de azt Egerváry tiszteletére magyar módszernek nevezte el, és azóta az egész világ így ismeri. Csupán ezzel a nagylelkű gesztussal Kuhn valószínűleg jóval többet tett a hazai matematika nemzetközi elismertségéért, mint Frobenius és Menger együttvéve. ♦

A továbbiakban nem feltétlenül páros gráfok párosításait, illetve a párosítások szempontjából hasznos paramétereit vizsgáljuk.

3.111. Definíció *A G gráf pontjainak U részhalmaza* független *(vagy* stabil*), ha U nem feszít élt, azaz G minden élének van nem U-beli végpontja. A G gráf legtöbb pontból álló, független ponthalmazának méretét $\alpha(G)$ jelöli.*

A G gráf éleinek F halmaza lefogó élhalmaz*, ha G minden pontjából indul F-beli él. Ha a G gráfnak van lefogó élhalmaza (azaz G-nek nincs izolált pontja), akkor a G gráf legkevesebb élből álló, lefogó élhalmazának méretét $\rho(G)$ jelöli.*

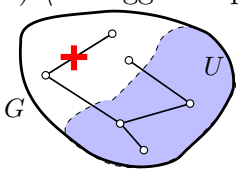
3.112. Megfigyelés *Tetszőleges, véges G gráfra $\alpha(G) \leq \rho(G)$.*

Bizonyítás. Már önmagában egy $\alpha(G)$ méretű független ponthalmaz lefogásához legalább $\alpha(G)$ él szükséges. □

3.113. Tétel (Gallai tétele) *Legyen G n pontú gráf.*

1. *Ha G-ben nincs hurokél, akkor $\tau(G) + \alpha(G) = n$.*
2. *Ha G-nek nincs izolált pontja, akkor $\nu(G) + \rho(G) = n$.*

Bizonyítás. 1.: Könnyen látható, hogy $U \subseteq V(G)$ pontosan akkor lefogó ponthalmaz, ha $V(G) \setminus U$ független ponthalmaz. Az állítás innen közvetlenül adódik.



2.: Mivel G-nek létezik $\nu(G)$ diszjunkt éle, ezek $2\nu(G)$ pontot fognak le. A maradék $n - 2\nu(G)$ pont mindegyike lefogható egy-egy új éllel (hisz nincs izolált pont), azaz $\nu(G) + n - 2\nu(G) = n - \nu(G)$ éllel minden pont lefogható. Innen $\rho(G) \leq n - \nu(G)$, ahonnan $\nu(G) + \rho(G) \leq n$ adódik.

Másrészről, könnyen látható, hogy ha F minimális méretű lefogó élhalmaz, akkor F körmentes, és nem tartalmaz 3 hosszú utat sem. Tehát F diszjunkt csillagok uniója. (A csillag olyan összefüggő gráf, melynek (legfeljebb) egy híján minden pontjának foka 1.) Ha a minimális lefogó élhalmazban k csillag van, akkor e halmaz $n - k$ élt tartalmaz, másrészt e halmaz tartalmaz k diszjunkt élt, tehát $\nu(G) \geq k$. Azt kaptuk, hogy $\rho(G) + \nu(G) \geq n - k + k = n$, és innen a másik irányú egyenlőtlenség figyelembevételével következik a tétel. □

A Gallai tétel egy lehetséges alkalmazása a

3.114. Tétel (Kőnig tétel) *Ha a G véges, páros gráfnak nincs izolált pontja, akkor $\alpha(G) = \rho(G)$*

Bizonyítás. Páros gráfban hurokél nem lehet, így az állítás következik Kőnig előző tételéből és Gallai két tételéből: $\alpha(G) = |V(G)| - \tau(G) = |V(G)| - \nu(G) = \rho(G)$. □

A maximális párosítás méretének (azaz a $\nu(G)$ gráfparaméternek) a meghatározása nem csak páros gráfok esetén érdekes. Ezért hasznos megfigyelés, hogy a javító alternáló utakkal való növelés (elméletileg) itt is maximális párosítást ad. (A páros gráfokon használt alternáló ill. javító út fogalma értelemszerűen kiterjed nem páros gráfokra is.)

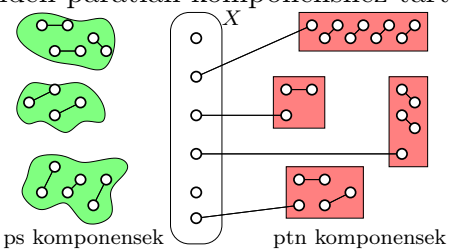
3.115. Tétel (Berge tétele) *A G gráf M párosítása pontosan akkor maximális, ha nincs M-hez javító út.*

Bizonyítás. Ha M nem maximális, akkor létezik egy $|M|$-nél több élt tartalmazó N párosítás. Az $M \cup N$ élhalmaz egy komponense vagy a két párosítás közös éle, vagy egy olyan M-alternáló út, mely egyben N-alternáló is egyúttal (ún. MN-alternáló út), vagy egy olyan kör, melynek élei felváltva M ill. N-beliek (MN-alternáló kör). Mivel $|N| > |M|$, ezért kell olyan MN-alternáló útnak lennie, ami több N-beli élt tartalmaz, mint M-belit. Az ilyen út az M párosítás javító útja. □

Hogyan lehet bebizonyítani, hogy egy adott gráf nem tartalmaz teljes párosítást? Páros gráf esetén láttuk, hogy egy, a színosztályméretnél kisebb lefogó ponthalmaz megfelelő bizonyíték. Jó ez a bizonyíték nem páros gráfokra is, de pl. már K_3 esetén sem elég jó: $\nu(K_3) = 1 < 2 = \tau(K_3)$. Nem páros esetre a következő állítás mutat egy lehetséges bizonyítékot. Egy G gráf páratlan komponenseinek számát $c_p(G)$ jelöli.

3.116. Állítás *Ha a G véges gráfnak létezik k olyan pontja, melyek elhagyása után több, mint k páratlan komponens keletkezik (azaz $c_p(G - X) > |X|$ valamely $X \subseteq V(G)$-re), akkor G-nek nincs teljes párosítása.*

Bizonyítás. Ha G-nek van teljes párosítása és $X \subseteq V(G)$, akkor $G - X$ minden páratlan komponensének van olyan v pontja, hogy a v-t fedő párosításél nem a komponensen belül fut, azaz kilép a belőle. Ezen párosításél másik végpontja szükségképp X-ben van. Tehát minden páratlan komponenshez tartozik egy-egy különböző X-beli pont.



□

A fenti állítás alkalmas megfordítása is igaz.

3.117. Tétel (Tutte tétele) *A véges G gráfnak pontosan akkor van teljes párosítása, ha tetszőleges $X \subseteq V(G)$ esetén $c_p(G - X) \leq |X|$ teljesül.*□

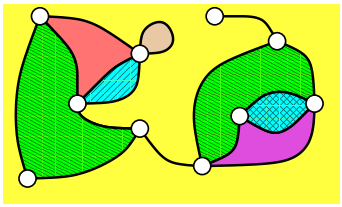
A Tutte tétel egy fontos következménye az alábbi.

3.118. Tétel (Petersen tétele) *Minden véges 3-reguláris 2-élösszefüggő gráfnak van teljes párosítása.*

Bizonyítás. Legyen $G = (V, E)$ egy 3-reguláris, 2-élösszefüggő gráf. Tutte tétele miatt csak azt kell igazolni, hogy V tetszőleges X részhalmazára $c_p(G - X) \leq |X|$ áll. Legyen tehát K a $G-X$ egy páratlan komponense. A K komponensből kilépő élek a K definíciója folytán mind X-be futnak, és mivel G 2-élösszefüggő, ezért K-ból legalább két él lép ki. Mivel azonban K-ban a fokszámösszeg $3 \cdot |K|$ páratlan, ezért K-ból páratlan sok élnek kell kilépnie. Azt kaptuk tehát, hogy $G - X$ minden páratlan komponenséből legalább 3 él lép ki, így X és a $G - X$ páratlan komponensei között futó élek száma legalább $3 \cdot c_p(G - X)$. Másrészt ezen élek mindegyikének van X-beli végpontja, ezért (mivel X minden csúcsa 3-adfokú) legfeljebb $3 \cdot |X|$ ilyen él létezhet. Vagyis $3|X| \geq 3c_p(G - X)$, azaz $c_p(G - X) \leq |X|$. Nekünk pedig pontosan ezt kellett bizonyítanunk. □

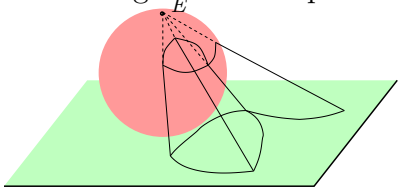
3.6. Síkgráfok

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, és külső tartományról nem beszélünk.



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

Bizonyítás. 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.))



G tetszőleges síkbarajzolását a sztereografikus projekció a G gömbre rajzolásába viszi, továbbá, ha az északi sarok egy gömbi tartomány belsejében fekszik, akkor G gömbre rajzolását a G síkbarajzolásába képezi. 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. □

3.120. Következmény *Tetszőleges konvex poliéder élhálója síkbarajzolható.*

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

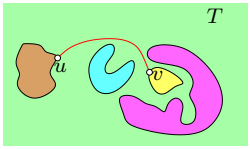
3.121. Megjegyzés *A fenti állítás megfordítása úgy igaz, hogy tetszőleges G síkbarajzolható gráfhoz létezik egy P konvex poliéder, úgy, hogy G a P élhálójának egy részgráfjával izomorf.*

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

Bizonyítás. 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

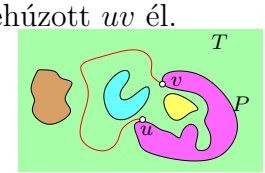
rendre $e_i = i$, t_i ill. k_i. Húzzunk be G_i-be egy $(i+1)$-dik élt (mondjuk uv-t). Így kapjuk a G_{i+1} gráfot. Vizsgáljuk meg, G_{i+1} megfelelő paramétereit, azaz az $e_{i+1}, t_{i+1}, k_{i+1}$ számokat!

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 feltehető, hogy annak a tartománynak a határán halad, amelyik tartományba 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, amelyek G_i-é voltak. Legyen T a G_i gráfnak az a tartománya, aminek a belsejében vezet az imént behúzott uv él.



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

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

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

3.124. Következmény *Ha G síkbarajzolható, akkor bármely síkbarajzolásának ugyanannyi tartománya van.* □

3.125. Következmény *Ha G egyszerű, legalább 3 pontú, síkbarajzolható gráf, akkor $e \leq 3n - 6$.*

Bizonyítás. Húzzunk be annyi további élt a síkbarajzolhatóság megtartásával, amennyit csak tudunk. Világos, hogy egy n csúcsú, síkbarajzolható, összefüggő G' gráfot kapunk. Legyen G' éleinek és tartományainak száma rendre e' és t'. Minden tartományt 3 él, és minden él 2 tartományt határol G'-ben, ezért $2e' = 3t' = 3(e' + 2 - n) = 3e' + 6 - 3n \Rightarrow 3n - 6 = e' \geq e$. □

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

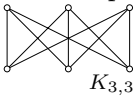
3.127. Következmény *Ha G síkbarajzolható és egyszerű, akkor van legfeljebb 5-ödfokú csúcsa, azaz $\delta(G) \leq 5$.*

Bizonyítás. 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. □

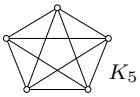
3.128. Következmény *Sem K_5, sem $K_{3,3}$ nem síkbarajzolható.*

Bizonyítás. 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. □

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



$K_{3,3}$

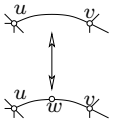


K_5

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.

3.130. 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.*



3.131. Tétel (Kuratowski tétele) *A G gráf pontosan akkor síkbarajzolható, ha nem tartalmaz sem $K_{3,3}$-mal, sem K_5-tel topologikusan izomorf részgráfot.*

Bizonyítás. Szükségesség: ha G síkbarajzolható, akkor minden H részgráfja síkbarajzolható. Ha H síkbarajzolható és K topologikusan izomorf H-val, akkor K is síkbarajzolható. Így $K = K_5$ ill. $K = K_{3,3}$ nem lehetséges ha G síkbarajzolható volt. Az elégségesség nem triviális, itt nem bizonyítjuk.□

3.132. Tétel (Fáry-Wagner tétel) *Ha G egyszerű, síkbarajzolható gráf, akkor G úgy is síkba rajzolható, hogy minden él egyenes szakaszként van lerajzolva.*

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.)

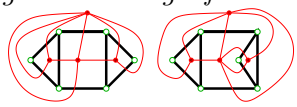
Igy megkapjuk egy G'-t részgráfként tartalmazó, csupa háromoldalú tartománnyal rendelkező G^* gráf egyenes szakaszokkal való síkbarajzolását. Helyettesítsük G^* minden élét egy gumiszalaggal, rögzítsük az A, B és C csúcsok helyzetét, majd hagyjuk, hogy a gumik összehúzódásával a rendszer egyensúlyba 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.) □

3.6.1. Síkgráfok dualitása

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.

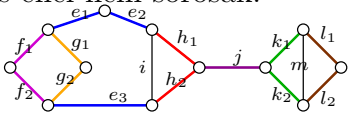
3.133. Megjegyzés *A G^* duális gráf nem(csak) G-től, hanem G adott síkbarajzolásától függ. Adott síkgráf különböző síkbarajzolásai nemizomorf duálisokat definiálhatnak.*



A fenti ábra illusztrálja, hogy különböző síkbarajzolásokhoz különböző duális tartozhat. (Egyszer van 6-odfokú csúcs, másszor nincs.

3.134. Definíció *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.*

Az ábrán látható G gráf azonos színnel és betűvel jelzett élei egymással páronként sorosak, míg a j a G egyedüli elvágó éle. Az i és m élek sem nem elvágó élek, sem pedig más éllel nem sorosak.



3.135. Tétel *Legyen $G = (V, E)$ síkbarajzolható. (1) Ha G^* a G duálisa, akkor G^* síkbarajzolható és összefüggő.*

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

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

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

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

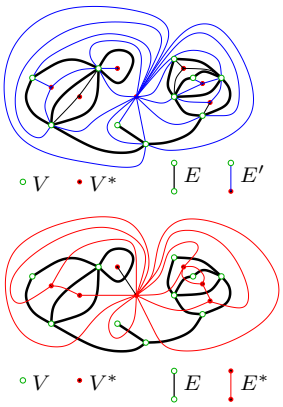
(6) Ha G összefüggő, akkor $G = (G^*)^*$, és ekkor G pontjai bijektíven G^* lapjainak felelnek meg.

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

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

Bizonyítás. (1): Elkészítünk egy $G' = (V', E')$ gráfot az alábbiak szerint. A síkbarajzolt G gráf minden l lapján felveszünk egy v_l pontot, legyen $V^* := \{v_l : l \text{ } G \text{ lapja}\}$, és legyen $V' := V \cup V^*$. A G' gráf minden éle egy V-beli és egy V^*-beli pont között fut. Az éleket úgy kapjuk, hogy minden V-beli v csúcsból annyi E'-élt indítunk, ahány E-beli indul v-ből, mégpedig úgy, hogy v körül felváltva következzenek az E-beli ill. E'-beli élek. Ha egy v-ből induló E'-beli 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 megkapjuk a $G'' := G' \cup E$ gráf egy síkbarajzolását.

Vizsgáljuk meg G'' fenti síkbarajzolásának tartományait! Mivel minden E'-beli élnek van V-beli végpontja, és a V-beli pontok körül az E-beli és E'-beli élek felváltva követik egymást, ezért G'' minden lapjának van V-beli csúcsa és G'' minden lapját határolja E-beli él. Legyen l'' a G'' egy tetszőleges lapja, amit a G gráf egy uv éle határol. Mivel G'' a G gráfból élek behúzásával keletkezik, ezért l'' a G valamely l lapjának része, és ezért l''-t határolnia kell az uv_l és vv_l éleknek is. Azt kaptuk tehát, hogy G'' minden lapját három él határolja, és ezek közül pontosan egy él lesz E-beli.



A G' és G^* gráfok

Ha tehát sorra elhagyjuk a G'' gráf E-beli éleit, akkor a minden éltörléskor két háromszöglapból keletkezik egy új négyszöglap, és a végén kapott G' gráf minden lapját 4 él határolja. Ezek szerint G' olyan síkbarajzolt gráf aminek segítségével úgy kapható G egy síkbarajzolása G bizonyos négyszöglapjaiba (a lapon belül haladva) behúzunk egy átlót. Világos, hogy azt is megtehetjük, hogy ugyanezen négyszöglapokon nem a V-beli csúcsokat összekötő átlót húzzuk be, hanem (szintén a lapon belül maradva) a V^*-belieket összekötőt. Ezáltal újfent egy síkbarajzolt gráfot kapunk, ami definíció szerint épp a G^* duális gráf lesz.

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

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

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

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

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

ekvivalenciák másik iránya a fentiekhez hasonlóan bizonyítható.

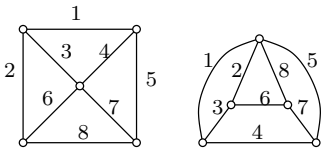
(8) F a G max körmentes részgráfja $\iff$ $f(F)$ a G^* max (elvágó élhalmaz)-mentes részgráfja $\iff$ $F^* := G^* - f(F)$ a G^* min összefüggő részgráfja, $\iff$ F^* feszítőfa (hisz G^* (1) miatt összefüggő). □

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.

3.136. Definíció *A G gráf a H gráf* absztrakt duálisa*, ha létezik egy $\varphi : E(G) \to E(H)$ bijekció úgy, hogy az alábbi két ekvivalencia teljesüljön:*

1. *C a G köre $\iff$ $\varphi(C)$ a H vágása és*
2. *Q a G vágása $\iff$ $\varphi(Q)$ a H köre.*

3.137. Megjegyzés *A fenti definícióban elegendő lenne csupán az első ekvivalencia teljesülését megkívánni, mert abból a második már következik, de ezt nem bizonyítjuk.*



3.138. Példa *Az ábrán látható két gráf egymás absztrakt duálisa, a számozás adja az élek közti bijekciót.*

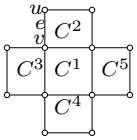
Világos, hogy minden síkbarajzolható G gráfnak létezik absztrakt duálisa (akár több, nemizomorf is), hiszen tetszőleges síkbarajzoláshoz tartozó G^* duálisgráf megfelel. Nem világos azonban, hogy vajon létezik-e nem síkbarajzolható gráfoknak duálisa.

3.139. Tétel (Whitney tétel) *A G gráfnak pontosan akkor létezik absztrakt duálisa, ha G síkbarajzolható.*

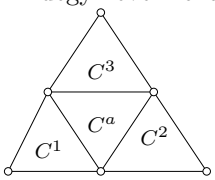
Bizonyítás. (Vázlat) Világos, hogy ha $G^{(*)}$ a G gráf absztrakt duálisa, és H a G részgráfja, akkor az $E(H)$-nak megfelelő élek $G^{(*)}$-nak egy olyan $H^{(*)}$ részgráfját alkotják, ami a H gráf absztrakt duálisa. A Kuratowski tétel szerint Whitney fenti tételét bebizonyíthatjuk úgy, hogy igazoljuk,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

Nézzük a K_5-t! Ennek van 5 db olyan vágása, amelyek mindegyike $1-1$ pontot vág le, és ezek $4-4$ élt tartalmaznak. Ha indirekt létezik egy $K_5^{(*)}$ absztrakt duális, akkor ennek pontosan 5 db 4-hosszú

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



Tegyük fel ezután indirekt, hogy a $K_{3,3}$ gráfnak létezik egy $K_{3,3}^{(*)}$ absztrakt duálisa. A $K_{3,3}$-nak 6 db 3 élű vágása van (amelyek 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.□

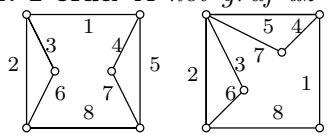


□

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

3.140. Definíció *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.*

3.141. Példa *A két gráf az ábrán gyengén izomorf, az élek közti bijekciót a számozás adja.*



3.142. Tétel (Whitney tétele) *Ha G síkbarajzolható, továbbá G és H gyengén izomorf, akkor*

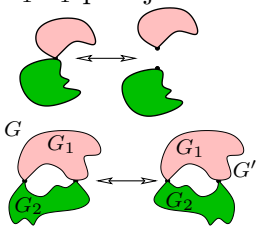
(1) H is síkbarajzolható,

(2) G^* és H^* is gyengén izomorf, végül

(3) G és $(G^*)^*$ gyengén izomorf.

Bizonyítás. (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 síkbarajzolható. (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 $(G^*)^*$ összefüggő, a (6) állítás szerint tehát G^* duálisa $(G^*)^*$-nak és persze G-nek is. De ekkor G és $(G^*)^*$ egymással gyengén izomorfak. □

Hogyan kaphatunk gyengén izomorf gráfokat? Ha G két különböző komponensének egy-egy pontját azonosítjuk, akkor a körök halmaza nem változik. Az inverzoperáció, amikor egy elvágó pontot széthúzunk szintén 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.



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

Megjegyzés: Gráfok és elektromos hálózatok
Ahogyan ezt a Kruskal algoritmus alkalmazásaként már láttuk, egy olyan elektromos hálózatot, amelyik kizárólag kétpólusú elemeket (azaz ellenállásokat, áram-, ill. feszültségforrásokat, kapacitív elemeket (kondenzátorokat) valamint induktív elemeket (tekercseket)) tartalmaz, tekinthetünk egy, a kapcsolási rajzzal megadott G gráfnak is: G csúcsai a csatlakozási pontok lesznek, minden élnek pedig egy-egy kétpólusú áramköri elem fog megfelelni. Egy ilyen elektromos hálózat megoldása nem más, mint G minden egyes élén az áramerősségnek és a feszültségkülönbségnek (mint függvénynek) a meghatározása. A megoldást a Kirchhoff-féle csomóponti- és huroktörvények és az Ohm törvények (ill. az induktív elemekre és a kapacitív elemekre felírt differenciálegyenletek) felírásából adódó egyenletrendszerből kaphatjuk meg (és persze innen derül ki az is, ha esetleg nincs megoldása az adott hálózatnak).

A csomóponti törvény lényegében azt mondja ki, hogy G tetszőleges vágása esetén a vágás élein folyó áramok előjeles összege 0, míg a huroktörvény szerint G tetszőleges köre mentén a potenciálkülönbségek összege 0.

Ha a G gráf véletlenül összefüggő és síkbarajzolható, és G^* a G egy duálisa, akkor –mint azt láttuk– G és G^* élei között természtes bijekció van, és e szerint G vágásai és körei G^* köreinek és vágásainak felelnek meg, továbbá G . Ezért a G-beli Kirchhoff törvényeket úgy is tekinthetjük, mint amelyeket a G^* gráf éleire írtunk fel azzal, hogy a feszültségkülönbségek ill. az áramerősségek szerepét felcseréltük. A fizikai törvények egy érdekes következménye, hogy G^* éleihez lehetséges úgy áramköri elemeket rendelni, hogy azok az áramerősség és a feszültségkülönbség szempontjából pontosan úgy viselkedjenek, mint ahogyan a G-beli megfelelőjük a feszültségkülönbség ill. az áramerősség szempontjából működik. Ez pl azt jelenti, hogy egy R nagyságú ellenállásnak egy $\frac{1}{R}$ nagyságú ellenállás, egy x nagyságú feszültségforrásnak egy x nagyságú áramforrás, valamint egy y nagyságú induktivitásnak egy y nagyságú kapacitás felel meg. Ha most az így konstruált duális G^* hálózatot szeretnénk megoldani, akkor pontosan ugyanazt az egyenletrendszert kell megoldanunk, mint amelyet a G-hez tartozó hálózathoz, azzal a különbséggel, hogy ami G-ben áramerősség volt, az G^*-ban feszültségkülönbség, ill. ami G-ben feszültségkülönbség volt, az G^*-ban áramerősség lesz. A G^* megoldását tehát úgy kaphatjuk meg G megoldásából, hogy az áramerősség és feszültségkülönbség szerepét felcseréljük. Ezt a jelenséget hívják a villamos hálózatok elméletében dualitási elvnek.

A 3.139. Whitney tételből az következik, hogy duális hálózatot pontosan akkor tudunk készíteni egy adott hálózathoz, ha az eredeti hálózatnak megfelelő gráf síkbarajzolható. Láttuk azonban azt is, hogy a G^* duális gráf nem egy síkbarajzoható G-hez, hanem G egy konkrét síkbarajzolhásához tartozik: különböző síkbarajzolásokhoz tartozhatnak nemizomorf duálisok. Ezek a duálisok tehát olyan hálozatokra adnak példát, amelyekben bár ugyanazok az áramköri elemek találhatók, de „topológiájuk" különbözik, és mégis, a megoldásuk azonos: az egyik duális minden egyes e élén ugyanannyi lesz az áramerősség és a feszültségkülönbség, mint a másik duálisban az e-nek megfelelő élen. Sőt. Ahhoz, hogy két azonos áramköri elemeket tartalmazó hálózatnak ugyanaz legyen a megoldása, nem kell más, mint hogy létezzék a két hálózat áramköri elemei között körtartó és vágástartó bijekció, azaz, hogy a két hálózat egymással gyengén izomorf legyen. Itt látszik a 3.143. Whitney tétel egy fontos alkalmazási lehetősége: a hálózat G gráfjának síkbarajzolhatóságától függetlenül ha G'-t a Whitney operációkkal kapjuk G-ből, akkor a G'-höz tartozó hálózat megoldása megegyezik a G-hez tartozó hálózat megoldásával.

♦

3.7. Gráfok színezései

3.144. Definíció *A G gráf k* színnel színezhető*, ha G minden csúcsa kiszínezhető k adott szín valamelyikére úgy, hogy G bármely élének két végpontja különböző színű legyen. A G gráf* kromatikus száma $\chi(G) = k$*, ha G kiszínezhető k színnel, de $k-1$ színnel még nem.*

Amikor egy gráf *kiszínezéséről* beszélünk (hacsak nem jelezzük az ellenkezőjét), mindig a csúcsoknak a fenti szabály szerinti színezésére gondolunk. Egy konkrét színezés esetén az azonos színűre festett csúcsok halmazát (amely halmaz tehát nem feszíthet élt) *színosztálynak* nevezzük. Jegyezzük meg, hogy a színosztály mindig a színezéstől függ, és általában nem egyértelmű, hogy egy G gráfot hogyan is kell $\chi(G)$ színnel kiszínezni.

3.145. Megjegyzések *1. Ha G k-színezhető, akkor G-ben nincs hurokél, hisz egy hurokél végpontját nem lehet a fenti szabály szerint megszínezni.*

2. A G gráf k-színezése tekinthető olyan $c : V(G) \to \{1, 2, \ldots, k\}$ leképezés, amelyre $c(u) = c(v) \Rightarrow uv \notin E(G)$ teljesül. (Ez voltaképp a formális definíció.)

3. A G gráf egy (adott színezéshez tartozó) színosztályának csúcsai között nem fut él. A lehetséges színosztályokról szól a következő definíció.

3.146. Definíció *A G gráf csúcsainak U részhalmaza* független*, ha G-nek nincs olyan éle, melynek mindkét végpontja U-beli. A G gráf* független csúcsainak maximális száma $\alpha(G) = l$*, ha létezik G-nek l pontú független ponthalmaza, de $l+1$ páronként összekötetlen csúcs már nincs G-ben.*

A kromatikus számot ezek szerint úgy is definiálhatjuk, hogy $\chi(G)$ a legkisebb olyan k egész, melyre G csúcshalmaza lefedhető k független ponthalmazzal.

Mik azok a gráfok amelyeket egy színnel kiszínezhetünk, azaz mit jelent, hogy $\chi(G) = 1$? Világos, hogy amint G-nek van éle, a két végpontjára két különböző színt kell használni, illetve, ha G egy ú.n. *üresgráf*, aminek minden csúcsa izolált, akkor egy szín elegendő. Tehát az 1-színezhető gráfok éppen az üresgráfok (azaz a teljes gráfok komplementerei). Ennél izgalmasabb osztályt alkotnak azok a gráfok, amelyekhez két szín elegendő. A 2-színezhető gráfok (vagyis azok, amelyek kromatikus száma legfeljebb 2) olyanok, hogy él csak a két színosztály között futhat, azaz a gráf bizonyosan páros. (Egyúttal magyarázatot kaptunk a páros gráf két csúcshalmazának elnevezésére is.) Az is világos, hogy ha G páros, akkor a színosztályait különböző színűre színezve $\chi(G) \leq 2$ adódik.

A fentiekkel szemben a 3-színezhető gráfok már nem írhatók le ilyen egyszerűen, sőt, a bonyolultságelmélet részben azt is látni fogjuk, hogy nem várható olyan algoritmus, ami egy inputgráfról hatékonyan eldönti, kiszínezhetők-e a csúcsai mindössze 3 színnel.

3.147. Definíció *A G gráf* klikkje *a G teljes részgráfja. A G gráf $\omega(G)$-vel jelölt* klikkszáma *G legnagyobb klikkjének pontszáma, azaz a legnagyobb olyan k szám, melyre létezik G-ben k páronként összekötött csúcs, de $k+1$ már nem létezik.*

3.148. Állítás *Minden irányítatlan, véges G gráfra $\omega(G) \leq \chi(G) \leq \Delta(G)+1$ valamint $\chi(G)\alpha(G) \geq n$ teljesül, ahol n a G csúcsainak számát jelenti.*

Bizonyítás. G pontjainak kiszínezésével a maximális klikk pontjait is kiszínezzük, mégpedig különböző színekkel. Ebből világos az első egyenlőtlenség.

Másrészt az ún. mohó színezés mutatja, hogy bármely G gráf $(\Delta(G)+1)$-színezhető. Színezzük ki G pontjait $v_1, v_2, \dots v_n$ sorrendben úgy, hogy az i-dik lépésben v_i-t olyan színre színezzük, ami nem szerepel v_i kiszínezett szomszédain. Mivel v_i-nek legfeljebb $\Delta(G)$ kiszínezett szomszédja lehet, és mindegyik szomszéd legfeljebb egy-egy színt zár ki, v_i színezése elvégezhető a rendelkezésre álló színek valamelyikével. v_n kiszínezése után G egy $(\Delta(G)+1)$-színezését kapjuk, ami a második egyenlőtlenséget igazolja.

A tétel második része azért igaz, mert ha G-t kiszínezzük $\chi(G)$ színnel akkor minden egyes színosztály legfeljebb $\alpha(G)$ méretű, hisz független pontokból áll. Ezek szerint G csúcsait $\chi(G)$ darab, legfeljebb $\alpha(G)$ méretű halmaz uniójára bontottuk, ahonnan $n \leq \chi(G) \cdot \alpha(G)$. □

3.149. Megjegyzés *A fenti állításban egyik egyenlőtlenséget sem lehet* általában *megjavítani: az első alsó becslés pl. az ún. perfekt gráfokra éles, és a második alsó becslésre is könnyű azt egyenlőséggel teljesítő gráfot konstruálni. A felső becslés teljes gráfokra és ptn körökre is pontos:* $\chi(K_n) = n = \Delta(K_n) + 1$ *ill.* $\chi(C_{2n+1}) = 3 = \Delta(C_{2n+1}) + 1$. *A felső becslés azonban lényegében csak az utóbbi gráfokra éles.*

3.150. Tétel (Brooks tétele) *Legyen G véges, egyszerű, összefüggő gráf. Ha G nem teljes gráf és nem páratlan kör, akkor $\chi(G) \leq \Delta(G)$.* □

Egy, a Brooks tétel valamivel gyengébb állítást igazolunk, amit néha „gyenge Brooks tételnek” hívnak.

3.151. Tétel *Ha a G véges gráf összefüggő és G nem reguláris, akkor $\chi(G) \leq \Delta(G)$.*

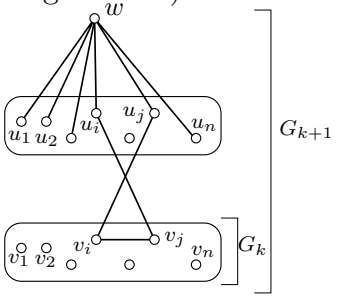
Bizonyítás. A tétel azzal ekvivalens, hogy G kiszínezhető $\Delta(G)$ színnel. Ezt a mohó színezéssel fogjuk megmutatni. Láttuk, hogy a mohó színezéskor legfeljebb eggyel több színt használunk fel, mint ahány korábban kiszínezett szomszédja lehet G egy csúcsának. A $\Delta(G)$ színnel való színezés lehetősége következik tehát abból, ha G csúcsainak sikerül olyan $v_1, v_2, \dots, v_n$ sorrendjét megadnunk, amire az teljesül, hogy minden v_i-nek legfeljebb $\Delta(G) - 1$ kisebb indexű szomszédja van. A $v_1, v_2, \dots, v_n$ sorrend viszont automatikusan ilyen lesz, ha az teljesül rá, hogy v_n kivételével minden v_i-nek van i-nél nagyobb indexű szomszédja, továbbá, hogy v_n fokszáma $\Delta(G)$-nél kisebb.

Mivel G nem reguláris, létezik $\Delta(G)$-nél kisebb fokszámú csúcsa, legyen ez v_n. Tekintsük G egy F feszítőfáját (ami G összefüggő tulajdonsága miatt létezik), legyen ennek v_1 egy v_n-től különböző levele. Ilyen van, hisz minden (legalább kétpontú) fának van legalább két levele. Legyen v_2 az $F - v_1$ fa egy v_n-től különböző levele, és így tovább, azaz v_i az $F - \{v_1, v_2, \dots, v_{i-1}\}$ fa egy v_n-től különböző levele. Ez a Prüfer kódoláshoz hasonló levéltörlési eljárás a G gráf csúcsainak olyan $v_1, v_2, \dots, v_n$ sorrendjét határozza meg, amire v_n nem maximális fokszámú, és minden más v_i-nek van a sorrendben őt követő szomszédja is. Nekünk pedig pontosan erre volt szükségünk a tétel bizonyításához. □

Az alábbi tétel pedig azt mutatja, hogy az $\omega(G) \leq \chi(G)$ alsó becslés sokszor bizony fabatkát sem ér.

3.152. Tétel (Mycielski) *Tetszőleges $k \geq 2$ pozitív egészhez létezik olyan G gráf, melyre $\chi(G) = k$ és $\omega(G) = 2$.*

Bizonyítás. Megadunk egy G_k gráfot a kívánt tulajdonsággal. A konstrukció egyébként Mycielski nevéhez fűződik. A k paraméter szerinti indukcióval bizonyítunk. A $G_2 = K_2$ megfelelő gráf, tehát $k = 2$-re az indukciós állítás igaz. Tegyük fel, hogy valamely k-ra a G_k gráfot már sikerült elkészíteni. Legyen $V(G_k) = \{v_1, v_2, \ldots, v_n\}$, és $V(G_{k+1}) = \{v_1, v_2, \ldots, v_n\} \cup \{u_1, u_2, \ldots, u_n\} \cup \{w\}$, ahol az u_i és w az eddigiektől és egymástól különböző, új csúcsok. Legyen $E(G_{k+1}) := \{wu_i : 1 \leq i \leq n\} \cup \{v_iu_j, v_ju_i : v_iv_j \in E(G_k)\} \cup E(G_k)$, azaz kössük össze w-t minden u_i-vel, továbbá minden G_k-beli él (önmagán kívül) két élért felelős G_{k+1}-ben.



Mivel az u_i pontok függetlenek, továbbá w-ből nem fut él v_i-be, ezért G_{k+1}-ben minden háromszög legalább két G_k-beli pontot (mondjuk v_i-t és v_j-t) tartalmaz. A háromszög harmadik pontja nem lehet w, hisz az nem szomszédos egyik v_i-vel, és nem lehet G_k-nak sem pontja, hisz G_k az indukciós feltevés szerint nem tartalmaz háromszöget. Ha tehát a háromszög a harmadik pontja mondjuk u_l, akkor G_{k+1} definíciója v_i, v_j, v_l a G_k-ban háromszöget alkotnak, ami ismét csak ellentmond az indukciós feltevésnek. Azaz $\omega(G_{k+1}) = 2$.

Azt kell már csak bebizonyítani, hogy G_{k+1} $(k+1)$-kromatikus. k szerinti indukciót használunk: $k = 2$-re $\chi(K_2) = 2$ miatt az állítás igaz. Világos, hogy a G_{k+1} gráf $k+1$ színnel színezhető, azaz, hogy $\chi(G_{k+1}) \leq k+1$, hisz a v_i-ket a G_k egy k-színezése szerint színezve, minden u_i-nek a v_i-vel azonos színt adva és w-re egy $(k+1)$-dik színt használva G_{k+1} egy $(k+1)$-színezését kapjuk.

Azt kell megmutatnunk, hogy G_{k+1} nem színezhető ki k színnel. Indirekt bizonyítunk: tegyük fel, hogy G_{k+1} mégis kiszínezhető k színnel. Tekintsünk egy ilyen színezést, és színezzük át a w-vel azonos színt kapó v_i pontokat a megfelelő u_i csúcs színére. Ezáltal a $\{v_1, v_2, \ldots, v_n\}$ pontok mindegyike w-étől különböző színt kap. Tehát G_k pontjai $(k-1)$-féle színt kaptak. Az indukciós feltevés szerint $\chi(G_k) = k > k-1$, ezért G_k nem színezhető jól $k-1$ színnel, vagyis az iménti színezésben lesz két azonos színt kapó, szomszédos csúcs, mondjuk v_i és v_j. Ezek az eredeti színezésben természetesen különböző színt kaptak, tehát az egyikük (mondjuk v_i) a w-vel azonos színt kapott, és ezért

átszíneztük u_i színére. Azonban v_j és u_i is szomszédosak G_{k+1}-ben, tehát eredeti színük különböző volt. Ezért az átszínezés után sem fordulhat elő, hogy v_i és v_j azonos színt kapott. Ez az ellentmondás igazolja az indukciós állítást, azaz $\chi(G_{k+1}) = k + 1$. □

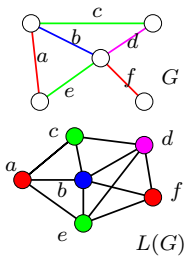
3.7.1. Gráfok élszínezése

3.153. Definíció *A G gráf* élgráfja *az az $L(G)$ gráf, aminek a csúcsai G éleinek felelnek meg, és $L(G)$ két csúcsa pontosan akkor van éllel összekötve, ha G megfelelő élenek van közös végpontja.*

3.154. Definíció *A G gráf k-élszínezhető, ha G élei k színnel színezhetők úgy, hogy szomszédos élek különböző színt kapnak. A G gráf* élkromatikus száma $\chi'(G) = \chi_e(G) = k$, *ha G k-élszínezhető, de G nem $(k-1)$-élszínezhető.*

3.155. Megjegyzés *G pontosan akkor k-élszínezhető, ha $L(G)$ k-színezhető. Tetszőleges G gráf esetén $\chi'(G) = \chi(L(G))$.*

3.156. Állítás *Tetszőleges G gráfra $\omega(L(G)) \geq \Delta(G)$, továbbá, ha $\Delta(G) \geq 3$, akkor $\omega(L(G)) = \Delta(G)$.*



Bizonyítás. Az egy csúcsból induló éleknek megfelelő pontok klikket alkotnak $L(G)$-ben. Másfelől $L(G)$ minden klikkje vagy G egy csúcsból induló néhány élének, vagy G egy háromszögének felel meg. □

3.157. Állítás *Tetszőleges G gráfra $\chi'(G) \geq \Delta(G)$ áll.*

Bizonyítás. Az egy csúcsból induló élek egymástól különböző színt kapnak, és ez speciálisan a maximális fokszámú csúcsból induló élekre is igaz. Ugyanez formálisan: $\chi'(G) = \chi(L(G)) \geq \omega(L(G)) \geq \Delta(G)$. □

3.158. Tétel (Kőnig tétel) *Ha $G = (A, B; E)$ páros gráf, akkor $\chi'(G) = \Delta(G)$.*

Bizonyítás. Az előző állítás miatt elegendő azt igazolni, hogy $\chi'(G) \leq \Delta(G)$, azaz csupán egy $\Delta(G)$-élszínezést kell mutatni. Létezik olyan H páros gráf, melynek G részgráfja, és H minden csúcsának fokszáma $\Delta(G)$. (Ilyen H-t például úgy kaphatunk, hogy G mellé felvesszük még G-nek egy $G' = (A', B'; E')$ másolatát, H színosztályai $A \cup B'$ és $B \cup A'$ lesznek, és minden v csúcs és annak v' másolata közé behúzunk további $\Delta(G) - d(v)$ párhuzamos élt.) Ha sikerül a $\Delta(G)$-reguláris H gráf éleit $\Delta(G)$ színnel kiszínezni, akkor egyúttal a G részgráf éleinek is megkapjuk egy ugyanennyi színnel való színezését.

A H gráf élszínezéséhez pedig elegendő azt megmutatni, hogy tetszőleges reguláris páros gráfban van teljes párosítás. Ugyanis akkor H egy teljes párosítását kiszínezve az első színnel, a színezetlen élek

egy $(\Delta(G)-1)$-reguláris páros gráfot alkotnak, abban is találunk teljes párosítást, ez a második színt kapja, sít.

Miért létezik tehát egy r-reguláris páros gráfnak teljes párosítása? A Hall feltétel teljesülését kell csupán ellenőrizni. Ha az egyik színosztályból kiválasztunk egy k pontú X halmazt, akkor az X-beli csúcsokból összesen kr él indul ki. Mindezen élekből a másik színosztály bármely csúcsa legfeljebb r-t fogadhat be, tehát a kr darab él megérkezéséhez legalább k pontra van szükség: $|N(X)| \geq |X|$. A Hall feltétel az r-reguláris gráf bármelyik színosztályára teljesül, tehát csakugyan létezik teljes párosítás, és pontosan ezt kellett bizonyítanunk. □

Míg a $\chi \geq \omega$ becslés általában nem túl jó (mutatják ezt a Mycielski gráfok), addig a fenti becslés közel jár az igazsághoz.

3.159. Tétel (Vizing tétele) *Ha G véges, egyszerű gráf, akkor $\chi'(G) \leq \Delta(G)+1$.*□

3.160. Tétel (Shannon tétele) *Ha G véges, gráf, akkor $\chi'(G) \leq \frac{3}{2} \cdot \Delta(G)$.*□

3.161. Megjegyzés *Ha egy K_3 minden élét k párhuzamos éllel helyettesítjük, akkor az így kapot G gráfra $\chi'(G) = \frac{3}{2} \cdot \Delta(G)$.*

3.7.2. Síkgráfok színezése

Láttuk, hogy a 2-színezhető gráfok pontosan a páros gráfok. A 3-színezhető gráfok már sokkal bonyolultabb struktúrát alkotnak: mint látni fogjuk, annak a felismerése, hogy egy adott G gráf 3-színezhető-e (azaz G csúcsai előállnak-e 3 független ponthalmaz uniójaként), bizonyíthatóan nehéz. Érdekes viszont, hogy a 4-színezhető gráfok osztálya tartalmazza a síkbarajzolható gráfokat.

3.162. Tétel (4-szín tétel) *Minden egyszerű, síkbarajzolható gráf 4-színezhető.*□

Történelem: A 4-szín tétel

Síkbarajzolt gráfok színezése legtermészetesebben a térképszínezés kapcsán merül fel: egy politikai térképen szeretnénk az országokat úgy kiszínezni, hogy szomszédos országok színe különbözzék. Más szóval, egy síkbarajzolt gráf tartományait kell színeznünk, ami ekvivalens az adott gráf duálisának színezésével.

(Egyébként a politikai térképek nem szükségképpen 4-színezhetők, hisz pl. Kalinyingrádot is az Oroszországhoz használt színnel kell festeni. Ha ezt jól megértettük, akkor nem meglepő az az állítás sem, hogy tetszőleges k-hoz létezik olyan politikai térkép, ami nem színezhető ki k színnel. Szorgalmi házi feladat: keressünk további példákat nem összefüggő országokra, tengerrel való elválasztottság nem számít.)

A 4-szín tételt először Francis Guthrie sejtette meg 1852-ben: megfigyelte, hogy Anglia megyéi úgy 4-színezhetők, hogy szomszédos megyék különböző színt kapnak. Többszörös áttétellel értesült erről Cayley, aki nem talált bizonyítást, ezért 1878-ban publikálta a sejtést. 1879-ben Kempe közölt egy bizonyítást, melyet Tait bizonyítása követett 1880-ban. 1890-ben Heawood hibát talált Kempe bizonyításában, 1891-ben pedig Petersen a Tait-félében. A hibák egyikét sem sikerült azóta sem kijavítani. Sokak hosszú, eredménytelen

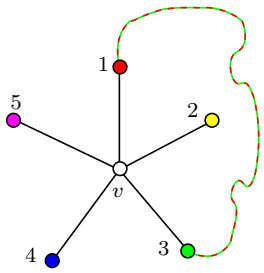
próbálkozásai után Appel és Haken 1976-ban jelentették be, hogy igazolták a tételt. Módszerükkel az állítás egy hihetetlenül bonyolult, szerteágazó esetvizsgálatra vezetett, amit számítógéppel végeztek el. Mivel a bizonyítás helyességének ellenőrzése elképzelhetetlen számítógép nélkül, felmerült az a metamatematikai probléma, hogy mi tekinthető teljes értékű bizonyításnak: mennyire lehetünk biztosak abban, hogy a számítógép programja valóban azt végzi el, amit arról feltételezünk. A történet következő allomásához 1996-ban érkezett, amikoris Robertson, Sanders, Seymour és Thomas talált egy, az Appel-Haken-félénél jóval egyszerűbb bizonyítást, mely arra vezet, hogy 633 kis gráf ú.n. redukálhatóságát kell ellenőrizni. Természetesen Robertsonék is számítógéppel végeztették ezt el, ezért továbbra sem lehetünk abszolút bizonyosak afelől, hogy a bizonyítás korrekt. Sajnos ezen ma sem tud senki segíteni. Történt azért még valami, ami említést érdemel. Ha nincs ember, aki ellenőrizhetné a bizonyítást, miért ne tehetné meg azt a gép? Léteznek ugyanis mechanikus bizonyításellenőrző programok, ezek egyike az ú.n. coq. 2004-ben Georges Gonthier átírta Robertson és társai bizonyítását a bizonyításellenőrző által értelmezhető formális nyelvre, és ellenőriztette azt. A munka egyáltalán nem volt triviális, és bár a teszt sikeres volt (úgyhogy mostanra aztán tovább csökkentek a kételyek, ha voltak még egyáltalán), de nem ez a lényeg. Az eredmény jelentősége abban rejlik, hogy a bizonyítások egyre komplexebbé válásával a levezetések ellenőrzését nem tudjuk mindig mi magunk elvégezni. Eljöhet –egyesek szerint közel van már– az idő, amikor egy-egy bizonyítás ellenőrzése jelentősen nehezebb lesz, mint magának a bizonyításnak a megtalálása. De úgy tűnik, van remény, és nem fog emiatt megállni a tudomány: lehetőség lesz az ellenőrzés gépesítésére, hisz a ma ismert bizonyítások egyik legkomplexebbike esetében ez sikerrel megtörtént.

De térjünk vissza a próféciáktól az eredeti 4-szín tételre adott hibás bizonyításhoz. Kempe 11 évig megtévesztette a világot, ami szép teljesítmény, még ha nem is szándékos. A hiba megtalálása után azonban a bizonyítás menthetetlennek tűnt. Az ott használt módszer azonban annyiból nem haszontalan, hogy alkalmas egy gyengébb, ám nemtriviális eredmény igazolásásra. ♦

3.163. Tétel (5-szín tétel) *Minden egyszerű, síkbarajzolható G gráf 5-színezhető, azaz $\chi(G) \leq 5$.*

Bizonyítás. Legfeljebb 3 pontú gráfokra a tétel triviálisan igaz. Nagyobb gráfokra pontszám szerinti indukcióval bizonyítunk: tegyük fel, hogy a legfeljebb $(n-1)$ pontú gráfokra a tétel igaz. Legyen G egy n pontú ($n > 3$), egyszerű, síkbarajzolható gráf. Tudjuk, hogy G élszáma legfeljebb $3n-6$, azaz G pontjainak fokszámösszege legfeljebb $6n-12$. Van tehát G-nek egy legfeljebb 5-ödfokú v csúcsa.

Mivel $G-v$ is egyszerű és síkbarajzolható, ezért az indukciós feltevés miatt 5-színezhető. Ha tehát v szomszédai legfeljebb 4 színt kapnak e színezésben, akkor v megkaphatja az ötödik színt. Ez akkor nem működik, ha $d(v) = 5$ és mind az öt szomszéd különböző színű. (Ha csak a 6-színtételt szeretnénk igazolni, akkor ez sem okozna problémát, és a bizonyítást itt be is fejezhetnénk.) (Ld. az ábrát.) Tekintsük az 1-es és 3-as színek által feszített G_{13} részgráfot $(G-v)$-ben. Ha a v csúcs 1-es ill. 3-as színű szomszédai G_{13} különböző komponenseibe esnek, akkor pl. az 1-es szomszéd komponensében felcserélve az 1-es és 3-as színeket, a $G-v$ olyan 5-színezését kapjuk, amiben v-nek nincs 1-es színű szomszédja. Ekkor v 1-es színre színezhető.



Ellenkező esetben van v 1-es és 3-as színű szomszédja között egy olyan út, ami csak 1-es és 3-as színű csúcsokat használ. A síkbrarajzoltság miatt biztos nincs v 2-es és 4-es színű szomszédja között olyan út $(G-v)$-ben, ami csak 2-es és 4-es színű csúcsokat használ, vagyis a G_{13}-hoz hasonlóan definiált G_{24} gráfban az említett két szomszéd különböző komponensekben van. A 2-es színű szomszéd komponensében felcserélve a 2-es és 4-es színt $G-v$ olyan 5-színezését kapjuk, amiben v szomszédai között nem fordul elő a 2-es szín. A v csúcs tehát megkaphatja a 2-es színt. □

3.164. Megjegyzés *Érdemes meggondolni, Kempe mit nézett el, azaz, hogy a fenti bizonyítás miért is nem működik* 4 *színre.*

Mutatunk az 5-színtételre egy másikm, a fentitől lényegesen különböző bizonyítást is, amelyben szereplő ötlet máskor is hasznos lehet.

A 3.163. Tétel újabb bizonyítása. Az előző bizonyítás első bekezdésében leírtak szerint járunk el. Van tehát egy legfeljebb 5-ödfokú v csúcsunk. Ha $d(v) \leq 4$, akkor $G-v$ síkbarajzolható lévén az indukció szerint 5-színezhető, és ebben a színezésben választható v-nek olyan szín a lehetséges 5-ből, amit nem használtunk a legfeljebb 4 szomszédja egyikéhez sem.

Végül ha $d(v) = 5$, akkor v-nek van két egymással nem szomszédos szomszédja, mondjuk u és w, hisz ellenkező esetben lenne G-nek K_6-tal izomorf részgráfja, amiről már láttuk, hogy nem lehetséges. Húzzuk össze az uv és vw éleket. Az így keletkező G' gráf síkbarajzolható lesz, így az indukció miatt 5 színnel színezhető. Legyen az u, v, w csúcsoknak megfelelő G' csúcs színe piros. Ha most G csúcsait a G' színezése szerint színezzük, továbbá az u és w csúcsnak piros színt adunk, akkor v öt szomszédja összesen 4 féle színt kap, tehát a rendelkezésre álló 5 szín közül v-nek is választhatunk alkalmasat. Ezáltal G csúcsait sikerült 5 színnel színezni, az indukciós lépést igazoltuk, a bizonyítást befejeztük.

3.165. Megjegyzés *A fenti bizonyítás nemcsak síkbarajzolható gráfokra működik. Mindössze annyit használ* G*-ről, hogy* G *nem tartalmaz* K_6*-minort (azaz* G*-ből csúcsok elhagyásával és élek összehúzásával nem kapható* K_6*, továbbá, hogy* G *bármely feszített részgráfjának kevesebb mint* 3*-szor annyi éle van mint a csúcsainak száma.*

3.8. Perfekt gráfok

3.166. Definíció *A G véges gráf* perfekt*, ha G minden feszített G' részgráfjára $\chi(G') = \omega(G')$ teljesül.*

A fenti definícióban az egyenlőség persze magára a G gráfra is teljesül, de a vizsgán már annyiszor hallottunk helytelen definíciót, hogy itt is igyeszünk hangsúlyozni, hogy nem csak az eredeti gráfra kívánjuk meg a leírt tulajdonságot.

A 3.166. definíciót az motiválja, hogy azoknak a gráfoknak a szerkezetére vagyunk kíváncsiak, amelyekre a kromatikus számra vonatkozó, $\chi(G) \geq \omega(G)$ alsó becslés egyenlőséggel teljesül. Ebben a formában a kérdés nem szerencsés, mert tetszőleges (véges) G gráfhoz egy $\chi(G)$ méretű klikk-komponenst hozzávéve $\chi(G) = \omega(G)$ fog teljesülni. Ezért kívánjuk meg az egyenlőséget minden feszített részgráfra.

3.167. Példa

1. *Ha G nemüres, páros gráf, akkor $\chi(G) = 2 = \omega(G)$ (üres páros gráfra $\chi(G) = \omega(G) = 1$). Mivel páros gráf feszített részgráfja is páros gráf, ezért minden páros gráf perfekt.*

2. *Minden út páros gráf, ezért minden út perfekt. Minden fa (sőt erdő is) páros gráf, ezért egyúttal perfekt.*

3. *$\chi(K_n) = n = \omega(K_n)$, továbbá minden klikk feszített részgráfja klikk, ezért minden klikk perfekt.*

4. *Ha $n \geq 2$, akkor $\chi(C_{2n+1}) = 3 \neq 2 = \omega(C_{2n+1})$, tehát a páratlan kör (a $C_3 = K_3$ kivételével) nem perfekt gráf. (Viszont minden feszített részgráfja perfekt, tehát a legalább 5 hosszú ptn kör egy* minimális imperfekt gráf*.)*

Az alábbi tételek további gráfosztályok perfektségét igazolják.

3.168. Tétel *Ha G komplementere páros gráf, akkor G perfekt.*

Bizonyítás. Ha G páros gráf komplementere, akkor G minden feszített részgráfja is páros gráf komplementere, ezért elegendő azt bizonyítani, hogy $\chi(G) = \omega(G)$ ha G komplementere páros. Kőnig és Gallai tételei alapján (páros gráfban nincs hurokél) $\omega(G) = \alpha(\overline{G}) = n - \tau(\overline{G}) = n - \nu(\overline{G})$. A $\chi(G) = \omega(G)$ egyenlőség igazolásához a triviális $\chi(G) \geq \omega(G)$ egyenlőtlenség miatt elegendő a $\chi(G) \leq \omega(G)$ bizonyítása, azaz G egy $\omega(G) = n - \nu(\overline{G})$ színnel történő színezésének megadása. Ilyet pedig úgy kapunk, hogy rögzítjük $\overline{G}$-nek egy $\nu(\overline{G})$ élből álló, M maximális párosítását, és minden csúcsot különböző színnel színezünk, kivéve, hogy M minden élének végpontjai azonos színt kapnak. Ezáltal a felhasznált színekben az n-hez képest $\nu(\overline{G})$ megtakarítást érünk el. □

3.169. Tétel *Páros gráf élgráfja perfekt.*

Bizonyítás. Ha G páros gráf, akkor $L(G)$ élgráfjának tetszőleges feszített részgráfja azonos G egy alkalmas részgráfjának élgráfjával, azaz szintén egy páros gráf élgráfja. Elegendő tehát azt bizonyítani, hogy $\chi(L(G)) = \omega(L(G))$ tetszőleges G páros gráfra.

Mivel G háromszög-mentes, ezért $L(G)$ minden klikkje G egy csúcsból induló éleinek felel meg, így $\omega(L(G)) = \Delta(G)$. Kőnig páros gráfok élszínezéséről szóló tételének felhasználásával $\omega(L(G)) = \Delta(G) = \chi'(G) = \chi(L(G))$ következik. □

3.170. Tétel *Páros gráf élgráfjának komplementere perfekt.*

Bizonyítás. Ha G páros gráf, akkor $\overline{L(G)}$ feszített részgráfja nem más, mint $\overline{L(G')}$, ahol G' a G alkalmas részgráfja. Mivel G' páros, ezért elegendő azt igazolni, hogy $\chi(\overline{L(G)})) \leq \omega(\overline{L(G)})$ tetszőleges G páros gráfra (a másik irányú egyenlőtlenség triviális).

A Kőnig tétel alapján $\omega(\overline{L(G)}) = \alpha(L(G)) = \nu(G) = \tau(G)$, ezért elegendő $\tau(G)$ színnel kiszínezni $\overline{L(G)}$-t. Legyen $U \subset V(G)$ egy $\tau(G)$ pontból álló lefogó ponthalmaz, és válasszunk G minden egyes e éléhez e-nek egy U-beli végpontját. Ha minden élt a kiválasztott végpontnak megfelelően színezünk, akkor $\tau(G)$ színt használunk, és az azonos színű élek páronként szomszédosak, azaz a nekik megfelelő pontok $\overline{L(G)}$-ben függetlenek. Tehát ez csakugyan egy $\tau(G)$ színnel történő színezése $\overline{L(G)}$-nek. □

További példát is adunk perfekt gráfra, de ehhez értelmezzük a rendezést.

3.171. Definíció *Ha D irányított gráf, akkor $u \xrightarrow{D} v$ jelöli azt, hogy u-ból vezet v-be D-ben irányított út.*

A D irányított gráf aciklikus*, ha nem tartalmaz irányított kört.*

A D irányított gráf v csúcsa forrás (nyelő)*, ha v-be nem fut be (v-ből nem indul ki) G-nek éle.*

3.172. Állítás *Ha a D véges, irányított gráf aciklikus, akkor létezik forrása és nyelője is.*

Bizonyítás. Tetszőleges pontból kiinduló sétát az aciklikus tulajdonság miatt sosem érinthet korábban érintett pontot, ezért a séta előbb-utóbb elakad egy nyelőben. A megfordított éleken haladó séta hasonló okok miatt forrásba jut. □

A $\preceq$ relációt az X halmazon *részbenrendezésnek* nevezzük, ha létezik az X ponthalmazon egy aciklikus D irányított gráf, melyre $(x \preceq y) \iff (x \xrightarrow{D} y)$. (Az x-t akkor tekintjük kisebbnek y-nál, ha x-ből irányított úton y-ba juthatunk.) A $\preceq$ részbenrendezés szerint x és y *összehasonlítható*, ha $x \preceq y$ vagy $y \preceq x$.

3.173. Megjegyzés *A részbenrendezés szokásos definíciója három tulajdonságot kíván meg:*

(1) reflexivitás*:* $x \preceq x \qquad \forall x \in X$,

(2) antiszimmetria*: ha $x \preceq y$ és $y \preceq x$, akkor $x = y$, valamint*
(3) tranzitivitás*: ha $x \preceq y$ és $y \preceq z$, akkor $x \preceq z$.*

Könnyű ellenőrizni, hogy aciklikus D irányított gráf esetén a $\preceq := \overset{D}{\longrightarrow}$ reláció kielégíti a fenti 3 feltételt. Másrészt az is közvetlenül adódik, hogy ha $\preceq$ a fenti 3 tulajdonságot teljesítő reláció, akkor az X halmazon bevezetve minden xy élt, melyre $y \neq x \preceq y$, egy olyan aciklikus D irányított gráfot kapunk, melyre $\preceq = \overset{D}{\longrightarrow}$. Tehát a részbenrendezés hagyományos definíciója egyenértékű a fenti, irányított gráfossal.

3.174. Példa *1. A valós számok a $\leq$ rendezéssel. (Bármely két szám összehasonlítható, tehát ez egy* teljes rendezés*.)*

2. Az X halmaz részhalmazain értelmezett $\subseteq$ reláció. (Vannak nem összehasonlítható részhalmazok.)

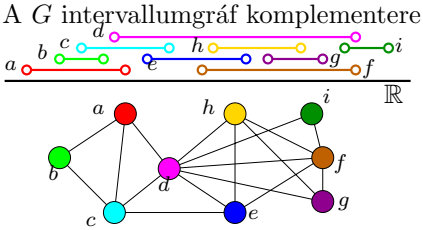
3. Az $\mathbb{N}$ halmazon az oszthatóság. (Vannak nem összehasonlítható számok.)

4. Intervallumrendezés: $I_1, I_2, \ldots$ valós intervallumok. $I_i \preceq I_j$, ha $I_i = I_j$, vagy $x_i < x_j$ minden $x_i \in I_i$, $x_j \in I_j$ esetén. (Az I_j intervallum teljes egészében jobbra van I_i-től.)

3.175. Definíció *Legyen $\preceq$ az X halmaz részbenrendezése. A $G_{\preceq}$* összehasonlítási gráf *csúcshalmaza X, élei pedig azon xy-k, melyekre $x \neq y$, továbbá x és y összehasonlítható: $x \preceq y$ vagy $y \preceq x$.*

3.176. Példa *Legyenek az $I_1, I_2, \ldots$ valós intervallumok a G gráf csúcsai, és fusson az I_i és I_j csúcsok között él, ha $I_i \cap I_j \neq \emptyset$. (Az ilyen típusú gráfok neve* intervallumgráf*.)*

A G intervallumgráf komplementere az intervallumrendezésnek megfelelő összehasonlítási gráf.



3.177. Tétel *Ha $\preceq$ a véges X halmaz részbenrendezése, akkor a $G_{\preceq}$ összehasonlítási gráf perfekt.*

Bizonyítás. Először megfigyeljük, hogy $G_{\preceq}$ minden feszített részgráfja is összehasonlítási gráf. Valóban: a $G_{\preceq}$ ponthalmazának egy U részhalmaza által feszített gráf nem más, mint az U-ra megszorított $\preceq|_U$ részbenrendezés $G_{\preceq|_U}$ összehasonlítási gráfja. (Az világos, hogy a $\preceq|_U$ megszorítás is részbenrendezés.)

A tétel igazolásához tehát annyit kell megmutatni, hogy ha $G_{\preceq}$ összehasonlítási gráf, akkor $\omega(G_{\preceq}) \geq \chi(G_{\preceq})$. (Itt felhasználtuk a korábban általában bizonyított $\omega(G_{\preceq}) \leq$

$\chi(G_{\preceq})$ egyenlőtlenséget.) Legyen D olyan aciklikus irányított gráf, melyre $\preceq = \overset{D}{\longrightarrow}$. Jelölje V_i a G azon v csúcsainak halmazát, amire az igaz, hogy a v-ből induló leghosszabb D-beli irányított út pontosan i csúcsot tartalmaz. Mivel D aciklikus, ezért a definícióból adódik, hogy $V(G)$ a diszjunkt $V_1, V_2, \ldots, V_k$ halmazok uniója, és az is, hogy minden V_i halmaz független. Ezért $\chi(G) \leq k$. Másrészt, ha $x \in V_k$, akkor létezik egy x-ből induló, k pontú irányított út D-ben, és ezen út csúcsai egy k méretű klikkjét alkoltják a G gráfnak. Ezek szerint $\omega(G) \geq k \geq \chi(G)$, és ezt akartuk igazolni. □

3.178. Tétel (Gyenge perfekt gráf tétel) *Ha G perfekt, akkor (és csak akkor) $\overline{G}$ is perfekt.*

3.179. Következmény *Minden intervallumgráf perfekt.*

Bizonyítás. Az intervallumgráf komplementere az intervallumrendezés összehasonlítási gráfja, tehát perfekt. A gyenge perfekt gráf tétel miatt az intervallumgráf is perfekt. □

A gyenge perfekt gráf tételt először Lovász bizonyította be, az alábbi állítás igazolásával.

3.180. Tétel (Lovász tétele) *A G gráf perfekt $\iff$ G minden G' feszített részgráfjára $\alpha(G') \cdot \omega(G') \geq |V(G')|$.*

A 3.180. Lovász tételében a szükségesség bizonyítása. Mivel G egy $\chi(G)$-színezésének $V_1, V_2, \ldots$ színosztályai diszjunkt független halmazok, ezért $|V(G)| = |V_1| + |V_2| + \ldots \leq \alpha(G) \cdot \chi(G)$. Ha G' a G perfekt gráf feszített részgráfja, akkor $\chi(G') = \omega(G')$ miatt $|V(G')| \leq \alpha(G') \cdot \chi(G') = \alpha(G') \cdot \omega(G')$. □

Gasparian bizonyítása Lovász tételére. Az elégségességet igazoljuk. A szükségességet láttuk, így elegendő azt megmutatni, hogy ha G minimális imperfekt (azaz G nem perfekt, de minden valódi feszített részgráfja az), akkor $\alpha(G) \cdot \omega(G) < |V(G)|$. Legyen $\alpha := \alpha(G)$, $\omega := \omega(G)$. Figyeljük meg, hogy ha $A \subseteq V(G)$ független, akkor $\omega + 1 \leq \chi(G) \leq \chi(G - A) + 1 = \omega(G - A) + 1 \leq \omega + 1$, tehát $\omega = \omega(G - A) = \chi(G - A)$. Létezik tehát G minden α méretű A független halmazához egy ω méretű, A-tól diszjunkt $K(A)$ klikk G-ben.

Legyen $A_0 = \{a_1, a_2, \ldots, a_\alpha\}$ a G egy α méretű független halmaza. $G - a_i$ perfekt, és $\chi(G - a_i) = \omega(G - a_i) = \omega$, tehát legyenek az $A_i^1, A_i^2, \ldots A_i^\omega$ független halmazok a $G - a_i$ gráf egy ω-színezésének színosztályai. Vegyük észre, hogy az ω méretű $K(A_i^j)$ klikk a $\omega - 1$ db A_i^k $(k \neq j)$ színosztály mindegyikét legfeljebb 1 pontban metszi, ezért $|K(A_i^j) \cap A_i^k| = 1$ és $a_i \in K(A_i^j)$. Mivel a $K(A_i^j)$ klikk az A_0 független sem metszheti 2 pontban, ezért $l \neq i$-re $a_l \notin K(A_i^j)$, vagyis $K(A_i^j) \subseteq G - a_l$. Az ω méretű $K(A_i^j)$ klikk a $G - a_l$ gráf ω-színezésének $A_l^1, A_l^2, \ldots A_l^\omega$ színosztályait tehát $1-1$ pontban metszi. Az is világos, hogy az ω méretű $K(A_0)$ klikk diszjunkt a_i-től, azaz a $G - a_i$ gráf ω-színezésének $A_i^1, A_i^2, \ldots A_i^\omega$ színosztályait $1-1$ pontban metszi.

Legyen $\mathcal{A}$ az a mátrix, melynek $\alpha \cdot \omega + 1$ sora az

$$A_0, A_1^1, A_1^2, \ldots A_1^\omega\, A_2^1, A_2^2 \ldots, A_\alpha^\omega$$

független halmaznak megfelelő incidenciavektorok, a $\mathcal{K}$ mátrix $\alpha \cdot \omega + 1$ sora pedig legyen rendre a

$$K(A_0), K(A_1^1), K(A_1^2), \ldots K(A_1^\omega), K(A_2^1), K(A_2^2) \ldots, K(A_\alpha^\omega)$$

klikkek incidenciavektora. Mindkét mátrix tehát $(\alpha \cdot \omega + 1) \times |V(G)|$ méretű, így az $(\alpha \cdot \omega + 1) \times (\alpha \cdot \omega + 1)$ méretű $M = \mathcal{A} \cdot \mathcal{K}^T$ szorzatmátrix rangja is legfeljebb $|V(G)|$. Márpedig M minden eleme a megfelelő független halmaz és klikk közös elemeinek számát tartalmazza, azaz M főátlójában 0-k, minden főátlótól különböző helyén pedig 1-esek állnak. Könnyen látható, hogy M rangja $\alpha \cdot \omega + 1$, azaz $\alpha \cdot \omega < |V(G)|$. □

Az intervallumgráfok perfektségét közvetlenül (a gyenge perfekt gráf tétel nélkül) is bebizonyítjuk.

Az intervallumgráfok perfektségének közvetlen bizonyítása. Figyeljük meg, hogy az intervallumgráf minden feszített részgráfja intervallumgráf, amit épp a feszített részgráf csúcsainak megfelelő intervallumok határoznak meg. Ezért elegendő azt igazolni, hogy tetszőleges G intervallumgráfra $\chi(G) = \omega(G)$. Láttuk, hogy a $\chi(G) \geq \omega(G)$ egyenlőtlenség minden gráfra teljesül, ezért a feladatunk mindössze annyi, hogy a $\chi(G) \leq \omega(G)$ egyenlőtlenséget igazoljuk, azaz, színezzük ki G-t k színnel és ugyanakkor találjunk egy k méretű klikket is G-ben.

A G gráf kiszínezését a már látott mohó színezéssel végezzük, ahol a csúcsokat a megfelelő intervallumok balvégpontjainak növekvő sorrendjében vesszük. (Az ábrán látható intervallumgráf esetén ez az $abcdefhgi$ sorrendnek felel meg.) Tehát G csúcsait ebben a sorrendben színezzük úgy, hogy minden újabb intervallumnak megfelelő csúcs kiszínezésekor a legkisebb sorszámú olyan színt használjuk, ami nem okoz azonos színű végpontokkal rendelkező élt. Tegyük fel, hogy k színt használtunk fel eközben. Mit mondhatunk annak az x csúcsnak megfelelő intervallumról, amit a k-dik színre festettünk? Nos, x-nek vannak olyan $v_1, v_2, \ldots, v_{k-1}$ szomszédai, amelyeket korábban már az első $k-1$ színnel megszíneztünk. Ezek szerint a $v_1, v_2, \ldots, v_k$ intervallumok mindegyikének van közös pontja az x intervallummal. Az intervallumok feldolgozási sorrendjéből adódóan ez azt jelenti, hogy x bal végpontját minden egyes v_i intervallum tartalmazza, azaz, a $v_1, v_2, \ldots, v_{k-1}, x$ csúcsok G-ben egy k méretű klikket alkotnak. Nekünk pedig éppen ezt kellett bizonyítanunk. □

Az intervallumgráfok perfektségére adunk egy másik bizonyítást is a gyenge perfekt gráf tétel felhasználása nélkül, amivel általánosabb eredmény igazolható.

3.181. Lemma *Tegyük fel, hogy a G gráf olyan, hogy minden feszített részgráfjának van* szimpliciális csúcsa*, azaz olyan v pontja, melynek szomszédai klikket alkotnak G-ben. Ekkor G perfekt.*

Bizonyítás. A G gráf n pontszáma szerinti indukcióval bizonyítunk. Ha $n = 1$, akkor G perfekt, az állítás igaz. Tegyük fel, hogy a legfeljebb n pontú gráfokra igaz a lemma, és legyen az állításban leírt tulajdonságú G gráfnak $n + 1$ csúcsa. A G gráf minden valódi feszített részgráfja legfeljebb n csúccsal rendelkezik, ezért igaz rájuk az indukciós állítása. Vagyis csupán annyit kell bizonyítanunk, hogy $\chi(G) = \omega(G)$ áll.

Legyen v a G szimpliciális csúcsa és legyen $G' = G - v$ az e pont törlésével keletkező, n csúcsú gráf! Mivel v törlése legfeljebb eggyel csökkenti a klikkszámot, ezért $\omega(G) \geq \omega(G') \geq \omega(G) - 1$. Ha tehát $\omega(G) > \omega(G')$, akkor $\omega(G) = \omega(G') + 1 = \chi(G') + 1 \geq \chi(G)$, ahol a második egyenlőség azért igaz, mert a G' gráfra teljesül az indukciós állítás, az egyenlőtlenség pedig abból következik, hogy ha G'-t kiszínezzük $\chi(G')$ színnel, és v-nek egy újabb színt adunk, akkor G egy jó színezését kapjuk. Ezt összevetve a minden gráfra teljesülő, korábban bizonyított $\chi(G) \geq \omega(G)$ egyenlőtlenséggel, $\chi(G) = \omega(G)$ adódik.

Az $\omega(G) = \omega(G')$ esetet kell még ellenőriznünk. Mivel v a szomszédaival együtt is klikket alkot, ezért v-nek legfeljebb $\omega(G) - 1$ szomszédja lehet. Innen $\omega(G) = \omega(G') \geq \chi(G) \geq \omega(G)$ adódik, ahol az utolsó egyenlőtlenség a szokásos triviális becslés. Az utolsó előtti egyenlőtlenség magyarázata, hogy G' az indukciós állítás szerint kiszínezhető $\omega(G')$ színnel, de v-nek $\omega(G')$-nél kevesebb szomszédja van, tehát v számára is marad felhasználható szín. Ez G-nek egy $\omega(G')$ színnel történő színezését adja, ennél G kromatikus száma nem lehet nagyobb. □

Be lehet bizonyítani, hogy az ú.n. *merevkörű* gráfok (melyekben 3-nál hosszabb körök nem fordulhatnak elő feszített részgráfként) rendelkeznek szimpliciális csúccsal. Innen azonnal adódik, hogy a merevkörű gráfok perfektek.

Az intervallumgráfok perfektségéről szóló 3.179. Következmény harmadik bizonyítása. A fenti lemma miatt csupán azt kell igazolni, hogy az intervallumgráf tetszőleges feszített részgráfjának van szimpliciális csúcsa. Mivel az intervallumgráf minden feszített részgráfja intervallumgráf, ezért elegendő csupán annyit megmutatni, hogy tetszőleges intervallumgráfnak létezik szimpliciális csúcsa. Legyen G tehát egy intervallumgráf, és legyenek $I_1, I_2, \ldots$ a G-t meghatározó intervallumok. Feltehetjük, hogy az I_1 intervallum jobbvégpontja a legkisebb az adott intervallumok jobbvégpontjai között. Állítjuk, hogy a G gráf I_1-nek megfelelő csúcsa szimpliciális. Ehhez mindössze azt kell igazolni, hogy az I_1-t metsző intervallumok egymást is páronként metszik. Mivel minden I_j intervallum jobbvégpontja jobbra van I_1 jobbvégpontjától, ezért minden I_1-t metsző intervallum tartalmazza I_1 jobbvégpontját, és éppen ezt akartuk bizonyítani. □

A fenti bizonyítás módszere alkalmas a tétel általánosítására, és intervallumgráfok helyett részfagráfokról megmutatni, hogy perfektek. Egy G gráf *részfagráf*, ha csúcsai egy F fa részfáinak felelnek meg úgy, hogy két csúcs között pontosan akkor fut él, ha a megfelelő két részfának létezik közös csúcsa. Ha F egy út, akkor az F-hez tartozó részfagráf intervallumgráf, és minden intervallumgráf részfagráfja egy alkalmas útnak. Ha tekintjük F egy v csúcsát, akkor vagy minden részfa tartalmazza v-t, és akkor G egy klikk, ami perfekt, vagy létezik egy olyan T részfa, aminek a v-hez legközelebbi u csúcsa v-től a lehető legtávolabb van. Könnyen látható, hogy minden T-t metsző részfa tartalmazza u-t, vagyis a G gráf T-nek megfelelő csúcsa szimpliciális.

3.182. Tétel (Perfekt gráf tétel (Chudnovsky, Robertson, Seymour és Thomas)) *Egy G véges gráf pontosan akkor perfekt, ha sem G, sem $\overline{G}$ nem feszít legalább 5 hosszú, páratlan kört.*□

Történelem: A perfekt gráf tétel (nők a matematikában)
A perfekt gráf tételt Claude Berge már 1960-ban sejtette. Széles körben ismertté válását követően népes matematikushadsereg próbálta bebizonyítani, de csak részeredményeket sikerült igazolni. A sejtés fokozatosan a gráfelmélet egyik centrális jelentőségű megoldatlan problémájává vált: számos fontos kérésről derült ki, hogy szorosan kapcsolódik a problémához. A 2002-ben megtalált bizonyítás, mely jelentős részben az akkor 25 éves, ukrán származású Maria Chudnovsky nevéhez fűződik, komoly áttörés a gráfelméletben. Maria időközben több nehéz problémát oldott meg, ezzel is bebizonyítva, hogy részéről nem véletlen szerencse volt a sejtés igazolása. Mindez jelzi azt is, mekkora ostobaság az a múlt században talán népszerű vélekedés, miszerint a férfiak agya a nőkénél jóval alkalmasabb a matematika művelésére, hiszen a komoly matematikai tételek szinte minegyike férfiakhoz köthető. Érdekes, hogy míg Magyarországon 30 éve a matematikus évfolyamokon még csak elvétve tanultak lányok, addig a Szovjetunióban a hallgatóknak majdnem a felét tették ki. Valószínűleg a matematika hagyományos férfidominanciája leginkább a múltbeli erősebb társadalmi elvárásokban és kötöttebb szerepekben gyökerezik. Természetesen a fenti gondolatmenet is propaganda, de korántsem a feminizmus mellett. Sokkal inkább azt igazolandó, hogy mindig érdemes a közkeletű igazságok mélyére nézni azok kritika nélküli elfogadása helyett. ♦

4. fejezet

Számelmélet

4.1. Oszthatóság, prímek, közös osztók

4.1. Definíció *Az a, b egész számokról azt mondjuk, hogy a* osztja *b-t, illetve b az a* többszöröse*, (jelölése $a \mid b$), ha $b = aq$ valamely q egész számra. Világos, hogy $n \neq 0$ esetén $\pm 1, \pm n \mid n$, ezek az n* triviális osztói*. Az n nemtriviális osztóit* valódi osztóknak *nevezzük.*

4.2. Példa $1 \mid -7, 19 \mid 0, -3 \mid 9, 0 \nmid 2, 0 \mid 0$.

Az a és b egész számokra (ahol $a \neq 0$) értelmezhető a maradékos osztás, aminek később használ vesszük. Világos, hogy a b számot fel tudjuk írni $b = a \cdot \frac{b}{a} = a \cdot \left\lfloor \frac{b}{a} \right\rfloor + m$ alakban, ahol $0 \leq \frac{b}{a} - \left\lfloor \frac{b}{a} \right\rfloor < 1$ miatt $0 \leq m < b$ adódik. A így definiált m-et a b *szám a-val való oszási maradékának* nevezik. Például 111-nek a 9-es osztási maradéka 3, (-18)-nak az 5-ös osztási maradéka 2, és 17-et (-1)-gyel osztva 0 maradékot kapunk .

4.3. Definíció *A $p \in \mathbb{Z}$ szám* felbonthatatlan *(néha* irreducibilis*, ómagyarul* törzsszám*), ha $|p| \neq 1$ és p-t csak triviális módon tudjuk egészek szorzataként előállítani, azaz $p = ab$ $(a, b \in \mathbb{Z})$ esetén $|a| = 1$ vagy $|b| = 1$. Ugyanezt úgy is mondhatjuk, hogy p akkor felbonthatatlan, ha p-nek csak triviális osztói vannak, és $|p| \neq 1$.*

4.4. Megjegyzés *A 4.3. Definíciót helytelenül úgy szokás mondani, hogy p akkor prím, ha p-t csak az 1 és önmaga az osztója. Mindössze három okból butaság ez. Ebben a definícióban egyrészt felbonthatatlanokról van szó, másrészt pedig azt kellene kikötni, hogy p-t csak a ± 1 és a $\pm p$ osztja, és persze azt is, hogy $p \neq \pm 1$.*

4.5. Példa $2, -5, 11$ *felbonthatatlanok, a -1 ill. a $-9 = 3 \cdot (-3)$ pedig nem azok.*

4.6. Megjegyzés *Korábban azt tanították, hogy a most definiált számok a prímszámok. Ez így nem pontos. Látni fogjuk, hogy a prímek definíciója egészen más, mint a felbonthatatlanoké. Jóllehet, az egészek körében a két fogalom azonos számhalmazt definiál,*

a felbonthatatlan és prím tulajdonság más „számkörökben" értelmezve, nem feltétlenül ugyanazt jelenti. A lényeg, amire itt rá szeretnék mutatni, hogy tudjunk arról, hogy más a prím és más a felbonthatatlan definíciója, és korántsem triviális, hogy egészek körében a két fogalom egybeesik.

4.7. Állítás *Bármely z egész szám előáll felbonthatatlan számok szorzataként ha $|z| > 1$.*

Bizonyítás. $|z|$ szerinti teljes indukciót alkalmazunk. Világos, hogy $|z| = 2$ esetén z felbonthatatlan, és mint egytényezős szorzat megfelel. Tegyük fel, hogy k-ig már bizonyítottunk, azaz minden olyan számra igaz a tétel, aminek az abszolút értéke legfeljebb k. Legyen $|z| = k + 1$. Ha z felbonthatatlan, akkor z megfelel, mint egy egytényezős szorzat. Ha z nem felbonthatatlan, akkor z nemtriviális módon felbomlik $z = ab$ alakban, ahol $1 < |a| \leq k$ és $1 < |b| \leq k$. Az indukciós feltevés értelmében a és b is előáll felbonthatatlan számok szorzataként, ezért ez a szorzatukra, z-re is igaz. □

4.8. Tétel (A számelmélet alaptétele) *Ha egy z egész számra $|z| > 1$, akkor z előáll felbonthatatlan számok szorzataként, és a z ilyen előállításai csak a tényezők sorrendjében és előjeleiben különbözhetnek.*

4.9. Példa *A -24 néhány lehetséges előállítása $-24 = 2 \cdot 3 \cdot (-2) \cdot 2 = (-3) \cdot (-2) \cdot (-2) \cdot 2 = (-2)^3 \cdot 3$, és ezek csakugyan az előjelekben és a sorrendben különböznek csupán.*

4.10. Definíció *Az $1 < n \in \mathbb{N}$ szám* kanonikus alakján *egy olyan $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ előállítást értünk, amiben $p_1, p_2, \ldots, p_k$ különböző (pozitív) felbonthatatlanok és az $\alpha_1, \alpha_2, \ldots, \alpha_k$ számok pedig pozitív egészek. Időnként szokás azt is feltenni, hogy $p_1 < p_2 < \ldots < p_k$.*

Az imént bizonyított állítás miatt minden 1-nél nagyobb egésznek létezik kanonikus alakja és ez a kanonikus alak a számelmélet alaptétele szerint a sorrendtől eltekintve egyértelmű.

A számelmélet alaptétele nem axióma. Bármennyire is magától értetődőnek érezzük (elsősorban az általános- és középiskolás súlykolás miatt), bizonyításra szorul. Az alábbi bizonyítás egyúttal arra is rámutat, hogy mi az az ok, ami miatt az egészek alkotta számkörben igaz a tétel.

A számelmélet alaptételének bizonyítása. A már bizonyított állítás szerint a vizsgált számok előállnak felbonthatatlanok szorzataként. Mivel egy szám pontosan akkor felbonthatatlan, ha az ellentettje felbonthatatlan, elegendő pozitív egészekre szorítkoznunk a bizonyításban. A felbontás egyértelműségéhez tehát csak azt kell igazolni, hogy ha $z = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l$ két olyan előállítás, amire $p_1 \leq p_2 \leq \ldots \leq p_k$ és $q_1 \leq q_2 \leq q_l$, teljesül, akkor $k = l$ és a $p_i = q_i$ minden i-re. Ezt is z szerinti teljes indukcióval bizonyítjuk. Ha $z = 2$, akkor z felbonthatatlan, nincs mit igazolunk. Tegyük

fel tehát, hogy a z-nél kisebb számokra már megmutattuk a felbontás egyértelműségét. Tekintsük a fenti $z = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l$ felbontásokat. Az általánosságot az sem korlátozza, ha kikötjük, hogy $p_1 \leq q_1$.

I. eset: $p_1 = q_1$. Ekkor $\frac{z}{p_1} = p_2 \cdot p_3 \cdot \ldots \cdot p_k = q_2 \cdot q_3 \cdot \ldots \cdot q_l$. Mivel $\frac{z}{p_1} < z$, az indukciós állítás szerint $k = l$ és $p_2 = q_2, p_3 = q_3, \ldots, p_k = q_l$. Így $p_1 = q_1$ miatt z-re is igaz az indukciós állítás.

II. eset: $p_1 < q_1$.

Ekkor

$$z = p_1 \cdot p_2 \cdot \ldots \cdot p_k = (q_1 - p_1) \cdot q_2 \cdot \ldots \cdot q_l + p_1 \cdot q_2 \cdot \ldots \cdot q_l,$$

tehát

$$p_1(p_2 \cdot p_3 \cdot \ldots \cdot p_k - q_2 \cdot q_3 \cdot \ldots \cdot q_l) = (q_1 - p_1) \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_l =: z' \ .$$

Világos, hogy $z' < z$, ezért z'-re tudjuk, hogy igaz a számelmélet alaptétele. A fenti két felírás alapján elkészíthetjük a z' felbonthatatlanok szorzataként történő kétféle felírását, mégpedig úgy, hogy a bal oldalon a $(p_2 \cdot p_3 \cdot \ldots \cdot p_k - q_2 \cdot q_3 \cdot \ldots \cdot q_l)$, a jobb oldalon pedig a $(q_1 - p_1)$ tényezőt helyettesítjük egy-egy felbonthatatlanok szorzatáként történő előállításukkal. E két felírásból a bal oldalon p_1 lesz az egyik tényező, így az indukciós feltevés szerint p_1-nek szerepelnie kell a jobb oldalon is. Mivel p_1 mindegyik q_i-nél kisebb ezért p_1-nek az $(q_1 - p_1)$ felbontásában kell szerepelnie. Ekkor azonban $p_1 \mid q_1 - p_1$, ezért $p_1 \mid q_1$, és ez $1 < p_1 < q_1$ miatt ellentmond q_1 felbonthatatlanságának. Az ellentmondás azt mutatja, hogy a II. eset nem valósulhat meg, és ezzel az indukciós bizonyítást befejeztük. □

4.11. Megjegyzés *Min múlik a fenti bizonyítás? A kulcs a II. eset gondolatmenete. Itt van ugyanis szükségünk a számhalmazunkon a természetes rendezésre. Lényegében azt mutatjuk ugyanis meg, hogy ha van egy olyan szám, amire a felbontás nem egyértelmű, akkor van egy másik ilyen szám is, és ez a másik kisebb, mint amit épp vizsgálunk. Más szóval bármely „rossz" számnál van kisebb „rossz" szám is, ami természetes számokon lehetetlenség.*

A bizonyítás lelke tehát a számkör „természetes rendezése". Ennek a rendezésnek pontosan arra a tulajdonságára van szükségünk, amiből az is következik, hogy van „maradékos osztás", azaz minden $a \geq b$ esetén létezik egy $a = q \cdot b + m$ felírás, ahol $0 \leq m < b$. Ezért a fenti bizonyítás minden olyan struktúrában elmondható, ahol van maradékos osztás. A felbonthatatlanság definíciójának értelemszerű módosításával a számelmélet alaptétele igaz marad pl. az ú.n. Gauss-egészekre*, azaz az $a + bi$ alakú komplex számokra, ahol $a, b \in \mathbb{Z}$ és az egész együtthatós polinomok körében, jóllehet ez utóbbi struktúrában nincs maradékos osztás.*

Itt az ideje, hogy végre eláruljuk mik is a prímek.

4.12. Definíció *A $p \in \mathbb{Z}$ szám* prím*, ha $|p| > 1$ és tetszőleges $a, b \in \mathbb{Z}$-re teljesül, hogy $p \mid ab \Rightarrow p \mid a$ vagy $p \mid b$.*

Szavakban: egy szám akkor prím, ha csak úgy tud osztani egy szorzatot, ha a szorzat valamelyik tényezőjét osztja. A számelmélet alaptételének fontos következménye a prím és a felbonthatatlan ugyanazokat a számokat jelenti.

4.13. Következmény *1. Ha a p egész szám prím, akkor p felbonthatatlan.*
2. Ha a p egész szám felbonthatatlan, akkor p prím.

Bizonyítás. 1. Tegyük fel, hogy p prím és tegyük fel, hogy felbomlik $p = a \cdot b$ alakban. Ekkor persze $p \mid ab$, így a prímtulajdonság miatt $p \mid a$ vagy $p \mid b$, és az általánosság megszorítása nélkül feltehető, hogy $p \mid a$. Ekkor azonban $a = p \cdot k$ és $p \neq 0 \neq a$ miatt $|p| \leq |a| \leq |a| \cdot |b| = |ab| = |p|$ következik, tehát végig egyenlőség áll, vagyis $a = \pm p$. Így p bármely felbontása triviális, azaz p felbonthatatlan. Figyeljük meg, hogy ez az állítás független volt a számelmélet alaptételétől.

2. Most tegyük fel azt, hogy p felbonthatatlan és $p \mid ab$. Mivel $z = \frac{ab}{p}$ egész, ezért z-nek egy felbonthatatlanok szorzataként történő előállítását p-vel megszorozva az ab egy felbonthatatlanok szorzataként való előállítását kapjuk. A számelmélet alaptétele szerint ekkor a $\pm p$ tényezőnek az ab tetszőleges olyan szorzattábontásában szerepelni kell, amiben a tényezők felbonthatatlanok. Így aztán abban a felbontásban is, amit úgy kapunk, hogy az a ill. a b egy-egy felbonthatatlanok szorzataként történő előállítását összeszorozzuk. Ezek szerint tehát $\pm p$ szerepel az a vagy a b felbonthatatlanok szorzataként történő előállításában, vagyis $p \mid a$ vagy $p \mid b$ (esetleg mindkettő) teljesül. Ez pedig éppen a p prímtulajdonságát igazolja. □

4.14. Megjegyzés *Általában is igaz, hogy ahol igaz a számelmélet alaptétele, ott a prímek és a felbonthatatlanok ugyanazok. Mivel mind a Gauss-egészek, mind az egész együtthatós polinomok részstruktúraként tartalmazzák $\mathbb{Z}$-t, érdekes megvizsgálni, mik az ottani prímek. Az egész együtthatós polinomok körében a prímeket* irreducibilisnek *szokás nevezni. A 0-fokú irreducibilis polinomok éppen a szokásos prímek, de irreducibilis pl a $2x + 7$ vagy az $x^2 - 3x + 1$ is. A Gauss egészek körében viszont az az érdekesség is előfordul, hogy egy egész prím nem Gauss-prím. Pl. $2 = (1 + i)(1 - i)$ vagy $5 = (2 + i)(2 - i)$. Egész pontosan minden $4k + 3$ alakú egész prím Gauss-prím is, de az összes többi prím két (egymással konjugált) Gauss-prím szorzatára bontható.*

A valós ill. a komplex együtthatós polinomok olyan további struktúrák, amelyekben van maradékos osztás, így igaz a számelmélet alaptétele. Láttuk, hogy a $p(x) = x^2 - 3x + 1$ irreducibilis az egészek felett. Ugyanez a polinom a valósak felett felbomlik két gyöktényező szorzatára $p(x) = (x - \alpha_1)(x - \alpha_2)$ alakban, ahol α_1 és α_2 a két gyöke a p polinomnak, és e gyöktényezők nyilván nem bonthatók további polinomok szorzatára nemtriviális módon. Az algebra alaptétele (miszerint minden n-edfokú polinomnak (multiplicitással számolva) pontosan n komplex gyöke van) úgy is fogalmazható, hogy a komplex együtthatós polinomok között a prímek pontosan az első fokú polinomok. (Ez a gyöktényezők kiemelhetőségéből látszik.)

A valós együtthatós $x^2 - 3x + 4$ polinomnak nincs valós gyöke, ezért irreducibilis a valós együtthatós polinomok körében. Persze nem az a komplex együtthatósok között, ahol az elsőfokúak a prímek. Mivel egy valós együtthatós p polinom minden komplex gyökének a konjugáltja is gyök, ezért a két gyöktényező szorzata (ami egy másodfokú valós együtthatós polinom) irreducibilis faktora lesz a p polinomnak. Ebből az következik, hogy a valós együtthatós polinomok körében a prímek az elsőfokú és a valós gyökkel nem rendelkező (azaz negatív diszkriminánsú) másodfokú polinomok.

Természetesen a fentieket sem kell tudni a vizsgán. De abban reménykedek, egyeseknek talán nem érdektelen, ha a matematika viszonylag távolinak tűnő területei között kapcsolatot látnak, a többiektől pedig elnézést kérek. Egyébként a fenti gondolatmenetben néhány dolgot elsunnyogtam: akit érdekel, kérdezzen rá, ha rájön, hogy mi az. FT

A számelmélet alaptétele által biztosított kanonikus alak segítségével jellemezhető az oszthatóság.

4.15. Állítás *A $d \in \mathbb{N}$ szám pontosan akkor osztója a $n \in \mathbb{N}$ számnak, ha d kanonikus alakjában kizárólag n kanonikus alakjában megtalálható prímek szerepelnek, és minden ilyen p_i prím kitevője legfeljebb annyi d-ben, mint n-ben.*

Bizonyítás. Ha $d \mid n$, akkor $n = d \cdot d'$ valamely d' egészre. Az n kanonikus alakját úgy kapjuk, hogy összeszorozzuk d és d' kanonikus alakjait, vagyis a szükséges feltétel teljsesül. Az elégségesség igazolásához tegyük fel, hogy a kanonikus alakok az állításban leírt tulajdonsággal rendelkeznek, azaz $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ és $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$, és $\beta_i \leq \alpha_i$. Ekkor $n = d \cdot p_1^{\alpha_1-\beta_1} \cdot p_2^{\alpha_2-\beta_2} \cdot \ldots \cdot p_k^{\alpha_k-\beta_k}$, tehat $d \mid n$. □

Innen aztán remekül kiszámíthatjuk egy szám osztóinak számát a kanonikus alak segítségével.

4.16. Következmény *Legyen $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ az n szám kanonikus alakja. Az n pozitív osztóinak száma $d(n) = \prod_{i=1}^{k}(\alpha_i + 1)$. Az n pozitív osztóinak összege $\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1}-1}{p_i-1}$.*

Bizonyítás. Bármely $d \mid n$ osztó kanonikus alakja olyan, hogy azt alkalmas prímekkel megszorozva n kanonikus alakját kapjuk, azaz $d = \prod_{i=1}^{k} p_i^{\beta_i}$, ahol $0 \leq \beta_i \leq \alpha_i$ teljesül minden i-re. Világos, hogy minden osztóhoz tartozik egy $(\beta_1, \ldots, \beta_k)$ kitevősorozat, és különböző kitevősorozatok (a prímfelbontás egyértelműsége miatt) különböző osztókhoz tartoznak. (A $d = 1$ osztóhoz pl. a csupa-0 sorozat tartozik.) Vagyis a pozitív osztók száma azonos a lehetséges $(\beta_1, \ldots, \beta_k)$ sorozatok számával, ahonnan $d(n) = \prod_{i=1}^{k}(\alpha_i+1)$ adódik, hisz minden β_i a többi kitevőtől függetlenül $\alpha_i + 1$ érték valamelyikét veszi fel.

Világos, hogy az osztók összege $\sigma(n) = (1 + p_1 + p_1^2 + \ldots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \ldots + p_2^{\alpha_2}) \ldots (1 + p_k + p_k^2 + \ldots + p_k^{\alpha_k}) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1}-1}{p_i-1}$, hisz minden osztó egyértelműen áll elő, mint az első szorzat egy kifejtési tagja, míg a második egyenlőség a mértani sorozatok összegzésével adódik.

4.17. Definíció *Legyen $a, b \in \mathbb{Z}$ olyan, hogy $a \neq 0$ vagy $b \neq 0$ teljesül. Az a és b számok (a, b)-vel jelölt* legnagyobb közös osztója *a legnagyobb olyan szám, ami osztója a-nak és b-nek is.*

Az a, b számokat relatív prímnek *mondjuk, ha $(a, b) = 1$.*

Az $a, b \in \mathbb{Z}$ számok legkisebb közös többszöröse az a legkisebb $n \in \mathbb{N}$ szám, amire $a \mid n$ és $b \mid n$ áll. Jelölése: $[a, b]$.

4.18. Példa $(15, 24) = 3$, $(-22, 18) = 2$, $(-20, 0) = 20$ *és* $(0, 0)$ *nem értelmezett, hisz a közös osztók $\mathbb{Z}$ halmazának nincs legnagyobb eleme.* $[-5, -17] = 85$, $[-9, 0] = 0$ *és* $[0, 0] = 0$.

Az osztók kanonikus alakjára vonatkozó állítás segítségével könnyen kiszámíthatjuk a legnagyobb közös osztót ill. a legkisebb közös többszöröst.

4.19. Állítás *Ha* $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ *ill.* $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_k^{\beta_1}$ *(ahol* $\alpha_i = 0$ *és* $\beta_i = 0$ *is megengedett), akkor*

$$(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdot \ldots \cdot p_k^{\min(\alpha_k,\beta_k)} \text{ ill.} [a,b] = p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdot \ldots \cdot p_k^{\max(\alpha_k,\beta_k)},$$

más szóval a lnko-hoz a kanonikus alakokban szereplő közös prímeket kell a kisebb hatványon, a lkkt-höz pedig a kanonikus alakokban szereplő valamennyi prímet a nagyobb hatványon kell összeszorozni.

Tetszőleges a, b *pozitív egészekre* $ab = (a,b) \cdot [a,b]$.

Bizonyítás. Ha d közös osztó, akkor d kanonikus alakjában csak az a és b kanonikus alakjában szereplő közös prímek szerepelhetnek, legfeljebb a kisebbik kitevőn, ezért az lnko-ra adott képlet helyes. A lkkt-nek a és b is osztója, ezért a kanonikus alakban minden a-ban vagy b-ben előforduló prímnek legalább az a ill. b-beli kitevőn kell szerepelnie, ez pedig a második képletet indokolja.

A szorzatra vonatkozó azonosság azért igaz, mert minden prím ugyanazon a hatványon szerepel a jobb- ill. baloldal kanonikus alakjában.

Ha a kanonikus alak nincs kéznél, akkor is boldogulhatunk a legnagyobb közös osztóval.

4.20. Állítás *Ha* a *és* b *egészek, akkor* $(a,b) = (a-b,b)$.

Bizonyítás. Tegyük fel, hogy d az a és b közös osztója, azaz $d \mid a$ és $d \mid b$. Ekkor $d \mid a-b$, azaz d az $a-b$-nek és a b-nek is közös osztója. Ha pedig d az $a-b$-nek és a b-nek is közös osztója, azaz $d \mid a-b$ és $d \mid b$, akkor $d \mid a-b+b = a$, tehát d ekkor az a-nak és a b-nek is közös osztója.

Azt kaptuk, hogy ugyanazok a számok lesznek az a és b közös osztói, amelyek az $a-b$-nek és a b-nek közös osztói, tehát e közös osztók legnagyobbika megegyezik. □

4.21. Következmény *Ha* a *és* b *egészek, akkor* $(a,b) = (a-b,b) = (a-2b,b) = \ldots = (a-kb,b)$.

Két szám legnagyobb közös osztója hatékonyan meghatározható.

Euklideszi algoritmus: Input: a, b egészek (mondjuk $b \leq a$). Output: (a,b).

Működés: Legyen $a_0 := a$, $a_1 := b$. Ha már meghatároztuk az $a_0 \geq a_1 \geq \ldots \geq a_i$ számokat, akkor legyen $a_{i-1} = q_i a_i + a_{i+1}$, azaz osszuk el maradékosan a_{i-1}-t a_i-vel és legyen a_{i+1} a maradék, amire tehát $0 \leq a_{i+1} < a_i$ teljesül. Az eljárás akkor ér véget, ha $a_{k+1} = 0$. Ekkor az algoritmus válasza $(a,b) = a_k$.

Az euklideszi algoritmus helyességének igazolása. Az euklideszi algoritmus azért ér véget, azaz előbb-utóbb $a_{k+1} = 0$ lesz, mert (a_i) nemnegatív egészek csökkenő sorozata, tehát az eljárás lépésszámára $|a_0|$ felső becslés. Mivel $a_{i-1} - q_i a_i = a_{i+1}$, ezért az előző következmény miatt $(a,b) = (a_0,a_1) = (a_0 - q_1 a_1, a_1) = (a_2,a_1) = (a_1,a_2) = (a_1 - q_2 a_2, a_2) = (a_2,a_3) = \ldots = (a_k,a_{k+1}) = (a_k,0) = a_k$. □

4.22. Megjegyzés *Az euklideszi algoritmus valójában ennél sokkal hatékonyabb: belátható, hogy* $a_{i+2} \leq \frac{a_i}{2}$*, ezért a szükséges maradékos osztások száma legfeljebb* $2 \cdot \log_2(a_0)$*, vagyis* a_0 *bináris jegyeinek számával arányos. Sőt: ha az euklideszi algoritmusban az* a_{i+2} *„maradékot" úgy választjuk, hogy* $-\left\lfloor \frac{a_{i+1}}{2} \right\rfloor \leq a_{i+2} < \left\lceil \frac{a_{i+1}}{2} \right\rceil$ *teljesüljön (amit szintén megtehetünk), akkor* $|a_{i+2}| \leq |\frac{a_{i+1}}{2}|$ *is teljesülni fog, amitől az algoritmus elméleti hatékonysága tovább növekszik.*

Az Euklideszi algoritmus segítségével egy másik fontos állítást is igazolunk.

4.23. Tétel *Tetszőleges* $a \geq b$ *egész számokhoz léteznek olyan* k *és* l *egészek, amelyekre* $(a, b) = k \cdot a + l \cdot b$ *teljesül.*

A 4.23. Tétel szavakban: bármely két egész legnagyobb közös osztója előáll a két egész szám *egészkombinációjaként.* (Itt az egészkombináció kifejezés a lineáris kombinációra rímel. Arról van ugyanis szó, hogy míg lineáris kombinációban tetszőleges skalárok lehetnek az összeg tagjainak együtthatói, itt most csak egészek lehetnek az együtthatók.)

Bizonyítás. Hajtsuk végre az Euklideszi algoritmust az a és b számokra. Világos, hogy az $a_0 = 1 \cdot a + 0 \cdot b$ és az $a_1 = 0 \cdot a + 1 \cdot b$ számok előállnak az a és a b egészkombinációjaként. A teljes indukcióhoz tegyük fel, hogy az $a_0, a_1, \ldots, a_i$ számokra már bebizonyítottuk ugyanezt.

Az Euklideszi algoritmus definíciója alapján $a_{i-1} = q_i a_i + a_{i+1}$. Mivel a_i az a és b egészkombinációja, ezért $q_i a_i$ is előáll az a és b egészkombinációjaként. Nyilvánvaló, hogy egészkombinációk különbsége egészkombináció így $a_{i+1} = a_{i-1} - q_i a_i$ is az a és b egészkombinációja lesz. Ezek szerint $a_k = (a, b)$ is előáll az a és b egészkombinációjaként. □

Végül a prímszámokról közlünk néhány hasznos ismeretet.

4.24. Tétel *A prímszámok száma végtelen.*

Bizonyítás. Elegendő azt megmutatni, hogy minden $2 \leq n \in \mathbb{N}$-re létezik n-nél nagyobb prímszám. Mivel $n!$ az $1, 2, \ldots, n$ számok mindegyikével osztható, ezért $N := n! + 1$ az $1, 2, \ldots, n$ számok mindegyikéhez relatív prím, tehát N nem osztható egyetlen n-nél kisebb prímmel sem. Vagyis N kanonikus alakjában kizárólag n-nél nagyobb prímek fordulnak elő. □

A 4.24. Tételnek igaz az alábbi általánosítása is:

4.25. Tétel *A prímek reciprokait kellően sokáig összeadva tetszőlegesn nagy számnál nagyobbat kaphatunk:* $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \ldots = \infty$.□

4.26. Tétel *Tetszőlegesen hosszú sorozat képezhető szomszédos összetett számokból, azaz bármely* $n \in \mathbb{N}$*-re létezik olyan* N*, amire az* $N+1, N+2, \ldots, N+n$ *számok mindegyike összetett.*

Bizonyítás. Legyen $N := (n+1)! + 1$. Ekkor tetszőleges $2 \leq k \leq n+1$ esetén $k \mid (n+1)! + k = N + (k-1)$, tehát $N+1, N+2, \ldots, N+n$ számok mindegyike összetett.□

A prímek eloszlásáról szólnak a következő állítások.

4.27. Tétel (Csebisev tétel) *Tetszőleges n pozitív egészre létezik p prím, melyre $n < p \leq 2n$.*□

4.28. Tétel (Dirichlet tétel) *Ha a és d relatív prím, akkor az $a, a+d, a+2d, \ldots$ számtani sorban végtelen sok prím fordul elő.*□

4.29. Tétel (Nagy prímszámtétel)

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1 \ ,$$

ahol ln *az e alapú logaritmust, $\pi(x)$ pedig az x-nél nem nagyobb prímek számát jelöli.*□

A nagy prímszámtétel jelentősége az, hogy kiderül belőle, hogy x környékén a prímszámok sűrűsége kb $\frac{x}{\ln x}$.

4.30. Sejtés (Goldbach sejtés) *Minden 2-nél nagyobb páros szám előáll két prím összegeként.*

A Goldbach sejtés bizonyítása nagyon erős eszközt adna a kezünkbe. Azonnal következne belőle például a Csebisev tétel: ha $2n+2$ mondjuk $p+q$ alakban áll elő, akkor p és q közül a nagyobbik $n+1$ és $2n$ közé esik.

4.31. Definíció *Az a, b számok* ikerprímek*, ha prímek, és különbségük* 2*.*

Megoldatlan probléma annak eldöntése, hogy véges vagy végtelen sok ikerprím van-e.

Történelem: Erdős és a prímek
Az első elemi bizonyítást a Csebisev tételre Erdős Pál még középiskolás korában találta.

A prímszámtétel bizonyítása több lépésben történt. Az utolsó lépést egymástól függetlenül Hadamard és de la Vallée Poussin tették meg 1896-ban. 1949-ben szintén furcsa holtverseny alakult ki az első elemi (azaz felsőbb analízist nem használó) bizonyítások tekintetében: a befutók Atle Selberg és Erdős Pál voltak, akik egymás eredményeire támaszkodtak a bizonyításaikban. A két szerző között az eredmény Erdős általi bejelentését követően csúf vita támadt. Selberg a bizonyításért Fields érmet kapott, Erdős a kevésbé tekintélyes Cole díjat vehette át. Érdekesség, hogy a Selberg által bevezetett módszerrel később Chen igazolta a Goldbach sejtéssel kapcsolatos egyik legjobb ismert eredményt, ami szerint minden páros pozitív egész előáll egy prím és egy olyan szám összegeként, aminek legfeljebb két prímosztója van. ♦

4.2. Kongruenciák

Sokszor bizonyul hasznosnak az a megfigyelés, hogy egész számok összegének paritása csak az összeg tagjainak paritásától függ. (Pl egy összeg csak úgy lehet páratlan, ha páratlan számú (legalább egy) páratlan tagja van.) Azonban nem csak a kettővel való oszthatóságból származhatnak érdekes eredmények, hanem szükség lehet időnként arra, hogy más osztó szerint próbáljuk osztályozni az egészeket, és a szerint számoljunk velük. Ezt a gondolatot formalizáljuk az alábbiakban.

4.32. Definíció *$a, b, m \in \mathbb{Z}$, $0 < m$ esetén azt mondjuk, hogy a* kongruens *b* modulo *m (jelölése $a \equiv b \pmod{m}$, röviden $a \equiv b(m)$), ha $m \mid a - b$.*

4.33. Példa $2 \equiv 17(5)$. *A 2-vel kongruens számok modulo 5 a $2, 7, 12, 17, 22, \ldots$ ill. $-3, -8, -13, -18, \ldots$*

Tetszőleges $m \geq 2$ egész esetén az egész számok $\mathbb{Z}$ halmaza m diszjunkt osztály uniójára bomlik fel, mégpedig úgy, hogy $0 \leq i \leq m-1$ esetén az i-dik osztályban az $k \cdot m + i$ alakú számok vannak, ahol k végigfut az egészeken. (Más szóval, az i-dik osztályba az m-mel osztva i maradékot adó számok tartoznak.) Ezeket az osztályokat az m *szerinti* (vagy másképpen *modulo* m) *maradékosztályoknak* nevezzük. A maradékosztályok jelentősége az, hogy ha két szám azonos maradékosztályba esik (modulo m), akkor kongruensek egymással modulo m, ha pedig különböző maradékosztályból valók, akkor nem kongruensek.

4.34. Állítás *1. Ha $a \equiv b(m)$ és $c \equiv d(m)$ akkor $a + c \equiv b + d(m)$ és $ac \equiv bd(m)$, azaz két kongruencia összeadható és összeszorozható.*

2.Ha $d \mid a$ és $d \mid b$ és $a \equiv b(m)$, akkor $\frac{a}{d} \equiv \frac{b}{d}(\frac{m}{(m,d)})$, azaz kongruencia osztásakor nemcsak a kongruencia két oldalát osztjuk, hanem a modulust is (az osztó és a modulus legnagyobb közös osztójával).

Bizonyítás. 1. Tudjuk, hogy $m \mid a-b$ és $m \mid c-d$. Ezért $m \mid a-b+c-d = a+c-(b+d)$, azaz $a+c \equiv b+d(m)$. Az is igaz, hogy $m \mid c(a-b)+b(c-d) = ac-bd$, azaz $ac \equiv bd(m)$.

2. Legyen $a = a'd, b = b'd$, $D = (m, d)$, $d = d'D$ és $m = m'D$. Ekkor az $a \equiv b(m)$ kongruencia $a'd'D \equiv b'd'D(m'D)$ alakot ölt, ami definíció szerint azt jelenti, hogy $m'D \mid a'd'D - b'd'D = (a' - b')d'D$, azaz $m' \mid (a' - b')d'$ adódik. Mivel D az m és d legnagyobb közös osztója, ezért az $m' = \frac{m}{D}$ és a $d' = \frac{d}{D}$ számoknak már nem lehet közös prímosztójuk. Tehát $m' \mid a' - b'$ is igaz, ami éppen azt jelenti, hogy $a' \equiv b'(m')$, azaz $\frac{a}{d} \equiv \frac{b}{d}(\frac{m}{(m,d)})$. □

Sokszor az a célunk, hogy egy kongruencián ekvivalens átalakítást végezzünk, azaz ne csak a következtetésünk legyen helyes, hanem az utóbb kapott kongruenciából az eredeti is következzen. Erről szól az alábbi állítás.

4.35. Következmény *1. Az $a \equiv b(m)$ kongruencia pontosan akkor teljesül, ha $a + k \equiv b + k(m)$.*

2. Ha d relatív prím az m-hez, akkor az $a \equiv b(m)$ kongruencia ekvivalens a $ad \equiv bd(m)$ kongruenciával, tehát kongruencia szorzása csak akkor ekvivalens átalakítás, ha a modulushoz relatív prím számmal szorzunk.

3. Az $d > 0$ rögzített egész, akkor az $a \equiv b(m)$ kongruencia ekvivalens a $ad \equiv bd(md)$ kongruenciával.

Bizonyítás. 1. Az, hogy az egyik kongruenciából következik a másik, a $k \equiv k(m)$ ill. a $-k \equiv -k(m)$ kongruencia hozzáadásával adódik.

2. Az $a \equiv b(m)$ kongruenciát a $d \equiv d(m)$ kongruenciával beszorozva $ad \equiv bd(m)$ adódik. Az osztásra vonatkozó állítás miatt pedig az $ad \equiv bd(m)$ kongruenciából $a \equiv b\left(\frac{m}{(m,d)}\right)$ következik, ami $(m,d) = 1$ miatt $a \equiv b(m)$ alakot ölt.

3. $a \equiv b(m) \iff m \mid a-b \iff md \mid (a-b)d \iff md \mid ad-bd \iff ad \equiv bd(md)$. □

Tehát egy kongruencián ekvivalens átalakítás mindkét oldalhoz konstanst hozzáadni, a modulushoz relatív prímmel szorozni mindkét oldalt a modulus változatlanul hagyásával ill. az egész kongruenciát (a modulust is beleértve) egy számmal végigszorozni vagy leosztani. Ennek hamarosan, a lineáris kongruenciák tárgyalásakor fogjuk hasznát venni.

4.3. Redukált maradékrendszer, Euler-Fermat tétel

4.36. Megfigyelés *Ha $a \equiv b(m)$, akkor $(a,m) = (b,m)$. Speciálisan, ha egy maradékosztály valamely eleme relatív prím az m modulushoz, akkor annak a maradékosztálynak minden eleme relatív prím m-hez.*

Bizonyítás. Tudjuk, hogy $m \mid a-b$, ezért $b = a + km$ valamely k egészre. Az Euklideszi algoritmus előtt bizonyított tétel szerint viszont $(a,m) = (a+m,m) = (a+2m,m) = \ldots = (a+km,m) = (b,m)$ □

4.37. Definíció *Rögzített $m > 1$ egész esetén az m elemű $T = \{a_1, a_2, \ldots, a_m\}$ halmazt* modulo m teljes maradékrendszernek *(*TMR*-nek) nevezzük, ha T minden m szerinti maradékosztályból pontosan egy elemet tartalmaz. Az $R \subset \mathbb{Z}$ halmaz pedig* redukált maradékrendszer (RMR) modulo m*, ha R minden m-hez relatív prím m szerinti maradékosztályból pontosan egy elemet tartalmaz. A modulo m RMR méretét, azaz azoknak az m szerinti maradékosztályoknak a számát, amelyek m-hez relatív prím számot tartalmaznak $\varphi(m)$-mel jelöljük.*

4.38. Példa *TMR modulo m a $\{0,1,2,\ldots,m-1\}$ vagy az $\{1,2,\ldots,m\}$ halmaz. Modulo 10 TMR a $\{100,21,-21,42,-42,13,-13,44,55,66\}$ halmaz.*

4.39. Megfigyelés *RMR-t pl. úgy kapunk , hogy egy TMR-ből elhagyjuk a modulushoz nem relatív prím elemeket. Ezek szerint RMR-t alkotnak az* 1 *és* m *közötti,* m*-hez relatív prím egészek. Ezért a* $\varphi(m)$ *függvényt definiálhattuk volna úgy is, mint az* 1 *és* m *közé eső,* m*-hez relatív prím számok számát. Ha* p *prím, akkor* 1 *és* $p-1$ *között minden egész relatív prím* p*-hez, ezért* $\varphi(p) = p - 1$*.*

A relatív prím maradékosztályok fontos tulajdonsága, hogy két ilyen maradékosztály szorzata is relatív prím maradékosztály lesz. Ennél jóval több is igaz.

4.40. Tétel *Legyen* $(a, m) = 1$ *és* $k \in \mathbb{Z}$*. Ha* $R = \{r_1, r_2, \dots r_{\varphi(m)}\}$ *redukált maradékrendszer modulo* m *és* $T = \{t_1, t_2, \dots, t_m\}$ *pedig teljes maradékrendszer modulo* m*, akkor* $aR := \{ar_1, ar_2, \dots ar_{\varphi(m)}\}$ *redukált maradékrendszer modulo* m*,* $aT = \{at_1, at_2, \dots, at_m\}$ *és* $T + k = \{t_1 + k, t_2 + k, \dots, t_m + k\}$ *pedig teljes maradékrendszerek modulo* m*.*

Bizonyítás. Azt kell igazolni, hogy az ar_i-k páronként különböző, m-hez relatív prím maradékosztályokhoz tartoznak, hisz ekkor szükségképpen minden relatív prím maradékosztályból pontosan egy reprezentáns szerepel. Minden ar_i relatív prím maradékosztályba tartozik, mert m-nek sem a-val, sem r_i-vel nincs közös prímosztója, így $(m, ar_i) = 1$. E maradékosztályok pedig különbözők, hiszen ha $ar_i \equiv ar_j(m)$, akkor a-val oszthatunk az osztásról szóló következmény szerint, azaz $r_i \equiv r_j(m)$, ahonnan $i = j$ következik.

Az aT és $T + k$ halmazok TMR volta hasonlóan igazolható. Mindkét halmaz m elemű, ezért csak azt kell igazolni, hogy elemeik különböző m szerinti maradékosztályokba tartoznak. Ha pl $at_i \equiv at_j(m)$, akkor (a, m) miatt oszthatunk a-val, és $t_i \equiv t_j(m)$, amiből T TMR volta miatt $i = j$ következik. Hasonlóan, ha $t_i + k \equiv t_j + k(m)$, akkor $t_i \equiv t_j(m)$, azaz $i = j$. □

A fenti megfigyelésből következik a kongruenciák elméletének egyik legfontosabb tétele, mellyel meghatározható a korábban hivatkozott modulo m reciprok.

4.41. Tétel (Euler-Fermat tétel) *Ha* $(a, m) = 1$*, akkor* $a^{\varphi(m)} \equiv 1(m)$*.*

Bizonyítás. Legyen $R = \{r_1, r_2, \dots r_{\varphi(m)}\}$ RMR modulo m. Az előző megfigyelés szerint $aR := \{ar_1, ar_2, \dots ar_{\varphi(m)}\}$ is RMR modulo m. Mivel kongruenciákat lehet szorozni, ezért $\prod_i r_i \equiv \prod_i ar_i(m)$, ami azt jelenti, hogy $\prod_i r_i \equiv a^{\varphi(m)} \prod_i r_i(m)$. Mivel $(m, \prod_i r_i) = 1$, a modulus változtatása nélkül tuduk osztani, azaz $a^{\varphi(m)} \equiv 1(m)$, ami épp a bizonyítandó állítás. □

4.42. Következmény (kis Fermat tétel) *Ha* p *prím, akkor bármely* a *egészre* $a^p \equiv a(p)$*.*

Bizonyítás. Világos, hogy $\varphi(p) = p - 1$ (hisz 1-től $p - 1$-ig minden egész relatív prím p-hez), ezért ha $(a, p) = 1$, akkor $a^{p-1} \equiv 1(p)$, ahonnan $a^p \equiv a(p)$. Ha $(a, p) \neq 1$, akkor p prímtulajdonsága miatt $p \mid a$, azaz $a \equiv 0(p)$, és $a^p \equiv 0 \equiv a(p)$. □

4.43. Megjegyzés *Az Euler-Fermat tétel egyik jelentősége, hogy következik belőle a redukált maradékrendszerben a reciprok létezése, amit a későbbiek miatt inverznek fogunk hívni. Ha tehát R egy RMR modulo m, akkor azt mondjuk, hogy $r' \in R$ az $r \in R$* inveze, *ha $rr' \equiv 1(m)$. Az Euler-Fermat tétel szerint tehát minden $r \in R$-nek létezik inverze, hiszen $r \cdot r^{\varphi(m)-1} = r^{\varphi(m)} \equiv 1(m)$, vagyis a $r' \equiv r^{\varphi(m)-1}(m)$ választás megfelelő. Világos, hogy ha r inverze r', akkor r' inverze r lesz. Az is könnyen adódik, hogy minden $r \in R$-nek pontosan egy inverze van: tegyük fel ugyanis, hogy $rr' \equiv 1(m)$ és $rr^* \equiv 1(m)$ valamely $r', r^* \in R$ esetén. Ekkor $rr' \equiv rr^*(m)$, és $(r, m) = 1$ miatt oszthatunk r-rel: $r' \equiv r^*(m)$, de ebből $r' = r^*$ következik. Érdemes még azt is látni, hogy az 1 és a -1 önmaguk inverzei.*

Láttuk, hogy $\varphi(p) = p - 1$, ha p prím. Ahhoz, hogy az Euler-Fermat tételt valóban használni tudjuk (pl. az inverz kiszámítására), jó ha ki tudjuk számítani $\varphi(m)$-t tetszőleges m modulusra. Prímhatványmodulusra könnyű dolgunk van: ha $m = p^\alpha$ valamely p prímre, akkor a és m pontosan akkor relatív prímek , ha $p \nmid a$. Ezért $\varphi(m)$ nem más, mint 1 és m között a p-vel nem osztható egészek száma. A p-vel oszthatók száma $\frac{m}{p} = p^{\alpha-1}$, így $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Az alábbi tételben az bizonyítjuk, hogy a φ számelméleti függvény multiplikatív. Ennek alapján meghatározható a $\varphi(n)$ értéke n kanonikus alakjából.

4.44. Tétel *Ha $(m, n) = 1$ akkor $\varphi(mn) = \varphi(m)\varphi(n)$.*

Bizonyítás. Azt kell meghatározni, hogy a $T = \{0, 1, 2, \ldots, mn - 1\}$ halmazban hány mn-hez relatív prím van. Egy a szám pontosan akkor relatív prím mn-hez, ha a m-hez is és n-hez is relatív prím. A kérdés tehát úgy is fogalmazható, hogy T halmazban m-hez relatív prímek között hány szám relatív prím n-hez.

0	1	2	$\ldots$	j	$\ldots$	$m-2$	$m-1$
m	$m+1$		$\ldots$	$m+j$	$\ldots$	$2m-2$	$2m-1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
im	$im+1$	$im+2$	$\ldots$	$im+j$	$\ldots$		$(i+1)m-1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$(n-1)m$	$(n-1)m+1$		$\ldots$	$(n-1)m+j$	$\ldots$		$nm-1$

Írjuk fel a T halmaz elemeit növekvő sorrendben egy olyan táblázatba, aminek n sora és m oszlopa van. Ekkor az i-dik sor j-dik eleme $(i-1)m+j-1$ lesz. Ha tehát rögzítünk egy oszlopot (vagyis egy j-t), akkor az ottani elemek azonos maradékosztályban lesznek modulo m. Mivel a táblázat m oszlopának mindegyike más-más mod m maradékosztálynak felel meg, ezért a táblázatban az m-hez relatív prím számok pontosan $\varphi(m)$ oszlopot töltenek ki. Vizsgáljunk egy oszlopot, azaz rögzítsünk egy j-t, és nézzük a j-dik oszlop meghatározta $\{j-1, m+j-1, 2m+j-1, \ldots, (n-1)m+j-1\}$ halmazt. Ezek a számok úgy keletkeznek, hogy az $T_n = \{0, 1, \ldots, n-1\}$ mod n TMR minden elemét végigszorozzuk m-mel, majd hozzáadunk mindegyikükhöz $(j-1)$-et. Mivel $(n, m) = 1$, ezért minden oszlop egy TMR-t alkot modulo n. Vagyis minden oszlopban pontosan $\varphi(n)$ db n-hez relatív prím elem található. Eszerint a táblázatban az olyan elemek, amelyek m-hez is és n-hez is relatív prímek, $\varphi(m)$ oszlopban helyezkednek el, mindegyik oszlopban pontosan $\varphi(n)$ db. A keresett elemek száma tehát $\varphi(mn) = \varphi(m)\varphi(n)$. □

A $\varphi(n)$ értéke a szita formulából is megkapható annak tanulságos alkalmazásával.

4.45. Tétel *Ha $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ az n kanonikus alakja, akkor*

$$\varphi(n) = n \prod_{p|n,\ prím} \left(1 - \frac{1}{p}\right) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) \ .$$

Bizonyítás. Azt kell megszámolnunk, hogy az $1, 2, \ldots, n$ TMR-ben hány szám relatív prím n-hez. Ezt úgy tesszük meg, hogy megszámoljuk azokat, amelyek nem relatív prímek, és az eredményt levonjuk n-ből. Egy szám akkor nem relatív prím n-hez, ha van n-nel közös prímosztója, azaz a $p_1, p_2, \ldots, p_k$ számok valamelyikének többszöröse. Ha tehát az A_i halmaz tartalmazza az 1 és n közötti p_i-vel osztható számokat, akkor az n-hez nem relatív prím, 1 és n közötti számok éppen az $\bigcup_{i=1}^{k} A_i$ halmaz elemei lesznek. Alkalmazhatjuk tehát a szita formulát:

$$\varphi(n) = n - |\bigcup_{i=1}^{k} A_i| = n - \sum_{\emptyset \neq I \subseteq \{1,2,\ldots,k\}} (-1)^{|I|+1} \left|\bigcap_{i \in I} A_i\right| = \sum_{I \subseteq \{1,2,\ldots,k\}} (-1)^{|I|} \frac{n}{\prod_{i \in I} p_i} = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}) \ ,$$

ahol az utolsó egyenlőség teljesülése a zárójeleket felbontva látszik. A tételben állított második egyenlőség pedig azért igaz, mert a jobboldali tényezőkből $p_i^{\alpha_i}$-t kiemelve és a szorzat elé gyűjtve épp a baloldalt kapjuk. □

4.46. Tétel (Wilson tétel) *Ha p prím, akkor $(p-1)! \equiv -1(p)$.*

Bizonyítás. Minden $1 \leq a \leq p-1$ egészhez tartozik egy $1 \leq b \leq p-1$ egész, amire $ab \equiv 1(p)$, hiszen az $ax \equiv 1(p)$ kongruenciát pontosan egy modulo p maradékosztály oldja meg. Könnyen látható, hogy ha a-hoz b tartozik, akkor b-hez a tartozik, tehát az $1, 2, \ldots, p-1$ számok úgy rendezhetők párokba, hogy minden pár szorzata 1-et ad maradékul p-vel osztva.

A párokba rendezés azért nem egészen pontos, mert bizonyos számok esetleg önmagukkal állnak párban. Ezekre az a számokra $a^2 \equiv 1(p)$ teljesül, azaz $p \mid a^2 - 1 = (a+1)(a-1)$, ahonnan p prímtulajdonsága miatt $p \mid a+1$ vagy $p \mid a-1$ adódik. Eszerint az önmagukkal párban álló számok kizárólag az 1 és a $p-1$ lesznek.

Rendezzük át a $(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1)$ tényezőit úgy, hogy párosával álljanak a fenti értelemben egymáshoz tartozó számok. Ekkor minden pár szorzata 1 lesz modulo p, és lesznek még a páratlanul maradt 1 illetve a $p-1$ tényezők. Más szóval $(p-1)! \equiv 1^{\frac{p-3}{2}} \cdot 1 \cdot (p-1) \equiv p-1 \equiv -1(p)$ adódik, és éppen ezt akartuk bizonyítani. □

A fenti gondolatmenetet felhasználva az az általánosabb tény is igazolható, hogy ha 1-től $(m-1)$-ig összeszorozzuk az m-hez relatív prím számokat, akkor a szorzat 1 vagy -1 maradékot ad m-mel osztva. Ha (a faktoriálisoknál maradva) azt szeretnénk tudni, milyen maradékot ad n-nel osztva az $(n-1)!$, akkor ezt összetett n-ekre is könnyen megkaphatjuk. Ha n felbontható két különböző nemtriviális a és b osztójának szorzatára, akkor $n = ab \mid (n-1)!$ miatt $(n-1)! \equiv 0(n)$. Ha n nem ilyen összetett szám, akkor n egy p prím négyzete, de ekkor $p > 2$ esetén $n \mid p \cdot 2p \mid (n-1)!$ miatt szintén $(n-1)! \equiv 0(n)$ adódik, míg a kimaradó egyetlen eset a $p = 2$, amikoris $n = 4$, és $(n-1)! \equiv 2(n)$.

4.4. Lineáris kongruenciák

4.47. Definíció Lineáris kongruencián *egy* $ax \equiv b(m)$ *kongruenciát értünk, ahol* a *és* b *adott egészek,* m *pedig adott pozitív egész. (Az* $m = 1$ *eset nem túl izgalmas, általában* $m \geq 2$*-vel fogunk foglalkozni.) A* lineáris kongruencia megoldása *azt jelenti, hogy meghatározzuk mindazon egészeket, amelyeket* x *helyébe írva a kongruencia igaz lesz.*

Amikor egy lineáris kongruenciával dolgozunk, akkor általában úgy végzünk műveleteket, hogy a kongruencia mindkét oldával ugyanazt tesszük. Az alábbi tétel segítségével könnyen elönthető, hány megoldása van egy adott lineáris kongruenciának.

4.48. Tétel *Az* $ax \equiv b(m)$ *kongruencia esetén pontosan akkor oldható meg, ha* $(a, m) \mid b$*. A kongruencia megoldáshalmaza* (a, m) *darab maradékosztály modulo* m*.*

Bizonyítás. Legyen $d := (a, m)$, $a = a'd, m = m'd$. Ha az $ax \equiv b(m)$ kongruencia megoldható, akkor $d \mid m \mid ax - b$, így $d \mid a \mid ax$ miatt $d \mid ax - (ax - b) = b$ következik. Ezzel a szükségességet igazoltuk.

Tegyük fel tehát, hogy $d \mid b$, azaz $b = db'$. A kongruenciát (a modulust is beleértve) d-vel végigosztva ekvivalens átalakítást végzünk, és azt kapjuk, hogy $a'x \equiv b'(m')$. Mivel d az m és a legnagyobb közös osztója, ezért a leosztás után $(a', m') = 1$ áll. Az Euklideszi algoritmus után láttuk, hogy az Euklideszi algoritmus segítségével a lnko előáll egész kombinációként, azaz kiszámíthatunk olyan k és l egész számokat, amire $ka' + lm' = 1$. Világos, hogy k-nak és m'-nek nem lehet közös p prímosztója, hiszen ha volna, akkor $p \mid ka' + lm' = 1$ állna. Ezért k és m' relatív prímek.

A $a'x \equiv b'(m')$ kongruenciának a modulushoz relatív prím k-val történő megszorzása ekvivalens átalakítás, azaz $ka'x \equiv kb'(m')$, ami k és l választása miatt $(1 - lm')x \equiv kb'(m')$ alakba írható. A kongruenciához hozzáadva az $lm'x \equiv 0(m')$ kongruenciát azt kapjuk, hogy $x \equiv kb'(m')$. Az elvégzett átalakítások ekvivalens volta miatt az $ax \equiv b$ kongruencia megoldásai pontosan azok az x egész számok, amelyek modulo m' a kb'-vel egy maradékosztályba tartoznak.

Hátra van még, hogy a megoldásokat modulo m adjuk meg. Minthogy $m = m'd$, ezért minden m' szerinti maradékosztály pontosan d darab m szerinti maradékosztály uniója, a konkrét esetben az alábbi reprezentánsokkal írható fel a megoldás: $x \equiv kb'(m)$, vagy $x \equiv kb' + m'(m)$, vagy $x \equiv kb' + 2m'(m)$, vagy ..., vagy $x \equiv kb' + (d-1)m'(m)$.□

4.49. Megjegyzés *Az* $a'x \equiv b'(m')$ *kongruenciát az Euklideszi algoritmusból kapott* k *számmal történő beszorzással kaptuk meg. Ha nekünk nem lineáris kongruenciát, hanem az* $ax = b$ *lineáris egyenletet kellene megoldanunk, akkor a megoldás az* a*-val való osztás lenne, amit szerencsésebb úgy tekinteni, mint az a reciprokával történő szorzást. Az a reciproka a szokásos szorzás esetén természetesen* $\frac{1}{a}$*. A lineáris kongruencia fenti megoldásakor kapott* k*-val történő beszorzás teljesen hasonlóan működik, hiszen itt is azt kapjuk, hogy* $ka' \equiv 1(m')$*, tehát a szóbanforgó* k *tekinthető az* a' *reciprokának modulo* m'*. A fenti bizonyítás gondolatmenetéből az is adódik, hogy pontosan az* m*-hez relatív prím számoknak van modulo* m *reciproka.*

Tehát, míg az $ax = b$ egyenlet pontosan akkor oldható meg, ha a-nak van reciproka vagy $a = 0$ és $b = 0$, addig lineáris kongruenciákra ez úgy módosul, hogy az $ax \equiv b(m)$ akkor megoldható, ha a-nak van „modulo m reciproka" vagy ha a-nak nincs (mert $(a, m) \neq 1$), akkor b-nek is „legalább annyira" nincs reciproka, azaz $(a, m) \mid (b, m)$.

A fenti bizonyításban szereplő, Euklideszi algoritmussal dolgozó módszer segítségével hatékonyan tudunk megoldani a lineáris kongruenciát. Ha azonban a modulus elég kicsi, akkor az is kellően hatékony lehet, hogy egy TMR minden elemét behelyettesítjük a kongruenciába, és pontosan azok a maradékosztályok alkotják a megoldáshalmazt, amelyikeknek a reprezentánsait behelyettesítve teljesült a kongruencia.

Egy harmadik módszert alkalmazhatunk, ha ismert az m kanonikus alakja, és így ki tudjuk számítani $\varphi(m)$-t. Ekkor az Euler-Fermat tételt felhasználva tudjuk megoldani az $ax \equiv b(m)$ kongruenciát, a leosztás után, amikoris már $(a, m) = 1$ teljesül. Ha ugyanis mindkét oldalt beszorozzuk a modulushoz relatív prím $a^{\varphi(m)-1}$ számmal (és így ekvivalens átalakítást végzünk), akkor azt kapjuk, hogy

$$x \equiv 1 \cdot x \equiv a^{\varphi(m)}x \equiv a^{\varphi(m)-1}ax \equiv a^{\varphi(m)-1}b(m) \ ,$$

azaz megkapjuk a lineáris kongruencia egyértelmű megoldását.

A gyakorlatban (pl a zh-n) leginkább egy negyedik módszert alkalmazunk. Gyakran oldunk meg konkrét (mondjuk $ax \equiv b(m)$) lineáris kongruenciát ekvivalens átalakítások segítségével. Ennek során az alábbi átalakításokat végezzük.

1. Az a-t vagy a b-t vele kongruens másik számmal helyettesítjük.
2. Ha $(a, b) > 1$, akkor osztunk (szükség esetén az m modulust is)
3. A **modulushoz relatív prímmel** szorzunk (és a modulust nem bántjuk).

Az átalakítások során a cél az a együttható abszolút értékének csökkentése, egészen 1-ig.

4.50. Példa *Megoldandó a*
$62x \equiv 24(36)$ *kongruencia. Mivel* $62 \equiv 26(36)$*,ezért a*
$26x \equiv 24(36)$ *kongruenciát kapjuk.* $(26, 36) = 2$*, tehát osztunk:*
$13x \equiv 12(18)$ *adódik. Sajnos nem szorozhatunk* $2, 3$ *ill.* 4*-gyel, így inkább* $13 \equiv -5(18)$*-t helyettesítünk:*
$-5x \equiv 12(18)$, *majd szorzunk* (-1)*-gyel, mert nem szeretjük a negatív együtthatót.*
$5x \equiv -12(18)$, *ismét helyettesítünk:*
$5x \equiv 6(18)$ *Most jó lenne* 4*-gyel szorozni, hogy* 2 *legyen az együttható, de ezt nem tehetjük, hisz a* 2 *nem relatív prím* 18*-hoz. Viszont ügyesen észrevesszük, hogy* 7*-tel szorozhatunk:*
$35x \equiv 42(18)$, *és megint helyettesítünk:*
$-x \equiv 6(18)$, *szorzunk* (-1)*-gyel:*
$x \equiv -6 \equiv 12(18)$. *Most már csak a* 36 *modulusra kell áttérni:*
$\underline{\underline{x \equiv 12(36)}}$ *vagy* $\underline{\underline{x \equiv 12 + 18 = 30(36)}}$, *győztünk.*

A fenti, „ügyeskedő” módszer előnye, hogy a segítségével sokszor nagyon gyorsan meg tudunk oldani egy-egy lineáris kongruenciát. Lehetséges azonban olyan példát mutatni, amelyen körülményes próbálkozásokkal tudunk csak célt érni. (Ilyen helyzet adódott a fenti példában a harmadik átalakításnál.) Az alábbiakban bemutatott módszer előnye, hogy mindig működik, és minden kongruencián viszonylag gyorsan végez. A módszer egyesíti magában az Euklideszi algoritmust, és használ egy olyan gondolatot, ami lineáris kongruenciák Gauss-eliminációval történő megoldásakor került elő.

Ha tehát az $ax \equiv b(m)$ kongruenciát szeretnénk megoldani, akkor ezt a kongruenciát egy olyan kongruenciarendszerrel helyettesítjük, amelynek a megoldásai pontosan azok az x-ek lesznek, amelyek az eredeti kongruenciát is megoldják. A rendszer konkrétan két kongruenciából áll: az $ax \equiv b(m)$ kongruencia mellé bevesszük az $mx \equiv 0(m)$ kongruenciát, amit persze minden egész x megold. Ha most ezek után két kongruenciánk van, mondjuk $a_1x \equiv b_1(m)$ és $a_2x \equiv b_2(m)$, ahol mondjuk $a_1 > a_2$, akkor az $a_1x \equiv b_1(m)$ kongruencia helyettesíthető a két kongruencia különbségével, azaz a $(a_1 - a_2)x \equiv b_1 - b_2(m)$ kongruenciával. Világos, hogy ha x megoldása az $a_1x \equiv b_1(m)$ és $a_2x \equiv b_2(m)$ kongruenciáknak, akkor x megoldja az $(a_1-a_2)x \equiv b_1-b_2(m)$ kongruenciát is. Visszafelé, ha x-re teljesülnek az $(a_1-a_2)x \equiv b_1-b_2(m)$ és az $a_2x \equiv b_2(m)$ kongruenciák, akkor ezek összege, azaz $a_1x \equiv b_1(m)$ is igaz rá. Tehát a nagyobb együtthatós kongruencia lecserélése után is pontosan ugyanazon x-ek maradnak a megoldások. Végül, ahogyan az Euklideszi algoritmus esetén is, itt is megtehetjük azt, hogy több lépést egyszerre végzünk el, azaz a kisebb együtthatós kongruenciát annyiszor vonjuk le a nagyobb együtthatósból, hogy az együttható a_2-nél is kisebb legyen. Lássuk az előző példának ezen módszer szerinti megoldását!

4.51. Példa *Megoldandó a*
$62x \equiv 24(36)$ *kongruencia, pontosabban a*
$26x \equiv 24(36)$ $\quad 36x \equiv 0(36)$ *kongruenciarendszer. Az első kongruenciát kivonjuk a másodikból (és felcseréljük a kongruenciák sorrendjét, ahogy a későbbiekben is):*
$10x \equiv 12(36)$ $\quad 26x \equiv 24(36)$. *Az első kongruencia kétszeresét vonjuk ki a másodikból:*
$6x \equiv 0(36)$ $\quad 10x \equiv 12(36)$. *Ismét az első kongruenciát vonjuk ki a másodikból:*
$4x \equiv 12(36)$ $\quad 6x \equiv 0(36)$. *Megint az első kongruenciát vonjuk ki a másodikból:*
$2x \equiv 24(36)$ $\quad 4x \equiv 12(36)$. *Most az első kétszeresét vonjuk ki a másodikból:*
$0x \equiv 0(36)$ $\quad 2x \equiv 24(36)$.
A megoldások tehát mindazon x egész számok lesznek, amelyekre teljesül a $2x \equiv 24(36)$ kongruencia. Mivel x együtthatója nem 1, ezért le kell azzal osztani, tehát a megoldás $x \equiv 12(18)$, avagy 36-os modulussal felírva $\underline{\underline{x \equiv 12(36)}}$ vagy $\underline{\underline{x \equiv 12 + 18 = 30(36)}}$.

5. fejezet

Általános algebra

5.1. Algebrai struktúrák, csoportok

5.1. Definíció *A H* halmazon értelmezett *n*-változós művelet*en egy tetszőleges $f : H^n \to H$ leképezést értünk, azaz minden, H elemeiből képzett rendezett n-eshez (pl. $(h_1, h_2, \ldots, h_n)$-hez) H-nak egy bizonyos elemét (itt $f(h_1, h_2, \ldots, h_n)$-t) rendeljük.*

5.2. Megjegyzés *Rendszerint kétváltozós műveletekkel fogunk foglalkozni. Ilyen esetben a művelet jelét az összeművelt elemek közé (és nem elé) írjuk, azaz nem $+(2, 2)$-ről, hanem $2 + 2$-ről beszélünk. Ez a konvenció a továbbiakban nem fog félreértést okozni.*

5.3. Példa *Kétváltozós művelet pl. a valós számokon az összeadás, szorzás, kivonás. A pozitív számokon az osztás és a hatványozás. Egyváltozós műveletnek tekinthető pl. az ellentett képzése (x-hez $-x$-t rendelünk), a pozitív számokon a reciprok vagy a 18 alapú logaritmus. Nullaváltozós művelet pl. az egészeken az, hogy 5. Háromváltozós művelet a valós számokon ami az x, y, z számokhoz $x(y + z) + \frac{\log(|x^3|+5)}{y^2+3}$-t rendel. Vektortérben a vektorösszeadás kétváltozós művelet, egy vektortér lineáris leképezéseinek kompozíciója (egymásutánja) szintén kétváltozós művelet, utóbbi esetben $Hom(V, V)$ az alaphalmaz. A valós polinomokon kétváltozós művelet az összeadás, ill. a kompozíció (ami itt a behelyettesítés). Egyváltozós művelet a deriválás, vagy a $[0, x]$ intervallumon történő integrálás.*

Nem művelet (ebben az értelemben) a hatványozás a valós számokon, mert $(-1)^{\frac{1}{2}} = \sqrt{-1}$ nem valós szám. Nem művelet a valós számokon az osztás sem, mert a $\frac{0}{0}$ nem valós szám. Azonban mind a hatványozás, mind az osztás művelet a pozitív számokon, hiszen bármely pozitív szám pozitív kitevős hatványa és bármely két pozitív szám hányadosa is egyaránt pozitív szám. Szintén nem művelet a skalárral való szorzás vektortereken, mert a két összeművelendő elem nem azonos halmazból kerül ki.

Egy műveletet meg lehet adni az ú.n. Cayley táblájával is, ami a szorzótábla általánosítása. Ha tehát $\{a, b, c, d, e\}$ az alaphalmaz, akkor a

$\star$	a	b	c	d	e
a	c	c	d	a	b
b	b	a	a	c	e
c	b	d	d	d	d
d	e	e	e	e	c
e	d	e	c	b	a

Cayley tábla szerint $a \star c = d$, és $c \star a = b$ ill. $d \star d = e$ teljesül.

5.4. Definíció *Ha f_i egy, a H halmazon értelmezett n_i-változós művelet minden $i \in I$ esetén, akkor az $\mathcal{S} = \langle H, \{f_i : i \in I\}\rangle$ párt* algebrai struktúrának *mondjuk.*

5.5. Példa *Algebrai struktúra a valós számok halmaza az összeadásra és kivonásra, formálisan $\langle \mathbb{R}, \{+, -\}\rangle$. Szintén algebrai struktúra $\langle \{x \in \mathbb{R} : x > 0\}, \cdot\rangle$, azaz a pozitív számok halmaza a szorzásra, mint kétváltozós műveletre nézve, de algebrai struktúra $\langle \mathbb{R}, +\rangle$ is.*

Az 5.5. Példában szereplő két utolsó algebrai struktúra „lényegében"azonos, u.i. $\log xy = \log x + \log y$, azaz a pozitív számok szorzásra pontosan úgy viselkednek, mint a logaritmusaik az összeadásra. Erről szól a következő definíció.

5.6. Definíció *Az $\mathcal{S} = \langle H, \{f_i : i \in I\}\rangle$ és az $\mathcal{S}' = \langle H', \{f'_i : i \in I\}\rangle$ algebrai struktúrák* izomorfak, *ha az f_i és f'_i műveletek tetszőleges $i \in I$ esetén ugyanannyi (mondjuk n_i) változósak, továbbá létezik egy $\varphi : H \to H'$ bijekció, amire $\varphi(f_i(h_1, h_2, \ldots, h_{n_i}) = f'_i(\varphi(h_1), \varphi(h_2), \ldots, \varphi(n_{n_i}))$ tetszőleges $i \in I$ és $h_1, h_2, \ldots, h_{n_i} \in H$ esetén. (Vagyis a leképezés* művelettartó*: az összeművelt elemek képét úgy kapjuk, hogy összeműveljük a képeket.)*

5.7. Példa *Vektorterek korábban megismert izomorfizmusa egy speciális izomorfia a két összeadásművelettel ellátott algebrai struktúra között. A specialitás abból adódik, hogy a skalárral való szorzásra (ami ugyebár nem* algebrai értelemben vett *művelet) szintén megkívánjuk a „művelettartást".*

5.8. Definíció *Tegyük fel, hogy $\mathcal{S} = \langle H, \{f_i : i \in I\}\rangle$ egy algebrai struktúra, és a $H' \subset H$ halmaz olyan, hogy egyetlen f_i művelet sem vezet ki belőle (azaz $f_i(h_1, h_2, \ldots, h_{n_i}) \in H'$ ha $h_1, h_2, \ldots, h_{n_i} \in H'$). Ekkor az $\mathcal{S}' = \langle H', \{f_i|_{H'} : i \in I\}\rangle$ algebrai struktúrát az $\mathcal{S}$ struktúra* részstruktúrának *nevezzük, és ezt a tényt $\mathcal{S}' \leq \mathcal{S}$-sel jelöljük. ($f_i|_{H'}$ az f_i művelet H'-re megszorított változatát jelenti. A továbbiakban a megszorítás jelölését mellőzzük, ha ez nem okoz féreértést.)*

5.9. Példa $\langle \mathbb{N}, \{+, \cdot\}\rangle \leq \langle \mathbb{R}, \{+, \cdot\}\rangle$. *Ha V vektortér, és U egy altere, akkor $\langle U, +\rangle \leq \langle V, +\rangle$.*

5.10. Megfigyelés *Ha az $\mathcal{S}_j = \langle H_j, \{f_i : i \in I\}\rangle$ struktúra minden $j \in J$-re az $\mathcal{S} = \langle H, \{f_i : i \in I\}\rangle$ struktúra részstruktúrája, akkor a $\bigcap_{j\in J} \mathcal{S}_j := \langle \bigcap_{j\in J} H_j, \{f_i : i \in I\}\rangle$ metszetstruktúra is részstruktúrája az $\mathcal{S}$ algebrai struktúrának.*

Bizonyítás. Csak azt kell ellenőrizni, hogy az f_i-k megszorításai műveletek, azaz nem vezetnek ki a metszetből. Ám mivel egyik H_j-ből sem vezetnek ki, azért a metszetből sem. □

5.11. Definíció *Legyen $\mathcal{S} := \langle H, \{f_i : i \in I\}\rangle$ egy algebrai struktúra, és a $K \subset H$. A K által generált* $\langle K\rangle$ részstruktúra *a legszűkebb olyan részstruktúrája $\mathcal{S}$-nek, ami K-t tartalmazza, azaz* $\langle K\rangle := \bigcap_{K\subset\mathcal{S}'\leq\mathcal{S}} \mathcal{S}'$.

A továbbiakban speciális algebrai struktúrákat fogunk tanulmányozni. A számunkra érdekes struktúrák egytől egyig olyanok, amelyeken a lényeges művelet kétváltozós. A félcsoportokon és csoportokon egy, míg a gyűrűkön és testeken két műveletet lesz értelmezve. enumerate

5.1.1. Félcsoportok és csoportok

Láttuk, hogy a műveletekre az egyetlen lényegi megkötés, hogy ne vezessenek ki az adott struktúrából, így aztán az ezekkel kapott algebrai struktúrák annyira általánosak, nem is várható, hogy jól használható, mély tételeket kapjunk. Célszerű tehát további megkötéseket tenni a vizsgált struktúrákra. Erre a legtermészetesebb mód, hogy a műveletektől különböző tulajdonságokat várunk el.

5.12. Definíció *A H halmazon értelmezett, 2-változós $\star$ művelet* asszociatív *(magyarul* átzárójelezhető*), ha tetszőleges $x, y, z \in H$ elemekre $x\star(y\star z) = (x\star y)\star z$ áll. A $\star$ művelet* kommutatív *(magyarul* felcserélhető*), ha tetszőleges $x, y \in H$ elemekre $x \star y = y \star x$ teljesül.*

5.13. Példa *1. A valós számokon értelmezett + művelet asszociatív és kommutatív,*

2. *a pozitív számokon értelmezett hatványozás nem asszociatív és nem kommutatív (hisz $2^{(2^3)} = 256 \neq 64 = (2^2)^3$ ill. $2^3 = 8 \neq 9 = 3^2$),*

3. *az $\mathbb{R} \to \mathbb{R}$ függvények kompozíciója (azaz egymásba helyettesítése) asszociatív művelet, ám nem kommutatív (hisz $[(p \circ q) \circ r](x) = p(q(r(x))) = [p \circ (q \circ r)](x)$ de általában $(p\circ q)(x) = p(q(x)) \neq q(p(x)) = (q\circ p)(x)$, pl ha $p(x) = 2x$ és $q(x) = x+1$, akkor $(p \circ q)(x) = 2(x + 1) = 2x + 2 \neq 2x + 1 = (q \circ p)(x)$.*

4. *míg a valós számokon értelmezett számtani közép művelet kommutatív, de nem asszociatív (hisz $a\star b := \frac{a+b}{2} = \frac{b+a}{2} = b\star a$, de pl $(0\star0)\star1 = 0,5 \neq 0,25 = 0\star(0\star1)$).*

5.14. Definíció *Az $\mathcal{S} = \langle H, \star\rangle$ struktúra* félcsoport*, ha $\star$ a H-n asszociatív. Ha $\star$ kommutatív is, akkor $\mathcal{S}$* Abel félcsoport*.*

5.15. Példa *Az $n\times n$-es mátrixok a szorzásra félcsoportot alkotnak. Az $n\times n$-es, szimmetrikus mátrixok e félcsoportnak egy Abel részfélcsoportját alkotják.*

5.16. Definíció *Legyen $\star$ kétváltozós művelet H-n. Az $e \in H$ elem az $\star$ művelet* egységeleme*, ha $e \star h = h \star e = h$ a H tetszőleges h elemére.*

5.17. Megfigyelés *Ha az $\mathcal{S}$ struktúra $\star$ műveletének van egységeleme, akkor egyetlen egységeleme van.*

Bizonyítás. Tegyük fel, hogy $e, e' \in H$ egyaránt egységelemek, ekkor $e = e \star e' = e'$. $\square$

5.18. Definíció *Ha az $\mathcal{S} = (H, \star)$ struktúrában $e \in H$ a $\star$ művelet egységeleme, és $h \star h' = h' \star h = e$, akkor az mondjuk, hogy h' a h* inverze *a $\star$ műveletre. (Egyúttal h a h' inverze $\star$-ra nézve.)*

5.19. Példa *A $\langle \mathbb{R}, \{+, \cdot\} \rangle$ struktúrában az összeadás egységeleme a 0, az x elem inverze $-x$. A szorzás egységeleme az 1, az $x \neq 0$ elem inverze az $\frac{1}{x}$.*

5.20. Definíció *A $\mathcal{S} = \langle G, \cdot \rangle$ struktúra* csoport, *ha (1) $\mathcal{S}$ félcsoport, (2) a $\cdot$ műveletnek létezik egységeleme, és (3) minden $g \in G$ elemnek létezik inverze a $\cdot$ műveletre.*

5.21. Megjegyzés *Ha a csoportműveletet $\cdot$ jelöli, és a csoport megadásakor ennek elhagyása nem okoz félreértést, akkor a fenti csoportot egyszerűen G-vel jelöljük. Ha nem okoz félreértést, akkor a $\cdot$ műveleti jelet a műveleteknél sem írjuk ki, így pl. a gh jelentése a g és h összeműveléséne (összeszorzásának) eredménye, azaz $g \cdot h$. A csoportban ezen konvenció értelmében beszélhetünk hatványozásról: egy g elem n-dik hatványa nem más, mint az elemet n-szer összeszorozzuk (egészen pontosan összeműveljük) önmagával. A 0-dik hatványt az egységelemként definiáljuk, a $(-n)$-dik hatvány pedig a g^{-1} inverzelem n-dik hatványa. A G csoport* rendje $|G|$. *A G csoport* Abel csoport, *ha G csoportművelete kommutatív.*

5.22. Példa

1. *$\langle \mathbb{R}, + \rangle, \langle \mathbb{Z}, + \rangle, \langle \mathbb{R} \setminus \{0\}, \cdot \rangle, \langle \mathbb{R}^{n \times k}, + \rangle$ Abel csoportok, ahol $\mathbb{R}^{n \times k}$ jelöli az $n \times k$ méretű valós mátrixokok halmazát. Ha $\mathbb{Z}_n$ jelöli a modulo n maradékosztályok halmazát, akkor $\mathbb{Z}_n$ a $+_n$-ra (modulo n összeadásra) csoportot alkot. Az egységelem a 0 maradékosztály. Ennek a csoportnak az elemei nem számok, hanem maradékosztályok, azaz végtelen számhalmazok. Két ilyen maradékosztály összege egy újabb maradékosztály lesz. Akinek ez szokatlan, az gondoltat a $\langle \mathbb{Z}_n, + \rangle$ csoportra úgy is, mint $\langle \{0, 1, 2, \ldots, n-1\}, +_n \rangle$, ahol az alaphalmazt n szám (egy mod n TMR) alkotja, $+_n$ pedig a modulo n összeadás: ha az alaphalmazból két szám hagyományos összege nem szerepel az alaphalmazban, akkor a hagyományos összeg helyett vesszük az alaphalmazból az összeggel modulo n kongruens reprezentánst.*

2. *A $\mathbb{Z}_n$ halmazon a modulo n szorzás is egy asszociatív művelet, ráádásul az 1 maradékosztály egységelem erre a műveletre. De pl. a 0 maradékosztálynak nincs iverze, így a $\langle \mathbb{Z}_n, \cdot \rangle$ nem csoport, csak egységelemes félcsoport. Ha azonban $\mathbb{Z}_n^*$ jelöli az n-hez prím maradékosztályok halmazát, akkor belátható, hogy $\mathbb{Z}_n^*$ zárt a szorzásra, és ebben a struktúrában nemcsak egységelem van, de minden elemnek inverze is: az a szám maradékosztályának inverze az Euler-Fermat tétel miatt éppen*

az $a^{\varphi(n)-1}$ szám maradékosztálya lesz. A $\langle Z_n^*, \cdot \rangle$ tehát (Abel) egy $\varphi(n)$ rendű csoport. Hasonlóan az előző példához, erre a csoportra is gondolhatunk úgy, hogy elemei az n-hez relatív prím, n-nél kisebb pozitív egészek, a művelet pedig $\cdot_n$, azaz a modulo n szorzás.

3. *A legváratlanabb helyzetekben bukkanhatnak fel egészen furcsa csoportok. A Nim összeadást például úgy értelmezzük a nemnegatív egészeken, hogy azokat kettes számrendszerben felírva adjuk össze, de nem törődünk az egyes helyiértékeken adódó maradékokkal. Más szóval, a számokat a kettes számrendszerbeli alakjuk szerint 0/1-vektoroknak tekintjük, amelyeket koordinátánként összeXOR-ozunk. Tehát például $19 \oplus 6 = 21$, hiszen $10011_2 XOR 00110_2 = 10101_2$. Können látható, hogy a Nim összeadás asszociatív és kommutatív, egységeleme a 0, és minden pozitív egésznek van inverze (azaz Nim-ellentettje), mégpedig önmaga. További érdekes tulajdonság, hogy tetszőlege a, b pozitív egészekre $0 \leq a \oplus b \leq a + b$ teljesül.*

   Miért érdemes jól begyakorolni egy ilyen természetellenes művelet elvégzését? Kétségkívül az SzA ill. BSz tárgyakból tanultak legfontosabb alkalmazási területéhez érkeztünk. Legtöbbünk életében elkövetkezik az a pillanat, amikor rábízzák a hiperaktív unokaöccsét: kezdjen vele valamit, mialatt a szülei revitalizálják a házasságukat. Tapasztaltabbak tudják, hogy ilyenkor a veszteség minimalizálása a cél, amit úgy lehet elérni, ha le tudjuk kötni valami számára is érdekessel a kis gengszterfiókát. Ha már ígértünk neki csokit a K_5 síkbarajzolásáért és eleget próbálkozott egy vonallal lerajzolni a $K_{5,3}$-at, akkor áttérhetünk vele a Nim játékra, amiben verhetetlenek leszünk, ha gyorsan tudunk Nim összeadni.

   A Nim (kínaiul csien-szü-dzü) játék tehát a következő: adott k kupac, amelyek rendre $a_1, a_2, \ldots, a_k$ kavicsot tartalmaznak. (Színes lego kockával játszva még csak szét se kell válogatni a kupacokat, az a játék végére automatikusan megtörténik, és két legyet ütünk egy csapásra.) Két játékos játszik, felváltva lépnek. Egy lépésben a soron következő játékos egy neki tetsző kupacból elvesz tetszőleges számú kavicsot, de legalább egyet. Az győz, aki az utolsó kavicsot veszi el.

   Két kupaccal játszva még egy óvodást is betaníthatunk a nyerésre. Ha ugyanis a két kupac mérete nem egyezik meg, akkor a soron következő játékos nyerő lépése az, ha a nagyobb kupacból elvéve két egyforma méretű kupacot képez, míg egyforma kupacok esetén a soron következő nem nyerhet, amennyiben az ellenfele így játszik. (Ha az unokaöcsénk magától rájön erre, bátran javasoljuk neki a BME Villanykart.) Nem világos azonban, hogyan is érdemes kettőnél több kupac esetén játszani. Hasznos megfigyelés például, hogy ha van két egyforma méretű kupac, akkor azokat el is felejthetjük, mert ha az ellenfél az egyikből vesz el, úgy a másikon mi is ugyanazt a lépést végezzük, ha pedig más kupachoz nyúl, akkor a mi is a maradék kupacokon lépünk.

   A titok nyitja, hogy a Nim játék akkor nyerhető meg bizonyosan, ha a kupacokban

lévő kavicsok számának Nim összege $a_1 \oplus a_2 \oplus \ldots \oplus a_k \neq 0$. *Ekkor (bár korántsem triviális, de igaz, hogy) valamelyik kupacból el tudunk venni néhány kavicsot úgy, hogy kapott kupacok méretének Nim összege pontosan* 0 *legyen. (A legnagyobb olyan helyiértéket kell nézni kettes számrendszerben, ahol páratlan sok* a_i *felírásában áll egyes, és egy olyan* a_i*-hez kell nyúlni, amiben ezen a helyiértéken egyes áll.) Márpedig ha mindig* 0 *Nim-összegű kupacrendszeren kényszerül lépni az ellenfél, akkor az ő lépése után sosem lesz* 0 *a kupacok Nim összege. Vagyis mi mindig tudni fogunk lépni, és persze úgy, hogy ismét* 0 *legyen a Nim összeg. Veszteni tehát nem tudunk, ezért muszáj nyernünk, ha így játszunk.*

Sajnos a fent leírt módszer nehezen általánosítható: a dögös nők rendszerint nem esnek hasra a mégoly meggyőző Nim tudásunktól sem, a legtöbb férfit pedig –valljuk be– frusztrálja, ha egy nő az eszével győzi le őt. Mindenképp érdemes tehát valami olyan nem hétköznapi tevékenységben is jártasságot szereznünk, amivel a remélt célközönséget lenyűgözhetjük. A skála a kerékpárszereléstől a társastáncon át a celebek magánéletének kulisszatitkai beható ismeretéig terjed, ki-ki egyéni ízlésétől függően. (Matematikai szempontból természetesen pazarul általánosítható a fenti módszer: a Grundy számokra érdemes ráguglizni.)

5.23. Megfigyelés *Ha* G *csoport, akkor* G *minden elemének egyértelmű inverze van.*

Bizonyítás. Ha x és y a g inverzei és e a G egységeleme, akkor $x = xe = x(gy) = (xg)y = ey = y$. □

A Cayley tábla segíthet az adott algebrai struktúra csoport voltának eldöntésében. Bár az asszociativitás nem látszik közvetlenül a Cayley táblából, a kommutativitás pontosan a tábla (mint mátrix) szimmetrikus voltát jelenti. Az egységelem létezése pedig olyan (egymásnak megfelelő) sort és oszlopot jelent, amelyekben a pontosan az adott sorhoz ill. oszlophoz tartozó alaphalmazelemek szerepelnek. Könnyen ellenőrizhető ezen kívül, hogy a $\star$ művelet pontosan akkor határoz meg csoportot, ha $\star$ asszociatív és a Cayley tábla minden sorában és minden oszlopában az alaphalmaz elemeinek egy permutációja szerepel. Az utóbbi feltétel úgy is megfogalmazható (ami a csoportoknak egy másik fontos tulajdonságára mutat rá), hogy az alaphalmaz tetszőleges a, b elemire mind az $a \star x = b$, mind az $x \star a = b$ egyenletek egyértelműen oldhatók meg.

5.24. Példa *Láttuk, hogy* $\mathbb{R}$ *Abel csoport az összeadásra, és könnyen látható, hogy a pozitív valósak Abel csoportot alkotnak a szorzásra nézve. (Utóbbi esetben egységelem az* 1*, inverz a reciprok.) Érdemes azt is látni, hogy ez a két csoport lényegében ugyanaz: a (mondjuk* 2 *alapú)* log *függvény olyan bijekciót létesít a pozitív és a valós számok között, ahol a szorzásból összeadás lesz:* $\log(a \cdot b) = \log(a) + \log(b)$. *Csoportoknak az ilyesfajta azonosságáról szól az alábbi definíció.*

5.25. Definíció *(1) Két csoport (mondjuk G és H)* izomorf*, ha van köztük művelettartó bijekció, azaz létezik egy $\phi : G \to H$ bijekció, amire tetszőleges $g, g' \in G$ esetén $\phi(g \cdot g') = \phi(g) \cdot \phi(g')$ áll. (Figyeljük meg, hogy a baloldali szorzás a G, a jobboldali pedig a H művelete.)*

(2) A G csoport H részhalmaza a G részcsoport*ja (jelölése $H \leq G$), ha H maga is csoport a G csoportműveletére.*

5.26. Megfigyelés *Tetszőleges G csoport részcsoportjainak metszete is G részcsoportja.*

5.27. Definíció *Tetszőleges $K \subseteq G$ által* generált $\langle K \rangle$ csoport *a G csoport K-t tartalmazó részcsoportjainak metszete.*

5.28. Megfigyelés *Ha G csoport, akkor tetszőleges $K \subset G$ esetén $\langle K \rangle$ a G csoport egy részcsoportja.*

5.1.2. Ciklikus csoportok

5.29. Definíció *Az olyan csoportot, amit valamely eleme generál,* ciklikus csoport*nak nevezzük.*

A G csoport g elemének rendje *a g által generált $\langle g \rangle$ részcsoport elemszáma.*

Az elem rendjének definíciója úgy is kimondható, hogy a g elem rendje az a legkisebb n szám, amire $g^n = e$. Ha ugyanis létezik ilyen n, akkor, $g^{-1} = g^{n-1}$, és a $g, g^2, g^3, \ldots, g^n$ elemek különbözők (hisz ha $g^i = g^j$, akkor $g^{i-j} = e$), ezért $\langle g \rangle$ n-elemű. Ha pedig nem létezik ilyen n, akkor a $g, g^2, g^3, \ldots$ elemek mind különbözők, ezért $\langle g \rangle$ végtelen.

Ha az $\langle G, \cdot \rangle$ ciklikus csoport $g \in G$ generálja, akkor G minden eleme előáll $g^i (= g \cdot g \cdot \ldots \cdot g$ [i-szer]) alakban, ahol $i \in \mathbb{Z}$. Ha G rendje véges, akkor elegendő a pozitív i kitevőkre szorítkozni. Ha G végtelen, akkor a generátorelemnek semelyik hatványa sem egységelem, mert egyébként a generátorelem csak véges sok elemet generálna.

Hányfélék lehetnek a ciklikus csoportok, azaz izomorfia erejéig hogy néznek ki a ciklikus csoportok? Nyilvánvaló, hogy ha két ciklikus csoport rendje különböző, akkor nem izomorfak. Ha azonban $|G| = |H| = n$ a G és H ciklikus csoportra, akkor $G \cong H$. Legyen ugyanis g ill. h a G ill H generátoreleme. Ekkor g^n ill. h^n a G ill. H egységeleme, a két csoport minden eleme g^i ill. h^i alakú, és könnyen látható, hogy $\varphi(g^i) := h^i$ izomorfizmus. Tehát a véges ciklikus csoportot az elemszáma izomorfia erejéig meghatározza. Az n-elemű ciklikus csoportot C_n jelöli, és könnyen látható, hogy $C_n \cong \mathbb{Z}_n$, ahol $\mathbb{Z}_n$ a $\langle \mathbb{Z}_n, + \rangle$ csoportot jelöli, ahol $\mathbb{Z}_n$ a modulo n maradékosztályok halmaza. Minden véges ciklikus csoportot leírtunk tehát. Ha G végtelen ciklikus csoport, akkor a g generátorelem semelyik hatványa sem egységelem, mert egyébként g véges csoportot generálna. Mivel a g által generált e, g^i, g^{-i} elemek részcsoportot alkotnak (e az egységelem), ezért g éppen ezt a részcsoportot generálja, így ez a részcsoport maga a csoport. Azt kaptuk tehát, hogy minden végtelen, ciklikus csoport a $\langle \mathbb{Z}, + \rangle$ csoporttal izomorf.

5.30. Tétel *Ciklikus csoport minden részcsoportja ciklikus.*

Bizonyítás. Legyen a G ciklikus csoport egy generátoreleme g, és legyen $H \leq G$ részcsoport. Tekintsük a minimális $0 < k$-t, amire $g^k \in H$ (ilyen létezik, ha H nem a triviális, egyelemű csoport (ami persze ciklikus)). Megmutatjuk, hogy g^k generálja H-t, amiből azonnal adódik, hogy H ciklikus. Nyilván g^k generálja az e, g^{ik}, g^{-ik} elemeket tetszőleges pozitív egész i esetén. Tegyük fel, hogy a H részcsoport g^l elemét g^k nem generálja, azaz $k \nmid l$. Osszuk el l-t k-val maradékosan, azaz $l = ak + r$, ahol $1 \leq r < k$. Mivel $g^k, g^l \in H$, ezért $g^l \cdot ((g^k)^{-1})^a = g^{ak+r} \cdot g^{-ak} = g^{ak+r-ak} = g^r \in H$, ami ellentmond k választásának. Tehát H-t g^k csakugyan generálja, vagyis H valóban ciklikus. □

5.1.3. Diédercsoportok

Fontos példák csoportokra a szimmetriák alkotta csoportok. Legyen X egy halmaz, és tekintsük $f : X \to X$ bijekcióknak egy olyan $\mathcal{F}$ nemüres halmazát, ami zárt a kompzícióra, vagyis $f, g \in \mathcal{F}$ esetén $f \circ g \in \mathcal{F}$, ahol $f \circ g(x) := f(g(x))$ $\forall x \in X$, továbbá, minden $f \in \mathcal{F}$ bijekció f^{-1} inverze is $\mathcal{F}$-ben van. A függvénykompozíció művelet definíció szerint asszociatív. A fenti választás éppen azt a célt szolgálta, hogy legyen egység és inverz, így e miatt $\langle \mathcal{F}, \circ \rangle$ csoport. A csoport egységeleme az id identikus (azaz a minden pontot helybenhagyó) leképezés (ez azért $\mathcal{F}$-beli, mert $id = f \circ f^{-1}$ tetszőleges $f \in \mathcal{F}$-re), a kompozícióra vonatkozó inverz az adott függvény inverze lesz, a kompozícióművelet asszociativitása pedig közvetlenül adódik a definícióból.

Az egyik legfontosabb példa a fenti szimmetriacsoportra a D_n *diédercsoport*, amikoris X a sík egy szabályos, n oldalú sokszöge, a D_n csoport elemei az X egybevágóságai (azaz a sík mindazon egybevágóságai, amelyek az X sokszöget (mint halmazt) fixen hagyják), a csoportművelet pedig az egybevágóságok egymás utáni elvégzése.

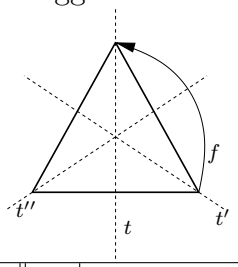
Van ám itt egy bosszantó konvenció. Nevezetesen, hogy az egybevágóságok voltaképpen függvények, márpedig egy függvény felírásakor az argumentumot a függvény jele *után* írjuk (zárójelek között): $f(x)$ módon. A függvénykompozíció definíciója szerint az $f \circ g$ függvény egy x értékhez az $(f \circ g)(x) := f(g(x))$ értéket rendeli. Ott okoz ez zavart, hogy ha csak az $f \circ g$ kifejezést látjuk, azt gondolhatnánk, hogy *először* kell az f-t és csak *utána* a g függvényt alkalmazni. Láttuk, hogy ennek épp a fordítottja igaz. A lényeg tehát, hogy a $\circ$ kompozícióműveletnél jobbról balra haladva kell a függvényeket sorban kiértékelni, ha minket a kompozíciófüggvény konkrét jelentése érdekel. Számolni a kompozícióval, mint művelettel azonban hajszálpontosan úgy kell, mint bármely más művelettel.

Az egyik ilyen egybevágóság a sokszög középpontja körüli $\frac{2\pi}{n}$-szögű f forgatás, egy másik lehetséges egybevágóság a sokszög egy szimmetriatengelyére való t tükrözés. Lényeges tulajdonsága a diédercsoportnak, hogy $n > 2$-re nem kommutatív (u.i. $t \circ f \neq f \circ t$). Az f és t szimmetriák a sokszög minden szimmetriáját generálják, hiszen a körüljárástaró egybevágóságok középpont körüli forgatások, a körüljárásváltók pedig úgy kaphatók, hogy először tükrözünk, majd forgatunk. A D_n diédercsoportnak tehát $2n$ eleme van.

A $t \circ t = id$, $f^n = f \circ f \circ \ldots \circ f[n\text{-szer}] = id$ ill. $f \circ t = t \circ f^{n-1}$ azonosságok teljesülése egyszerűen ellenőrizhető. Ebből az látszik, hogy D_n minden eleme vagy f^k, vagy $t \circ f^k$ alakú valamely $0 \leq k < n$-re: ha ugyanis f és t is szerepel a kompzícióban, akkor a t-ket baloldalra csoportosíthatjuk a harmadik azonosság miatt. Lássuk a D_3 diédercsoport példáján, hogy néz ez ki a gyakorlatban!

A szabályos háromszögnek t, t' és t'' jelöli a három szimmetriatengelyét, ill. f a középpontja körüli $\frac{2\pi}{3}$ szögű forgatást (az ábrán látható módon). Tudjuk, hogy $t^2 = id = f^3$, továbbá könnyen ellenőrizhető, hogy $f \circ t = t \circ f^2 = t'$, és ebből következően $f^2 \circ t = f \circ (f \circ t) = f \circ (t \circ f^2) = (f \circ t) \circ f^2 = (t \circ f^2) \circ f^2 = t \circ f^4 = t \circ f = t''$ áll. Tehát

a D_3 diédercsoport hat egybevágósága az $id, f, f^2, t, t' = t \circ f^2$ és a $t'' = t \circ f$. Ezen összefüggések felhasználásával megkapható a D_3 csoport szorzótáblája is.



	id	f	f^2	t	$t' = t \circ f^2$	$t'' = t \circ f$
id	id	f	f^2	t	$t \circ f^2 = t'$	$t \circ f = t''$
f	f	f^2	id	$f \circ t = t'$	$f \circ t' = f \circ (t \circ f^2) = t''$	$f \circ t'' = f \circ (t \circ f) = t$
f^2	f^2	id	f	$f^2 \circ t = t''$	$f^2 \circ t' = f^2 \circ (t \circ f^2) = t$	$f^2 \circ t'' = f^2 \circ (t \circ f) = t'$
t	t	$t \circ f = t''$	$t \circ f^2 = t'$	$t \circ t = id$	$t \circ t' = t \circ (t \circ f^2) = f^2$	$t \circ t'' = t \circ (t \circ f) = f$
t'	t'	$t' \circ f =$ $(t \circ f^2) \circ f = t$	$t' \circ f^2 = t' \circ f^2 =$ $(t \circ f^2) \circ f^2 = t''$	$t' \circ t =$ $(t \circ f^2) \circ t = f$	$t' \circ t' = id$	$t' \circ t'' =$ $(t \circ f^2) \circ (t \circ f) = f^2$
t''	t''	$t'' \circ f =$ $(t \circ f) \circ f = t'$	$t'' \circ f^2 =$ $(t \circ f) \circ f^2 = t$	$t'' \circ t =$ $(t \circ f) \circ t = f^2$	$t'' \circ t' =$ $(t \circ f) \circ (t \circ f^2) = f$	$t'' \circ t'' = id$

Érdemes megfigyelni, hogy a forgatások (f hatványai) a D_n egy ciklikus részcsoportját alkotják.

5.1.4. Permutációcsoportok

Korábban már vizsgáltuk n elem lehetséges permutációinak számát; most a permutációk csoportstruktúráját vesszük szemügyre. Világos, hogy az $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ bijekciók zártak a kompozícióra és az inverzképzésre, ezért az $\{1, 2, \ldots, n\}$ halmaz permutációi szimmetriacsoportot alkotnak a kompozícióra.

5.31. Definíció *Az S_n* szimmetrikus csoport *$\{1, 2, \ldots, n\}$ halmaz permutációi alkotta csoport a függvénykompozíció műveletre nézve.*

5.32. Példa *Érdemes megnézni, hogyan hat konkrétan a függvénykompozíció a permutációkon. Egy π permutációt úgy adunk meg, hogy 1-től n-ig minden i-re meghatározzuk (mondjuk egy táblázattal megadva) $\pi(i)$ értékét. Emlékeztetünk, hogy a $\pi \circ \sigma$ permutáció kiszámításakor először alkalmazzuk a σ permutációt, és aztán a π-t. Konkrétan, ha például*

$$\pi = \begin{array}{|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 \\ \hline 2 & 4 & 3 & 1 & 5 \\ \hline \end{array} \quad \text{és } \sigma = \begin{array}{|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 \\ \hline 3 & 2 & 1 & 5 & 4 \\ \hline \end{array} \text{ akkor } \pi \circ \sigma = \begin{array}{|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 \\ \hline 3 & 4 & 2 & 5 & 1 \\ \hline \end{array} \text{ adódik.}$$

Annak igazolásához, hogy a permutációkon a kompozíció csakugyan csoportot határoz meg, csupán annyit kell látni, hogy a kompozíció, mint kétváltozós művelet asszociatív (ez világos), létezik egységelem (az identikus (mindent helybenhagyó) leképezés egy permutáció, és ezzel akár jobbról, akár balról komponálunk, egységként viselkedik), ill., hogy

minden π permutációnak létezik egy π^{-1} inverze, amire $\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = id$, de az inverzleképezés (ami szintén permutáció) látnivalóan rendelkezik ezzel a tulajdonsággal.

A diédercsoportok után tehát a szimmetrikus csoport a második fontos példa a szimmetriacsoportra. Korábbi tanulmányainkat kamatoztatandó megfigyelhetjük, hogy az S_n szimmetrikus csoport rendje az $\{1, 2, \ldots, n\}$ permutációinak száma, vagyis $n!$. Láttuk, hogy a diédercsoport sem volt kommutatív, és mivel a D_n diédercsoport tekinthető a szabályos n-szög *csúcsain* ható permutációk egy halmazának, ezért $D_n \leq S_n$, így aztán S_n sem kommutatív $n > 2$-re.

Következő célunk a permutációk hatványait megvizsgálni, hogy konkrét permutációk rendjét meghatározhassuk. Legyen $i \in \{1, 2, \ldots, n\}$, $\sigma \in S_n$, és tekintsük az $i, \sigma(i), \sigma^2(i), \sigma^3(i), \ldots$ elemeket. Ezek az elemek (tehát azok, melyekbe a σ permutáció i-t elviszi) az i σ szerinti *orbitját* alkotják. σ bijektívitása miatt az orbitot alkotó sorozatban az elemek ciklikusan ismétlődnek, azaz $\sigma^{j+k}(i) = \sigma^j(i)$, ahol k az orbit mérete. Ha tehát leírjuk az $(i, \sigma(i), \sigma^2(i), \sigma^3(i), \ldots \sigma^{k-1}(i))$ elemeket, akkor i orbitjának minden egyes eleméről látjuk, hogy a σ a felsorolás következő elemébe viszi (az utolsót az elsőbe). Az fenti ciklikus sorrend a σ permutáció egy *ciklusa*. Mivel két elem orbitja vagy diszjunkt, vagy azonos, ezért igaz az alábbi megfigyelés.

5.33. Tétel *Minden permutáció felírható diszjunkt ciklusok szorzataként.*□

A gyakorlatban is alkalmazzuk ezt a felírást, azaz ahelyett, hogy a σ permutációt az értelmezési tartomány minden elemén megadnánk, csupán egymás mellé írjuk a ciklusokat, amelyek közül (ha n ismert) az egypontúakat (vagyis a fix pontokat) kihagyjuk. Így pl a fenti példában szereplő permutációk felírása $\pi = (124)$ ill. $\sigma = (13)(45)$ lenne. *Ciklikus permutáció*nak nevezünk egy permutációt, ha pontosan egy ciklusa van. Ha a σ permutációt hatványozzuk, akkor az elemek a ciklusukon belül mozognak, mégpedig minden elem kitevőnyit lép jobbra. Ebből látszik, hogyan lehet meghatározni σ legkisebb hatványát, ami minden elemet helyben hagy, vagyis azt a legisebb k kitevőt, amire $\sigma^k = id$ az egységelem.

5.34. Tétel *Ha σ ciklusai $k_1, k_2, \ldots, k_l$ méretűek, akkor σ rendje a $k_1, k_2, \ldots k_l$ számok legkisebb közös többszöröse.*□

*Transzpozíció*nak nevezzük az olyan permutációt, aminek a fix pontjain kívül egyetlen kételemű ciklusa van, azaz a permutáció két elemet felcserél, a többit fixen hagyja.

5.35. Állítás *A tranzpozíciók generálják az S_n szimmetrikus csoportot.*

Bizonyítás. Minden permutáció diszjunkt ciklusok szorzata, ezért elegendő megmutatni, hogy bármely ciklus előáll olyan transzpozíciók szorzataként, amelyek csak a ciklus elemeit használják. Mivel az $(i_1, i_2, \ldots, i_k)$ ciklikus permutáció a $(i_1, i_k), (i_1, i_{k-1}), \ldots, (i_1, i_2)$ transzpozíciók szorzata, ezért az állítást igazoltuk. □

Értelmes kérdés, hogy legalább hány transzpozíció kell S_n generálásához. Minden transzpozíciónak megfelel egy él az $\{1, 2, \ldots, n\}$ ponthalmazon. Transzpozíciók egy halmazának tehát egy n-pontú gráf felel meg. Világos, hogy ha egy ilyen gráf nem összefüggő, akkor a szóbanforgó transzpozíciók nem generálják S_n-t, sőt: általában nem generálnak egyetlen olyan permutációt sem, ami a komponensek között (is) hat. Tehát minden, transzpozíciókból álló generátorrendszernek összefüggő gráf felel meg, vagyis legalább $n-1$ transzpozíció kell S_n generálásához. Ennyi egyébként elegendő is: az $(1, 2), (1, 3), \ldots, (1, n)$ transzpozíciók alkalmas kompozíciójával tetszőleges S_n-beli permutáció előállítható. Ennek belátásához elegendő azt megmutatni, hogy a fenti $n-1$ transzpozíció segítségével minden más transzpozíció előáll, hisz azok már –mint láttuk– minden permutációt generálnak. Konkrétan az (i, j) transzpozíció egy lehetséges előállítása $(i, j) = (1, j) \circ (1, i) \circ (1, j)$.

5.36. Definíció *Az S_n szimmetrikus csoport részcsoportjait* permutációcsoportnak *nevezzük.*

Hányfélék lehetnek a permutációcsoportok? A válasz, hogy a permutációcsoportok (izomorfia erejéig) minden (véges) csoportot felölelnek.

Cayley tétel: Minden véges G csoport izomorf egy alkalmas permutációcsoporttal.

Bizonyítás. Az általánosság megszorítása nélkül feltehető, hogy G n-edrendű, és G elemei az $1, 2, \ldots, n$ számok. Ekkor G minden g elemének megfeleltethető egy σ_g permutáció az alábbiak szerint: $\sigma_g(i) := g{\cdot}i$. Ellenőrizzük, hogy a megfeleltetés művelettartó: $\sigma_{gh} = \sigma_g \circ \sigma_h$. Csakugyan, tetszőleges $i \in \{1, 2, \ldots, n\}$ esetén $\sigma_{gh}(i) = (gh)i = g(hi) = g(\sigma_h(i)) = \sigma_g(\sigma_h(i)) = \sigma_g \circ \sigma_h(i)$. Az kell még, hogy a $g \mapsto \sigma_g$ leképezés injektív, azaz $g \neq h$ esetén $\sigma_g \neq \sigma_h$. De ez is igaz, mivel $\sigma_g(e) = ge = g \neq h = he = \sigma_h(e)$. Tehát a $\{\sigma_g : g \in G\}$ permutációk az S_n szimmetrikus csoport egy G-vel izomorf részcsoportját alkotják. □

Könnyen ellenőrizhető, hogy páros permutációk szorzata is páros permutáció, páros permutáció és páratlan permutáció szorzata páratlan permutáció, továbbá, hogy két páratlan permutáció szorzata pedig páros permutáció. Ez azt jelenti, hogy a páros permutációk az S_n szimmetrikus csoportnak egy részcsoportját alkotják. E részcsoport az A_n-nel jelölt *alternáló csoport*, rendje S_n rendjének fele, azaz $\frac{n!}{2}$.

5.1.5. A kvaterniócsoport

A Q kvaterniócsoport elemei $1,\ -1,\ i, -i\ , j\ , -j\ , k\ , -k$, a szorzásműveletet definiálják (az asszociativitáson túl) az $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $(-1)^2 = 1$, $(-1)x = -x = x(-1)$, $-(-x) = x$, ill. az $1x = x1 = x$ $(\forall x \in Q)$ azonosságok. Pl. $ji = j(jk) = j^2k = (-1)k = -k$. (A csoport-tulajdonság igazolásához az asszociativitást valóban ellenőrizni kell (kicsit fáradságos), egységelem az 1, a -1 inverze önmaga, a többi elem inverze a saját ellentettje.

Mivel $ij \neq ji$, ezért Q nem Abel csoport, így nem is ciklikus. Nem izomorf Q az ugyancsak 8-adrendű D_4 diédercsoporttal sem, mert Q-ban 1 rendje 1, -1 rendje 2, a többi elemé pedig 4, míg D_4-ben id rendje 1, minden tengelyes tükrözés $(t, f \circ t, f^2 \circ t, f^3 \circ t)$ és a középpontos tükrözés (f^2) rendje 2, míg a forgatások (f, f^3) rendje 4. A Q kvaterniócsoport tehát különbözik az eddig megismert összes csoporttól.

5.1.6. A csoportelmélet alapjai

Ebben a részben véges csoportokkal foglalkozunk.

5.37. Definíció *A G csoport K és H részhalmazainak* komplexusszorzatán

$$HK := \{hk : h \in H, k \in K\} \subseteq G$$

halmazt értjük. Ha $H \leq G$ és $g \in G$, akkor a gH (Hg) komplexusszorzat a H részcsoport baloldali (jobboldali) mellékosztálya. *Ha $a \in gH$ $(a \in Hg)$, akkor a-t a gH (Hg) mellékosztály* reprezentánsának *nevezzük.*

5.38. Példa *Tetszőleges $n > 1$ pozitív egész esetén $H = \langle n\mathbb{Z}, + \rangle \leq \langle \mathbb{Z}, + \rangle = G$, ahol $n\mathbb{Z} := \{nz : z \in \mathbb{Z}\}$ az n többszöröseit jelöli. Egy adott $k \in Z$ esetén a G csoport k szerinti baloldali mellékosztálya a $k + nZ$ halmaz lesz, vagyis mindazon egészek, amelyek k-val kongruensek modulo n.*

Egy részcsoport mellékosztályainak figyelemreméltó struktúrája van.

5.39. Megfigyelés *Legyen $H \leq G \ni g, g'$. Ekkor (1) $g \in Hg$, (2) $g' \in Hg \Rightarrow Hg = Hg'$, (3) $Hg = Hg'$ vagy $Hg \cap Hg' = \emptyset$ (4) $|H| = |Hg|$*

Bizonyítás. (1): $e \in H \Rightarrow g = eg \in Hg$.
(2): $g' = hg$ valamely $h \in H$-ra, ezért $Hg' = H(hg) = (Hh)g \subseteq Hg$. Mivel $g = h^{-1}g'$, ezért $g \in Hg'$, így az előző gondolatmenet szerint $Hg \subseteq Hg'$ is igaz.
(3): (2) miatt, ha $g^* \in Hg \cap Hg'$, akkor $Hg = Hg^* = Hg'$.
(4): Ha $h, h' \in H$ és $h \neq h'$, akkor $hg \neq h'g$, ezért a $h \mapsto hg$ bijekció H és Hg között. □

5.40. Következmény (Lagrange tétel) *Ha $H \leq G$, akkor $|H| \mid |G|$. Speciálisan, G bármely g elemének rendje (a g által generált részcsoport elemszáma) osztja G rendjét.*

Bizonyítás. Az előző megfigyelés szerint a G csoport néhány H szerinti (jobboldali) mellékosztály uniója, és minden mellékosztály $|H|$ elemet tartalmaz. □

5.41. Következmény *Ha G csoport, akkor bármely $g \in G$ elemének rendje a G csoport rendjének osztója.*

Bizonyítás. A g elem rendje a $\langle g \rangle$ részcsoport rendje, ami a Lagrange tétel miatt $|G|$ osztója. □

5.42. Definíció *A $H \leq G$ részcsoport* indexe *a $|G|$ és $|H|$ hányadosa, jele $|G : H|$.*

5.43. Következmény *Minden prímrendű csoport ciklikus.*

Bizonyítás. Bármely, $e \neq g \in G$ elem a Lagrange tétel miatt kénytelen az egész csoportot generálni. □

Láttuk tehát, hogy minden csoport előáll, mint tetszőleges részcsoportja jobboldali mellékosztályainak diszjunkt uniója. Természetesen ugyanez a baloldali mellékosztályokra is igaz, azonban *általában* nem igaz, hogy ez a két előállítás azonos. Ha pl. a G csoport Abel, és $H \leq G$ részcsoport, akkor a kommutativitás miatt $Hg = gH$ a G minden g elemére, így ilyenkor a két felbontás valóban megegyezik. Ugyanez a szituáció nemkommutatív csoportokban is előfordul, és az ezt megvalósító részcsoportok különösen érdekesek.

5.44. Definíció *A G csoport N részcsoportja a G* normálosztója *(jelölése $N \trianglelefteq G$), ha $Ng = gN$ a G minden g elemére.*

Világos, hogy minden részcsoport egyszerre bal- és jobboldali mellékosztálya önmagának. Ha tehát egy csoport indexe 2, akkor a részcsoport komplementere egyúttal jobb- és baloldali mellékosztály is, azaz minden 2 indexű részcsoport szükségképpen normálosztó. Például $A_n \trianglelefteq S_n$. A normálosztó tulajdonság ekvivalens módon jellemezhető az alábbiak szerint.

5.45. Állítás *(1)* $N \trianglelefteq G \iff$ *(2)* $g^{-1}Ng = N\ \forall g \in G \iff$ *(3)* $g^{-1}ng \in N\ \forall g \in G,\ \forall n \in N$.

Bizonyítás. (1)⇒ (2): $Ng = gN \Rightarrow g^{-1}Ng = N$.
(2)⇒ (3): $g^{-1}Ng = N \Rightarrow g^{-1}ng \in N$.
(3)⇒ (1): $g^{-1}ng \in N\ \forall n \in N \Rightarrow ng \in gN\ \forall n \in N \Rightarrow Ng \subseteq gN$. De $|Ng| = |gN|$ miatt $Ng = gN$ tetszőleges $g \in G$ elemre. □

5.46. Megfigyelés *Ha* $N \trianglelefteq G$*, akkor* $(Ng)(Nh) = N(gN)h = N(Ng)h = (NN)(gh) = N(gh)$ *a* G *tetszőleges* g, h *elemeire.*□

A fenti megfigyeles szerint a mellékosztályokon a komplexusszorzás művelet: két mellékosztályhoz rendel egy harmadikat. E műveletnek az egységeleme az N mellékosztály, és inverz is létezik: Ng inverze Ng^{-1}, hisz $NgNg^{-1} = Ngg^{-1} = N$.

5.47. Definíció *Ha* $N \trianglelefteq G$*, akkor az* N *mellékosztályainak csoportját a komplexusszorzásra a* G *csoport* N *szerinti* faktorcsoport*jának nevezzük, és* G/N*-nel jelöljük.*

A faktorcsoport rendje nyilván N indexe, azaz $|G : N|$. Ha G Abel, akkor bármely H részcsoportja normálosztó, és a H szerinti faktorcsoport is Abel. Ha G mindezen túl ciklikus is, akkor a faktorcsoport is ciklikus lesz, és G minden generátorelemének mellékosztálya generálja a faktorcsoportot.

A normálosztók szoros kapcsolatban állnak a csoportok közötti, művelettartó leképezésekkel.

5.48. Definíció *Ha* G *és* H *csoportok, akkor a* $\varphi : G \to H$ *leképezés* homomorfizmus*, ha művelettartó, azaz bármely* $g, g' \in G$ *elemekre* $\varphi(gg') = \varphi(g)\varphi(g')$*. (Értelemszerűen, az egyenlőség baloldalán álló szorzás a* G*, a jobboldali a* H *csoportművelete.)* *Ha* φ *homomorfizmus, akkor* $\mathrm{Ker}(\varphi) := \{g \in G : \varphi(g) = e_H\}$ *a* φ magja, *és* $\mathrm{Im}(\varphi) := \{\varphi(g) : g \in G\}$ *a* φ képe.

5.49. Megfigyelés *Ha* $\varphi : G \to H$ *homomorfizmus, akkor (1)* $\varphi(e_G) = e_H$*, (2)* $\varphi(g^{-1}) = \varphi(g)^{-1}$*, (3)* $\mathrm{Ker}(\varphi) \trianglelefteq G$ *és (4)* $\mathrm{Im}(\varphi) \leq H$*.*

Bizonyítás. (1): $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G) \Rightarrow e_H = \varphi(e_G)^{-1}\varphi(e_G) = \varphi(e_G)^{-1}\varphi(e_G)\varphi(e_G) = \varphi(e_G)$.
(2): $e_H = \varphi(e_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1}) \Rightarrow \varphi(g)^{-1} = \varphi(g^{-1})$
(3): Ha $\varphi(g) = \varphi(h) = e_H$, akkor $\varphi(gh) = \varphi(g)\varphi(h) = e_H e_H = e_H$, ill. $\varphi(g^{-1}) = \varphi(g)^{-1} = e_H^{-1} = e_H$, azaz $\mathrm{Ker}(\varphi) \leq G$. A normálosztó-tulajdonsághoz csak annyi kell, hogy tetszőleges $n \in \mathrm{Ker}(\varphi)$ és $g \in G$ esetén $g^{-1}ng \in \mathrm{Ker}(\varphi)$. Lássuk: $\varphi(g^{-1}ng) = \varphi(g^{-1})\varphi(n)\varphi(g) = \varphi(g)^{-1}e_H\varphi(g) = e_H$, csakugyan.
(4) Láttuk, hogy $\varphi(g^{-1}) = \varphi(g)^{-1}$, ill. $\varphi(gh) = \varphi(g)\varphi(h)$, azaz $\mathrm{Im}(\varphi)$ zárt az inverzképzésre és a H csoportműveletére, azaz $\mathrm{Im}(\varphi) \leq H$. □

Tehát minden homomorfizmus magja normálosztó. Ennek az állításnak a fordítottja is igaz, azaz minden normálosztó egyben homomorfizmus magja is, nevezetesen a $N \trianglelefteq G$ normálosztó a $\varphi_N : G \to G/N$ *természetes homomorfizmus* magja, ami a $\varphi_N(g) := Ng$ leképezéssel van megadva. (φ_N csakugyan homomorfizmus, hiszen $\varphi_N(gh) = Ngh = NNgh = NgNh = \varphi_N(g)\varphi_N(h)$.)

Homomorfizmus tétel: Ha $\varphi : G \to H$ csoport-homomorfizmus, akkor $G/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$.

Bizonyítás. Azt kell csak meggondolni, hogy φ bár G elemeit viszi H-ba, de egyúttal az $N := \mathrm{Ker}(\varphi)$ normálosztó mellékosztályain is homomorfizmus, amihez csak azt kell látni, hogy φ minden mellékosztályon konstans. Legyen $a, b \in Ng$ a g mellékosztályának elemei, azaz $a = ng$, $b = mg$ valamely $n, m \in \mathrm{Ker}(\varphi)$-re. Mivel $\varphi(n) = \varphi(m) = e_H$, ezért $\varphi(a) = \varphi(ng) = \varphi(n)\varphi(g) = \varphi(g) = \varphi(m)\varphi(g) = \varphi(mg) = \varphi(b)$. Tehát definiálható a $\varphi'(Ng) := \varphi(g)$ egy művelettartó $\varphi' : G/N \to H$ leképezést (azaz homomorfizmust) definiál. Az izomorfia igazolásához csak annyi kell, hogy a leképezés bijektív. Legyen hát $\varphi'(Ng) = \varphi'(Ng')$. Ekkor $\varphi(g) = \varphi(g')$, és g' felírható $g' = (g'g^{-1})g = fg$ alakban. Innen $\varphi(g) = \varphi(g') = \varphi(fg) = \varphi(f)\varphi(g)$, ahonnan $\varphi(f) = e_H$, azaz $f \in \mathrm{Ker}(\varphi) = N$, vagyis $g' \in Ng$, azaz $Ng' = Ng$. □

5.2. Direkt összeg, véges Abel csoportok alaptétele

Ha adott két csoport akkor a segítségükkel definiálhatunk egy harmadikat, azaz a csoportok osztályán is értelmezünk egyfajta műveletet.

5.50. Definíció *Ha $\langle G, \cdot\rangle$ és $\langle H, \star\rangle$ két csoport, akkor* direkt összegük *az a $G \oplus H = \langle G \times H, *\rangle$ csoport lesz, amire $g, g' \in G$ és $h, h' \in H$ esetén $(g, h) * (g', h') := (g \cdot g', h \star h')$.*

A fenti definíció voltaképpen egy algebrai struktúrát ír le, azt ellenőrizni kell, hogy ez valóban csoport. (A struktúrához az kell is, hogy a $*$ művelet a Descartes szorzaton, de ez ránézésre triviális. A $*$ asszociativitása egyszerű: ha $g, g', g'' \in G$ és $h, h', h'' \in H$, akkor

$$((g, h) * (g', h')) * (g'', h'') = (g \cdot g', h \star h') * (g'', h'') = ((g \cdot g') \cdot g'', (h \star h') \star h'') =$$
$$= (g \cdot (g' \cdot g''), h \star (h' \star h'')) = (g, h) * ((g', h') * (g'', h'')) \ .$$

Szükséges, még, hogy legyen egységelem a direkt összegben, és persze ez nem lesz más, mint (e_G, e_H), ahol e_G ill. e_H a G ill. H csoportok egységelemei, hiszen $(g, h) \in G \times H$ esetén $(g, h) * (e_G, e_H) = (g \cdot e_G, h \star e_H) = (g, h) = (e_G \cdot g, e_H \star h) = (e_G, e_H) * (g, h)$. A (g, h) elem inverze pedig nem túl meglepő módon a (g^{-1}, h^{-1}) elem lesz, ugyanis $(g, h) * (g^{-1}, h^{-1}) = (g \cdot g^{-1}, h \star h^{-1}) = (e_G, e_H) = (g^{-1} \cdot g, h^{-1} \star h) = (g^{-1}, h^{-1}) * (g, h)$.

5.51. Megfigyelés *A direkt összeg rendje a két direkt összeadandó rendjének szorzata.*

Bizonyítás. Triviális: $|G \times H| = |G| \cdot |H|$. □

5.52. Példa *A $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ csoportot úgy kapjuk, hogy az első koordinátában modulo 2, a másodikban pedig modulo 3 adunk össze. Az alábbiakban egymás mellett tüntettük fel a $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ és a $\mathbb{Z}_6$ csoportok Cayley táblázatait (ami a a szorzótáblát, helyesebben a műveleti táblát jelenti).*

$\mathbb{Z}_2 \oplus \mathbb{Z}_3$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$
$(0,0)$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$
$(1,1)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$	$(0,0)$
$(0,2)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$	$(0,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,1)$	$(1,2)$	$(0,0)$	$(1,1)$	$(0,2)$
$(0,1)$	$(0,1)$	$(1,2)$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$
$(1,2)$	$(1,2)$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$

$\mathbb{Z}_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Könnyen látható, hogy a $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ és a $\mathbb{Z}_6$ csoportok izomorfak, hiszen ha a fenti táblázatok megfelelő soraihoz és oszlopaihoz tartozó elemek egymásnak felelnek meg, akkor a két csoport művelete pontosan ugyanúgy hat a két alaphalmazon.

A véges Abel csoportok struktúrájának megértéséhez különösen fontos a direkt összeadás, amint azt az alábbi tétel mutatja.

A véges Abel csoportok alaptétele: Tetszőleges G véges Abel csoporthoz léteznek $p_1^{\alpha_1}, p_2^{\alpha_2} \dots p_k^{\alpha_k}$ prímhatványok úgy, hogy $G \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \dots \oplus \mathbb{Z}_{p_k^{\alpha_k}}$, azaz tetszőleges Abel csoport felírható prímhatványrendű ciklikus csoportok direkt összegeként.□

5.53. Következmény *Az n-edrendű nemizomorf Abel csoportok száma annyi, ahányféleképp az n felbontható prímhatványok szorzatára. Így pl. tetszőleges 36-edrendű Abel csoport izomorf az alábbi csoportok valamelyikével: $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9, \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3, \mathbb{Z}_4 \oplus \mathbb{Z}_9$.*

5.3. Gyűrűk, testek

Eddig egyműveletes struktúrákkal foglalkoztunk. Ha azonban a $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ vagy $\mathbb{C}$ számhalmazokról szeretnénk többet tudni, érdemes mindkét alapműveletet (az összeadást és a szorzást is) figyelembe venni. Ez (is) indokolja az olyan algebrai struktúrák vizsgálatát, ahol két kétváltozós művelet értelmezett.

5.54. Definíció *A $\langle R, \{+, \cdot\}\rangle$ algebrai struktúra* gyűrű, *ha $\langle R, +\rangle$ Abel csoport, $\langle R, \cdot\rangle$ félcsoport, továbbá teljesülnek a* disztributív azonosságok*: $a(b+c) = ab+ac$ ill. $(a+b)c = ac + bc$ ($\forall a, b, c \in R$). Ha röviden csak R gyűrűt mondunk, akkor konvenció szerint R két művelete $+$ és $\cdot$ a fentiek szerint.*

Az R gyűrű kommutatív*, ha a szorzás kommutatív. Az R gyűrű összeadásának egységelemét* nullelemnek *nevezzük, és* 0*-val jelöljük. Az R gyűrűben az $a \in R$ elem inverzét az összeadásra $-a$ jelöli. Az R gyűrű* egységelemes*, ha a szorzásműveletnek van egysége, amit (ha van)* 1 *jelöl.*

5.55. Megfigyelés *Ha R gyűrű, és $a, b \in R$, akkor $0a = a0 = 0$ ill. $(-a)b = -ab = a(-b)$.*

Bizonyítás. A disztributivitás miatt $0 = 0a + (-0a) = (0 + 0)a + (-0a) = 0a + 0a + (-0a) = 0a$. Innen $-ab = -ab + 0 = -ab + 0b = -ab + (a + (-a))b = -ab + ab + (-a)b = (-a)b$. Az $a0 = 0$ ill. $-ab = a(-b)$ azonosságok hasonlóan következnek a baldisztributivitásból. □

5.56. Példa *(1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ gyűrűk. $\mathbb{N}$ nem gyűrű, mert nem csoport az összeadásra (nincs inverz).*

(2) Egy tetszőleges $n \in N$ szám többszörösei ($n\mathbb{Z}$) is gyűrű.

(3) A mod m *maradékosztályok szintén.*

(4) Az $n \times n$-es (racionális, valós vagy komplex) mátrixok is gyűrűt alkotnak.

(5) Az egész együtthatós polinomok detto.

(6) A Gauss egészek (az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$) ugyancsak gyűrű.

(7) Tetszőleges H halmazra $\langle \mathcal{P}(H), \{\nabla, \cap\}\rangle$ a H halmaz Boole gyűrűje, *ahol ∇ a szimmetrikus különbséget jelöli: $A \nabla B := (A \setminus B) \cup (B \setminus A)$. Itt a nullelem az $\emptyset$, az egység pedig a H.*

5.57. Definíció *Az R gyűrűben a $a \neq 0$ elem* nullosztó, *ha létezik olyan $0 \neq b \in R$, amire $ab = 0$. Az R gyűrű* nullosztómentes, *ha R-ben nincs nullosztó. Az R gyűrű* integritási tartomány, *ha kommutatív és nullosztómentes.*

5.58. Példa *(1) $n\mathbb{Z}$ kommutatív és nullosztómentes, ezért integritási tartomány.*

(2) $\mathbb{Z}_n$ nem nullosztómentes, ha vannak olyan $a, b \in \mathbb{Z}_n$ számok, amelyekre $a \neq 0 \neq b$ (azaz $a \not\equiv 0 \not\equiv b (\mathrm{mod}\ n)$) és $ab \equiv 0 (\mathrm{mod}\ n)$, azaz ha n összetett. Ha $n = p$ prím, akkor a prímtulajdonság miatt, ha $ab = 0$, azaz $ab \equiv 0(p)$, vagyis $p \mid ab$, akkor $p \mid a$ vagy $p \mid b$, így $a = 0$ vagy $b = 0$ (a $\mathbb{Z}_p$ gyűrűben(!)). Tehát $\mathbb{Z}_p$ nullosztómentes, így integritási tartomány.

(3) Az $\mathbb{R}^{n\times n}$ mátrixgyűrűben A nullosztó, ha létezik olyan B mátrix, amire $AB = \mathbf{0}$. Ez pontosan akkor van, ha az $Ax = 0$ egyenletnek van nemtriviális megoldása, azaz, ha A szinguláris.

(4) A $\langle \mathcal{P}(H), \{\nabla, \cap\}\rangle$ Boole gyűrűben H minden valódi részhalmaza nulloszó, mert $A \cap (H \setminus A) = \emptyset$.

5.59. Definíció *Az R gyűrű* részgyűrűje *az $\langle R, \{+, \cdot\}\rangle$ olyan részstruktúrája, ami gyűrű. (Csupán a műveletekre való zártságot és az ellentettek meglétét (tkp a kivonásra való zártságot) kell ellenőrizni.)*

5.60. Megfigyelés *Ha $n \in \mathbb{Z}$, akkor $n\mathbb{Z}$ a $\mathbb{Z}$ részgyűrűje. A $\mathbb{Z}$ gyűrű minden részgyűrűje $n\mathbb{Z}$ alakú.*

Bizonyítás. Láttuk korábban, hogy $n\mathbb{Z}$ gyűrű. Ha R a $\mathbb{Z}$ részgyűrűje, akkor $\langle R, +\rangle$ részcsoportja a $\langle \mathbb{Z}, +\rangle$ csoportnak. Mivel az utóbbi csoport ciklikus, ezért minden részcsoportja is az, tehát R-t egyetlen elem (mondjuk n) generálja, így $R = n\mathbb{Z}$. □

Láttuk, hogy a gyűrűben tudunk kivonni, azaz egy elem ellentettjét hozzáadni ($a - b := a + (-b)$). Felettébb bosszantó, hogy osztani nem tudunk, azaz nem tudunk egy elem ellentettjével szorozni, hiszen a szorzás nem csoport- (csak félcsoport-) művelet, így nincs a szorzásra nézve inverz. Nyugodjunk meg: a szokásos számkörökben ($\mathbb{R}, \mathbb{C}$) sem tudunk osztani, mert az osztás nem *algebrai értelemben vett* művelet, hisz nem tudunk bármely két számot elosztani. Általában sem várhatjuk, hogy a gyűrűben a szorzásra nézve minden elemnek legyen inverze, hisz ha a x a 0 inverze, akkor $1 = 0x = (0+0)x = 0x + 0x = 1 + 1$, ahonnan $0 = 1$ adódik. Innen $0 = 0a = 1a = a$, azaz a gyűrű triviális, csak a 0 elemből áll. Kiderül, hogy a szorzás invertálhatóságának nem kell ennél jobban sérülnie.

5.61. Definíció *A T gyűrű* ferdetest*, ha $\langle T \setminus \{0\}, \cdot \rangle$ csoport. Ha a szorzás kommutatív, akkor T* test*.*

5.62. Példa *(1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ testek. (Láttuk, hogy kommutatív gyűrű. Minden nemnulla számnak van reciproka, így a szorzás is csoport a nemnulla számokon.)*

(2) Ha p prím, akkor $\mathbb{Z}_p$ test, aminek a szokásos jelölése $\mathbb{F}_p$. (Láttuk, hogy $\mathbb{Z}_p$ kommutatív gyűrű, és az Euler-Fermat tételből adódik a reciprok kiszámítása.) Ha m nem prím, akkor (láttuk) van $\mathbb{Z}_m$-ben nullosztó, tehát $\mathbb{Z}_m$ nem test.

(3) A valós polinomok hányadosteste *a következő. $\mathbb{R}(x) := \{\frac{p}{q} : p, q \in \mathbb{R}[x], q \not\equiv 0\}$. A műveletek: $\frac{p}{q} + \frac{r}{s} := \frac{ps+qr}{qs}$, ill. $\frac{p}{q} \cdot \frac{r}{s} := \frac{pr}{qs}$. (A polinomok hányadosteste a legszűkebb, az $\mathbb{R}[x]$ gyűrűt (azaz a valós polinomok gyűrűjét) tartalmazó test. Ugyanazzal a konstrukcióval kapjuk, mint racionális számtestet, ami a legszűkebb, az egészek gyűrűjét tartalmazó test.)*

(4) Az $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ halmaz is test, hiszen $(a + b\sqrt{2})^{-1} = \frac{1}{(a+b\sqrt{2})} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2}$ miatt létezik inverz. (Itt használtuk, hogy ha $a, b \in \mathbb{Q}$, akkor $a^2 \neq 2b^2$. Igaz az is, hogy a példabeli $\sqrt{2}$ helyett állhatna $\sqrt{t}$ is $(0 < t \in \mathbb{Q}_+)$.

(5) A kvaterniók ferdeteste *a következő: $\{a+bi+cj+dk : a, b, c, d \in \mathbb{R}\}$. Az összeadást a természetes módon definiáljuk, a nullelem a $0 + 0i + 0j + 0k$, $a + bi + cj + dk$ ellentettje $-a - bi - cj - dk$, tehát az összeadás valóban kommutatív csoport. A szorzásnál pedig használjuk a Q-bel szorzást, pl $(i+2j)(3+k) = 3i + ik + 6j + 2jk = 3i - j + 6j + 2i = 5i + 5j$. A kvaterniószorzás asszociativitásából adódóan a szorzás itt is asszociatív lesz. Könnyen látható, hogy a szorzás egységeleme az $1 = 1 + 0i + 0j + 0k$ lesz, az inverz pedig $(a + bi + cj + dk)^{-1} = \frac{1}{a+bi+cj+dk} = \frac{a-bi-bj-bk}{(a+bi+cj+dk)(a-bi-cj-dk)} = \frac{a-bi-bj-bk}{a^2+b^2+c^2+d^2} = \frac{a}{a^2+b^2+c^2+d^2} - \frac{b}{a^2+b^2+c^2+d^2}i - \frac{c}{a^2+b^2+c^2+d^2}j - \frac{d}{a^2+b^2+c^2+d^2}k$-nak adódik. (Hasonlóan a komplex számokhoz, itt is a konjugálttal kell bővíteni.) Jegyezzük meg, hogy a kvaterniók nem test, hisz pl. $ij = k \neq -k = ji$.*

5.63. Megjegyzés *Hasonlóan ahhoz, ahogyan azt az egész számok körében tettük, a gyűrűben is értelmezhető a felbonthatatlan és a prím fogalma. Láttuk, hogy a számelmélet alaptételének teljesülése azon múlott, hogy a prím és a felbonthatatlan szám ugyanazt jelentette az adott struktúrában. Általában kommutatív gyűrűkben is igaz, hogy a számelmélet alaptétele pontosan akkor teljesül, ha a prím és a felbonthatatlan az alaphalmaz ugyanazon részhalmazát jelenti. Ez nincs mindig így. Az $a + b\sqrt{-5}$ alakú komplex számok (mint az könnyen ellenőrizhető) egy R kommutatív gyűrűt alkotnak. Az R-beli komplex számok abszolutértékének négyzete egész szám, és azt is tudjuk, hogy komplex számok szorzatának abszolútértéknégyzete megegyezik a tényezők abszolútértéknégyzeteinek szorzatával. Ebből az következik, hogy az $r = 2$ szám (aminek abszolútértéknégyzete 4) csak triviális módon bontható R-beli számok szorzatára, azaz felbonthatatlan. (Nincs ugyanis olyan R-beli szám, aminek az abszolútértéknégyzete 2 lenne.) Azonban $2 \mid 6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$, és $2 \nmid 1 + \sqrt{-5}, 2 \nmid 1 - \sqrt{-5}$ miatt a 2 nem prím.*

5.64. Tétel *Minden véges integritási tartomány test.*

5.65. Megjegyzés *A végesség szükséges, hisz pl. $n\mathbb{Z}$ integritási tartomány, de nem test.*

Bizonyítás. Az integritási tartományban a szorzás kommutatív, így csak azt kell bizonyítani, hogy létezik a szorzásnak egységeleme, és minden nemnulla elemnek van reciproka,

azaz a szorzásra vonatkozó inverze. Legyen R véges integritási tartomány, és legyen $0 \neq a \in R$. Ha $ab = ab'$, akkor $0 = ab + (-ab') = ab + a(-b') = a(b + (-b'))$, ezért a nullosztómentesség miatt $b + (-b') = 0$, azaz $b = b'$. Eszerint az $ar_1, ar_2, \ldots$ elemek mind különbözők (ahol $R = \{r_1, r_2, \ldots\}$), így R végessége miatt a teljes R halmaz előáll: $R = \{ar : r \in R\}$. Van tehát olyan $e \in R$, amire $ae = a$. Azt szeretnénk igazolni, hogy e a szorzás egységeleme, azaz $be = b$ minden $b \in R$ esetén. A szorzás kommutativitása miatt $ab = (ae)b = a(eb) = a(be)$, azaz $0 = a(be)+(-ab) = a(be)+a(-b) = a(be+(-b))$, amiből a nullosztómentesség miatt $be + (-b) = 0$, azaz $eb = be = b$ adódik. Tehát R valóban egységelemes.

Láttuk, hogy rögzített $0 \neq a \in R$ esetén R minden eleme előáll ar alakban (alkalmas $r \in R$-re). Ez persze $e \in R$-re is igaz, tehát létezik olyan $r \in R$, amire $ar = e$, azaz bármely $0 \neq a$-nak létezik inverze, vagyis R csakugyan test. □

5.66. Definíció *A T test* prímtest*, ha nincs valódi részteste.*

5.67. Állítás *$\mathbb{Q}$ és $\mathbb{F}_p$ (ha p prím) prímtest, és más prímtest nincs.*

Bizonyítás. Láttuk, hogy testek, és hogy $0 \neq 1$. Legyen T prímtest. Világos, hogy $n := 1 + 1 + \ldots + 1$ [n-szer] benne van T-ben. Ha $n = 0$ valamely $n > 0$-ra, akkor a $\mathbb{Z}_n \subseteq T$ a minimális ilyen n-re. Mivel a T test nullosztómentes, ezért Z_n is az, vagyis n prím. Ekkor tehát $\mathcal{F}_p \subset T$. Látjuk egyrészt, hogy $\mathcal{F}_p$ prímtest, másrészt, hogy ekkor $T = \mathcal{F}_p$. Ha $n \neq 0$ minden $n > 0$-ra, akkor $0, 1, -1, 2, -2, \ldots$ mind T-beliek és különbözők, tehát $\mathbb{Q} \subseteq T$. A T test prímtulajdonsága miatt ekkor $\mathbb{Q} = T$. □

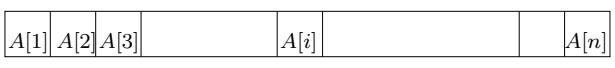
6. fejezet

Adatszerkezetek, algoritmusok és bonyolultságelmélet

6.1. Alapvető adatszerkezetek

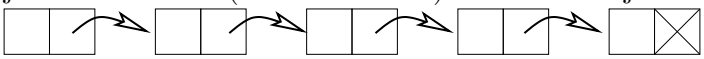
A legtöbb számítógéppel végrehajtható feladat során adatokat (rekordokat) kell tárolnunk és azokkal dolgozni, például műveleteket végezni velük. Ezt a célt valamiféle adatszerkezet felépítésével érjük el. Egy konkrét adatszerkezet tehát meghatározza, miféle módon tároljuk az adatainkat, mik az adatszerkezet elemei között a kapcsolatok és azt is, hogy miféle műveleteket tudunk az adatainkkal végrehajtani. Természetesen attól függően, hogy miféle célból tároljuk az adatokat, különféle adatszerkezetek lehetnek előnyösek. Ebben a részben néhány alapvető adatszerkezettel fogunk megismerkedni, de már itt hangsúlyozzuk, hogy egy-egy konkrét feladatra elképzelhető, hogy érdemes nekünk magunknak valamiféle nemsztenderd adatszerkezetet kifejleszteni.

Az egyik legismertebb adatszerkezet a *tömb* (angolul: array). Ez arra alkalmas, hogy az adatainkat közvetlen hozzáféréssel valamiféle sorrendben tároljuk. Egy tömb a deklarálásánál meghatározott számú rekordot tartalmazhat, ezek számára külön memóriaterületet tartunk fenn. Ezért ha hangsúlyozni szeretnénk az A tömb méretét, akkor szokás $A[1..n]$ módon is jelölni (amennyiben n rekordot tárolunk benne). Az A tömbben tárolt i-dik rekordot $A[i]$ jelöli, és az alapvető műveletek egy tömbnél az OLVAS[i] és ÍR[i], amikoris az i-dik rekordot kiolvassuk vagy beírjuk, esetleg átírjuk. A tömb előnye, hogy a tárolt rekordokhoz konstans idő alatt hozzáférünk, ám hátránya, hogy nem dinamikus, nehéz pl. beszúrni a tömbbe, ha a beszúrandó rekordot két szomszédos elem közé akarjuk illeszteni.



Ezeket a nehézségeket a *láncolt lista* (angolul: linked list) segítségével tudjuk sikeresen leküzdeni. A láncolt lista elemei az ú.n. cellák vagy csomópontok: minden cella

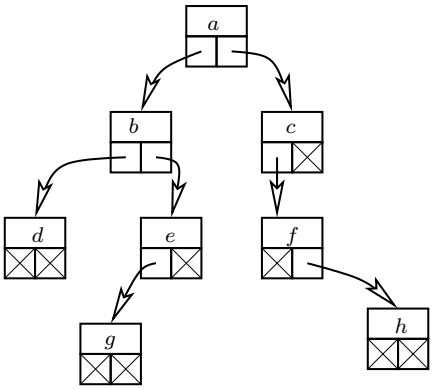
egy adatmezőből (amin tetszőleges formájú adatot tudunk tárolni) és (a lista utolsó celláját kivéve) egy mutatóból állnak, ahol a mutató a lista következő cellájára mutat. A *kétszeresen láncolt lista* (doubly linked list) ettől abban különbözik, hogy minden cellához két mutató tartozik, melyek közül a második a cellát megelőző cellára mutat. Az alapvető műveletek itt ELSŐ ELEM, AKTUÁLIS ELEM (az aktuális cellában tárolt rekord), KÖVETKEZŐ ELEM (az aktuális elem mutatójának segítségével határozzuk meg), kétszeresen láncolt list esetén az ELŐZŐ ELEM (amit a „másik" mutató jelez), BESZÚRÁS (az aktuális elem után), ill. (az aktuális elem utáni elem) TÖRLÉSe. A beszúrás úgy történik, hogy létrehozunk egy új cellát a beszúrandó elemnek, az aktuális elem mutatóját bemásoljuk az új cella mutatójába, végül az aktuális elem mutatója az új cellára fog mutatni. Törlés esetén pedig úgy járunk el, hogy az aktuális cella mutatóját átírjuk a következő (törlésre kerülő) cella mutatójára.



A láncolt lista előnye, hogy dinamikus adatszerkezet, nem foglal feleslegesen sok memóriát, gyors a beszúrás és a törlés, ám hátránya, hogy az ott tárolt rekordok nem közvetlenül hozzáférhetők, és ezért a keresés sem túl gyors egy ilyen listában.

Ha a tárolandó rekordokon értelmezett valamiféle rendezés, akkor sokszor hasznos a fenti adatszerkezetek rendezett változata: a rendezett tömb és a rendezett láncolt lista. Itt az a további megkötés a tárolt rekordokkal, hogy a tömbben a rekordok a tömb egy kezdőszeletét töltik ki, és mind a lista, mind a tömb esetén nagyság szerint jönnek egymás után.

A láncolt lista egy általánosítása a *bináris fa* (angolul: binary tree) adatszerkezet. Ha egy a láncolt lista celláit egy gráfnak tekintjük, és a mutatókat pedig irányított éleknek, akkor a kapott gráf egy irányított út lesz. A bináris fa minden cellája legfeljebb két mutatót tartalmaz, akárcsak a kétszeresen láncolt lista, de a két mutató itt nem a „következő" és a „megelőző" cellára mutat, hanem két „új" cellára: a bal fiúra és a jobb fiúra. Az a megkötés, hogy legyen a bináris fának egy gyökere (olyan cellája, amire nem mutat a bináris fa más cellájának mutatója) és a mutatók definiálta gráf aciklikus (irányított körmentes) legyen. A bináris fában lehet a celláknak egy harmadik „apa" mutatójuk is, amelyik arra a cellára mutat, amelyiknek az adott cella a bal- vagy jobbfia. Világos, hogy minden láncolt lista tekinthető bináris fának, de a bináris fához általában nem tartozik a celláknak egy sorrendje. A bináris fán értelmezett alapvető műveletek a GYÖKÉR, AKTUÁLIS ELEM, BALFIÚ, JOBBFIÚ, APA, BALRÉSZFA, JOBBRÉSZFA. A GYÖKÉR művelet a bináris fa gyökércelláját adja, az AKTUÁLIS ELEM az aktuális cellában tárolt rekordot, a JOBBFIÚ az aktuális elem jobbfiú mutatója szerinti celláját, a BALFIÚ pedig a balfiú mutató szerintit adja vissza. Az APA művelet eredménye az aktuális cellára mutató cella. Végül a BALRÉSZFA ill. JOBBRÉSZFA műveletek az adott bináris fa gyökerének bal- ill. jobb fiában gyökerező bináris részfát adják eredményül.



A bináris fában tárolt rekordoknak (szemben a láncolt listával) nincs egy természetes sorrendje, ám definiálható mindjárt háromféle igen hasznos konkrét sorrend is egy bináris fa celláin. Ezen sorrendeket a bináris fa egy-egy bejárása határozza meg. Mindhárom esetben a gyökérből indulunk, és rekurzívan bejárjuk a bal, majd a jobb részfát. Attól függően, hogy a gyökeret a két részfa bejárásához képest mikor járjuk be, definiálhatjuk a *preordert, inordert* és *posztordert*. Az x bináris fán értelmezett háromféle bejárás pszeudokódja az alábbi.

pre(x)	in(x)	post(x)
begin	begin	begin
látogat(x)	in(bal(x))	post(bal(x))
pre(bal(x))	látogat(x)	post(jobb(x))
pre(jobb(x))	in(jobb(x))	látogat(x)

A fenti ábrán látható bináris fa rekordjainak pre-, in-, ill. posztorder szerintti sorrendje $abdegcfh$, $dbgeafhc$, ill. $dgebhfca$. Világos, hogy mindhárom bejárás algoritmusában egy konkrét cellával konstans sok lépést végzünk, tehát bármelyik sorrend meghatározásának lépésszáma legfeljebb $konst \cdot n$, ahol n a tárolt rekordok száma.

Ha a bináris fában tárolt rekordokon van valamiféle rendezés (azaz bármely rekordhoz rendelhető egy valós szám, és két rekord összehasonlításakor a hozzájuk rendelt számok nagyságviszonyát vizsgáljuk), akkor hasonlóan a rendezett tömbhöz ill. rendezett láncolt listához, itt is megkívánhatunk egy további tulajdonságot, amitől a bináris fával végzett műveletek könnyebbé válnak. Egy bináris fát tehát *bináris keresőfának* (angolul: binary search tree) nevezünk, ha teljesül rá a keresőfa tulajdonság, azaz

- a keresőfa tetszőleges x csúcsának bal részfájában tárolt egyetlen rekord sem nagyobb az x-ben tárolt rekordnál, míg az x csúcs jobb fiában gyökerező jobb részfában tárolt egyetlen rekord sem kisebb az x-ben tárolt rekordnál.

Ha feltesszük, hogy a keresőfában tárolt rekordokon szigorú rendezés van (azaz bármely két rekord közül az egyik kisebb a másiknál), akkor a keresőfa tulajdonság úgy is megfogalmazható, hogy tetszőleges csúcs bal részfájában a csúcsban tároltnál kisebb, a jobb részfájában pedig annál nagyobb rekordokat tárolunk. A bináris keresőfák egyik hasznos tulajdonságára utal az alábbi megfigyelés.

6.1. Lemma *Tetszőleges bináris keresőfa inorder szerinti bejárása a fában tárolt rekordokat nagyság szerinti rendezi.*

Bizonyítás. Azt kell csupán megmutatni, hogy a fában tárolt tetszőleges x és y rekordok esetén x és y sorrendje az inorder szerinti felsorolásban éppen a nagyság szerinti sorrendjük lesz. Tegyük fel, hogy a bináris fában x és y egymás leszármazottja, mondjuk x az y őse. Ekkor az in(x) hívásakor látszik, hogy y a szerint előzi meg vagy követi x-et az inorder szerinti sorrendben, hogy kisebb vagy nagyobb nála. Ha pedig x és y nem egymás leszármazottja (és mondjuk x kisebb y-nál), akkor legyen a z rekord az x és y rekordok legközelebbi közös őse a bináris fában, tehátx a z bal, y pedig a z jobb részfájában található. Ekkor az in(z) hívása mutatja, hogy x megelőzi y-t az inorder sorrendben. □

További érdekes megfigyelés, hogy bármely bináris fa háromféle ismertetett bejárása (azaz a pre-, in- és posztorder) a fa leveleit ugyanolyan sorrendbe rendezi. A konkrét példán mindhárom bejárásban dgh a levelek sorrendje.

A bináris keresőfában további műveleteket tudunk értelmezni: ilyenek a KERES, BESZÚR, MIN, MAX vagy a TÓLIG. A KERES(s) művelethez a gyökérből indulunk, és s-t a gyökérrel összehasonlítva vagy megtaláltuk s-t, vagy tudjuk, hogy a bal- vagy a jobb részfában folytassuk a keresést, ahol előröl kezdjük a fenti eljárást. A BESZÚR(s) eljárás egy KERES(s) eljárással indul, és ha s nincs a bináris keresőfában, akkor az s-t az alá a levél alá szúrjuk be értelemszerűen bal- vagy jobbfiúként, amelyikben a keresés véget ért. A MIN és MAX műveletek is hasonlók a kereséshez: a gyökérből addig megyünk balra ill. jobbra, amig van arra rekord, ha nincs, akkor megtaláltuk a legkisebb ill. legnagyobb rekordot. Mindhárom művelet lépésszáma a bináris keresőfa mélységével arányos. A TÓLIG(a, b) művelet abból áll, hogy megkeressük a-t és b-t, miáltal megkapjuk az az a és b közti elemeket tartlamazó részfát, és ezt inorder szerint bejárjuk. A lépésszámot itt az inorder dominálja, ez tehát $konst \cdot n$, ahol n a tárolt rekordok száma.

A legvégül következő adatszerkezetet akkor használhatjuk, ha a tárolt adatokon adott egy rendezés, és szükségünk van arra, hogy a legkisebb rekordot gyorsan meg tudjuk találni és ki tudjuk törölni. Itt a tárolt rekordokra egy, bináris keresőfánál használttól különböző feltételt írunk elő, és a bináris keresőfa alakjára is teszünk megkötést.

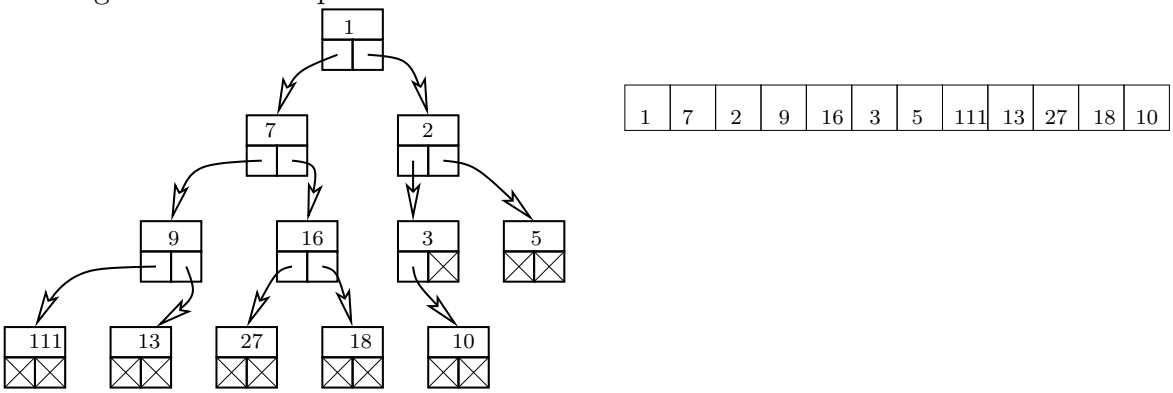
Egy l-szintes bináris fát szokás teljesnek nevezni, ha pontosan $2^{l+1} - 1$ rekordot tárol, azaz az első $l - 1$ szinten található cellák mindegyikének pontosan két mutatója van. Ha persze nem pontosan $2^n + 1$ rekordot kell tárolnunk, akkor nincs esélyünk ilyen módon teljes fával dolgozni, be kell érnünk egy kevésbé szigorú megkötéssel. Egy bináris fát tehát általános értelemben *teljesnek* hívunk, ha úgy kapható meg, hogy egy l szintes, $2^{l+1} - 1$ rekordot tároló bináris fából, hogy annak valamelyik levelétől jobbra álló minden levelét töröljük. (Ezt úgy is meg lehet fogalmazni, hogy az l szintes, $2^{l+1} - 1$ rekordot tároló bináris fából a háromféle bejárás valamelyike szerint vett levélsorrend szerinti utolsó néhány levelet töröljük.)

A teljes bináris fa egy fontos tulajdonsága, hogy tárolható a mutatók megadása nélkül egy egyszerű tömbben. Sőt: minden tömb tekinthető teljes bináris fának ugyanígy. Konkrétan, az $A[1..n]$ tömbnek megfelelő teljes bináris fát úgy kapjuk, hogy az $A[i]$ rekord bal fia $A[2i]$, jobb fia pedig $A[2i+1]$ (már amennyiben $2i \leq n$ ill. $2i+1 \leq n$ teljesül).

Egy (pl. tömbként megadott) teljes bináris fa akkor *kupac* (angolul: heap), ha teljesül rá az ún. kupactulajdonság, azaz

- egyetlen rekord sem nagyobb a fiaiban tárolt rekordok egyikénél sem, azaz $A[i] \leq A[2i]$ és $A[i] \leq A[2i+1]$ teljesül minden $1 \leq i \leq n$ esetén.

Világos, hogy a kupac gyökerében (tömbös reprezentációban az első helyen tárolt rekord) a kupacban tárol rekordok legkisebbike. (Azt sem nehéz látni, hogy egy kupacban tárolt legnagyobb rekord a levelek bármelyike lehet.) Az alábbi ábra egy konkrét kupac kétféle megadására mutat példát.



A kupac rendkívül hasznos adatszerkezet, érdemes tehát megvizsgálni, hogyan építhetünk egy rendezetlen $A[1..n]$ tömbből kupacot. A tömböt eközben természetesen teljes bináris fának tekintjük. Az a cél, hogy a tömb minden elemére teljesüljön a kupactulajdonság (ami a tömb $A[\lfloor \frac{n}{2} \rfloor + 1] \ldots A[n]$ elemeire, azaz a teljes bináris fa leveleire fiak híján automatikusan teljesül), és ezt a tömb elemein jobbról balra haladva érjük el: meghívjuk egymásután a kupacol($\lfloor \frac{n}{2} \rfloor$]), kupacol($\lfloor \frac{n}{2} \rfloor] - 1$), kupacol($\lfloor \frac{n}{2} \rfloor] - 2$), ..., kupacol(1) eljárásokat. A kupacol(i) eljárás során megkeressük az $A[i], A[2i]$ és $A[2i+1]$ elemek legkisebbikét. Ha ez $A[i]$, akkor a kupactulajdonság teljesül i-re, végeztünk. Ha ez mondjuk $A[j]$ (ahol $j > i$), akkor felcseréljük az $A[i]$ és $A[j]$ rekordokat, és meghívjuk a kupacol(j) eljárást. Könnyen látható hogy a kupacol(1) végeztével csakugyan kupacot kapunk. Mivel egy kupacol(i) eljárás az általa esetlegesen meghívott kupacol(j) eljárástól eltekintve konstans számú lépést használ, ezért a kupacépítés lépésszáma a meghívott kupacol eljárások konstansszorosával becsülhető. Márpedig a bináris fa k-dik szintjén tárolt $A[i]$ rekordhoz tartozó kupacol eljárás kapcsán legfeljebb $l - k$ kupacol eljárást hívunk meg

(ahol l a kupachoz tartozó bináris fa szintjeinek száma). Ezért a kupacépítés lépésszáma

$$(l-1)\cdot 1+(l-2)\cdot 2+(l-3)\cdot 4+\ldots+(l-i)\cdot 2^{i-1}+\ldots+1\cdot 2^{l-2}=$$
$$=\sum_{i=1}^{l-1}(l-i)\cdot 2^{i-1}=\sum_{i=1}^{l-1}2^{i-1}+\sum_{i=1}^{l-2}2^{i-1}+\sum_{i=1}^{l-3}2^{i-1}+\ldots+\sum_{i=1}^{1}2^{i-1}=$$
$$=2^{l-1}-1+2^{l-2}-1+\ldots 2^0-1\leq=2^{l-1}+2^{l-2}+\ldots 2^0\leq 2^l\leq 2n\ ,$$

ahol az utolsó egyenlőtlenség oka az, hogy az l-szintes bináris fa első $l-1$ szintjén az utolsó szint egy levelével együtt összesen legalább 2^{l-1} rekord található, tehát $n\geq 2^{l-1}$.

A kupac adatstruktúrában a két legfontosabb művelet a MINTÖR és a BESZÚR. A MINTÖR törli a kupacban tárolt minimális rekordot (ami a bináris fa gyökerében, azaz a tömb első helyén áll), majd helyreállítja a kupactulajdonságot. Ehhez a tömb utolsó elemét a kitörölt első elem helyére mozgatja és végrehajt egy kupacol(1) eljárást, aminek a lépésszáma a bináris fa mélységével, azaz $\log_2 n$ konstansszorosával felülről becsülhető.

A BESZÚR művelet során egy új elemet illesztünk a kupacba, amit a tömb végére írunk. Ezzel a kupactulajdonság egyedül az utolsó elem apjában romolhatott el, és ha ez történt, akkor ezt egy cserével helyre lehet állítani, annak árán, hogy a nagyapában esetleg elromlik a kupactulajdonság. A kupactulajdonság helyreállításához tehát az utolsó helyre beszúrt elemet „felszivárogtatjuk" egészen addig, mig felette mar kisebb fog állni, amihez szintén legfeljebb a kupac mélységével arányos számú lépés szükséges.

6.2. Keresés, rendezés

6.2.1. Keresési feladatok

A keresési feladat (itt) abból áll, hogy valamely adatstruktúrában kell megkeresni egy adott x rekordot, vagy arra a következtetésre jutni, hogy x nem szerepel az adatstuktúrában. Világos, hogy ha az elemek valamiféle „véletlen sorrendben" vannak tárolva az adott adatstruktúrában, akkor nincs jobb módszer, mint a teljes adatstruktúra végigolvasása. Az általunk vizsgált keresési feladatban azonban adott egy lineáris rendezés az adatstruktúrában tárolt rekordokon, és a rekordok e rendezés szerint valamiféle értelmes módon vannak tárolva. Ezért a továbbiakban a rekordok halmazát egyszerűen egy számhalmaznak tekintjük, és a rekordok rendezése pedig a nagyság szerinti rendezés lesz.

Lineáris keresés

Egy lehetséges módszer a rendezett halmaz tárolására a láncolt lista, ami (mondjuk) növekvő sorrendben tartalmazza a tárolt rekordokat. Mivel itt nincs lehetőség a lista tetszőleges elemének kiolvasására, ezért a legjobb, amit tehetünk, hogy elindulunk a lista elejéről, és addig olvassuk ki a lista soron következő elemeit, míg vagy megtaláljuk x-t,

vagy pedig x-nél nagyobb rekordot találunk, vagy netán a lista véget ér. Az utóbbi két esetben arra következtetünk, hogy x nincs a listában. Ezt a keresést hívják *lineáris keresésnek*, és lépésszáma a lista méretével arányos, hiszen legrosszabb esetben kénytelenek vagyunk az egész listát végigolvasni.

Ha az adatainkat kupacban tároljuk, akkor sem tudunk a lineáris keresésnél lényegesen jobbat mondani, legrosszabb esetben ki kell olvasni minden rekordot. Azonban míg rendezett láncolt listánál megállhattunk, amint a keresett x-nél nagyobb rekordra leltünk, itt akkor lesz a keresés eredménye negatív, ha nem találjuk meg x-et és valamely i-re az i-dik rekordtól egészen a $(2i-1)$-dik rekordig olvasunk x-nél nagyobbakat (vagy ha a kupac véget ér).

Végül ha az adataink nem egy rendezett adatstruktúrában vannak tárolva (azaz rendezett láncolt listában, rendezett tömbben, kupacban, bináris keresőfában vagy valami ezekhez hasonlóban), akkor sincs a keresésre jobb módszer, mint az összes rekord kiolvasása, ami lényegében a lineáris keresésnek az adott struktúrára való alkalmazását jelenti.

Bináris keresés

Ha a rendezett halmaz elemei egy n méretű tömbben vannak (szintén növekvő sorrendben felsorolva), akkor a tömb bármely elemét közvetlenül kiolvashatjuk, és ez jelentős javulást eredményez a lineáris kereséshez képest. Tegyük fel, hogy k olyan egész, melyre $2^{k-1}-1 < n \leq 2^k - 1$. Ha kiolvassuk a tömb 2^{k-1}-dik elemét, akkor három dolog történhet. Vagy megtaláljuk x-t, vagy x-nél nagyobb elemet olvastunk, ezért x-t a továbbiakban elegendő a tömb első $2^{k-1}-1$ eleme között keresni, vagy x-nél kisebb elemet olvastunk, ami azt jelenti, hogy x-t a továbbiakban a tömb $(2^{k-1}+1)$-dik és n-dik eleme között kell keresnünk. Mindkét utóbbi esetben a feladat egy olyan keresési feladat, amelyben a rendezett tömb mérete legfeljebb $2^{k-1}-1$ lesz. Mivel egy $2^1 - 1 = 1$ méretű tömbre a keresési feladat egyetlen eleme kiolvasását igényli, ezért a fentiek szerint egy legfeljebb $2^k - 1$ méretű tömb esetén k érték kiolvasásával megoldható a feladat. A fentiekben leírt *bináris keresés* lépésszáma tehát $k = \lfloor \log_2(n+1) \rfloor + 1$-nek legfeljebb konstansszorosa.

Az is könnyen látható, hogy erre a feladatra nem létezik olyan algoritmus, mely *minden esetben* hatékonyabb a bináris keresésnél. Ha ugyanis a keresőalgoritmus csak a tömb elemeit kérdezheti le, akkor az algoritmusnak fel kell készülnie arra, hogy az adott kiolvasáskor nem találja meg x-t, ezért a keresés egy olyan keresési feladattal válik ekvivalenssé, melyben egy legalább $n' = \lceil \frac{n-1}{2} \rceil$ méretű tömb van megadva. Ha n kettes számrendszerbeli alakját tekintjük, akkor n'-t úgy kapjuk, hogy n utolsó jegyét levágjuk. Legrosszabb esetben tehát muszáj feltenni annyi kérdést, mint ahány jegyű az n szám kettes számrendszerbeli alakja, azaz akár $\lfloor \log_2(n+1) \rfloor + 1$ cellát is ki kell olvasni.

A bináris keresés valójában speciális esete a bináris keresőfában már leírt keresési eljárásnak. Ha ugyanis egy tömböt nem úgy tekintünk bináris fának, ahogyan azt a kupac esetén tettük, hanem egy $A[1..n]$ tömbhöz tartozó bináris keresőfát (rekurzív módon) úgy

definiáljuk, hogy a gyökér az $A\left[\left\lfloor\frac{n}{2}\right\rfloor\right]$, a bal részfa az $A\left[1..\left\lfloor\frac{n}{2}\right\rfloor-1\right]$ tömb, a jobb részfa pedig az $A\left[\left\lfloor\frac{n}{2}\right\rfloor+1..n\right]$ tömb, akkor ezzel bináris keresőfát definiáltunk, amelyben a keresés pontosan az $A[1..n]$ tömbön végzett bináris keresés lesz. Láttuk, hogy bináris keresőfában a keresés lépésszáma a bináris keresőfa mélységével arányos, ami a rendezett tömbből készített bináris keresőfa esetén éppen a jegyek száma n kettes számrendszerbeli felírásban.

Minimumkeresés

Egy másik, algoritmikus szempontból érdekes feladat a minimumkiválasztási feladat. Itt rendezetlenül adottak az $a_1, a_2, \ldots, a_n$ számok, és ezek közül kell kiválasztani a minimálisat. Egy lépésben az algoritmus kiválaszthat egy a_i és egy a_j számot, amelyeket összehasonlítva megtudja, melyik a kisebb és melyik a nagyobb. Világos, hogy a minimumkiválasztás $n-1$ összehasonlítással megoldható: az i-dik összehasonlítás előtt ismerjük az $a_1, a_2, \ldots, a_i$ számok küzül a minimálisat, mondjuk a_j-t. Az i-dik lépésben a_j-t összehasonlítjuk a_{i+1}-gyel, és közülük a kisebbik lesz az $a_1, a_2, \ldots, a_{i+1}$ számok közül a legkisebb. Az $(n-1)$-dik lépés után tehát ismerni fogjuk az összes szám közül a legkisebbet.

Azt sem nehéz látni, hogy pusztán $n-2$ összehasonlítás eredményének ismerete sosem elegendő a minimum kiválasztására. Definiáljunk ugyanis egy gráfot, melynek csúcsai az a_i számok, és él akkor fusson két szám között, ha az algoritmus összehasonlította őket. Mivel egy n-pontú, összefüggő gráfnak van egy $(n-1)$-élű feszítőfája, ezért az imént definiált gráfnak nincs feszítőfája, vagyis legalább két komponense van. Ha az a_i-k minimuma mondjuk egy K_1 komponensében van a gráfnak, akkor megtehetjük azt, hogy a K_1 komponenstől különböző K_2 komponens minden egyes elemét egy rögzített x értékkel csökkentjük. Ezáltal nem változik meg egyetlen összehasonlítás eredménye sem, azonban x alkalmas választásával elérhető, hogy a minimum most már a K_2 komponensben legyen. Az $n-2$ összehasonlítás eredményének ismerete tehát sosem elegendő a minimum meghatározásához. Az erdőkről tanult ismereteket kamatoztatandó azt is bártran kijelenthetjük, hogy k összehasonlítás után legalább $n-k$ jelölt van a minimumra, hiszen a minimum a fent leírt gráf bármelyik komponensében lehet.

6.2.2. Rendezési feladatok

A fenti minimumkiválasztásnál egy nehezebb feladat az $a_1, a_2, \ldots, a_n$ elemek rendezése. Itt növekvő sorredenbe kell raknunk az elemeket és ehhez csak összehasonlításokat végezhetünk ill. azok eredményeire támaszkodhatunk. Először megbecsüljük, hogy tetszőleges, a rendezést végrehajtó algoritmusnak legrosszabb esetben legalább hány összehasonlítást kell végeznie. Tegyük fel, hogy az algoritmus először az a_{i_1} és a_{j_1} elemeket hasonlítja össze, ezt követően az a_{i_2} és a_{j_2} elemeket, általában az l-dik összehasonlításban az a_{i_l} és a_{j_l} elemek kerülnek összehasonlításra. Ha az algoritmus minden esetben legfeljebb

k összehasonlítás után rendezni tudja az $a_1, a_2, \ldots, a_n$ számokat, akkor az algoritmus futásához hozzárendelhetünk egy k hosszú 0/1 sorozatot, melynek az l-dik jegye 0, ha $a_{i_l} < a_{j_l}$, különben az l-dik jegy 1 (azaz, ha $a_{i_l} > a_{j_l}$, vagy ha az l-dik összehasonlításra már nem is kerül sor).

Az itt a lényeges észrevétel, hogy ennek a k hosszú 0/1 sorozatnak meg kell határoznia az $a_1, a_2, \ldots, a_n$ számok rendezését. Az első összehasonlításnak ugyanis nemcsak az eredménye ismert, hanem a_{i_1} és a_{j_1} is, hiszen az algoritmusnak mindig ugyanúgy kell kezdődnie. Ennek az összehasonlításnak az ismeretében ismerjük az a_{i_2} és a_{j_2} elemeket. Az összehasonlításuk eredményét ismerjük a sorozatból, innen adódik, hogy mi lesz a_{i_3} ill. a_{j_3}, sít. Tehát a k hosszúságú 0/1 sorozat meghatároz minden elvégzett összehasonlítást, és persze ezek kimenetelét is, ezért a sorozatnak meg kell határoznia az $a_1, a_2, \ldots, a_n$ elemek rendezését is.

Eszerint az algoritmus futását leíró k hosszúságú 0/1 sorozat legalább annyiféle lehet, mint az $a_1, a_2, \ldots, a_n$ lehetséges rendezéseinek száma. Minden egyes rendezés az $a_1, a_2, \ldots, a_n$ elemek egy permutációjának felel meg, és viszont. A lehetséges k hosszúságú sorozatok száma pedig nyilván 2^k. Ezért $n! \leq 2^k$, vagyis $k \geq \lceil \log_2(n!) \rceil = \log_2 n + \log_2(n-1) + \log_2(n-2) + \ldots + \log_2 1 \geq (\log_2 n + \log_2(n-1) + \log_2(n-2) + \ldots + \log_2 \frac{n}{2}) + (\log_2(\frac{n}{2}-1) + \ldots + \log_2 4) \geq \frac{n}{2} \cdot \log_2 \frac{n}{2} + (\frac{n}{2}-4) \log_2 4 = \frac{n}{2}(\log_2(n)-1) + 2(\frac{n}{2}-4) = \frac{1}{2}(n \log_2 n) - \frac{n}{2} + 2(\frac{n}{2}-4) = \frac{1}{2}(n \log_2 n) + \frac{n}{2} - 8 \geq \frac{1}{2}(n \log_2 n)$, utóbbi egyenlőtlenség $n \geq 16$ esetén igaz. (A becsléseket a vizsgára nem kell pontosan reprodukálni, elég az eredményt ismerni.)

Buborékrendezés (bubble sort)

Ezek után konkrét, összehasonlítás-alapú rendezőalgoritmusokat vizsgálunk. A *buborékalgoritmus* inputja egy n méretű T tömb, amiben a rendezendő számokat tároljuk. Az output egy n méretű tömb, melyben az inputtömb elemei növekvő sorrendben követik egymást. Az buborékalgoritmus fázisokból áll. Minden fázisban az algoritmus az aktuális T tömbön hajt végre összehasonlításokat, és cseréket. Egy fázisban az i-dik összehasonlítás a $T(i)$ és $T(i+1)$ összehasonlítása. Ha $T(i) > T(i+1)$, akkor felcseréljük a tömb i-dik és $(i+1)$-dik elemét (még az $(i+1)$-dik összehasonlítás előtt). Egy fázisban tehát $n-1$ összehasonlítás, és legfeljebb $n-1$ csere történik. Könnyen látható, hogy az i-dik fázis végére az i legnagyobb elem a helyére kerül, ezért legfeljebb $n-1$ fázisra van szükség, vagyis a buborékalgoritmus lépésszáma n^2 konstanszorosával felülről becsülhető.

Kiválasztásos rendezés (selection sort)

A kiválasztásos rendezés egy $A[1..n]$ tömb esetén úgy működik, hogy sorra megkeressük az $A[1..n]$, $A[2..n], \ldots, A[n-1..n]$ tömbök minimális elemeit, amelyeket azonmód felcserélünk az adott tömb első elemével. Láttuk, hogy a minimumkeresés lépésszáma becsülhető az adott tömb méretének konstansszorsával. Mivel maga a csere további

konstans számú lépés, így az eljárás lépésszáma legfeljebb $konst \cdot n^2$. Kicsit óvatosabb becsléssel az összehasonlítások száma $(n-1)+(n-2)+\ldots+2+1 = \binom{n}{2}$, a cserék száma pedig legfeljebb $n-1$.

Beszúrásos rendezés (insertion sort)

A *beszúrásos rendezés* során a rendezendő rekordokat egyenként szúrjuk be egy rendezett tömbbe. Tipikus esetben az input egy rendezetlen $A[1..n]$ tömb, az output pedig „ugyanez" a tömb, amelyben a rekordok immár a rendezés szerint következnek egymás után. A rendezőalgoritmus n beszúrási lépésből áll. Az i-dik lépés előtt a tömbünkben tárolt első $i-1$ rekord, azaz az $A[1..i-1]$ résztömb elemei már növekvő sorrendbe vannak rendezve. A beszúrási lépésben bináris kereséssel megkeressük az $A[i]$ helyét az aktuális $A[1..i-1]$ tömbben (legyen ez mondjuk a j-dik pozíció), majd a tömb $(i-1)$-dik, $(i-2)$-dik, $\ldots$, j-dik elemeit eggyel jobbra mozgatjuk, végül $A[i]$-t beillesztjuk a tömb j-dik helyére. Világos, hogy az n-dik beszúrás után éppen a kívánt rendezett tömböt kapjuk. Minden beszúrásnál a keresés legfeljebb $\lfloor \log_2 n \rfloor + 1$ összehasonlítást igényel, az adatmozgatás igénye pedig legfeljebb $n-1$. Az összlépésszám tehát n^2 konstansszorosával becsülhető. Ha az $a_1, a_2, \ldots$ számok eredetileg csökkenő sorrendben voltak, akkor a beszúrásos rendezés adatmozgatással kapcsolatos lépésszáma már önmagában $1+2+3+\ldots+(n-1) = \frac{n(n-1)}{2}$, azaz legrosszabb esetben szükség van kb $\frac{1}{2}bn^2$ lépésre.

Összefésüléses rendezés (merge sort)

Vannak a fentieknél jobb módszerek is. Az összefésüléses rendezés használja az ún. *összefésülés* eljárást, ami egy k méretű A ill. egy l méretű B rendezett tömbből készít egy $k+l$ méretű rendezett C tömböt. Az összefésülés eljárás összehasonlításokat végez, és az s-dik összehasonlítás után, meghatározza a C tömb s-dik elemét, ezt beírja a C tömbbe, és egyúttal kitörli ezt az elemet az A ill. B tömbök közül a megfelelőből. (Kezdetben a C tömb üres.) Tegyük fel, hogy az s-dik lépés előtt az A tömbből már kitöröltük az első i elemet, a B tömbből pedig az első j elemet, és ezeket okosan beírtuk a C tömbbe. Az s-dik lépésben összehasonlítjuk az A tömb $(i+1)$-dik és a B tömb $(j+1)$-dik elemét, a kisebbet kitöröljük a megfelelő tömbből, és beírjuk a C tömb s-dik cellájába. Világos, hogy az összefésülés eljárás azt adja, amit várunk, és az elvégzett összehasonlítások száma legfeljebb $k+l-1$. (Kevesebb is lehet, ha időközben valamelyik tömb elfogy: ekkor a maradék tömb elemeit minden további összehasonlítás nélkül sorban beírhatjuk a C tömbbe.)

Az *összefésüléses rendezés* egy rekurzív algoritmus. Inputja egy n méretű tömb, ami a rendezendő számokat tárolja valamilyen sorrendben. Az output egy n méretű tömb, melyben az inputtömb elemei növekvő sorrendben követik egymást. Az összefésüléses rendezés nem tesz mást, mint összefésüli az A_1 A_2 rendezett tömböket. A ravaszság annyi, hogy A_1 tömb úgy keletkezik, hogy (rekurzív hívással) összefésüléses rendezéssel

rendezzük az A tömb első $\lceil \frac{n}{2} \rceil$ elemét. Hasonlóan, az A_2 tömb az A tömb maradék $\lfloor \frac{n}{2} \rfloor$ elemének összefésüléses rendezésével keletkezik. (A rekurzió miatt szükséges azt is deklarálni, hogy egy 1 méretű tömb összefésüléses rendezése egyszerűen abból áll, hogy az inputot (hipphopp) kiadjuk outputként.)

Ha az összefésüléses rendezés egy n méretű tömbön legfeljebb $f(n)$ összehasonlítást igényel, akkor az

$$f(n) \leq \left\lceil \frac{n}{2} \right\rceil + \left\lfloor \frac{n}{2} \right\rfloor - 1 + f\left(\left\lceil \frac{n}{2} \right\rceil\right) + f\left(\left\lfloor \frac{n}{2} \right\rfloor\right) = n - 1 + f\left(\left\lceil \frac{n}{2} \right\rceil\right) + f\left(\left\lfloor \frac{n}{2} \right\rfloor\right)$$

rekurzió adódik. Világos, hogy $f(1) = 0, f(2) = 1$, ezért $n = 1, 2$ esetén fennáll az $f(n) \leq n\lceil \log_2 n \rceil$ egyenlőtlenség. n szerinti teljes indukcióval igazoljuk, hogy ez minden $n \in \mathbb{N}$-re fennáll. Tegyük fel, hogy $n < N$-re már bizonyítottuk ezt. Ekkor $f(N) \leq N - 1 + f(\lceil \frac{N}{2} \rceil) + f(\lfloor \frac{N}{2} \rfloor) \leq N - 1 + \lceil \frac{N}{2} \rceil \cdot \left\lceil \log_2(\lceil \frac{N}{2} \rceil) \right\rceil + \lfloor \frac{N}{2} \rfloor \cdot \left\lceil \log_2(\lfloor \frac{N}{2} \rfloor) \right\rceil \leq N + \lceil \frac{N}{2} \rceil \cdot \left\lceil \log_2(\frac{N}{2}) \right\rceil + \lfloor \frac{N}{2} \rfloor \cdot \left\lceil \log_2(\frac{N}{2}) \right\rceil \leq N + N \cdot \left\lceil \log_2(\frac{N}{2}) \right\rceil = N + N \cdot \lceil \log_2 N - 1 \rceil = N + N \cdot \lceil \log_2 N \rceil - N = N \cdot \lceil \log_2 N \rceil$, tehát egy n méretű tömbön az összefésüléses rendezés valóban legfeljebb $n\lceil \log_2 n \rceil$ összehasonlítást végez. (A becsléseket a vizsgára nem kell pontosan reprodukálni, elég az eredményt ismerni.) Azt sem nehéz megmutatni, hogy az összefésüléses rendezés összlépésszáma (amibe tehát nemcsak az összehasonlítások számítanak bele) $f(n)$ konstansszorosával becsülhető.

Kupacos rendezés (heap sort)

A kupacos rendezést legkényelmesebben egy rendezetlen tömbön tudjuk végrehajtani. Ebből első lépésként kupacot építünk (legfeljebb $konst \cdot n$ lépésben, ahol n a rekordok száma), majd n egymást követő MINTÖR művelet elvégzésével a rekordokat növekvő sorrendben kapjuk meg. Mivel egyetlen MINTÖR elvégzése $konst \cdot \log_2 n$ lépést igényel, az egész eljárás lépésszáma $n \cdot \log_2 n$ alkalmas konstansszorosával felülről becsülhető.

Gyorsrendezés (quick sort)

A gyorsrendezés egy ún. nemdeterminisztikus algoritmus, amely a véletlent is felhasználja a működéséhez. A gyakorlatban egy determinizált változatát szokás alkalmazni, arra számítva, hogy a rekordok valamiféle „véletlen” sorrendben vannak, és elhanyagolható az esélye annak, hogy pont olyan sorrendből kiindulva kelljen a rendezést végrehajtani, amely túlságosan sok lépést igényel. Ha a gyorsrendezést véletlen algoritmusnak tekintjük, akkor a várható lépésszámáról tudjuk elmondani, hogy igen versenyképes, ha pedig a determinisztikus változatát tekintjük, akkor bár az néhány inputtal sok lépésben végez, ám az inputok döntő többségén rendkívül gyors.

A gyorsrendezés inputja egy $A[1..n]$ rendezetlen tömb, outputja pedig a rekordok növekvő sorrendjében rendezett tömb. Az algoritmus alapja a PARTÍCIÓ(s) eljárás, ahol s az egyik (véletlenül választott) rekord. A gyakorlatban az s rekordot a tömb

első ($A[1]$) elemének szokás választani. A PARTÍCIÓ(s) eljárás inputja egy $X[1..k]$ tömb és egy benne tárolt s rekord, outputja pedig egy átrendezett tömb, amely három részből áll: tömb elejére, mondjuk az $X[1..t]$ tömbbe gyűjtjük az s-nél kisebb rekordokat, középen, az $X[t+1..l]$ tömbben találhatók az s-sel egyenlő rekordok, míg az X tömb végén elhelyezkedő $X[l+1..k]$ tömbben s-nél nagyobb rekordok következnek. Ezt úgy szokás implementálni, hogy elkezdjük kiolvasni az $X[1], x[2], \ldots$ rekordokat, amíg egy s-nél nem kisebb rekordot találunk, mondjuk $X[i]$-t. Ugyancsak addig olvassuk az $X[k], X[k-1], \ldots$ rekordokat, egészen addig, amíg egy s-nél kisebb rekordot találunk, mondjuk $X[j]$-t. Ekkor kicseréljük $X[i]$-t és $X[j]$-t, majd folyatjuk az eljárást, az $X[i+1], X[i+2], \ldots$ rekordok ill. az $X[j-1], X[j-2], \ldots$ rekordok olvasásával. Akkor állunk meg, ha az első sorozatban s-nél nem kisebbet, ill. a második sorozatban s-nél kisebb rekordot találunk, amelyeket ismét felcserélünk, majd folytatjuk az eljárást. Ha a két olvasási sorozat összeér, akkor e kapott rekordtól balra s-nél kisebb rekordok vannak a tömbben, mít attól jobbra az s-nél nem kisebbek találhatók. Ezt követően az s-sel egyenlő rekorodokat a tömb második részének elejére mozgatjuk.

A PARTÍCIÓ(s) eljárás segítségével a gyorsrendezés algoritmust a rekurzív QUICKSORT($A[1..n]$) eljárással valósítjuk meg a következő módon. Végrehajtunk egy PARTÍCIÓ(s) eljárást az $A[1..n]$ tömbre és egy benne tárolt véletlen s rekordra. A kapott $A[1..k], A[k+1..l], A[l+1..n]$ partíción első tömbjén végrehajtunk egy QUICKSORT($A[1..k]$) eljárást, míg a harmadik részen egy QUICKSORT($A[l+1..n]$) eljárást.

Az input tömb n mérete szerinti indukcióval könnyen látható, hogy a QUICKSORT eljárás helyesen működik. Nem triviális, de igazolható, hogy a QUICKSORT eljárás átlagos lépésszáma az $n \cdot \log_2 n$ konstanszorosával felülről becsülhető. Az is könnyen látható, hogy a QUICKSORT lépésszáma legrosszabb esetben (amikoris a véletlenül választott s rekord mindig a legkisebb vagy a legnagyobb elem az adott tömbben) az n^2-nek konstansszorosa alkalmas pozitív konstansra.

Az eddig ismertetett rendezési algoritmusok mindegyike összehasonlítás-alapú volt, és ezért teljesült rájuk a szakasz elején igazolt információelméleti felső korlát, azaz van olyan pozitív c konstans, hogy n rekord rendezésekor legrosszabb esetben legalább $c \cdot n \cdot \log_2 n$ összehasonlításra van szükség. Az alábbiakban két kulcsmanipulációs rendezési algoritmust tekintünk át, amelyek nem összehasonlítás-alapúak lévén akár $c \cdot n \cdot \log_2 n$-nél lényegesen kevesebb lépés után is végezhetnek.

Ládarendezés (binsort)

Létezik az összehasonlítás-alapú rendezések lépésszámára kapott alsó becslésnél kevesebb lépést használó rendezési algoritmus, de persze csak olyan, amelyik nem összehasonlítás-alapú. Ha például tudjuk, hogy az $a_1, a_2, \ldots, a_n$ számok mindegyike 1 és m közötti egész, és m kisebb (de legalábbis nem sokkal nagyobb) n-nél, akkor hasznos lehet az ún. *ládarendezés*. Itt készítünk egy m méretű T tömböt, melynek minden cellája egy lista (ezeket nevezik ládáknak). Sorra elolvassuk az a_1, $a_2, \ldots$ elemeket. Ha $a_i = j$-t olvasunk,

akkor a T tömb j-dik cellájában álló lista végére felírjuk az i értéket (azaz i-t betesszük a j-dik ládába). Tehát n lépés után kitöltjük a T tömböt. Ezután sorban végigolvassuk a tömb celláin álló listákat, és kitöltünk egy n méretű A tömböt, mely növekvő sorrendben fogja tartalmazni az a_i elemeket. Nevezetesen, ha egy üres ládát találunk, akkor a következő ládához lépünk. Ha egy nemüres ládát találunk, akkor végigolvassuk a ládához tartozó lista elemeit, és az ezeknek az indexeknek megfelelő a_i-ket sorban beírjuk az A tömb soron következő celláiba. Ha kiürül egy láda, akkor a T tömb soron következő celláján található ládát kezdjük olvasni. A ládarendezés lépésszáma felülről becsülhető $n + m$ konstansszorosával.

Radix rendezés

Van olyan eset is, melyben a ládarendezés nem kifizetődő, de mégis célt érhetünk egy $(n \log_2 n)$ konstansszorosánál jelentősen kevesebb lépést használó algoritmussal. Ha az $a_1, a_2, \ldots, a_n$ számok egészek, mindegyik s alapú számrendszerben van felírva, és mindegyik a_i legfeljebb k jegyű, akkor alkalmazható a *radix rendezés*. Először ládarendezéssel rendezzük az a_i-ket az utolsó jegyük szerint. Ezáltal helyesen lesznek rendezve az $a_1^1, a_2^1, a_3^1, \ldots$ számok, ahol a_i^j-t úgy kapjuk, hogy a_i utolsó j jegyét tekintjük az s alapú felírásban. Ezt követően ládarendezéssel rendezzük az imént rendezett tömböt az a_i-k utolsóelőtti jegye szerint. Ekkor helyesen lesznek rendezve az $a_1^2, a_2^2, a_3^2, \ldots$ számok. Általában, a $(j-1)$-dik ládarendezés után kapott számok $a_1^{j-1}, a_2^{j-1}, a_3^{j-1}, \ldots$ szerint helyesen vannak már rendezve. A j-dik fázisban ládarendezzük az adott sorrendet a hátulról j-dik jegyeik szerint. Ezáltal az $a_1^j, a_2^j, a_3^j, \ldots$ úgy lesznek rendezve, hogy ha valamelyiknek hátulról a j-dik jegye kisebb egy másiknál, akkor a j-dik fázisban történő ládarendezés szerint megelőzi a másikat, ha pedig egyenlők ezen a helyiértéken a jegyek, akkor a korábbi rendezések szeinti sorrendben állnak a rekordok. (Ezért volt szükség arra, hogy a ládarendezés konzervatív legyen, azaz ha két elem a ládarendezés szerint azonos, akkor a rendezést követő sorrendjük azonos legyen a kiindulási sorrenddel.) Ezek szerint a j-dik fázis után helyesen lesznek rendezve az $a_1^j, a_2^j, a_3^j, \ldots$ számok, vagyik a k-dik fázis után az a_i számok helyes rendezését kapjuk. Minden ládarendezés legfeljebb konstansszor $(n+s)$ lépést igényel, tehát a radix rendezés lépésszáma $k(n+s)$ konstansszorosa lesz. Ismételten hangsúlyozzuk, hogy radix rendezés helyes működéséhez elengedhetetlen, hogy a közben alkalmazott ládarendezések konzervatívak legyenek, vagyis azok során az egyes ládákban elhelyezett elemeket mindig a ládában található lista *végére* (és ne az elejére) írjuk. (Magához a ládarendezéshez erre nem volna szükség.) Ezzel érjük el ugyanis, hogy ha két elemet már korábban rendeztünk egymáshoz képest, és a soron következő ládarendezésben nem kell változtatni ezen, akkor a korábbi sorrend továbbra is megmaradjon.

6.3. Gráfok tárolása

Nemsokára...

6.4. Algoritmusok bonyolultsága

A gyakorlatban számos problémát számítógéppel, algoritmikus úton oldunk meg. Gyakran több út is kínálkozik a cél elérésére, és nyilván azt érdemes választani, ami az adott problémát a leghatékonyabban kezeli. Ilyenkor össze kell hasonlítanunk különböző algoritmusokat, de máskor is fontos lehet, hogy egy eljárás gyorsaságáról tudjunk valamit mondani. Egy algoritmust képzelhetünk úgy, hogy egy miáltalunk megadott bemenethez egy kimenetet állít elő. A bemenetet gondolhatjuk a „kérdésnek", amit az algoritmusnak felteszünk, a kimenet pedig a feltett kérdésre a „válasz". Nyilván, minél „nehezebb" a kérdés, annál több időt érdemes hagyni a számítógépnek a válaszra, azaz annál több lépést tehet az adott algoritmus. Hogyan kell hát a kérdés „nehézségét" mérni? Egy célszerűnek látszó módszer az input „hossza": tehát az, hogy hány bit a bemenet, vagyis milyen hosszan írtuk le a problémát az algoritmus nyelvén. Az algoritmus meghatároz tehát egy $f : \mathbb{N} \to \mathbb{N}$ függvényt. Ez a függvény minden n-re meghatározza azt az $f(n)$-t, ami az algoritmus legnagyobb lépésszáma egy n hosszú bemenet esetén. (Feltételezzük, hogy az algoritmus minden bemeneten előbb-utóbb megáll.) Ha egy A ill. A' algoritmus f ill. f' lépésszámfüggvényeire minden n esetén $f(n) \leq f'(n)$ áll, akkor bizonyos értelemben jogos az A algoritmust hatékonyabbnak tekinteni, mint az A' algoritmust. (Tehát rosszabb egy A algoritmus, ami az inputok $99,99\%$-án szinte azonnal végez, de néhány szerencsétlen inputon „elszáll", mint az az A' algoritmus ami minden inputon sokat erőlködik, de azért mindig megbízhatóan végez. Ez pl. akkor lehet különösen indokolt, ha az a fontos, hogy belátható időn belül megoldjuk a problémát (pl. kiszámítsuk az űrhajó pályamódosítását, a szembejövő meteor miatt, vagy atomerőművet vezéreljünk), mert az időtúllépések nem „átlagolódnak ki": elég egyetlen szerencsétlen input, és game over.)

Mi van azonban akkor, ha bizonyos n-ekre $f(n) \leq f'(n)$, más n-ekre pedig $f(n) > f'(n)$? Nos, ekkor az érdekel minket, hogy az input méretének növekedtével milyen gyorsan nő az algoritmus lépésszáma. A motiváció e mögött az, hogy nagyméretű feladatokat szeretnénk megoldani, és míg rövid input esetén a nagyobb lépésszám kompenzálható jobb számítógéppel, a bemenet méretének növekedtével ez nem tehető meg. Konkrétabban: ha az A algoritmus lépésszáma n hosszú inputon $10^5 \cdot n$, az A'-é pedig 2^n, akkor $n \leq 21$ esetén az A' algoritmus hatékonyabb, $n \geq 22$-re pedig az A. Ha tehát mondjuk 10^{10} lépést tudunk megengedni az algoritmusnak, hogy belátható időn belül eredményt kapjunk, akkor az A algoritmus $n \leq 10^5$ méretű bemenetken működik, míg az A' algoritmus számára $n \leq \log_2 10^{10} \leq \log_2 (10^3)^{\frac{10}{3}} = \frac{10}{3} \log_2 10^3 < \frac{10}{3} \cdot 10 < 34$ áll, azaz már a 34 hosszú bemenettel sem képes megbirkózni a program. A fenti példában a lényeges különbség a két algoritmus között az volt, hogy míg az első maximális lépésszáma az in-

putméret *polinomjával* volt becsülhető, addig a másik algoritmus futásideje *exponenciális* függvénye is lehetett a bemenet hosszának. Paradox módon jobbnak tekintünk tehát egy $10^{10^{10}} \cdot n^{10^{10}}$ lépésszámú algoritmust, mint egy $(1+1/10^{10^{10}})^{n/10^{10^{10}}}$ futásidejűt, még akkor is, ha a gyakorlatban az előbbi már $n = 2$ méretű bemenet esetén is kivitelezhetetlen, míg az utóbbi akkor is működik, ha a bemenet mérete a hihetetlenül hatalmas számok világából való. Még egyszer tehát az Állatfarmba illő szabály:

A polinomiális algoritmus jó, az exponenciális algoritmus rossz.

(A rend kedvéért tegyük hozzá, hogy ez így egyáltalán nem igaz. Itt és most azonban polinomiális lépésszámú algoritmusok érdekesek a számunkra.) Egy algoritmust a továbbiakban *polinomiálisnak* (néha, kissé félreérthetően *hatékonynak*) nevezünk, ha lépésszáma (így közvetve a futásideje) felülről becsülhető a bemenet méretének polinomjával.

6.4.1. Néhány egyszerű eljárás bonyolultsága

Megvizsgáljuk néhány számokkal operáló algoritmust hatékonyságát. Az algoritmus bemenete tehát néhány (általában két) szám, ezekkel végzünk műveletet. Először is gondoljuk meg, mi egy szám hossza. Itt az ésszerű eljárás a számot a szokásos módon megadni, ha nem is épp 10-es, de 2-es vagy mondjuk 16-os számrendszerben. Ekkor n hossza $\log_2 n$ ill. $\log_{16} n$ lesz, amelyek (mivel konstans szorzóban különböznek) az algoritmus polinomiális voltát nem befolyásolják. (Sőt, a polinom fokát sem, csupán a főegyüttható változik.) Mi tehát számrendszeralapú megadásban gondolkodunk, ekkor egy n és m szám együttes mérete $\log n + \log m$ lesz. A kérdés tehát, hogy ennek a számnak milyen függvénye egy-egy művelet lépésszáma.

Összeadás: Az általános iskolában tanult írásbeli összeadás remekül működik más számrendeszerekben is. A műveletigény minden helyiértéknél legfeljebb 2, hisz két számot adunk össze az adott helyiértéken, plusz még egy esetleges maradékot az előző helyiértékből. A lépésszámra felső korlát tehát a $2 \cdot \max(\log n, \log m) < 2 \cdot (\log n + \log m)$, ami lineáris, vagyis polinomiális. A kivonásra hasonló igaz.

Szorzás: A szokásos írásbeli szorzás működik, és megvalósítható $\log n$ db összeadással, ahol minden összeadandó az m egy egyjegyű számmal összeszorzott többszöröse. Egy egyjegyű számmal m-t $2 \log m$ lépésben össze lehet szorozni, ugyanis minden jegyet szorozni kell, és az esetleges maradékot a szorzathoz hozzáadni. Tehát az összlépésszám $2(\log n)(\log m) \leq (\log n + \log m)^2$, vagyis a szorzás polinomiális. Az írásbeli osztás is polinom időben elvégezhető, de szőrözni kell pindurit, mikor megbecsüljük a soron következő hányadost.

Hatványozás: Az n^m szám jegyeinek száma kb $k \cdot 2^l$, ahol k és l az n ill. m jegyeinek száma 2-es számrendszerben. Mivel itt a bemenet mérete $k + l$, ezért a végeredményt még leírni sem tudjuk a bemenet hosszának polinomjával becsülhető lépésben ezért nem létezik a hatványozásra polinomiális algoritmus.

Végül még két olyan eljárásra nézzük meg ugyanezt, amelyeket szerencsétlen módon

csak a jegyzet későbbi részében definiálunk.

Hatványozás modulo m: Az input n, k és m, a cél pedig $n^k \pmod m$ meghatározása.

Legyen $k = \sum_i k_i 2^i$, azaz $k = \underline{\ldots k_2 k_1 k_0}_2$ a kettes számrendszerbeli alak. Sorra kiszámoljuk a 0 és $n-1$ közé eső $n_0, n_1, n_2, \ldots$ számokat, ahol $n_0 \equiv n(m), n_1 \equiv n^2(m), \ldots, n_i \equiv n^{2^i}(m)$. Az n_{i+1}-t az $n_{i+1} \equiv n_i^2(m)$ alapján egy szorzással és egy maradékos osztással kaphatjuk, ráadásul n_i mérete mindig legfeljebb $\log m$ lesz. Tehát egy n_i kiszámítása egy legfeljebb $\log m$ méretű szám négyzetre emelését és a legfeljebb $2 \log m$ méretű eredmény maradékos osztását igényli. Az szükséges n_i-k kiszámításához mindezt $\log k$-szor kell megtenni. Az n^k meghatározását pedig $n^k = \prod_{i=1}^{\infty} n^{k_i 2^i} \equiv \prod_{i=1}^{\infty} n_i^{k_i}(m)$ alapján további, legfeljebb $\log k$ db, legfeljebb $\log m$ méretű szám szorzásával és $\log k$ db, legfeljebb $2 \log m$ méretű szám maradékos osztásával kapjuk.

6.2. Példa *Ha pl az* $n^{23} \pmod m$*-t szeretnénk kiszámítani, akkor kiszámítjuk an* $n \pmod m$*,* $n^2 \pmod m$*,* $n^4 \equiv (n^2)^2 \pmod m$*,* $n^8 \equiv (n^4)^2 \pmod m$*, és* $n^{16} \equiv (n^8)^2 \pmod m$ *értékeket modulo m, ami négy szorzással (ahol a tényezők m-nél nem nagyobbak) és öt (m-mel való) maradékos osztással jár. Ezután* $n^{23} \equiv n^{16} \cdot n^4 \cdot n^2 \cdot n \pmod m$ *miatt további három szorzás (a tényezők m-nél nem nagyobbak) és három maradékos osztás szolgáltatja a végeredményt.*

A modulo m hatványozás tehát összességében is polinomiális eljárás.

Euklideszi algoritmus: Az euklideszi algoritmus egy lépésében adott $a_{i+1} \leq a_i$ esetén kell egy maradékos osztást végezni, és meghatározni azt a $0 \leq a_{i+2} < a_{i+1}$-t, melyre $a_i = q_{i+1} \cdot a_{i+1} + a_{i+2}$ áll. Az a_i mérete legfeljebb akkora, mint a_0 és a_1 mérete közül a nagyobbik, tehát az euklideszi algoritmus minden lépése polinomiális időt igényel. A nagy észrevétel, hogy $a_{i+2} \leq \frac{a_i}{2}$, ezért a fentieket legfeljebb $\log a_0$-szor kell elvégezni, amitől az eljárás polinomiális marad.

6.5. A P és NP problémaosztályok

A továbbiakban *döntési problémákkal* foglalkozunk. Ilyen probléma pl. a később vizsgált prímtesztelés (bemenet egy n szám, a kimenet egy bit, mely 1, ha n prím, 0, ha nem), az összefüggőségi teszt (bemenet egy G gráf, a kimenet egyetlen bit: 1, ha G öf, 0 különben), a síkbarajzolhatósági teszt, az Euler (ill. Hamilton) kör létezésének eldöntése, stb. Jegyezzük meg, hogy számos esetben a megoldandó probléma nem döntési probléma. (Pl. mennyi egy hálózatban a maximális folyam, keressünk minimális költségű feszítőfát, találjunk Hamilton-kört, bontsunk egy adott számot prímtényezők szorzatára, stb.) Sokszor (de nem mindig) azonban a megfelelő π problémához tartozik egy π' döntési probléma, és az is igaz, hogy π'-re létezik hatékony algoritmus, akkor π is hatékonyan megoldható. Pl, ha hatékonyan el tudjuk dönteni, hogy egy gráfban van-e Hamilton-kör,

akkor hatékonyan tudunk találni is egyet. Ugyanis egymás után minden élt megpróbálunk elhagyni a gráfból. Ha az elhagyás után is van Hamilton-kör (amit hatékonyan tudunk tesztelni a döntési probléma algoritmusával), akkor hagyjuk el az adott élt, ha nincs H-kör az elhagyás után, akkor hagyjuk benn az élt a továbbiakban. Vagyis élszámnyi teszt után a gráfból éppen egy Hamilton-kör marad (már amennyiben eredetileg is volt Hamilton-köre a gráfnak). Nem ismeretes azonban olyan hatékony eljárás pl. a prímtényezőkre bontásra ami a megfelelő (prímtesztelési) döntési problémára alapoz. (A kanonikus alak megtalálására egyébként egyáltalán nem ismert hatékony algoritmus.)

Az előbbiek fényében fontos problémaosztály az olyan döntési problémáké, amelyekre létezik a problémát polinom időben eldöntő A algoritmus, azaz olyan eljárás, melyhez létezik egy p_A polinom azzal a tulajdonsággal, hogy bármely n méretű bemeneten A legfeljebb $p_A(n)$ lépést végez, és ezt követően mindig helyes választ ad. Az ilyen, polinom időben megoldható döntési problémák halmazát P jelöli. Mielőtt példákat mutatnánk P-beli problémákra, meghatározzuk néhány tipikus bemenet méretét. Ha pl. egy n-pontú, m-élű gráf a probléma bemenete, akkor a bemenet méretének azt tekintjük, hogy hány bittel tudjuk leírni az adott gráfot az algoritmus számára. Láttuk, hogy (egyszerű gráf esetén) a szomszédossági mátrix erre alkalmas, és ehhez nagyjából n^2 bit kell. Ha azonban éllistákkal dolgozunk, akkor a bemenet mérete nagyjából $n + 4m$ lesz, hiszen minden csúcshoz tartozik egy cella, és minden él két csúcs listájában lesz benne, és egy mutató is tartozik a megfelelő listaelemekhez. A fontos észrevétel itt, hogy a gráffal dolgozó algoritmus polinomiális volta nem függ a kétféle megadástól: a lépésszám pontosan akkor korlátozható n^2 egy polinomjával, ha $n + 4m$ egy polinomjával korlátozható. (Itt kell, hogy a gráf egyszerű. Amúgy a szomszédossági mátrix mérete sem n^2 volna.)

Ha az A algoritmus bemeneteként egy k számot kell megadnunk, akkor a binárisan alak mérete $\lfloor \log_2 k \rfloor + 1$ lesz. Ha k-t s alapú számrendszerben adjuk meg, akkor a mérete $\lfloor \log_s k \rfloor + 1$. Itt is hasonló a helyzet: A lépésszáma pontosan akkor korlátozható $\lfloor \log_2 k \rfloor + 1$ egy polinomjával, ha $\lceil \log_s k \rceil$ egy polinomjával korlátozható.

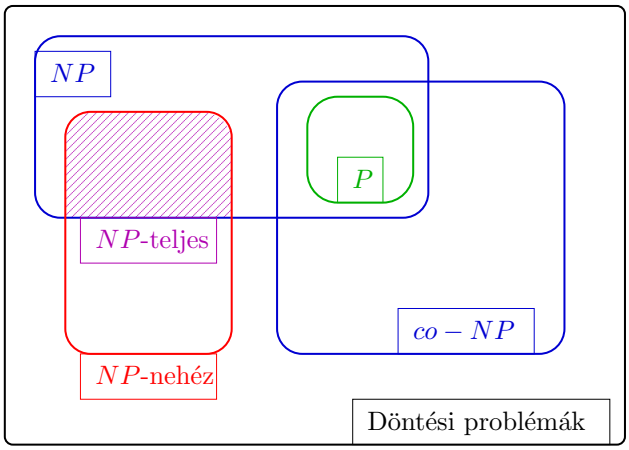
Lássunk ezután néhány P-beli (azaz polinom időben megoldható) problémát. Az Euler-teszt pl. ilyen probléma. Megadunk egy n-csúcsú, m-élű gráfot (a bemenet mérete $n + 4m$), és azt kérdezzük, van-e Euler-kör a gráfban. Korábbi tételünk alapján azt kell ellenőrizni, hogy (izolált pontoktól eltekintve) összefüggő-e a gráf, ill., hogy minden fokszám páros-e. Az utóbbi ellenőrzés $konst \cdot m$ időben elvégezhető, hisz végigmegyünk minden éllistán, és megnézzük, hogy ps hosszú-e. Az összefüggőség ellenőrzéséhez egy mélységi vagy szélességi kereséssel bejárjuk a gráfot. Ha a bejárási fának legfeljebb egy, éleket tartalmazó komponense van, akkor a gráf izolált pontoktól eltekintve öf, így ha az előző teszt is sikeres volt, akkor létezik Euler-kör, egyébként nem. A bejárás lépésszáma legfeljebb $m + n$ konstansszorosa, a bejárási fa ellenőrzése pedig $konst \cdot n$ lépést igényel. Azt kaptuk, hogy az Euler-kör létezésének eldöntésére létezik $konst \cdot (n + m)$ futásidejű algoritmus, aminek lépésszáma tehát a bemenet méretének legfeljebb konstanszorosa, így az Euler-teszt P-beli. Bizonyítható (a számolásokat mellőzzük), hogy az alábbi döntési problémák szintén P-beliek:

- A bemenet által megadott gráf összefüggő-e. (Pl. BFS-sel)
- A bemenet által megadott gráfnak létezik-e k méretű párosítása (azaz létezik-e k ftn él). (Minden élk-ast külön-külön ellenőrizhetünk.)
- A bemenet által megadott hálózatban létezik-e k nagyságú folyam. (Maximális nagyságú folyamot keresünk.)
- A bemenet által megadott PERT problémában elvégezhető-e a feladat legfeljebb k idő alatt. (Optimális ütemezést keresünk.)
- A bemenet által megadott élsúlyozott gráfnak létezik-e legfeljebb k-súlyú feszítőfája. (Kurskal algoritmust futtatunk.)
- A bemenet által megadott gráf síkbarajzolható-e. (Nem is olyan egyszerű.)

Természetesen elképzelhető olyan π döntési probléma, amire nincs polinom idejű algoritmus, sőt, még polinom méretű bizonyíték sincs a helyes válaszra. Persze lehet π olyan is, hogy minden bemenetre létezik a helyes válaszra polinom méretű bizonyíték. A fenti lehetőségekre példa a Hamilton-kör létezésének eldöntése. Ha egy bemeneti gráfra igen a válasz, akkor (bár nem tudunk hatékony algoritmust a Hamilton-kör megkeresésre) ha valaki megmutat egy Hamilton-kört, akkor polinom időben ellenőrizhető, hogy az adott kör Hamilton-kör, vagyis be tudjuk hatékonyan bizonyítani, hogy igen a válasz. Ha azonban nincs a gráfban Hamilton-kör, akkor azt sejtjük, nincs ilyen bizonyíték. Pontosabban: egyes gráfokhoz létezhet, de nem igaz az, hogy *minden* olyan gráfhoz, aminek nincs Hamilton-köre, ez polinom időben bebizonyítható a gráfról.

A fentiek motiválják az alábbi definíciót. NP jelenti az olyan π döntési problémák osztályát, melyekre létezik egy (π-től függő) p_π polinom azzal a tulajdonsággal, hogy π minden egyes olyan b bemenetéhez, melyre *igen* π-re a válasz, ez legfeljebb $p_\pi(|b|)$ lépésben bebizonyítható (itt $|b|$ a b bemenet méretét jelenti). A Hamilton teszt esetén a bizonyíték a Hamilton-kör leírása volt: ennek ismeretében $konst \cdot n$ lépésben demonstrálhatjuk, hogy van a gráfnak Hamilton-köre, azaz bizonyítható az igen válasz.

$co-NP$ jelenti azon π döntési problémák osztályát, amelyekre a fenti tulajdonság azokra a bemenetekre teljesül, amelyekre *nem* a válasz. Figyeljük meg, hogy ha $\pi \in P$, azaz π-re létezik polinomiális algoritmus, akkor $\pi \in NP$ és $\pi \in co-NP$ egyaránt teljesül (azaz $\pi \in NP \cap co-NP$). Létezik ugyanis π-re egy polinom időben futó A algoritmus, és A futása polinom időben bizonyítja az igen vagy a nem választ. Az az általános vélekedés a bonyolultságelméleti szaktekintélyek (a továbbiakban *beszt*-ek) körében, hogy a fenti megfigyelés fordítottja is igaz, azaz ha $\pi \in NP \cap co-NP$, akkor $\pi \in P$.



Például: tetszőleges $G = (A, B; E)$ páros gráf esetén polinom időben be tudom bizonyítani, ha van G-nek teljes párosítása (konkrétan megadom), és azt is, ha nincs (megadok egy $X \subseteq A$ halmazt, melyre $|N(X)| < |X|$), ezért a fentiek szerint kell léteznie polinomiális algoritmusnak, ami eldönti, létezik-e G-ben teljes párosítás (ilyen a már megismert javító utas módszer).

6.5.1. NP-teljesség

Legyen π és π' két döntési probléma, és tegyük fel, hogy π-re létezik egy A algoritmusunk. Elképzelhető, hogy π'-re tudunk olyan A' algoritmust konstruálni, ami felhasználja az A algoritmust, azaz az A' felírja A egy bemenetét, és meghívja A-t. Ha A meghívását egy lépésnek számítva A' egy polinomiális lépésszámú algoritmus, akkor azt mondjuk, hogy a π' probléma *(polinomiálisan) visszavezethető* a π problémára.

6.3. Megfigyelés *Ha a π'' döntési probléma polinomiálisan visszavezethető a π' problémára, és π' polinomiálisan visszavezethető a π problémára, akkor π'' polinomiálisan visszavezethető π-re is.*

Bizonyítás. Tudjuk, hogy π'-re létezik olyan A' algoritmus, ami egyszer meghív egy π-t megoldó A algoritmust, és ezen kívül A' polinomiális számú lépést végez. Azt is tudjuk, hogy π''-re létezik egy olyan A'' algoritmus, ami egyszer meghívja A'-t, és ezen kívül csak polinomiális számú lépést végez.

Ám az A'' algoritmus úgy is felfogható, mint egy olyan algoritmus, ami egyszer meghívja az A algoritmust. Az kell belátnunk, hogy A'' ebben az értelmezésben is (A hívásától eltekintve) csak polinomiálisan sok lépést végez (az b'' bemenet méretének függvényében). Világos, hogy az A' hívásán kívüli lépések száma legfeljebb polinomja $|b''|$-nek. Ezért A' meghívásakor az A'-re konstuált b' bemenet mérete is polinomja lesz $|b''|$-nek. Nekünk A' azon lépéseit, amelyek nem az A hívásából adódnak szintén be kell számolnunk A'' lépései köze. Ezen lépések száma $|b'|$ polinomja a visszavezetés definíciójából

adódóan. Azonban $|b'|$ polinomja egyúttal $|b''|$ polinomja is, hisz polinomok egymásba helyettesítése továbbra is polinom.

Azt kaptuk, hogy A hívásától eltekintve A'' polinomiális számú lépést végez, tehát π'' csakugyan polinomiálisan visszavezethető π-re. □

6.4. Állítás *Ha π' visszavezethető π-re és $\pi \in P$, akkor $\pi' \in P$.*

Bizonyítás. Legyenek A és A' a polinomiális visszavezetés definíciójában szereplő algoritmusok. Feltehetjük, hogy A polinomiális. Vegyük észre, hogy az A' algoritmus úgy is polinomiális lesz, ha A meghívását nem egy lépésnek vesszük, hanem becsületesen beszámítjuk az A által végzett lépéseket is. Az A algoritmust ugyanis olyan b bemenettel hívjuk meg, amit a π' probléma b' bemenetméretének polinomja számú lépésben kapunk, ezért $|b|$ a $|b'|$ polinomja. Az A lépésszáma pedig $|b|$ polinomjával becsülhető, de $|b|$ polinomja egyúttal $|b'|$ polinomja is, hisz polinomok kompozíciója (egymásba helyettesítése) is polinom.

Márpedig ha A' „rendesen számolva" is polinomiális számú lépést végez, akkor $\pi' \in P$ teljesül. □

Azt kaptuk tehát, hogy ha egy π' döntési problémát sikerül polinomiálisan visszavezetni egy P-beli problémára, akkor π' is P-beli. Némileg leegyszerűsítve azt mondhatjuk, hogy ha π' visszavezethető π-re, akkor π' nagyjából hasonló hatékonysággal eldönthető, mint π. Nem zárható ki persze, hogy π'-re létezik még hatékonyabb eljárás, de azt biztosan mondhatjuk, hogy ha π' visszavezethető π-re, akkor (bizonyos értelemben) π nehezebb probléma, mint π' . (Itt legyünk észnél. Ezt rendszeresen halljuk fordítva a vizsgákon. Tehát a könnyebb feladatot tudjuk a nehezebb megoldásának ismeretében megoldani, és nem fordítva.)

6.5. Definíció *Egy π döntési problémát NP-*nehéznek *mondunk, ha bármely NP-beli π' probléma polinomiálisan visszavezethető π-re. Ha $\pi \in NP$ is teljesül, akkor π-t NP-*teljesnek *nevezzük.*

Az eddigiek fényében világos, hogy ha egy NP-nehéz problémára létezne polinomiális algoritmus, akkor abból $P = NP = co - NP$ következekezne. A besztek azt gondolják, hogy ez utóbbi következtetés nem igaz, tehát egyetlen NP-nehéz problémára sem létezhet polinomidejű algoritmus. Ha egy NP-nehéz π' problémát sikerül egy NP-beli π problémára visszavezetni, akkor azzal igazoltuk, hogy π NP-teljes. (Ugyanis bármely NP-beli probléma visszavezethető π'-re, π' pedig π-re, azaz bármely NP-beli probléma π-re is visszavezethető.) Nem világos persze ezen a ponton, hogy vajon létezik-e egyáltalán NP-nehéz (hát még NP-teljes) probléma. Ez utóbbi kérdésre szerencsére ismert a válasz.

6.6. Tétel (Cook és Levin, 1971) *A SAT probléma NP-teljes.*□

A SAT probléma F bemenete egy speciális Boole-formula egy ú.n. *konjunktív normálforma*, ami a következőt jelenti. Ha F egy konjunktív normálforma, akkor F tagokból

áll, melyek egymással „és” kapcsolatban állnak. F minden egyes tagja néhány változóból ill. azok tagadásából áll, melyek közt „vagy” kapcsolat van. Egy konjunktív normálforma pl. az $(x \vee y \vee \bar{z}) \wedge (\bar{x} \vee a \vee \bar{b}) \wedge (\bar{y} \vee a \vee \bar{c} \vee z)$. A SAT problémát megoldó algoritmus kimenete arra válaszol, hogy vajon kielégíthető-e az F formula, azaz megválaszthatók-e az egyes logikai változók értékei úgy, hogy azokat F-be helyettesítve a kiértékelés „igaz” lesz.

A Cook-Levin tétel alapján már „könnyű” NP-teljes problémát találni: ha egy NP-beli π problémára sikerül visszavezetni a SAT-ot (vagy egy, a SAT segítségével már NP-teljesnek bizonyított problémát), akkor π is NP-teljes. Miért hasznos, ha tudjuk egy π problémáról, hogy NP-teljes? Természetesen azért, mert attól a ponttól kezdve, hogy ez bebizonyosodott, nem érdemes azzal küzdeni, hogy π-re P-beli algoritmust találjunk. (Már amennyiben elhisszük a $P \neq NP$ dogmát. Ha ebben nem hiszünk, akkor elegendő a számos lehetőség közül egyetlen NP-teljes problémára polinomiális algoritmust találni. Ezáltal a dogma rögtön megdől, egy életre híresek és gazdagok leszünk, hátralévő éveinkben csupán a tudományos díjakat kell egymás után a vitrinbe passzíroznunk, és postaládánkból rendszeresen kisöpörni a környegyszögesítő és szögharmadoló önjelöltek leveleit.)

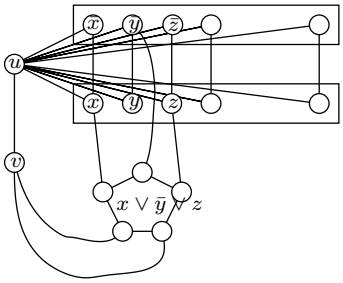
A továbbiakban tehát különféle problémák NP-teljességét fogjuk más problémák NP-teljességére visszavezetni, ezáltal egyfelől választékot biztosítunk a modernkori környegyszögesítőknek, másrészt pedig a tekintélyelvű dogmahívőket beszéljük le bizonyos feladatokat megoldó polinomidejű algoritmus kereséséről.

Nézzünk tehát konkrét döntési problémákat. A k-SAT probléma a SAT probléma speciális esete. A k-SAT bemenete csak olyan konjunktív normálforma lehet, aminek bármely tagjában összesen legfeljebb k (ponált vagy negált) változó van összesen. Könnyen látható, hogy a 2-SAT (és így az 1-SAT is) eldönthető polinom időben. Viszont a SAT probléma polinomiálisan visszavezethető a 3-SAT-ra (nem bizonyítjuk), ami azt jelenti, hogy a 3-SAT is NP-teljes. A 3-SZÍN probléma bemenete egy G gráf, a kimenete pedig válasz arra, hogy G vajon 3-színezhető-e. Az alábbi tétel lényege, hogy a 3-SZÍN probléma is NP-teljes.

6.7. Tétel *3-SZÍN*$\in NP$ *és a* 3*-SAT polinomiálisan visszavezethető a* 3*-SZÍN problémára.*

Bizonyítás. A 3-SZÍN probléma azért NP-beli, mert az igen válasz (hogy G valóban 3-színezhető) polinom időben bebizonyítható: egyszerűen megadjuk G csúcsainak egy 3-színezését.

Az F 3-SAT formulából készítsünk egy G_F gráfot: ebben minden x változónak két, egymással összekötött csúcs felel meg: egy x ill. egy $\bar{x}$. Van még a G_F gráfnak egy u csúcsa, ami minden változóhoz tartozó csúccsal össze van kötve, ill. u-nak van egy további v szomszédja is. F minden tagjának egy ötszög felel meg (az ábrán az $x \vee \bar{y} \vee z$-nek megfelelő látható), v össze van kötve az ötszög két szomszédos csúcsával, a másik három csúcs pedig a tagokban szereplő változóknak megfelelő csúcsokkal van összekötve.



Figyeljük meg, hogy a G_F gráf (mint input) mérete felülről becsülhető az F formula méretének polinomjával, sőt, G_F el is készíthető F-ből polinom időben. Megmutatjuk, hogy G_F pontosan akkor 3-színezhető, ha F kielégíthető. Tegyük fel, hogy F kielégíthető. Színezzünk zöldre egy x változónak megfelelő csúcsot, és pirosra a $\bar{x}$ csúcsot, ha a x kiértékelése igaz, egyébként legyen x piros és $\bar{x}$ zöld. Legyen továbbá u fehér és v piros. Ekkor a tagoknak megfelelő ötszögek kivételével minden ki van színezve. Minden ötszög kiszínezhető, hiszen az alsó két csúcsán tiltott szín a piros, a felső csúcsai között pedig van egy olyan, melyre a zöld a tiltott szín (hisz F kiértékelése igaz). Van tehát két olyan szoszmédos (mondjuk p és q) csúcsa az ötszögnek, amelyek kiszínezésére nem ugyanaz a két szín áll rendelkezésre. Színezzük ki p-t egy olyan színnel, amit nem használhatunk q-hoz, majd p-nek a q-tól különböző szomszédjától indulva, színezzük ki sorra a csúcsokat. Mindig ki tudjuk színezni a soron következő csúcsot, hisz két szín áll rendelkezésre, amiből az előzőnek színezett csúcs színét nem használhatjuk. Végül q-t is kiszínezhetjük, hisz nem fenyeget az a veszély, hogy p színét használnánk.

Ha G_F 3-színezhető, akkor feltehetjük, hogy u fehér és v piros. Ekkor minden változó és tagadása a zöld és piros színek egyikét kapja. Minden ötszögben az alsó két pont színe tehát zöld és fehér, ezért az ötszög felső 3 csúcsa között lesz olyan, melynek a színe piros. E csúcs szomszédja csakis zöld lehet. Tehát ha a zöld színek szerint értékeljük ki a változókat, akkor minden tagban lesz igaz változó, vagyis a kiértékelés igaz lesz. □

A k-SZÍN probléma bemenete egy G gráf, és a kimenet válasz arra a kérdésre, hogy G k-színezhető-e. Megmutatjuk, hogy a k-SZÍN probléma is NP-teljes.

6.8. Tétel *Ha $k > 3$, akkor a k-SZÍN$\in NP$ és a 3-SZÍN polinomiálisan visszavezethető a k-SZÍN problémára.*

Bizonyítás. Ha az adott G k-színezhető, akkor a k-színezés ismeretében ez polinom időben bizonyítható, tehát a probléma valóban NP-beli.

Legyen G a 3-SZÍN probléma bemenete. Vegyünk $k-3$ új pontot G-hez, és kössük össze azokat G minden pontjával és egymással. Ezáltal kapjuk a G' gráfot. Világos, hogy ha G 3-színezhető, akkor G' k-színezhető, hiszen az új pontok mindegyike kaphat egy új színt. Ha pedig G' k-színezhető, akkor az új pontok páronként különböző színt kapnak, és ezek a színek a G-re használt színektől is különbözők kell, hogy legyenek. Vagyis G kiszínezésére összesen 3 szín marad.

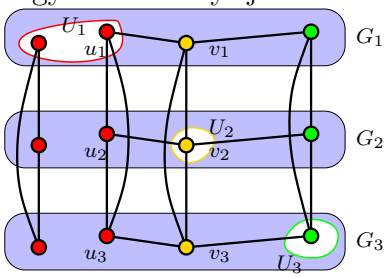
Mivel G' konstrukciója a G ismeretében G méretének polinomjával becsülhető számú lépésben megvalósítható, ezért a 3-SZÍN probléma polinomiálisan visszavezethető a k-SZÍN problémára. □

A következőnek bizonyított NP-teljes probléma a MAXFTN. Ennek bemenete egy G gráf és egy k szám, a kimenet arra válasz, hogy van-e G-nek k független csúcsa.

6.9. Tétel *A MAXFTN probléma NP-beli, és a 3-SZÍN polinomiálisan visszavezethető a MAXFTN-re.*

Bizonyítás. Ha mutatunk G-ben k független pontot, akkor azzal polinom időben be lehet bizonyítani, hogy „igen” a válasz a döntési problémára, tehát MAXFTN$\in NP$.

A polinomiális visszavezetéshez legyen az n-csúcsú G gráf a 3-SZÍN bemenete. Készítsük el a G' gráfot, mely 3, diszjunkt gráfból áll (mondjuk G_1, G_2 és G_3-ból), mindegyik G_i a G-vel izomorf, továbbá G_i és G_j egymásnak megfelelő pontjait összekötjük. Megmutatjuk, hogy G'-nek pontosan akkor létezik n méretű független ponthalmaza, ha G 3-színezhető. Mivel G' polinom idő alatt elkészíthető G-ből, ezért ha ezt igazoljuk, azzal csakugyan bebizonyítjuk a tétel második részét.



Tegyük fel, hogy G'-ben U egy n méretű független csúcshalmaz. Ekkor $U \cap V(G_1)$, $U \cap V(G_2)$ és $U \cap V(G_3)$ mindegyike a G gráf egy-egy független ponthalmazának felel meg. Legyenek ezek a ponthalmazok U_1, U_2 és U_3. A G' konstrukciója miatt e három halmaz diszjunkt, és mivel összesen n csúcsot tartalmaznak, együttesen fedik a teljes $V(G)$ csúcshalmazt. Ha tehát U_i pontjait az i-dik színnel színezzük ($i = 1, 2, 3$), akkor G egy 3 színnel való kiszínezését kapjuk.

Másfelől, ha G 3-színezhető, akkor csúcsai felbomlanak 3 színosztályra (mondjuk U_1, U_2 és U_3-ra), melyek mindegyike független. Tekintsük az U_i-nek megfelelő pontokat G_i-ben. Ezek önmagukon belül, és egymáshoz képest is függetlenek G'-ben, ezért az így kapott U halmaz a G' egy n csúcsból álló független ponthalmaza. □

6.10. Megjegyzés *A 2-SZÍN probléma P-beli, hiszen egy gráf pontosan akkor 2-színezhető, ha páros, és ez utóbbi polinom időben eldönthető. A fenti bizonyításhoz hasonlóan igazolható, hogy a 2-SZÍN probléma visszavezethető a 3-SZÍN problémára, ami NP-teljes. Márpedig ha $P \neq NP$, akkor a 2-SZÍN nem NP-teljes. Látjuk tehát, hogy ahhoz hogy egy π (NP-beli) probléma NP-teljességét bizonyítsuk, egy NP-teljes problémát kell π-re kell visszavezetni, és nem fordítva.*

A MAXKLIKK probléma bemenete egy G gráf és egy k szám, a kimenet pedig azt mondja meg, van-e G-ben k méretű klikk (azaz teljes részgráf). Természetesen ez a probléma is NP-teljes.

6.11. Tétel *A MAXKLIKK probléma NP-beli, és a MAXFTN visszavezethető rá.*

Bizonyítás. Mivel egy k-méretű klikk megadása után polinom időben bizonyítható, hogy az adott pontok G-ben klikket alkotnak, ezért $MAXKLIKK \in NP$.

Világos, hogy a G gráfból polinom időben elkészíthető a $\overline{G}$ komplementergráf. Mivel G-ben pontosan akkor van k méretű független ponthalmaz, ha $\overline{G}$-ben van k méretű klikk, ezért a MAXFTN csakugyan visszavezethető a MAXKLIKK problémára. □

A HAM probléma bemenete egy G gráf, és a kimenet arra a kérdésre válaszol, van-e Hamilton kör G-ben. Világos, hogy HAM$\in NP$, hisz a konkrét Hamilton kör megadása egy bizonyíték az igen válaszra. Itt nem bizonyítjuk, de lehetséges az NP-teljes 3-SAT problémát polinomiálisan a HAM problémára visszavezetni, tehát a továbbiakban felhasználhatjuk, hogy a HAM probléma is NP-teljes. Ebből pl azonnal következik, hogy ha a $P = NP \cap co - NP$ és a $P \neq NP$ sejtések igazak, akkor HAM$\notin co - NP$, azaz a Hamilton kör nemlétezésére nem várható polinomiális bizonyíték, más szóval a Hamilton kör létezésére nincs jól használható szükséges és elégséges feltétel.)

A HAMÚT probléma bemenete egy G gráf, és a kimenet megmondja, van-e G-nek Hamilton útja. A MAXÚT probléma a beadott G gráfról és k számról kérdezi, van-e G-ben k hosszú út. A RÉSZGR probléma a bemenetben megadott G és H gráfokról kérdezi, létezik-e G-nek H-val izomorf részgráfja. Megmutatjuk, hogy az utóbbi 3 probléma mindegyike NP-teljes.

6.12. Tétel *A HAMÚT, RÉSZGR és MAXÚT problémák mindegyike NP-teljes.*

Bizonyítás. Belátjuk, hogy mindhárom probléma NP-beli és hogy a HAM probléma a három probléma bármelyikére visszavezethető. Az NP-beliséghez csupán azt kell látni, hogy ha egy n-pontú gráfban létezik Hamilton út, ill. k hosszú út, akkor egy ilyen út leírható n-ben polinomiális számú bittel, és egy ilyen leírásról is eldönthető n-ben polinomiális számú lépésben, hogy valóban Hamilton utat ill. legalább k hosszú utat adtunk-e meg. A RÉSZGR probléma NP-belisége abból következik, hogy a G gráf H-val izomorf részgráfja, és maga az izomorfia együttesen is leírható n-ben polinomiális számú bittel, és polinom időben eldönthető, hogy egy leírás helyes-e, azaz csakugyan egy részgráfot ad-e meg, melyre izomorf H-val a megadott leképezés szerint.

Hátra van, hogy a HAM problémát külön-külön visszavezessük a három probléma mindegyikére. Ezt úgy tesszük meg, hogy tetszőleges G (n-pontú) gráf esetén n-ben polinomiális számú lépésben elkészítjük a G_1, G_2, G_3 ill. H_3 gráfokat továbbá meghatározzuk a k_2 számot úgy, hogy az alábbi négy állítás ekvivalens legyen.

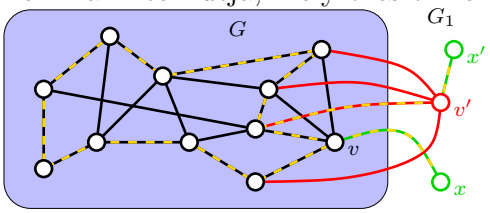
1. G-nek létezik Hamilton köre

2. G_1-nek van Hamilton útja.

3. G_2-nek létezik legalább k_2 hosszúságú útja

4. G_3-nak létezik H_3-mal izomorf részgráfja.

G_1 konstrukciójához legyen v a G egy tetszőleges pontja. Vegyünk fel egy új, v' pontot, és kössük össze v minden szomszédjával (néha ezt az operációt v klónozásának hívják). Vegyük fel még az x és x' új pontkat és húzzuk be az xv ill. $x'v'$ éleket. Legyen a kapott gráf G_1. Világos, hogy ha G-nek van Hamilton köre, akkor létezik x és x' között G_1-nek Hamilton útja, mely v és v' között lényegében a Hamilton kört járja végig.



Másrészt, ha G_1-ben van Hamilton út, akkor az bizonyosan x és x' között vezet, és az út v és v' közti része G-ben egy Hamilton kört határoz meg. Láttuk tehát, hogy (1) $\Longleftrightarrow$ (2).

Legyen $G_2 := G_1$, és $k_2 := n$, a G_1 pontszáma. Ezzel a választással a (2) és (3) állítás pontosan ugyanazt jelenti. Végül legyen $G_3 := G$, és $H_3 := C_n$. Ezzel a választással azt kell eldönteni, hogy G-ben létezik-e n-pontú kör, azaz Hamilton kör. Tehát HAM probléma a RÉSZGR problémára is visszavezethető. □

6.5.2. Nehéz problémák megoldása a gyakorlatban

A gyakorlatban előforduló problémák megoldásakor nagyon gyakran derül ki, hogy a megoldáshoz használt modellben egy NP-teljes problémát kell megoldanunk. Mégsem tárhatjuk szét a kezünket, valamiféle megoldást kell találnunk, mégpedig belátható időn belül. Sokszor segít az alábbi módszerek valamelyike:

1. Lehetséges, hogy az általunk megoldandó probléma nem annyira általános, mint a modellünk, azaz minket csak az NP-teljes probléma egy speciális esete érdekel, amire esetleg lehet polinomidejű algoritmus. Ha pl egy gráfban kell maximális méretű független halmazt keresnünk, elejét veheti a fejfájásnak, ha kiderül, hogy valójában csak páros gráfok kerülhetnek elő az inputban.

2. Ha ez nem segít, akkor érdemes lehet azon elgondolkodni, hogy tényleg olyan nagy baj-e az exponenciális futásidő. Ha szerencsénk van, akkor a számunkra érdekes inputon az algoritmus még belátható időn belül végez. Ha mégsem, akkor érdemes lehet az egy másik exponenciális futásidejű algoritmust keresni, ahol az exponens kisebb, így az inputméret növekedtével a futásidő lassabban növekszik, és talán

mégis megoldhatóvá válik a probléma. A gráf maximális méretű független ponthalmazának meghatározására van a minden részhalmazt megvizsgáló 2^n futásidejű algoritmusnál gyorsabb, ami kb $1,3^n$ lépésben végez.

3. A fenti módszernek egy kifinomultabb változata, amikor az algoritmus lépésszámát nem egyszerűen az input méretének függvényében keressük, hanem igyekszünk olyan inputtól függő paramétert (vagy paramétereket) találni amely az általunk megoldandó problémák esetén nem túl nagy. Ezek után az a cél, hogy olyan algoritmust konstruáljunk, amelynek a legrosszabb esetbeli lépésszámát úgy tudjuk az inputméret és a választott paraméterek segítségével felírni, hogy az inputmérettől való függés polinomiális, és ne exponenciális legyen. Természetesen a paraméter(ek)től való függés ilyenkor lehet exponenciális. Ha ezt sikerül elérni, akkor az azért szerencsés, mert az olyan inputokra, amelyekre a paraméter értéke rögzített (vagy korlátos), de minden esetre nem túl nagy, az algoritmus lépésszáma az inputméret polinomjával felülről becsülhető.

   Egy lehetséges példa a CSÚCSFEDÉS, ami a MAXFTN probléma rokona. Míg az utóbbi problémában az a kérdés, hogy a G inputgráfnak van-e k független csúcsa, itt azt kérdezzük, hogy található-e az inputgráfnak k csúcsa úgy, hogy azok komplementere G-ben független ponthalmaz legyen. Könnyen látható, hogy a CSÚCSFEDÉS probléma is NP-teljes, azonban könnyen adható rá olyan algoritmus, amelyek lépésszáma a G inputgráf méretében polinomiális, k-ban pedig exponenciális a következőképpen. Legyenek $e = uv$ a CSÚCSFEDÉS(G, k) probléme G inputgráfjának egy éle. Ha G üresgráf, akkor „igen” a válasz. Különben rekurzív módon oldjuk meg a CSÚCSFEDÉS$(G-u, k-1)$ ill. CSÚCSFEDÉS$(G-v, k-1)$ problémákat. Ha mindkét esetben „nem” a válasz, akkor az eredeti problémára is ez lesz, ám ha valamelyikre „igen”-t kapunk, akkor a CSÚCSFEDÉS(G, k)-ra is „igen” lesz a válasz. Indukcióval pedig könnyen látható, hogy a CSÚCSFEDÉS(G, k) lépésszáma felülről becsülhető $2^k \cdot p(n)$-nel, ahol n a G inputgráf csúcsainak száma, p pedig egy alkalmas polinom.

4. Persze lehetséges, hogy a fenti módszerek egyike sem hozza meg a kívánt eredményt. Elgondolkodhatunk: valóban olyan nagy baj, ha nem végez az algoritmus időben? (Atomerőműirányításnál hessegessük el ezt a gondolatot.) Mert ha nem, akkor lehet, hogy az algoritmusunknak bár a néhány szerencsétlen inputon elszáll, a gyakorlati esetek döntő többségében igen gyorsan végez. Példa erre a lineáris programozási feladatot megoldó szimplex algoritmus, ami a gyakorlatban sokkal jobb, mint amit a legrosszabb esetre vonatkozó becslés mutat.

5. Ha semmi sem segít, akkor azon morfondírozhatunk, hogy vajon csakugyan optimális megoldást kell-e találnunk az adott inputhoz. Lehet, hogy képesek vagyunk belátható időn belül az optimálisnál csak pár százalékkal rosszabb megoldással

előrukkolni, és ez a hiba még elviselhető. Ha egy egyszerű G gráf éleit kell kiszíneznünk, akkor NP-teljes annak eldöntése $\Delta(G)$ vagy $\Delta(G)+1$ szín kell-e, de $\Delta(G)+1$ színnel a színezés elég gyorsan végrehajtható.

Egy másik példa a ládapakolási feladat, aholis $a_1, a_2, \ldots, a_k$ térfogatú tárgyakat kell ládákba pakolni úgy, hogy minden ládába csak egységnyi össztérfogat rakható, és mindehhez a lehető legkevesebb ládát kellene felhasználni. (Ehhez hasonló problémával a költözéskor találkozunk, a nehézséget csak fokozza, hogy különböző méretűek a ládák.) Ismert, hogy annak eldöntése, hogy l láda elegendő-e NP-teljes. Azonban ha nem baj, hogy egykét ládával több kell, akkor van jó közelítés. Ha a tárgyaknak sorban egymás után találjuk meg a helyét, mégpedig úgy, hogy az első olyan ládába pakoljuk, amibe belefér, akkor legfeljebb 70%-kal több láda kell, mint az optimum. (Ez az ú.n. FF (first fit) algoritmus.) Ha ráadásul a tárgyakat csökkenő térfogat szerint vesszük egymás után az FFD (first fit decrease) algoritmus szerint, akkor garantáltan nem használunk több ládát, mint az optimálisan szükséges ládák számának $1,22$-szerese.

6. Ha már végképp semmi sem segít, akkor megpróbálkozhatunk heurisztikákkal. Ekkor nem fogunk optimális megoldást kapni, és garancia sem lesz arra nézve, hogy a megoldás az optimum közelében van. Mégis kapunk valamiféle megoldást, ami akár elfogadható is lehet. A heurisztikus algoritmusoknak komoly irodalma van, és ezeket különféle általánosan elfogadott adatokon (benchmark-okon) versenyeztetik. Időnként úgy tűnhet, a megfelelő heurisztika megtalálása inkább művészet, mint tudomány, de az eredmény ennek ellenére nagyon hasznos lehet egy-egy gyakorlati probléma megoldásakor.

Persze vannak olyan feladatok, ahol a fentiektől gyökeresen eltérő megközelítés vezethet célhoz, és végül olyan feladat is létezik, amire nem ismert kellően hatékony algoritmus.

6.6. A kriptográfia alapjai és az RSA

6.6.1. Prímtesztelés

Egy adott $n \in \mathbb{N}$ számról kell eldöntenünk, hogy prím-e. A bemenet mérete $\log n$, ennek polinomja lehet a lépésszám. Nem polinomiális tehát sem az erathosztenészi szita (lépésszáma n-ben lineáris, ami $\log n$-ben exponenciális), sem a naív módszer (ebben 1-től $\sqrt{n}$-ig ellenőrizzük az oszthatóságot $\sqrt{n}$-ben lineáris számú osztással).

A prímtesztelés kemény dió. Létezik ugyan rá olyan determinisztikus algoritmus, ami egyúttal polinomiális is, de ilyet csak a legutóbbi időben találtak. Ehelyett mutatunk egy sokkal gyakorlatibb módszert, aminek az a hibája, hogy nem ad halálbiztos eredményt. Megengedjük ugyanis a véletlen választást is az algoritmus futása során, amiből

az következik, hogy az eljárás nem lesz tévedhetetlen. A módszer azonban csak egy irányban tévedhet, azaz egy prímet sosem mond összetettnek de egy összetett számot esetleg („csillagászatian" kis valószínűséggel) prímnek gondolhat. A teszt alapja az Euler-Fermat tétel. Eszerint, ha egy n szám prím, akkor $k^{n-1} \equiv 1(n)$ minden $(k,n) = 1$ esetén. Ha tehát $(k,n) = 1$ és $k^{n-1} \not\equiv 1(n)$, akkor bizonyosan tudjuk, hogy n összetett, jóllehet, n egyetlen osztóját sem ismerjük. Az ilyen k számot az n szám *árulójának* nevezzük, hisz segítségével megtudtuk hogy n nem prím. Egy másik lehetőség n összetettségéről meggyőződni, hogy találunk egy olyan $0 < k < n$ számot, amire $(k,n) \neq 1$. Ekkor az euklideszi algoritmus az n egy valódi osztóját is megtalálja, ezért k még további információt ad n-ről. Az ilyen k számok az n *leleplezői*. Akárcsak a árulókra, a leleplezőkre is igaz hogy $k^{n-1} \not\equiv 1 \pmod{n}$, hiszen k^{n-1} nem relatív prím n-hez ha k sem volt az, tehát nem lehet a redukált maradékrendszer eleme sem.

Persze az is megtörténhet, hogy n összetett, és egy $0 < k < n$ számra $k^{n-1} \equiv 1(n)$ áll. Ekkor k az n *cinkosa*, hisz nem árulja el, hogy n összetett. Igaz viszont, hogy ha van áruló, akkor az $1, 2, \ldots, n-1$ számok között legalább annyi áruló van, mint cinkos (és akkor a leleplezőkről még nem is beszéltünk).

6.13. Állítás *Ha $1 \leq c_1 < c_2 < \ldots < c_l < n$ az n szám cinkosai, és a az n egy árulója, akkor $ac_1, ac_2, \ldots ac_l$ az n szám páronként (modulo n) különböző árulói.*

Egyébként a 6.13. Állításnál jóval több igaz: a modulo n redukált maradékrenszer a szorzásra csoportot alkot (ez volt a $\mathbb{Z}_n^*$ csoport), aminek cinkosok részcsoportját alkotják. Ha van áruló, akkor a részcsoport indexe legalább 2, így a részcsoport mérete legfeljebb fele a csoporténak. A szükséges fogalmakat a csoportelmélet résznél tárgyaltuk.

Bizonyítás. Ha $ac_i \equiv ac_j(n)$, akkor $(a,n) = 1$ miatt $c_i \equiv c_j(n)$, azaz $c_i = c_j$, tehát az $ac_1, ac_2, \ldots ac_l$ számok valóban különböző maradékosztályokból valók. Mivel $c_i^{n-1} \equiv 1(n)$ és $a^{n-1} \not\equiv 1(n)$, ezért $(ac_i)^{n-1} = a^{n-1}c_i^{n-1} \equiv a^{n-1} \not\equiv 1(n)$, tehát a fenti számok csakugyan árulók. □

A prímtesztelésre egy lehetséges módszer tehát a következő. Véletlenül választunk egy $0 < k < n$ számot. Ha k árulója vagy leleplezője n-nek, azaz $k^{n-1} \not\equiv 1 \pmod{n}$, akkor kész vagyunk, n összetett. Ha k cinkos, akkor n-ről azt valószínűsítjük, hogy prím. Ezen az elgondoláson alapszik a *Fermat-teszt*.

Persze a Fermat-teszt hibázhat, de az előző állítás szerint a hibája csak az lehet, hogy egy összetettet számot prímnek mond. Ráadásul, ha n-nek van árulója, akkor a hiba valószínűsége legfeljebb $\frac{1}{2}$. Ha tehát m-szer választunk (egymástól független) véletlen számokat, akkor a hiba valószínűsége legfeljebb $\frac{1}{2^m}$ lesz, ami már $m = 100$-ra is elhanyagolható a hardverhibából eredő tévedés valószínűségéhez képest. Jegyezzük meg, hogy a többször (mondjuk 100-szor) megismételt Fermat-teszt polinomiális számú, polinomiális időben elvégezhető lépést használ.

Van azonban a Fermat-tesztnek egy hibája. Csak akkor működik, ha n-nek létezik árulója. Sajnos léteznek olyan számok (az ú.n. *álprímek*, vagy más néven *Carmichael*

Fermat-teszt

Bemenet: $n \in \mathbb{N}$. Kimenet: döntés, hogy n prím-e

begin

Legyen $0 < k < n$ véletlen szám

if $k^{n-1} \not\equiv 1(n)$ **then STOP:** n nem prím.

else STOP: úgy tűnik, n prím

end if

end

---

számok), amelyeknek csak cinkosai és leleplezői vannak (utóbbiak elenyésző számban). Az ismételt Fermat-teszt ezeket a számokat majdnem biztosan prímnek találja. Olyan módszert szeretnénk tehát, ami a mégoly ritka álprímekre is teljesen megbízhatóan működik. A Fermat-teszt a fő lépésében azt ellenőrzi, vajon teljesül-e, hogy $n \mid k^{n-1}-1$. Ha ugyanis n prím, akkor ez minden $0 < k < n$-re teljesül. Ennél azonban több is igaz. Ha t.i. $n-1 = 2^t \cdot q$, ahol q páratlan, akkor az $(x+y)(x-y) = x^2 - y^2$ azonosság többszöri alkalmazásából az adódik, hogy

$$k^{n-1} - 1 = k^{2^t q} - 1 = (k^{2^{t-1}q} - 1)(k^{2^{t-1}q} + 1) = (k^{2^{t-2}q} - 1)(k^{2^{t-2}q} + 1)(k^{2^{t-1}q} + 1) = \ldots =$$
$$= (k^q - 1) \cdot (k^q + 1)(k^{2q} + 1)(k^{4q} + 1) \cdots (k^{2^{t-1}q} + 1) \; . \qquad (6.1)$$

Tehát ha $n = p$ prím, akkor p a 6.1 jobboldalának valamelyik tényezőjét is osztja. Hiába osztható tehát a baloldal n-nel: ha a jobboldal egyetlen tényezője sem n többszöröse, akkor n bizonyosan összetett, és k az n szám egy *Carmichel értelemben vett árulója*. (Figyeljük meg, hogy ha k cinkos, de Carmichael értelemben vett áruló, akkor a 6.1 jobboldalán álló tényezők valamelyike leleplező, így az Euklideszi algoritmussal megtalálható n egy osztója is.)

Igaz, hogy minden összetett szám redukált maradékrendszerének legalább $\frac{3}{4}$-edrésze Carmichael értelemben vett áruló. Ezért a 6.1 jobboldalán álló szorzat tényezőinek n-nel való oszthatóságát vizsgáló *Miller-Rabin teszt* egy összetett számról legalább $\frac{3}{4}$ valószínűséggel azonnal megállapítja, hogy nem prím.

A Miller-Rabin tesztet függetlenül választott véletlen számokkal 50-szer megismételve a hiba valószínűsége gyakorlatilag 0-ra csökken. A Miller-Rabin teszt hatékonyságáról érdemes megemlíteni, hogy sokkal jobb, mint amit az elméleti becslés garantál: mindössze egyetlen olyan összetett szám van 1 és $2,5 \cdot 10^{10}$ között, aminek $k = 2, 3, 5, 7$ mindegyike Carmichael-cinkosa. Az összes többi összetett szám kiszűrhető négy Miller-Rabin teszt elvégzésével a fenti k értékekre.

6.6.2. Nyilvános kulcsú titkosírások

A nyilvános kulcsú titkosírás az egyirányú függvény létezésére épít. A pontos definíció helyett nagyjából azt lehet mondani, hogy *egyirányú függvénynek* nevezünk egy

Miller-Rabin teszt

Bemenet: $n \in \mathbb{N}$. Kimenet: döntés, hogy n prím-e

begin

Legyen $0 < k < n$ véletlen szám

if $k^q \equiv 1(n)$ **then STOP:** n vszg prím.

else i:=0, **loop while** i<t

if $k^{2^i q} \equiv -1(n)$ **then STOP:** n vszg prím

else i:=i+1; **end if**

end loop

end if

STOP: n nem prím.

end

$f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ függvényt, ha f bijekció, mely hatékonyan (azaz polinomidejű algoritmusok felhasználásával, a gyakorlatban is gyorsan) számítható, azonban a fordított irányú f^{-1} leképezés kiszámítása pusztán f ismeretében reménytelen. (Pl. ha megvan a telefonkönyv, akkor egy adott személyhez hamar telefonszámot tudok rendelni, de egy telefonszámhoz az előfizető megtalálása már korántsem ilyen hatékony csupán a telefonkönyvben bogarászva). Elképzelhető, hogy f egyirányú függvény, és f^{-1} is kiszámítására is létezik hatékony eljárás. Persze ennek megtalálása pusztán f ismeretében (az egyirányúság definíciója szerint) reménytelen. Utóbbi függvényeket nevezzük *kiskapus egyirányú függvényeknek*. Rossz hír, hogy bár a nyilvános kulcsú titkosírási rendszerek biztonsága a kiskapus egyirányú függvények létezésére épít, nem tudjuk teljes bizonyossággal, vajon csakugyan léteznek-e kiskapus egyirányú függvények. Vannak azonban függvények, melyekről azt *sejtjük*, hogy ilyenek, de bebizonyítani ezt nem tudjuk. (Így aztán mindig van min dolgozniuk a rejtjelfejtő szakembereknek.)

Egy titkosírási rendszernél rögzítünk egy Σ-val jelölt ABC-t: ennek a jeleivel írjuk le az üzeneteinket. A kódolandó M üzenetről (M, mint message) feltehető, hogy t betűből áll, azaz $M \in \Sigma^t$, hiszen a hosszabb üzenetet t hosszúságú blokkokra vághatjuk, és minden blokkot külön üzenetnek tekinthetünk. Feltehetjük, hogy Σ^t szavai 1 és $|\Sigma|^t$ közötti természetes számoknak felelnek meg (pl. $\Sigma = \{0, 1\}$ esetén a bináris alak egy ilyen megfeleltetés, egyébként az üzenetet egy $|\Sigma|$ alapú számrendszerben felírt számnak tekintjük). A nyilvános kulcsú titkosírási rendszert egy olyan kiskapus egyirányú $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ függvény írja le, melyre $n \geq |\Sigma^t|$. Ezt a leképezést egy ú.n. *nyilvános kulcs* segítségével egyértelműen megadjuk, és bárki számára hozzáférhetővé tesszük. Feltételezzük továbbá, hogy az A-nak nevezett címzett, akinek a titkosított információt el akarjuk juttatni, képes f^{-1} hatékony számítására, mert rendelkezik az f^{-1}-t leíró *titkos kulccsal*. Ha tehát el szeretnénk juttatni A-nak egy M üzenetet, nincs más

dolgunk, mint kiszámítani $M' = f(M)$-t, amit a nyilvános kulcs ismeretében könnyen megtehetünk. Ezután M'-t bátran elküldhetjük A-nak. Ebből A hatékonyan ki tudja számítani $f^{-1}(M') = f^{-1}(f(M)) = M$-t, vagyis el tudja olvasni a pontos üzenetet. Bárki más, aki útközben lehallgatja az M' kódolt üzenetet, nem tudja abból M-t kihámozni, hisz még f-t ismerve sem tudja $f^{-1}(M)$-t megtalálni. A lehallgató mindössze arra képes, hogy ha valamilyen égi sugallat folytán megsejti, mi is az űzenet, akkor ellenőrizni tudja, csakugyan azt küldték-e el. Nem árt azért picit óvatosnak lenni. Ha például a lehallgató tudja, hogy az üzenet egy harci cselekmény kezdőnapját jelzi, akkor a nyilvános kulcs ismeretében kiszámíthatja az f(hétfő), f(kedd), ..., f(vasárnap) értékeket, és ha ezek egyikét fogta el, akkor mindent tud. Szóval nem érdemes ilyen után üzenni. Szerencsére vannak technikák, melyekkel ez a fajta támadás kivédhető. (Pl. minden t-es blokk egy kellően nagyméretű végszelete véletlen jeleket tartalmaz.)

A nyilvános kulcsú titkosírás alkalmas a *digitális aláírás* megvalósítására is, azaz segítségével bizonyítható, hogy egy adott üzenet kitől érkezett. Nevezetesen, tegyük fel, hogy minden szereplőnek van egy kiskapus egyirányú függvénye, pl. A-é f_A, míg B-é f_B. Ha most B alá akarja írni az M (titkosított vagy titkosítatlan) üzenetet, akkor A-nak az $M' = f_B^{-1}(M)$-t küldi el. Ezt A vissza tudja fejteni a nyilvános f_B leképezés ismeretében, hiszen $f_B(M') = f_B(f_B^{-1}(M)) = M$. Ráadásul a címzett bárki más (pl. a bíróság) számára is bizonyítani tudja, hogy az üzenetben egyfelől az áll, amit állít, másrészt, hogy az üzenet B-től ered. Ha ugyanis A felfedi M-t, és M'-t, akkor bárki ellenőrizheti B nyilvános kulcsának ismeretében, hogy $M = f_B(M')$, vagyis, hogy B valóban aláírta az M üzenetet. Ha pedig M egy A-nak szánt titkos üzenet volt, azaz $M = f_A(M^*)$, ahol M^* az igazi üzenet, akkor f_A nyilvános volta miatt bárki láhatja, hogy M az M^* titkosított változata. Az előbbiek szerint bizonyítható, hogy az M kódolt üzenetet B aláírta, tehát a digitális aláírás titkosított üzenetek esetén is használható. Fontos, hogy a bizonyításhoz csak a nyilvános kulcsokra van szükség: egyik félnek sem szükséges felfednie a titkos kulcsát.

Nézzük meg, hogyan lehet a fenti sémát megvalósítani, azaz hogyan lehet egy kiskapus egyirányúnak sejtett függvényt megadni. Az alábbiakban a nyilvános kulcsú RSA rendszert vázoljuk. (A név a rendszert kifejlesztő Rivest, Shamir és Adelman neveinek kezdőbetűiből származik. E három szerző mutatott rá először a digitális aláírás lehetőségére, és írt le először egy a mai napig kiskapus egyirányú függvénynek gondolt leképezést.)

Ahhoz, hogy bárki is titkosított levelet tudjon küldeni az A címzettnek, A előzőleg választ két kellően nagy prímszámot, mondjuk p-t és q-t. A kellően nagy azt jelenti, hogy a tudomány aktuális állása szerint reménytelen legyen a $n := pq$ szorzat faktorizálása, továbbá $n \geq |\Sigma^t|$ is teljesüljön. (Ez utóbbi úgy teljesíthető, hogy az üzenetdarabok t hosszát alkalmasan választjuk.) Legyen $m := \varphi(n) = (p-1)(q-1)$ és válasszuk az $1 \leq e \leq n$ számot úgy, hogy $(e, m) = 1$ teljesüljön (ilyen e könnyen található, és legyen $f(M) := M^e (\mathrm{mod}\ n)$. Ha ez megvan, akkor A közhírré teszi a nyilvános kulcsát, azaz mindenki számára hozzáférhetővé teszi az n és e számokat, hiszen ennek segítségével

bárki hatékonyan tudja f-t számítani, azaz képes lesz A számára titkos üzenetet küldeni. Hangsúlyozzuk, hogy A titokban tartja a p, q és m számokat.

6.14. Megjegyzés *Az e választásánál nem árt észnél lenni: ügyetlen választásnál a rendszer támadhatóvá válik. (Pl. az $e = 1$ egy matematikailag korrekt, ám hiperbuta döntés.) Van arra vonatkozó általános irányelv, hogyan érdemes e-t választani ahhoz, hogy a rendszer biztonsága ettől ne sérüljön. (Vagy egy kicsit pesszimistábban fogalmazva: ne ettől sérüljön.) Természetesen, ahogy egyre újabb támadási módszereket eszelnek ki (és hoznak nyilvánosságra), úgy az „általános irányelv" is időnkénti módosításra szorul. Arany életük van az elméleti kriptológusoknak.*

Természetesen A kíváncsi arra, mit tartalmaznak a neki címzett titkos üzenetek, ezért szüksége van arra, hogy az f^{-1} leképezést hatékonyan tudja számítani. Ehhez először megoldja d-re az $ed \equiv 1(m)$ kongruenciát, amit $(e, m) = 1$ miatt egyértelműen (és hatékonyan) megtehet. Annak, aki nem ismeri m-t, ez a feladat –úgy hisszük– reménytelen, így azt feltételezzük, hogy A-n kívül senki sem képes n és e alapján d-t kiszámítani. (Látjuk persze, hogy ha az n-t valaki faktorizálja, akkor m-t majd d-t könnyűszerrel kiszámíthatja. A titkosírási rendszer megtöréséhez azonban még csak erre sincs szükség: elég, ha valahogyan megszerzi m-t, mert d már akkor is meghatározható. Ha tehát A bölcsen jár el, akkor nyomban azután, hogy d-t kiszámította, megsemmisíti minden addigi számítását, különös tekintettel a p, q és m számokra.)

A d meghatározásával A megkapta az (n, d) *titkos kulcsot*, amit élete árán is megőriz. Az inverzleképezés ugyanis pontosan úgy működik, mint a nyilvános kulcsú titkosítás, csak persze a nyilvános helyett a titkos kulccsal. Konkrétan: ha A egy $X = f(M)$ titkosított üzenetet kap, akkor a dekódolt üzenet $f^{-1}(X) = X^d \pmod n$. Valóban:

$$X^d = (f(M))^d \equiv (X^e)^d = X^{ed} = X^{lm+1} = X^{lm} \cdot X = (X^m)^l \cdot X \equiv 1^l \cdot X \equiv X \pmod n ,$$

az Euler-Fermat tétel miatt. (A fenti számolásnál az $(X, n) = 1$azt feltételezéssle éltünk. Belátható, hogy a fenti inverztulajdonság a mégoly valószínűtlen $p \mid X$ és $q \mid X$ esetekben is igaz.) Tehát az (n, d) titkos kulcs ismeretében az inverzleképezés is hatékonyan számítható, ahogyan ezt egy kiskapus egyirányú függvénytől elvárjuk. Azt is láttuk, hogy (n, d) hatékonyan megkapható p, q és e ismeretében.

Miért gondoljuk, hogy a fent leírt f függvény valóban kiskapus egyirányú függvény? Csupán az egyirányúság szorul indoklásra, a kiskaput láttuk. Több jel mutat arra, hogy ha e-t jól választjuk (ennek mikéntje nem fér bele a jelen jegyzet kereteibe; lényeg, hogy létezik általánosan elfogadott módszer, mely biztosítja, hogy e alkalmas legyen), akkor n és e ismeretéből d meghatározása hasonlóan nehéz, mint n prímtényezőkre bontása. Az általános hiedelem szerint pedig ez reménytelen, ha a p és q prímszámok kellően nagyok: jelenleg a legalább 200-jegyű prímekben hisznek, ugyanis kb 100 jegyű prímek szorzatát elég hatékonyan tudják faktorizálni. (Az RSA-ban használt egyirányú függvényben a kiskapu tehát attól keletkezik, hogy először a prímeket választjuk, amelyekből egyszerű szorzással adódik n; az n számot nem tudjuk „közvetlenül" választani, hisz akkor kódtöréssel próbálkozókhoz hasonlóan mi magunk sem tudnánk n-et faktorizálni, ami szükséges

az inverz leképezés megadásához.) Az RSA módszer definíciójához immár csak annak az az eljárás hiányzik, amellyek a p és q prímeket választjuk. Ezen prímeket ráadásul úgy kell találni, hogy minden prímet lehetőleg egyforma eséllyel válasszunk, hisz ha bizonyos prímekhez túl nagy valószínűséggel nyúlunk (pl egy nagy „titkos" könyvből szemeljük ki), akkor ez óriásit könnyít a kódtörő helyzetén. A megoldás az, hogy próba szerencse alapon keresünk prímet, azaz választunk egy (kellően nagy) véletlen számot: ha prím, győztünk, ha nem, újat húzunk. Ehhez a módszerhez persze szükség van hatékony prímtesztre (ilyet már láttunk), másrészt azt kell biztosítanunk, hogy ne kelljen túlságosan sok véletlen számot generálni, míg végre-valahára egy prímnél kötünk ki. Szerencsére ez is teljesül: a prímszámtétel egy erősebb alakja szerint a prímek sűrűsége n közelében nagyon jó közelítéssel $\frac{1}{\ln n}$, vagyis e^{461} (azaz a 200 jegyű számok) környékén véletlen számokat választva kb. $\frac{1}{500}$ valószínűséggel bökünk prímre. Vagyis $500 \cdot k$ próbálkozás után kb e^{-k} a valószínűsége annak, hogy nem akadt prím a horogra. (A próbálkozások várható száma jelentős mértékben csökken, ha kiszűrjük a kis prímekkel osztható (legegyszerűbb esetben a páros) számokat, és azokat rögtön eldobjuk, nem teszteljük.)

Történelem: Ha sok időm lesz, erről is írok még...

6.7. Bizonyítás információközlés nélkül

(Vázlat)

Arról szeretnénk meggyőzni valakit, hogy tudunk valamit, ám arról, amit tudunk semmiféle információt sem szeretnénk adni azon túl, hogy ismerjük a dolgot. Valami hasonlóról van szó, mint amit egy áruló kapcsán megtudjuk, hogy egy szám összetett, de az osztóiról semmiféle információt nem kapunk az áruló hatványozásából.

A sztenderd példa egy adott gráf Hamilton körének ismerete. Az A játékos tehát ismeri G egy Hamilton körét, és ezt szeretné bebizonyítani B-nek úgy, hogy B ne tudjon semmit meg a Hamilton körről. Az A játékos tehát mutat B-nek egy G-vel izomorf H gráfot, és B választása szerint vagy mutat H-ban egy Hamilton kört vagy megmutatja B-nek a G és H közti izomorfiát. A B játékos ha nem hiszi, hogy A igazán ismer egy Hamilton kört G-ben, akkor H-t látva eldönti, hogy A hogyan csal szerinte. Ha B azt gondolja, hogy nem G-vel izomorf gráfot felmutatva próbál A az eszén túljárni, akkor B izomorfiát kérdez. Ha B elhiszi, hogy H izomorf G-vel, és azt gondolja, hogy A nem ismer Hamilton kört, akkor B Hamilton kört kér. Világos, hogy az A játékosnak nincs más lehetősége a csalásra, ezért ha csalni próbál, akkor 50% eséllyel lelepleződik, ha B fej vagy írás alapon kérdezi az izomorfiát ill. a Hamilton kört. Ha tehát 100-szor megismétlik a kísérletet, és A nem bukik el, akkor B-nek jó oka van azt gondolni, hogy A csakugyan ismer egy Hamilton kört G-ben.

Kérdés, hogy miért nem kap B információt a Hamilton kör mibenlétéről. Azt gondoljuk ugyanis (illetve a szakértők ezt hangoztatják, én elhiszem...), hogy a gráfizomorfia probléma bonyolult. Ezért B-nek nincs egyéb esélye a H és G gráfok izomorfiáját meg-

találni, mint rákérdezni erre A-tól, amikoris persze semmit sem fog megtudni a Hamilton körről.

7. fejezet

A halmazelmélet alapjai

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.

7.1. Definíció *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.

7.2. Definíció *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.*

7.3. Tétel (Cantor-Bernstein tétel) *Ha $|A| \leq |B|$ és $|B| \leq |A|$, akkor $|A| = |B|$.*

Történelem: Cantor, Dedekind és a halmazok
Az időnként Schröder-Bernstein ill. Bernstein-Schröder néven emlegetett 7.3. 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. (Cantornak rosszul esett, hogy Dedekind visszautasította a neki szánt hallei professzori kinevezést, ezt követően a korábbi szoros együttműködésüknek vége szakadt, és nem tárgyaltak egymással.) Cantor sejtésére Ernst Schröder 1896-ban adott egy hibás bizonyítást, majd Felix Bernstein 1898-ban talált egy helyeset. A tételnek számos elnevezése forog közszájon, abban azonban mindegyik közös, hogy a „Dedekind" karaktersorozat egyikben sem fordul elő.

Cantort számos személyes tragédia sújtotta, egyiknek magyar vonatkozása is van. 1904-ben Kőnig Gyula (Kőnig Dénes édesapja) tartott előadást a nemzetközi matematikai kongresszuson, amiben Cantor transzfinit halmazelméletét igyekezett alapjaiból cáfolni. Annak ellenére, hogy nem telt el egy nap, míg Zermelo kimutatta Kőnig érvelésében a hibát, a fiát már korábban elveszített Cantor úgy érezte, hogy kollégai és lányai előtt alázták meg. Ekkortól hatalmasodott el rajta a depresszió, került számos alkalommal szanatóriumba ahol élete utolsó öt évét is töltötte. Akárcsak Bolyainak, neki sem adatott meg, hogy munkájának jelentőségét még életében annak helyén értékeljék.

♦

Bizonyítás. Feltehetjük, hogy az A és B halmazok diszjunktak. Legyenek $f : A \to B$ és $g : B \to A$ injekciók, amelyek 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 a két kérdéses halmaz között.

7.4. Definíció *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).*

Megjegyzés:
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, amelyeket 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. ♦

7.5. Definíció *Az A halmaz* megszámlálható, *ha $|A| \leq |\mathbb{N}|$. Az $\mathbb{N}$ halmaz számosságát $\aleph_0$ (alef null) jelöli.*

7.6. Megjegyzés *Az $\aleph$ (alef) a héber ABC első betűje. Követi a ב (bet), ג (gimel), ד (dalet), és 18 további betű. Ne nézzünk bután, hogy csak az alefet ismerjük.*

7.7. 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.

7.8. Következmény *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:* $0, 1, -1, 2, -2, 3, \ldots$.

A 7.8. Következményben szereplő legutolsó állítás általánosítása következik.

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

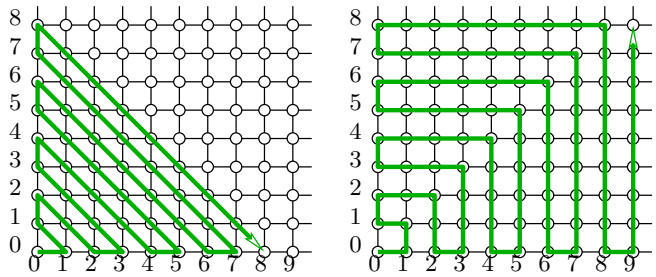
Bizonyítás. Tudjuk, hogy A és B elemei felsorolhatók, azaz $A = \{a_0, a_1, \ldots\}$ és $B = \{b_0, b_1, \ldots\}$. Ekkor $A \cup B = \{a_0, b_0, a_1, b_1, a_2, b_2, \ldots\}$, tehát $|A \cup B| \leq \aleph_0$. □

7.10. Következmény *Véges sok megszámlálható halmaz uniója is megszámlálható.*

Ennél azonban több is igaz.

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

Bizonyítás. 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, két lehetséges példát mutat az ábra.) Azt kaptuk, hogy $\bigcup_{i\in\mathbb{N}} A_i$ elemei sorba rendezhetők, ezért a halmaz megszámlálható. □



7.12. Következmény $|\mathbb{Q}| = \aleph_0$.

Bizonyítás. 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. □

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.□

A következő célunk, hogy megszámlálhatónál nagyobb számosságú halmazt találjunk.

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

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

Bizonyítás. 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. □

7.15. 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, amelyekre létezik olyan N küszöb, hogy minden 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.

7.16. Definíció *A $\mathcal{P}(\mathbb{N})$ halmaz számosságát* kontinuum *számosságnak nevezzük, és (ritkábban)* $\mathfrak{c}$*-vel (gót „c”-vel) vagy (gyakrabban)* $2^{\aleph_0}$*-lal jelöljük.*

7.17. Megjegyzés *A 7.16. Definícióban használt jelölés összhangban van azzal, hogy egy n elemű halmaznak 2^n részhalmaza van.*

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

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

Ennél azonban jóval több igaz.

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

Bizonyítás. 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, amelyeket 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, amelyek 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.

7.20. 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.*

7.21. Következmény *Megszámlálhatóan sok kontinuum méretű halmaz uniója kontinuum számosságú. Kontinuum és megszámlálható halmaz uniója kontinuum.*

Bizonyítás. 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. Nekünk pedig éppen erre van szükségünk. □

Érdemes meggondolni, hogy a fenti bizonyításban szereplő f miért is nem bijekció. (Ha ugyanis az volna, nem lett volna szükség a Cantor-Bernstein tétel alkalmazására.)

7.22. Következmény *Az $\mathbb{R}$ és $\mathbb{C}$ egyaránt kontinuum számosságú halmazok.*

Bizonyítás. $\mathbb{R}$ 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-ra 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.

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

A 7.23. kontinuum hipotézis általánosan is megfogalmazható.

7.24. (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.