

Bevezetés a matematikába

informatikai alkalmazásokkal

Szerkesztette: **Járai Antal** tanszékvezető egyetemi tanár

Írták: **Farkas Gábor** egyetemi docens (4., 5., 7., 8.)
Fülöp Ágnes egyetemi docens (7., 8.)
Gonda János egyetemi docens (9., 10.)
Járai Antal tanszékvezető egyetemi tanár (1– 10.)
Kovács Attila egyetemi docens (7., 8.)
Láng Csabáné egyetemi tudományos munkatárs (3., 6.)
Székely Jenő ny. egyetemi tudományos munkatárs (1., 2., 4.)

Szakmai lektor: **Rácz András** matematikus

Ötödik, elektronikus kiadás

ELTE Informatikai Kar, 2025

Tartalomjegyzék

Bevezetés	4
1 Halmazok	6
1.1 Logikai alapok	6
1.2 Halmazelméleti alapfogalmak	13
1.3 Relációk	20
1.4 Függvények	34
2 Természetes számok	44
2.1 Peano-axiómák	44
2.2 Műveletek természetes számokkal	52
2.3 A természetes számok rendezése	58
3 A számfogalom bővítése	73
3.1 Egész számok	73
3.2 Racionális számok	79
3.3 Valós számok	83
3.4 Komplex számok	94
4 Véges halmazok	107
4.1 Véges halmazok alaptulajdonságai	107
4.2 Kombinatorika	110
4.3 Binomiális és polinomiális tétel, szita formula	116
5 Végtelen halmazok	122
5.1 Kiválasztási axióma	122
5.2 Megszámlálható halmazok	128
5.3 Nem megszámlálható halmazok	130
6 Számelmélet	135
6.1 Oszthatóság	135
6.2 Kongruenciák	146
6.3 Számelméleti függvények	157
6.4 Lánctörtek	163
7 Gráfelmélet	169
7.1 Irányítatlan gráfok	169
7.2 Irányított gráfok	183
8 Algebra	202

8.1	Csoportok	202
8.2	Gyűrűk és testek	226
8.3	Polinomok	243
9	Kódolás	281
9.1	Kommunikáció és kódolás	281
9.2	Forráskódolás	285
9.3	Hibakorlátozó kódolás	320
10	Algoritmusok	340
10.1	Számítási modellek	340
10.2	Kiszámíthatóság	369
10.3	Idő és tár	380
	Irodalom	386
	Mutató	390

Bevezetés

A negyedik kiadás fűlszövege:

Ez a tankönyv az ELTE programtervező informatikus hallgatói számára készült, a matematika „diszkrét” – azaz a folytonossághoz nem kapcsolódó – témaköreinek ismertetését tartalmazza. A halmazelmélet, relációk, függvények, természetes számok és egyéb számkörök tárgyalásánál rámutatunk az alkalmazásokra is: szó esik a lekérdező nyelvekről, a relációs adtbázis kezelőkről, logikai függvényekről és elektronikai megvalósításukról, továbbá számábrázolásokról. A véges halmazok, a kombinatorika és a végtelen halmazok ismertetését az elemi számelmélet tárgyalása követi, amely tartalmazza az RSA kódolást, a digitális aláírást és a kulccsere módszerét is. A gráfelmélettel kapcsolatban néhány fontos adatstruktúra és számos gráfalgoritmus is szóba kerül. Az algebra megalapozza a kódoláselmélet és a komputeralgebra megértését, ezért röviden a véges testek elméletét is áttekintjük. A kódolás című fejezet rengeteg gyakorlati ismeretet is tartalmaz az adattömörítéssel és a hibajavító kódokkal kapcsolatban. Az utolsó fejezet már átvezet az elméleti informatikába: részletesen tárgyaljuk a gépmodellek ekvivalenciáját, bemutatjuk a kiszámíthatóság és felsorolhatóság fogalmait, az algoritmussal megoldhatatlan problémák létezését. A kötet a tárigény és a futásidő vizsgálatával, a P és NP problémaosztályok megfogalmazásával zárul. Minden témakörhöz számos különböző szintű feladat tartozik.

A negyedik kiadás előszava:

Ez az összefoglaló azzal a céllal készült, hogy tömör formában rögzítse a programtervező matematikus és programtervező informatikus hallgatók számára tartott „Bevezetés a matematikába” című előadás anyagát. Az előadáshoz képest lényeges különbség, hogy itt a magyarázatokat szinte teljesen mellőztük. Így ez az összefoglaló semmiképpen sem helyettesíti az előadást és a jegyzetelést az előadáson. Úgy gondoljuk azonban, közreadása mégis hasznos, mert segítséget nyújt a jegyzeteléshez, lehetővé teszi mindenki számára, hogy az előadáson készült jegyzeteit kiegészítse, hibáit javítsa, és világosan rögzíti, mi-ben tért el az előadás más jegyzetektől, mi a tananyag. Úgy gondoljuk, a vizsgára való felkészüléshez – ha valaki részt vett az előadásokon és gyakorlatokon, és követte az ott elhangzottakat – félvétenként legalább egy hét szükséges. A törzsanyagon kívüli részeket *-gal jelöltük. A °-rel megjelölt részek olyan fogalmakat is felhasználnak, amelyeket még nem definiáltunk, és csak magyarázatként szolgálnak. Néhány helyen középiskolai anyagot – geometriai fogalmak és tételek, trigonometrikus függvények, exponenciális függvény és inverzeik – is használunk. Bár az ilyen részek használata szigorú axiomatikus felépítésnél elkerülendő és elkerülhető lenne, itt szükségszerű, mert tárgyalásuk az analízis tanításakor történik. Az igazán komolyan felhasznált középiskolai ismeret azonban csak némi matematikai érettség és absztrakciós készség. A definícióban a definiált fogalmakat, az axiómákat és állításokat *dőlt* betűvel szedtük. A bizonyítások végét $\square$ jelzi.

Bár számos, a Komputer Algebra Tanszék munkatársai által összeállított feladatgyűjtemény áll rendelkezésre (Bruder [5], [6]; Gonda [28], [29]; Lángné [53], [54], [55],

[56], [57]), néhány terület egyáltalán nincs, vagy csak hiányosan van lefedve, elsősorban az anyag változása miatt. Ezért ebben az új, javított kiadásban az anyagot feladatok is kiegészítik; további kiegészítő számítógépes anyag található a szerkesztő honlapján: <http://compalg.inf.elte.hu/~ajarai>. Elsősorban olyan feladatokat igyekeztünk összegyűjteni, amelyek segítenek megérteni az előadáson tanult általános fogalmakat, illetve rávilágítanak az informatikai alkalmazásokra: ezeket $\rightarrow$ jelzi; a gyakorlat anyagát ezen feladatok megoldása képezi és ezeket mindenkinek ajánlatos megoldani. Minden feladat nehézségi fokát egy szám jelzi, logaritmikus skálán: eggyel nagyobb szám kb. kétszer akkora megoldási időnek felel meg. Ha az első gyakorlat előbb van, mint az első előadás, a teljes indukcióval kapcsolatos, illetve a síkbeli pontthalmazok felvázolásával foglalkozó feladatokkal érdemes kezdeni.

Az anyag és a feladatok nagy részét — mint a legtöbb tankönyvben teszik — máshonnan vettük át. Valószínűleg azok a részek, amelyeket nem átvettünk, is szerepelnek már valahol. Mivel az eredet kinyomozása lehetetlen, nem adunk meg részletes hivatkozást, de az irodalomjegyzékben szerepelnek azok a művek, amelyeket elsősorban használtunk.

Köszönettel tartozunk mindazoknak, akik ezen tankönyv létrejöttét segítették: az ELTE Informatikai Kar vezetésének, valamint az ELTE Eötvös Kiadó munkatársainak. Köszönetet mondunk Rácz Andrásnak, a könyv lektorának, aki az egész könyvet igen gondosan átnézte és rendkívül sok észrevétellel, javaslattal, kiegészítéssel segített.

Budapest, 2009. október 23.

A Szerzők

Az ötödik kiadás előszava:

Ez az ötödik, elektronikus változat csak pár, az alapáramkörökkel kapcsolatos oldalal bővült, de nagyon sok kisebb-nagyobb hibát, elírást javítottunk. Köszönetet mondunk mindazoknak, akik a hibákra felhívták figyelmünket, elsősorban hallgatóinknak.

Budapest, 2025. október 23.

A Szerkesztő

Halmazok

Ebben a fejezetben a logikai alapokat és a halmazokat, relációkat, függvényeket és műveleteket tárgyaljuk.

Az általános és középiskolai matematikában a számítási és szerkesztési eljárások valamint a feladatmegoldási módszerek mellett fontos szerepet játszottak a bizonyítások, amelyek során valamilyen matematikai állítást korábbi ismereteinkre alapozva logikai megfontolásokkal láttunk be.

A matematika axiomatikus felépítése (virtuálisan) egy olyan könyvet jelent, amelyben egy matematikai témakör (vagy az egész matematika) úgy van leírva, hogy abban — az axiómáknak mondott matematikai állítások kivételével — minden tétel szabályos logikai lépések sorából álló bizonyításával együtt szerepel, és — az axiómákban szereplő „axiomatikus alapfogalmak” kivételével — minden fogalom a logika szabályainak megfelelően van bevezetve („definiálva”).

Egyes szavak matematikai jelentése lényegesen eltér azok köznap használatától, például a jogi bizonyítás azt jelenti, hogy néhány elfogulatlan embert meggyőznek valamiről (pedig e módszer megbízhatóságát esetek tucatjai tették kérdésessé, a jogi értelemben is hibásnak bizonyult tévedésekről nem is beszélve); a reklámok gyakran „bizonyítást” említenek ott is, ahol csak egy-két alkalommal ellenőriztek egy állítást.

A matematikában egy állítás bizonyítása azt jelenti, hogy (valamilyen precízen körülírható értelemben) a logika szabályainak megfelelően belátjuk: az állítás következik az axiómákból.

1.1 Logikai alapok

1.1.1. Az axiomatikus módszer. Tegyük fel, hogy a valóság egy részének modellezésével foglalkozunk. Az *axiomatikus módszer* abban áll, hogy bizonyos feltevésekből, az elmélet axiómáiból a logika szabályai szerint következtetéseket vonunk le, azaz (az adott elméletben érvényes) tételeket bizonyítunk. Az így felépített matematikai elméletek (pl. euklideszi geometria) a valóság többé vagy kevésbé pontos közelítései. Ha az axiómák teljesülnek egy struktúrában, akkor ott a tételek is. A matematikában olyan elméletekkel foglalkozunk, amelyek szigorúan axiomatizálhatók, formalizálhatók. A számítógépes rendszerek is a valóság egy részének formalizálásai, ezért az informatikus számára is fontos, hogy pontosan értse, milyen feltevésekből indul ki.

A matematikai elméletek a halmazelmélet részének is tekinthetők. Más szóval, az egész matematikát a halmazelméletre fogjuk építeni.

1.1.2. Logikai jelek, predikátumok, formulák. Egy matematikai elméletben szerepel néhány definiálatlan alapfogalom, az úgynevezett *predikátumok*, amelyeknek változóik értékétől függően az értéke igaz (jele: $\uparrow$) vagy hamis (jele: $\downarrow$) lehet, úgy érteve, hogy a két közül pontosan az egyik. (Lehetnek nullváltozós predikátumok is, ezek a *kijelentések*, értékük igaz vagy hamis.) Például a síkgeometriában predikátumok: $E(x)$ („ x egyenes”),

$P(x)$ („ x pont”), $I(x, y)$ („ x illeszkedik y -ra”). Néha nem írjuk ki a zárójelet, és ha két változó van, akkor sokszor a predikátum jelét a változók közé írjuk. Például szinte minden elméletben használjuk az $=$ predikátumot, amelyet a változók közé írunk.

A *logikai formulák* (vagy *mondatok*) az adott elmélet predikátumaiból épülnek fel a $\neg$ („nem”, idegen szóval *negáció*), $\wedge$ („és”, *konjunkció*), $\vee$ (megengedő „vagy”, idegen szóval *diszjunkció*), $\Rightarrow$ („ha ... akkor ...”, *implikáció*) és $\Leftrightarrow$ („akkor és csak akkor” vagy „*pontosan akkor*”, *ekvivalencia*), $\oplus$ (kizáró „vagy”, gyakrabban „vagy ... vagy ...”: pontosan az egyik), $|$ („sem ... sem ...”), $\parallel$ (összeférhetetlen „vagy”, gyakrabban „vagy ... vagy ...”: legfeljebb az egyik, de lehet, hogy egyik se) *logikai jelek*, valamint a két kvantor, a $\exists$ („létezik” vagy „van olyan”) *egzisztenciális kvantor* és a $\forall$ („minden”) *univerzális kvantor* segítségével. Maguk a predikátumok a legegyszerűbb, úgynevezett *elemi formulák*, és ha $\mathcal{A}$ és $\mathcal{B}$ formulák, akkor $\neg\mathcal{A}$, $(\mathcal{A} \wedge \mathcal{B})$, $(\mathcal{A} \vee \mathcal{B})$, $(\mathcal{A} \Rightarrow \mathcal{B})$, $(\mathcal{A} \Leftrightarrow \mathcal{B})$, $(\mathcal{A} \oplus \mathcal{B})$, $(\mathcal{A} | \mathcal{B})$, $(\mathcal{A} \parallel \mathcal{B})$ is formulák, továbbá ha x egy változó, akkor $(\exists x \mathcal{A})$ és $(\forall x \mathcal{A})$ is formulák. Ezeken kívül más formulák nincsenek. Vegyük észre, hogy könnyen készíthető olyan program, amely adott predikátumok és változók esetén a formulákat generálja. (Tulajdonképpen ezzel definiáljuk a formulákat.) Olyan program is készíthető, amely egy véges jelsorozatról eldönti, hogy formula-e. Ha nem okoz félreértést, akkor a formula felírásából elhagyhatunk zárójeleket.

Néha nem minden logikai jelet illetve kvantort használunk. Ekkor az adott logikai jellel/jelekkel, illetve kvantorral/kvantorokkal felírható logikai formulákról beszélünk. Például gyakran csak a $\neg$, $\wedge$, $\vee$, $\Rightarrow$ és $\Leftrightarrow$ logikai jeleket és a két kvantort használjuk.

Egy formula egy $(\exists x \mathcal{A})$ vagy $(\forall x \mathcal{A})$ típusú részformulája esetén az x változó minden, a két zárójel közötti előfordulására (a kvantor után vagy $\mathcal{A}$ -ban) azt mondjuk, hogy a kvantor *hatáskörében* van. Ha egy formulában egy változó egy adott előfordulása egy kvantor hatáskörében van, akkor azt mondjuk, hogy az adott előfordulás *kötött előfordulás*, egyébként az adott előfordulás *szabad előfordulás*. Ha egy változónak egy formulában van szabad előfordulása, akkor azt mondjuk, hogy a változó *szabad változó*. Ha egy formulának nincs szabad változója, akkor a formulát *zárt formulának*, egyébként *nyitott formulának* nevezzük. Ha jelezni akarjuk, hogy egy formulának mik a szabad változói, akkor zárójelben az összes szabad változóját kiírjuk.

A síkgeometria példájánál maradva, az

$$\left((E(x) \wedge P(y)) \wedge I(x, y) \right)$$

formula azt fejezi ki, hogy az y pont illeszkedik az x egyenesre, a

$$\left((P(x) \wedge P(y)) \wedge \neg x = y \right)$$

formula pedig azt, hogy x és y különböző pontok. Mindkét formulában x és y szabad változók, így jelölhetjük az egyiket $\mathcal{A}(x, y)$ -nal, a másikat pedig $\mathcal{B}(x, y)$ -nal. Észrevehetjük, hogy itt az egyenlőséget tulajdonképpen „megtakaríthatjuk”, ha $I(x, y)$ -t úgy érjük, hogy ha x és y mindketten pontok vagy mindketten egyenesek, akkor az egyenlőségüket jelenti. Ekkor a $\mathcal{B}(x, y)$ formula így néz ki:

$$\left((P(x) \wedge P(y)) \wedge \neg I(x, y) \right).$$

A

$$\exists y \left((E(x) \wedge P(y)) \wedge I(x, y) \right)$$

formula azt fejezi ki, hogy van olyan pont, amely az x egyenesre illeszkedik. Most x minden előfordulása szabad, y -nak pedig minden előfordulása kötött. Ezt a formulát $\mathcal{C}(x)$ -szel jelölhetjük. A

$$\forall x \left(E(x) \Rightarrow \exists y (P(y) \wedge I(x, y)) \right)$$

zárt formula azt fejezi ki, hogy minden egyenesen van pont; ezt például $\mathcal{D}()$ -vel jelölhetjük, mert nincs szabad változója. A

$$\begin{aligned} & \forall x \forall y \left((P(x) \wedge P(y) \wedge \neg x = y) \right. \\ & \quad \Rightarrow \left(\exists z (E(z) \wedge I(x, z) \wedge I(y, z)) \right) \\ & \quad \left. \wedge \forall z \forall w \left((E(z) \wedge I(x, z) \wedge I(y, z) \wedge E(w) \wedge I(x, w) \wedge I(y, w)) \Rightarrow z = w \right) \right) \end{aligned}$$

zárt formula (amelyben számos zárójelet elhagytunk) pedig a síkgeometria egyik axiómája, azt fejezi ki, hogy bármely két különböző ponthoz pontosan egy egyenes van, amely mindkettőre illeszkedik. A $\exists!$ („*egyértelműen létezik*” vagy „*egy és csak egy létezik*” vagy „*pontosan egy létezik*”) jelölés felhasználásával egyébként ez az axióma a rövidebb

$$\forall x \forall y \left((P(x) \wedge P(y) \wedge \neg x = y) \Rightarrow \exists! z (E(z) \wedge I(x, z) \wedge I(y, z)) \right)$$

formába írható.

1.1.3. Megjegyzés. Bár a matematika teljesen formalizálható, nem formalizálva tárgyaljuk. Ha számítógéppel kommunikálunk, fontos a formalizálás. Például egy lekérdező nyelv (az SQL vagy akár a Google) használatakor predikátumokkal definiálnunk kell, amit kérdezni szeretnénk.

Néha nem is olyan könnyű eldönteni, hogyan formalizáljunk valamit. Például a magyar nyelvű mondatok formalizálásánál gondot okozhat a „vagy” háromféle használata. Az „Átok reá, ki gyávaságból Vagy lustaságból elmarad” mondatban a vagy megengedő értelmű, a „Vagy bolondok vagyunk s elveszünk egy szálíg, Vagy ez a mi hitünk valóságra válik” mondatban kizáró, a „vagy iszol, vagy vezetsz” mondatban pedig összeférhetetlen értelmű. (Lásd Quine [71] könyvének részletes elemzéseit.) A matematikában a „vagy” legtöbbször megengedő értelmű.

1.1.4. Példa. Az emberekre értelmezett $N(x)$ predikátum jelentse azt, hogy x nő. (Feltesszük, hogy ez egyértelműen eldönthető.) Ebben a szerény elméletben N az egyetlen predikátum, axióma pedig nincs. Az „ x és y nők” mondat formalizálva $(N(x) \wedge N(y))$ (de nem $N(x \wedge y)$, ami értelmetlen).

Az alábbi definícióval bevezethetjük a férfiak fogalmát:

$$F(x) := \neg N(x).$$

Ez tulajdonképpen azt jelenti, hogy egy új F predikátumot vezetünk be és a

$$\forall x(F(x) \iff \neg N(x))$$

axiómát. Ebben a bővebb elméletben

$$\forall x(F(x) \vee N(x))$$

és

$$\neg \exists x(F(x) \wedge N(x))$$

tételek. Ezen utóbbi formula ekvivalens a

$$\forall x \neg(F(x) \wedge N(x))$$

és a

$$\forall x(\neg F(x) \vee \neg N(x))$$

tételekkel. Vegyük észre, hogy a tételek attól függetlenül következnek az axiómából, hogy mit is jelent $N(x)$ és $F(x)$.

1.1.5. Példa. Másik példaként az emberekre $N(x)$ jelentse azt, hogy x nő, $G(x, y)$ pedig, hogy x gyermeke y -nak. Axiómaként kössük ki, hogy ha x gyermeke y -nak, akkor y nem gyermeke x -nek, formalizálva

$$\forall x \forall y (G(x, y) \Rightarrow \neg G(y, x)).$$

Azt, hogy x unokája y -nak, úgy definiálhatjuk, hogy van olyan z , amelyre x gyermeke z -nek, z pedig gyermeke y -nak. Formalizálva

$$U(x, y) := \exists z (G(x, z) \wedge G(z, y)).$$

Bebizonyítjuk a következő tételt (állítás, segéd-tételt, lemmát): senki sem unokája saját magának, formalizálva

$$\neg \exists x U(x, x).$$

A bizonyítás indirekt: tegyük fel, hogy van olyan x , amelyre $U(x, x)$. Ekkor U definíciója szerint van olyan z , hogy $G(x, z)$ és $G(z, x)$, de ez ellentmond az axiómának.

Vegyük észre, hogy a bizonyítás nem függ attól, hogy mi volt G , csak az axiómától és U definíciójától.

1.1.6. Példa. Tovább folytatva az előző példát, definiálhatjuk, hogy x az anyai nagymamája y -nak:

$$N_{mm}(x, y) := \left(N(x) \wedge \exists z \left(N(z) \wedge (G(y, z) \wedge G(z, x)) \right) \right).$$

Annak definíciója, hogy x apai nagyapja y -nak, valamivel bonyolultabb:

$$N_{pp}(x, y) := \left(\neg N(x) \wedge \exists z \left(\neg N(z) \wedge (G(y, z) \wedge G(z, x)) \right) \right),$$

de az $F(x) := \neg N(x)$ definícióval egyszerűbb lesz:

$$N_{pp}(x, y) := \left(F(x) \wedge \exists z \left(F(z) \wedge (G(y, z) \wedge G(z, x)) \right) \right).$$

1.1.7. Matematikai elméletek. A fenti példák mutatják, hogy egy matematikai elmélet hogyan épül fel: bizonyos zárt formulákat axiómáknak tekintünk, és ezekből kiindulva tételeket (más zárt formulákat) bizonyítunk be, közben esetleg definíciókkal bővítve az elméletet.

1.1.8. Matematikai logika. Nem tárgyaltuk a bizonyítási módszereket, ezeket ismertnek tesszük fel. Ezek felsorolhatók, ezek a logika axiómái. Részletes tárgyalásuk később, más tárgy keretében történik. Ugyancsak más tárgyak foglalkoznak azzal, hogyan bizonyíthatunk számítógéppel tételeket: ez mind a matematika, mind az informatika számára rendkívül fontos kérdés. Léteznek tételbizonyító algoritmusok is, egy ilyen alapul például a Prolog nyelv.

1.1.9. Egyenlőség. Minden olyan elmélet esetén, amelyben szerepel az egyenlőség (jele $=$), két lehetőségünk van: vagy logikai fogalomnak tekintjük (mi ezt tesszük), vagy predikátumnak, és az axiómák között felsoroljuk a tulajdonságait. (Például $x = y \iff y = x$, stb.)

* **1.1.10. Nyelvek műveletekkel.** A formulák fent definiált fogalma nem alkalmas olyan elméletek tárgyalására, amelyekben nem csak predikátumok, hanem műveletek is szerepelnek. (Meglépő, de a mindent magába foglaló halmazelmélet nem ilyen.) A matematikai logikában fogunk találkozni az általános esettel.

° **1.1.11. Az axiómák jelentése.** Az axióma szó Eukleidész munkáiban még olyan nyilvánvalóan helyes állítást jelentett, amelynek igazságát senki sem vonta kétségbe. Ma-napság egy állítás felvétele az axiómarendszerbe azt jelzi, hogy az adott rendszerben azt az állítást nem bizonyítjuk, de más tételek bizonyítása során mint igaz állítást felhasználhatjuk.

Az axiomatikus alapfogalmakat nem definiáljuk (nem is definiálhatjuk, mert „vég-telen leszálláshoz” jutnánk). Emiatt ezeken azt érthetünk, amit akarunk. A bizonyítások menetét az értelmezés nem befolyásolja, hiszen a fogalmak szemléletes jelentését amúgy sem használhatjuk fel a bizonyítások során.

Ha például valaki a geometriai „pont” alatt (X, Y) párokat ért, ahol X és Y is a „páros” vagy „páratlan” fogalom lehet, rövidítve e , illetve o (az angol „even”, illetve „odd” szóból), egyenes alatt pedig $AX + BY = C$ alakú egyenleteket, ahol az A , B , C együtthatók mindegyike e vagy o lehet, de A és B nem lehet mindkettő e , illeszkedés alatt pedig azt érti, hogy az (X, Y) pont koordinátái kielégítik az adott egyenletet, akkor olyan geometriához jut, amelyben 4 pont és 6 egyenes van, teljesül, hogy bármely két különböző pontra egy és csak egy egyenes illeszkedik, teljesül a párhuzamossági axióma, és még néhány más axióma is, például, hogy létezik három olyan pont, amely nem fekszik egy egyenesen. Egy másik példa a 3.4.4 ábrán látható úgynevezett Fano-sík. Ebben 7 „egyeses” és 7 pont van, és itt is teljesülnek a fent említett axiómák — kivéve a párhuzamossági axiómát: bármely két különböző egyeneshez pontosan egy pont van, amely mindkettőre illeszkedik. Egyébként pontosan ugyanezek az axiómák teljesülnek, ha az „egyeseket” tekintjük pontoknak, és a pontokat egyenesnek. Ezekben a geometriákban is érvényes minden olyan tétel, amelynek bizonyításához csak az adott geometriában teljesülő axiómákat használtuk fel. Ezekhez hasonló véges geometriák szerepet játszanak a kódoláselméletben.

* **1.1.12. Az axiómák kiválasztása.** Említettük már, hogy az axióma szó az ókori görög matematikában még olyan nyilvánvalóan helyes állítást jelentett, amelynek igazságát „józanészű ember nem vonhatja kétségbe” (Arisztotelész). Ez a megfogalmazás természetesen nem jelenti azt, hogy axiómaként felsorolták volna az összes nyilvánvalóan igaz állítást. Eukleidész a geometria felépítése során arra törekedett, hogy minél kevesebb

axiómát mondjon ki, és tételként bizonyított minden mást (például, hogy a csúcsszögek egyenlők stb.).

Az, hogy mely állításokat választjuk axiómának, meglehetősen önkényes. Alapelve, hogy az axiómák ne mondjanak ellent egymásnak. Általános elvárás, hogy az axiómák egyszerűek, jól érthetőek legyenek. Célszerű, ha minél kevesebb axióma van, de ha túl kevés állítást választunk ki, nem tudunk elég sok tételt bebizonyítani.

Eukleidész híres Elemek című munkájában (lásd Eukleidész [16]) így szól a sokat emlegetett 5. posztulátum (egyes átiratokban: a 11. axióma): „Ha két egyenest úgy metsz egy harmadik egyenes, hogy az egyik oldalon keletkező belső szögek összege két derékszögnél kisebb, akkor a harmadik egyenesnek ezen az oldalán metszi egymást az első két egyenes.”

Ezt igazán nem lehet egyszerűnek tartani. Már az ókorban kicserélték a ma is szokásos párhuzamossági axiómára: „Egy egyeneshez egy külső ponton át csak egy párhuzamos egyenes húzható.” Ez, a többivel együtt, ekvivalens az előzővel.

Ezek helyett Bolyai Farkas azt az állítást vette axiómának, hogy „három pont vagy egy egyenesen, vagy egy körön van”.

Ha az előbbi három állítás bármelyikét hozzá vesszük Eukleidész többi axiómájához (az úgynevezett maradék axiómarendszerhez), ugyanazt a geometriát kapjuk: bármelyik rendszerben bebizonyítható a másik két állítás.

→ **1.1.13. Feladat [5].** Pozitív egészeket tekintve, jelölje $P(x)$, $E(x)$, $O(x)$, illetve $D(x, y)$ rendre azt, hogy x prím, páros, páratlan, illetve, hogy x osztója y -nak. Fordítsuk le magyar nyelvre az alábbi formulákat. Tagadjuk a formulákat formálisan, illetve köznyelviileg. Melyik rövidíthető $\exists!$ használatával?

- (1) $P(7)$;
- (2) $(E(2) \wedge P(2))$;
- (3) $(\forall x(D(2, x) \Rightarrow E(x)))$;
- (4) $(\exists x(E(x) \wedge D(x, 6)))$;
- (5) $(\forall x(\neg E(x) \Rightarrow \neg D(2, x)))$;
- (6) $(\forall x(E(x) \Rightarrow (\forall y(D(x, y) \Rightarrow E(y))))$;
- (7) $(\forall x(P(x) \Rightarrow (\exists y(E(y) \wedge D(x, y))))$;
- (8) $(\forall x(O(x) \Rightarrow (\forall y(P(y) \Rightarrow \neg D(x, y))))$;
- (9) $((\exists x(E(x) \wedge P(x))) \wedge (\neg(\exists x(E(x) \wedge P(x) \wedge (\exists y(\neg x = y \wedge E(y) \wedge P(y))))))$.

→ **1.1.14. Feladat [7].** Az embereket tekintve, jelölje $J(x)$, $B(x)$, $U(x)$, $I(x)$, $E(x)$, $P(x)$, $K(x)$, $N(x)$, $H(x, y)$, illetve $T(x, y)$ rendre azt, hogy x jogász, bíró, ügyeskedő, idős, életerős, politikus, képviselő, nő, illetve hogy x házastársa y -nak, valamint hogy x tiszteli y -t. Formalizáljuk az alábbi állításokat:

- (1) minden bíró jogász;
- (2) vannak ügyeskedő jogászok;
- (3) nincs ügyeskedő bíró;
- (4) bizonyos bírók idősek, de életerősek;
- (5) d bíró sem nem idős, sem nem életerős;
- (6) a bírók kivételével minden jogász ügyeskedő;

- (7) néhány jogász, aki politikus, képviselő is;
- (8) egyetlen képviselő felesége sem idős;
- (9) minden idős képviselő jogász;
- (10) van olyan nő, aki jogász és képviselő;
- (11) minden olyan nő, aki jogász, tisztel néhány bírót;
- (12) bizonyos jogászok csak bírókat tisztelnek;
- (13) van olyan bíró, aki tisztel néhány nőt;
- (14) bizonyos ügyeskedők egyetlen jogászt sem tisztelnek;
- (15) d bíró egyetlen ügyeskedőt sem tisztel;
- (16) vannak jogászok és ügyeskedők is, akik tisztelik d bírót;
- (17) csak bírók tisztelnek bírókat;
- (18) minden bíró csak bírókat tisztel;
- (19) minden nő képviselő életerős;
- (20) azok a jogászok, akiknek életerős feleségük van, mind képviselők.

→ **1.1.15. Feladat [4].** Jelölje $N()$, $E()$, $H()$, illetve $B()$ azt, hogy ma süt a nap, hogy ma esik az eső, hogy ma havazik, illetve hogy tegnap borult volt az ég. Fordítsuk le magyar nyelvre (az üres zárójeleket nem írtuk ki):

- (1) $(N \Rightarrow \neg(E \wedge H))$;
- (2) $(B \iff N)$;
- (3) $(B \wedge (N \vee E))$;
- (4) $((B \Rightarrow E) \vee N)$;
- (5) $(N \iff ((E \wedge \neg H) \vee B))$;
- (6) $((N \iff E) \wedge (\neg H \vee B))$.

→ **1.1.16. Feladat [7].** Definíáljuk formulával az alábbi kapcsolatokat: x az y -nak fia, lánya, szülője, apja, anyja, unokája, nagyszülője, nagyapja, nagyanyja, apai nagyapja, anyai nagyapja, apai nagyanyja, anyai nagyanyja, anyai nagyanyja, testvére, fivére, nővére, féltestvére, unokatestvére, nagybátyja, nagynénje, unokaöccse, unokahúga.

1.1.17. Feladat [6]. Bevezetve a $H(x, y)$ predikátumot arra, hogy x és y házastársak, definiáljuk formulával az alábbi kapcsolatokat: x az y -nak férje, felesége, sógora, sógornője, apósa, anyósa, veje, menyee.

1.1.18. Feladat [5]. Az előző két feladatban használt predikátumok mellett milyen predikátumra van még szükségünk, ha a bátyja, húga, nénje stb. fogalmakat is formalizálni akarunk?

→ **1.1.19. Feladat [6].** Formalizáljuk az alábbi állításokat:

- (1) Márta nem szőke;
- (2) nem igaz, hogy Mátyás nem elég virtuóz;
- (3) esik az eső, de meleg van, bár a nap is elbújt, és az idő is későre jár;
- (4) Éva vagy Pisti ott volt;

- (5) ha a hegy nem megy Mohamedhez, Mohamed megy a hegyhez;
- (6) elmegyünk kirándulni, ha nem esik az eső, és a szél sem fúj;
- (7) kizárt, hogy se matekból, se fizikából ne menjek át elsőre;
- (8) ha a szemtanú megbízható, és az ujjlenyomatok a tettestől származnak, akkor téved az írásszakértő;
- (9) szivárvány csak akkor van, ha esik az eső, a Nap is süt, de nincs dél;
- (10) minden ajtón van kilincs;
- (11) nem mind molnár, ki szekercét fog hóna alá;
- (12) ki nem szólt, csak bégetett, az kapott dicséretet;
- (13) mindig fázom, ha fúj a szél.

1.1.20. Feladat [5]. Formalizáljuk az alábbi térgeometriai axiómákat a P , E , S , I (pont, egyenes, sík, illeszkedik) predikátumok segítségével:

- (1) ha egy egyenes két pontja benne van egy síkban, akkor minden pontja benne van;
- (2) van négy nem egy síkban fekvő pont;
- (3) párhuzamossági axióma.

→ **1.1.21. Feladat [0].** Tegyük fel, hogy a következő három állítás igaz: Ha Éva angolul tud, akkor tud németül vagy franciául is. Éva nem tud németül. Éva valamelyiken beszél a három nyelvből. Következik-e ezekből, hogy Éva tud franciául?

→ **1.1.22. Feladat [6].** Egy táncmulatságon fiúk és lányok táncolnak. Jelölje $T(L, F)$, hogy az L lány táncolt az F fiúval. Formalizáljuk pontosan az alábbi „gyorsírással” felírt formulákat. Döntsük el, hogy melyik következik a másikból. (Egy formulából következik egy másik formula, ha valahányszor az egyik igaz, a másik is.)

$$\begin{aligned}
 (1) \quad & \exists L \forall F T(L, F), \quad \forall F \exists L T(L, F), \quad \exists F \forall L T(L, F), \\
 & \forall L \exists F T(L, F), \quad \forall L \forall F T(L, F), \quad \exists L \exists F T(L, F);
 \end{aligned}$$

$$(2) \quad \neg \exists L \exists F T(L, F), \quad \forall F \exists L \neg T(L, F), \quad \forall L \exists F \neg T(L, F), \quad \forall L \forall F \neg T(L, F).$$

1.1.23. További feladatok. [64]: 14.1.1–14.1.8, 14.2.1–14.2.3.

1.2 Halmazelméleti alapfogalmak

1.2.1. Halmazelmélet. A halmazokról szemléletes elképzelésünk, hogy a *halmaz* (*rendszer, osztály, összesség, egyeseknél család, sokaság, gyűjtemény*) elemeinek gondolati burka („zsák”). A halmazelméletben (az egyenlőségen kívül) a „*halmaznak lenni*” (nincs jele) és az „*eleme*” ($\in$) predikátum szerepel. Az $x \in A$ (vagy $A \ni x$) jelentése, hogy az x (elem, dolog, objektum) eleme az A halmaznak, vagy másként x hozzátartozik A -hoz. Ennek tagadását $x \notin A$ jelöli. (Tehát tetszőleges x -re $x \in A$ és $x \notin A$ közül pontosan az egyik teljesül.) Hasonlóan, más esetekben is áthúzással jelöljük a predikátum tagadását, például $A \neq B$ jelentése, hogy A nem egyenlő B -vel. Egy halmaz elemei között lehetnek

alfa	$A \alpha$	éta	$E \eta$	nű	$N \nu$	üpszilon	$\Upsilon \upsilon$
béta	$B \beta$	théta	$\Theta \theta$	kszi	$\Xi \xi$	phi	$\Phi \phi, \varphi$
gamma	$\Gamma \gamma$	ióta	$I \iota$	pi	$\Pi \pi, \varpi$	khi	$X \chi$
delta	$\Delta \delta$	kappa	$K \kappa, \varkappa$	ró	$P \rho, \varrho$	pszi	$\Psi \psi$
epszilon	$E \epsilon, \varepsilon$	lambda	$\Lambda \lambda$	szigma	$\Sigma \sigma, \varsigma$	omega	$\Omega \omega$
zéta	$Z \zeta$	mű	$M \mu$	tau	$T \tau$	digamma	F

A görög ábécé

halmazok is. A jelölések tetszőlegesek, de általában a „bonyolultabb dolog, bonyolultabb betű” elvet követjük. A halmazelmélet (Zermelo német matematikustól származó) axiómáit használjuk, de az axiómákat csak a teljesség kedvéért fogalmazzuk meg.

1.2.2. Meghatározottság. Egy halmazt az elemei határoznak meg. Az A és B halmaz akkor és csak akkor egyenlő, ha ugyanazok az elemei. Nincs olyasmi, hogy valami „többször eleme” egy halmaznak. A meghatározottság az „ $\in$ ” egy lényeges tulajdonságát fejezi ki, például a „gyermeke” predikátum az emberek között nem rendelkezik ezzel a tulajdonsággal.

* **1.2.3. Meghatározottsági axióma.** A meghatározottság elvét az alábbi formában fogalmazhatjuk meg axiómaként:

Az A és B halmaz akkor és csak akkor egyenlő, ha ugyanazok az elemei.

1.2.4. Részhalmazok. Akkor mondjuk, hogy az A halmaz *részhalmaza* a B halmaznak, vagy B *bővebb* A -nál, ha A minden eleme a B halmaznak is eleme. Jele: $A \subset B$ vagy $B \supset A$. Ha A részhalmaza B -nek, de nem egyenlő vele, akkor azt mondjuk, hogy A *valódi részhalmaza* B -nek. Jele: $A \subsetneq B$ vagy $B \supsetneq A$. (Más, logikusabb, de kevésbé elterjedt jelölések: $A \subseteq B$ vagy $B \supseteq A$ a részhalmazra és $A \subset B$ vagy $B \supset A$ a valódi részhalmazra.) Minden halmaz részhalmaza saját magának (*reflexivitás*), és ha $A \subset B$, $B \subset C$, akkor $A \subset C$ (*transzitivitás*). Ha $A \subset B$ és $B \subset A$, akkor a meghatározottsági axióma szerint $A = B$ (*antiszimmetria*). Az egyenlőségre is teljesülnek az iménti tulajdonságok, de még az is teljesül, hogy ha $A = B$, akkor $B = A$ (*szimmetria*). A meghatározottság úgy is fogalmazható, hogy az A és B halmazok pontosan akkor egyenlőek, ha $A \subset B$ és $B \subset A$. Rendszerint ennek alapján bizonyítjuk halmazok egyenlőségét.

Egy A halmazra és egy $\mathcal{F}(x)$ formulára jelölje $\{x \in A : \mathcal{F}(x)\}$ (vagy $\{x \in A \mid \mathcal{F}(x)\}$) azt a halmazt, amelyhez A -nak pontosan azok az x elemei tartoznak, amelyekre $\mathcal{F}(x)$ igaz. Ha világos, hogy milyen A halmaz részhalmazára gondolunk, az „ $\in A$ ” részt a jelölésből elhagyjuk.

* **1.2.5. Részhalmaz-axióma.** Azt, hogy egy adott halmazhoz és formulához létezik a megfelelő részhalmaz, a következő axióma biztosítja:

Minden A halmazra és minden $\mathcal{F}(x)$ formulára létezik egy B halmaz, amelyhez A -nak pontosan azok az x elemei tartoznak, amelyekre $\mathcal{F}(x)$ igaz.

A meghatározottsági axióma miatt B egyértelmű.

* **1.2.6. Tétel.** *Nincs olyan halmaz, amelynek minden dolog eleme.*

Bizonyítás. Legyen A tetszőleges halmaz, és legyen $B = \{x \in A : x \notin x\}$. Megmutatjuk, hogy $B \notin A$. Indirekt módon tegyük fel, hogy $B \in A$. Tudjuk, hogy $B \in B$ és

$B \notin B$ közül pontosan az egyik teljesül. Ha $B \in B$, akkor B definíciója szerint $B \notin B$ is fennáll, ami ellentmondás. Ha $B \notin B$, akkor B definíciója szerint $B \in B$, ugyancsak ellentmondás. $\square$

*** 1.2.7. Megjegyzés.** Csábítónak tűnik a részhalmaz-axióma helyett azt tenni fel, hogy minden $\mathcal{F}(x)$ formulához van olyan B halmaz, amelyhez pontosan azok az x dolgok tartoznak, amelyekre $\mathcal{F}(x)$ igaz (korlátozás nélküli halmazképzés). Ez nyilván erősebb kikötés, mint a részhalmaz-axióma, és a $B = \{x: \mathcal{F}(x)\}$ jelölést használhatjuk. Első pillantásra úgy tűnik, ennek az axiómának a használata jelentősen egyszerűsítene a halmazelméletet. Sajnos, túlságosan is: az $U = \{x: x = x\}$ „összes dolgok halmazára” vagy „univerzumra” alkalmazva az előző tételt, ellentmondásra jutnánk (Russell-paradoxon). Van azonban olyan változata a halmazelmélet axiómarendszerének, a Neumann–Bernays–Gödel-féle, rövidítve NBG-axiómarendszer, amely ilyen „túl nagy” dolgokat is megenged, de ezeket nem halmaznak tekinti, hanem osztálynak. Lásd részletesebben Kelley [43] könyvének függelékét. A halmazelméletnek ezzel a változatával nem foglalkozunk, számunkra az „osztály” szó a „halmaz” szó szinonimája.

1.2.8. Néhány egyszerű halmaz. Egy olyan halmazt, amelynek nincsen eleme, *üres halmaznak* nevezzük. Mivel bármely üres halmaznak ugyanazok az elemei (hiszen nincs elemük), az üres halmazok egyenlők, azaz csak egyetlen üres halmaz létezik. Jele: $\emptyset$. Az üres halmaz minden halmaznak részhalmaz, és persze minden nem üres halmaznak valódi részhalmaz. Azt a halmazt, amelynek a az egyetlen eleme, $\{a\}$ jelöli. Annak a halmaznak a jele, amelynek az a és b az elemei, $\{a, b\}$. Ezt a halmazt az a, b -ből alkotott (rendezetlen) *párnak* nevezzük. Persze semmi nem tiltja, hogy $a = b$ legyen, ekkor $\{a, b\} = \{a\} = \{b\}$. Hasonlóan $\{a, b, c\}$ az a halmaz, melynek a, b és c az elemei, stb. (Ennek megfelelően az algebrai programozási nyelvekben az üres halmazra szokásos a $\{\}$ jelölés is.)

*** 1.2.9. Az üres halmaz axiómája.** Ahhoz, hogy egyáltalán legyen halmaz az elméletünkben, a halmazok létezését egy axiómával biztosítanunk kell. Speciálisan:

Van olyan halmaz, amelynek nincs eleme.

A meghatározottság axiómája miatt csak egy üres halmaz van. A részhalmaz-axióma miatt ekvivalens lett volna azt feltenni, hogy van halmaz, mert akármely A halmazra $\{x \in A: x \neq x\}$ az üres halmaz.

*** 1.2.10. Páraxióma.** Biztosítanunk kell párok létezését is.

Bármely a -hoz és b -hez van olyan halmaz, amelynek ezek és csak ezek az elemei.

A részhalmaz-axióma miatt azt is elég lett volna feltenni, hogy van olyan A halmaz, amelynek a és b elemei, mert ekkor $\{a, b\} = \{x \in A: x = a \vee x = b\}$.

1.2.11. Unió. Ha A és B halmazok, akkor azt a halmazt, amelynek pontosan azok az elemei, melyek elemei A -nak vagy B -nek (vagy mindkettőnek), $A \cup B$ -vel jelöljük, és a két halmaz *uniójának* nevezzük. Régebbi könyvek néha $\cup$ helyett $+$ -t írnak. (Unió helyett *egyesítést* is szokás mondani.)

Jóval általánosabban, ha $\mathcal{A}$ egy halmaz, melynek elemei mind halmazok, akkor azt a halmazt, amely pontosan azokat a dolgokat tartalmazza, amelyek $\mathcal{A}$ valamely elemének az elemei, az $\mathcal{A}$ *uniójának* nevezzük. Ennek a jelölése: $\cup \mathcal{A}$ vagy $\cup\{A: A \in \mathcal{A}\}$ vagy $\cup_{A \in \mathcal{A}} A$.

Nyilván $\cup \emptyset = \emptyset$ és ha A egy halmaz, akkor $\cup\{A\} = A$, ha pedig A és B halmazok, akkor $A \cup B = \cup\{A, B\}$.

* **1.2.12. Unióaxióma.** Halmazrendszer (azaz olyan halmaz, amelynek elemei mind halmazok) uniójának létezését axiómával kell biztosítani.

Ha $\mathcal{A}$ egy halmaz, amelynek elemei mind halmazok, akkor van olyan halmaz, amely pontosan azokat a dolgokat tartalmazza, amelyek $\mathcal{A}$ legalább egy elemének elemei.

Nyilván itt is elég lett volna feltenni, hogy van olyan halmaz, amely $\mathcal{A}$ minden elemének minden elemét tartalmazza.

1.2.13. Állítás: az unió tulajdonságai. Ha A, B, C halmazok, akkor

- (1) $A \cup \emptyset = A$;
- (2) $A \cup B = B \cup A$ (kommutativitás);
- (3) $A \cup (B \cup C) = (A \cup B) \cup C$ (asszociativitás);
- (4) $A \cup A = A$ (idempotencia);
- (5) $A \subset B$ akkor és csak akkor, ha $A \cup B = B$.

Bizonyítás. Az (1) és (4) egyenlőség mindkét oldalán álló halmaznak pontosan akkor eleme x , ha $x \in A$. Hasonlóan, (2) mindkét oldalán álló halmaznak pontosan akkor eleme x , ha $x \in A$ vagy $x \in B$. Nem nehezebb (3) bizonyítása sem. Végül, ha $A \subset B$, akkor $A \cup B \subset B$, az ellenkező irányú tartalmazás pedig mindig teljesül; megfordítva, ha $A \cup B \subset B$, akkor A minden eleme eleme B -nek is. $\square$

1.2.14. Metszet. Ha A és B halmazok, legyen $A \cap B := \{x \in A : x \in B\}$. Régebbi könyvekben néha $\cap$ helyett $\cdot$ áll (vagy semmi sem). Jóval általánosabban, ha $\mathcal{A}$ halmazok egy nem üres rendszere, akkor a halmazrendszer *metszetét* a

$$\cap \mathcal{A} := \{x : x \in A \text{ minden } A \in \mathcal{A}\text{-ra}\}$$

összefüggéssel definiáljuk. Az üres rendszer metszetét nem definiáljuk, mert az „univerzum” lenne. Más jelölések: $\cap\{A : A \in \mathcal{A}\}$ és $\cap_{A \in \mathcal{A}} A$. Ha teljesen pontosak akarnánk lenni, akkor

$$\cap \mathcal{A} := \{x \in \cup \mathcal{A} : x \in A \text{ minden } A \in \mathcal{A}\text{-ra}\}.$$

Ha A és B halmazok, akkor nyilván $A \cap B = \cap\{A, B\}$.

Ha $A \cap B = \emptyset$, akkor azt mondjuk, hogy A és B *diszjunktak* (vagy *idegenek*). Általánosabban, ha egy nem üres $\mathcal{A}$ halmazrendszer metszete az üres halmaz, akkor azt mondjuk, hogy a halmazrendszer *diszjunkt*. Ha már a halmazrendszer bármely két különböző halmazának a metszete üres, akkor azt mondjuk, hogy elemei *páronként diszjunktak*. (Más szóhasználatban a páronként diszjunkt halmazokból álló halmazrendszert nevezik diszjunktoknak.)

1.2.15. Állítás: a metszet tulajdonságai. Ha A, B, C halmazok, akkor

- (1) $A \cap \emptyset = \emptyset$;
- (2) $A \cap B = B \cap A$ (kommutativitás);
- (3) $A \cap (B \cap C) = (A \cap B) \cap C$ (asszociativitás);
- (4) $A \cap A = A$ (idempotencia);
- (5) $A \subset B$ akkor és csak akkor, ha $A \cap B = A$.

Bizonyítás. Az állítások bizonyítása hasonló az unióra vonatkozó megfelelő állítások bizonyításához. $\square$

→ **1.2.16. Feladat [2].** Egészítsük ki az előző pont bizonyítását.

→ **1.2.17. Feladat [0].** Legyen $\mathcal{A} = \{\{a, b, c\}, \{a, d, e\}, \{a, f\}\}$.

Mi lesz $\cup \mathcal{A}$ és $\cap \mathcal{A}$?

→ **1.2.18. Feladat [1].** Adjunk meg olyan halmazrendszert, amely diszjunkt, de nem páronként diszjunkt. Van-e olyan halmazrendszer, amely páronként diszjunkt, de nem diszjunkt?

→° **1.2.19. Feladat [5].** Határozzuk meg a $\{\{x \in \mathbb{R}: |x| < y\}: y \in \mathbb{R}, y > 0\}$ halmazrendszer unióját és metszetét. Mi a helyzet, ha $y \in \mathbb{N}$, illetve $y \in \mathbb{Z}$?

° **1.2.20. Feladat [5].** Határozzuk meg a

$$\{\{x \in \mathbb{R}: |x - y| < r\}: y, r \in \mathbb{R}, |y| \leq 1, 1 < r < 5\}$$

halmazrendszer unióját és metszetét. Mi a helyzet, ha $|y| < 1$?

° **1.2.21. Feladat [5].** Határozzuk meg azon nyílt körlapok rendszerének unióját, illetve metszetét, amelyek sugarára $2 < r < 3$, középpontjuk koordinátáira pedig $0 \leq x, y \leq 1$.

1.2.22. Állítás: disztributivitási szabályok. Ha A, B, C halmazok, akkor

(1) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (a metszet disztributivitása az unióra nézve);

(2) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (az unió disztributivitása a metszetre nézve).

Az állítások megértésében segít, ha az egyes halmazokat „általános helyzetben” lévő „krumplikat” rajzolva szemléltetjük. Ezek az úgynevezett *Venn-diagramok*.

Bizonyítás. Csak (1)-et bizonyítjuk, (2) bizonyítása hasonló. Az $A \cap (B \cup C)$ halmaznak x pontosan akkor eleme, ha $x \in A$ és $x \in B \cup C$. Ez utóbbi pontosan akkor teljesül, ha $x \in B$ vagy $x \in C$. Így x pontosan akkor eleme az $A \cap (B \cup C)$ halmaznak ha $x \in A$ és $x \in B$ vagy pedig $x \in A$ és $x \in C$. Ez viszont azzal ekvivalens, hogy $x \in (A \cap B) \cup (A \cap C)$. $\square$

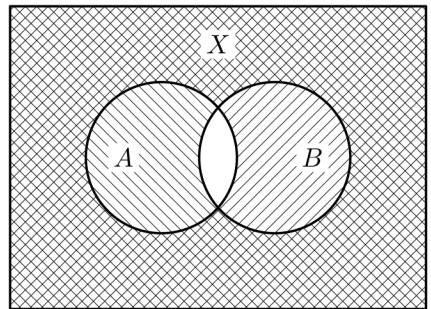
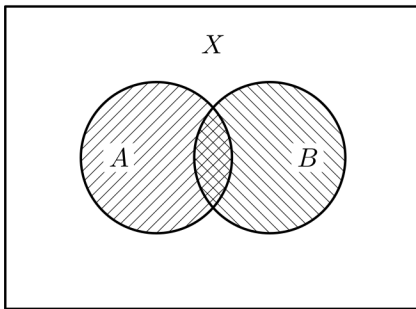
→ **1.2.23. Feladat [1].** Egészítsük ki az előző pont bizonyítását.

1.2.24. Különbőség és komplementer. Az unió- és metszetképzés mellett az alábbi halmazműveleteket is gyakran használjuk, például adatbázisok kezelésénél. Az A és B halmazok *különbőségét* (vagy *differenciáját*) az $A \setminus B := \{x \in A: x \notin B\}$ összefüggéssel definiáljuk. (Az $A - B$ jelölés is használatos.) A két halmaz *szimmetrikus differenciáját* (vagy *Boole-algebrái összegüket*) az $A \triangle B := (A \setminus B) \cup (B \setminus A)$ összefüggéssel definiáljuk. (Az $A + B$, $A \oplus B$, $A \circ B$ és $A \dot{+} B$ jelölések is használatosak.) Ha $A \subset X$, akkor az $X \setminus A$ halmazt néha A' -vel ($C_X A$ -val vagy $\overline{A}$ -sal) jelöljük, és az A halmaz X -re vonatkozó *komplementerének* (vagy *kiegészítő halmazának*) nevezzük. Ez természetesen nem csak A -tól, hanem az X „alaphalmaztól” is függ, ami az A' jelölésben nem jut kifejezésre. Emiatt, bár az A' jelölés rövidebb, általában mégis inkább kiírjuk helyette, hogy $X \setminus A$. A következő állításban meghagytuk a $'$ jelölést.

1.2.25. Állítás. Ha $A, B \subset X$, akkor az előző definíció jelöléseivel

- (1) $(A')' = A$;
- (2) $\emptyset' = X$;
- (3) $X' = \emptyset$;
- (4) $A \cap A' = \emptyset$;
- (5) $A \cup A' = X$;
- (6) $A \subset B$ akkor és csak akkor, ha $B' \subset A'$;
- (7) $(A \cup B)' = A' \cap B'$;
- (8) $(A \cap B)' = A' \cup B'$. $\square$

Az utolsó két állítást *De Morgan-szabályoknak* nevezik; általánosabb változatukat később tanuljuk. Megjegyezzük, hogy a (4) és (5) tulajdonságok együtt jellemzik A' -t, azaz pontosan egy olyan A' halmaz létezik, amelyre teljesül (4) és (5).



1.2.1 ábra: $A \cap B$ és $A' \cup B'$ Venn-diagramja.

→ **1.2.26. Feladat [3].** Részletezzük az előző pont bizonyítását.

→ **1.2.27. Feladat [4].** Melyik halmazművelet melyik logikai jellel van kapcsolatban?

→ **1.2.28. Feladat [5].** Legyenek $x = \{\text{alma}, \text{körte}\}$ és $y = \{\text{kutya}, \text{macska}\}$ halmazok. Az alábbi halmazok közül melyekre igaz, hogy x eleme, x részhalmaza, illetve x se nem eleme, se nem részhalmaza: $\{\{x\}, y\}$, x , $\emptyset \cap x$, $\{x\} \setminus \{\{x\}\}$, $\{x\} \cup x$, $\{x\} \cup \{\emptyset\}$.

→ **1.2.29. Feladat [0].** Bizonyítsuk be, hogy $(A \cup B) \setminus (A \cap B) = A \triangle B$.

→ **1.2.30. Feladat [3].** Mutassuk meg, hogy tetszőleges A, B, C halmazokra $A \triangle \emptyset = A$, $A \triangle A = \emptyset$, $A \triangle B = B \triangle A$ (kommutativitás), $(A \triangle B) \triangle C = A \triangle (B \triangle C)$ (asszociativitás), és $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$ (disztributivitás).

1.2.31. Feladat [3]. Mutassuk meg, hogy tetszőleges A, B halmazokra $A = \emptyset$ pontosan akkor, ha $B = A \triangle B$.

1.2.32. Feladat [3]. Mutassuk meg, hogy tetszőleges A, B, C halmazokra $A \triangle B \subset (A \triangle C) \cup (C \triangle B)$, és a tartalmazás lehet valódi.

° **1.2.33. Feladat [5].** Bizonyítsuk be, hogy ha $A_1, \dots, A_n$ halmazok, akkor x pontosan akkor eleme az $A_1 \triangle A_2 \triangle \dots \triangle A_n$ halmaznak, ha x az $A_1, \dots, A_n$ halmazok közül páratlan soknak eleme.

→ **1.2.34. Feladat [3].** Legyen $A, B, C, D \subset X$, és jelölje $'$ az X alaphalmazra vonatkozó komplementert. Egyszerűsítsük, amennyire lehet:

$$(1) \quad \left(A \cup (B \cap (C \cup D')) \right)';$$

$$(2) \quad ((A' \cup B) \cap (A \cup B'))';$$

$$(3) \quad (A \cap B \cap C) \cup (A' \cap B \cap C) \cup (A \cap B' \cap C) \cup (A \cap B \cap C') \\ \cup (A \cap B' \cap C') \cup (A' \cap B \cap C') \cup (A' \cap B' \cap C').$$

→ **1.2.35. Feladat [4].** Állapítsuk meg, hogy az alábbi állítások közül melyek igazak tetszőleges A, B, C halmazokra és melyek nem:

$$(1) \quad (A \cup B) \setminus A = B;$$

$$(2) \quad (A \cup B) \setminus C = A \cup (B \setminus C);$$

$$(3) \quad (A \setminus B) \cap C = (A \cap C) \setminus B = (A \cap C) \setminus (B \cap C);$$

$$(4) \quad A \setminus B = A \setminus (A \cap B).$$

1.2.36. Hatványhalmaz. Ha A halmaz, akkor azt a halmazrendszert, melynek elemei éppen A részhalmazai, az A *hatványhalmazának* nevezzük. Jele $\wp(A)$ (vagy $P(A)$), a $\wp$ betű a „Potenz” szóra utal (gyakori a 2^A jelölés is, ennek magyarázatát lásd később).

* **1.2.37. Hatványhalmaz-axióma.** A hatványhalmaz létezését is axiómával kell biztosítani.

Minden A halmazhoz létezik egy olyan halmazrendszer, amelynek elemei pontosan A részhalmazai.

Nyilván most is elég lett volna azt feltenni, hogy van olyan halmaz, amelynek A minden részhalmaza eleme.

→ **1.2.38. Feladat [3].** Írjuk fel a hatványhalmazt egy-egy 0, 1, 2, illetve 3 elemű halmazra.

→ **1.2.39. Feladat [5].** Írjuk fel a $\wp(\wp(\wp(\emptyset)))$ halmazt.

1.2.40. Feladat [6]. Bizonyítsuk be, hogy tetszőleges A, B halmazokra

$$(1) \quad \text{ha } A \subset B, \text{ akkor } \wp(A) \subset \wp(B);$$

$$(2) \quad A = B \text{ pontosan akkor, ha } \wp(A) = \wp(B), \text{ azaz } X \mapsto \wp(X) \text{ injektív};$$

$$(3) \quad \wp(A) \cap \wp(B) = \wp(A \cap B);$$

$$(4) \quad \wp(A) \cup \wp(B) \subset \wp(A \cup B).$$

Mikor teljesül egyenlőség (4)-ben?

→ **1.2.41. Feladat [5].** Ha X egy halmaz, legyen $X^+ = X \cup \{X\}$. Írjuk fel a $\emptyset^+$, $\emptyset^{++} := (\emptyset^+)^+$, $\emptyset^{+++}$ halmazokat. Igaz-e, hogy $\emptyset^+ \in \emptyset^{++}$, hogy $X \in X^+$, hogy $\emptyset^+ \subset \emptyset^{++}$, hogy $\emptyset^+ \cap \emptyset^{++} = \emptyset$, hogy $\emptyset^+ \cup \emptyset^{++} = \emptyset^{++}$, illetve hogy $(\emptyset \cap \emptyset^{++}) \in \emptyset^{++}$?

* **1.2.42. Végtelenségi axióma.** Van olyan A halmaz, amelynek az $\emptyset$ eleme, és ha valamely x halmaz eleme A -nak, akkor az $x \cup \{x\}$ halmaz is eleme A -nak.

Az axióma szemléletes tartalma, hogy az eddigiek alapján — az x halmazból az $x \cup \{x\}$ halmazt képezve — előállítható

$$\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \dots$$

halmazokat mind „bele tudjuk foglalni egyetlen halmazba”.

Nevezzük ideiglenesen a „ha x halmaz és $x \in A$, akkor $x \cup \{x\} \in A$ ” tulajdonságot rákövetkezésre zártágnak. Az axióma azt mondja ki, hogy van olyan A halmaz, amely tartalmazza az üres halmazt és zárt a rákövetkezésre. Mivel rákövetkezésre zárt halmazok minden nem üres rendszerének a metszete is zárt a rákövetkezésre, az A halmaz összes, az üres halmazt tartalmazó és a rákövetkezésre zárt részhalmazainak ω metszete tartalmazza az üres halmazt és zárt a rákövetkezésre. Az ω halmaz minden, az üres halmazt tartalmazó és a rákövetkezésre zárt halmaznak részhalmaza: ha B egy ilyen halmaz, akkor $A \cap B$ is, így $\omega \subset A \cap B \subset B$. Tehát ω a legszűkebb, az üres halmazt tartalmazó és rákövetkezésre zárt halmaz, és nem függ A választásától sem. Észrevehetjük, hogy ω elemei mind halmazok, ugyanis egy rákövetkezésre zárt halmaz minden olyan elemét elhagyva, amely nem halmaz, a rákövetkezésre zárt marad.

* **1.2.43. Megjegyzés.** Két további axióma még hátravan, ezeket a végtelen halmazoknál tárgyaljuk.

1.2.44. További feladatok részletes megoldással. [6]: 1–23.

1.2.45. További feladatok. [3]: I.1–I.13; [36]: 1.6, 1.8, 1.11, 1.14–1.34; [56]: 0–1.–2.0–30; [59]: I.1.1–I.1.18, I.1.1.20, I.1.24–I.1.28, I.1.30–I.1.33; [64]: 1.2.1–1.2.18; 1.[83]: II.8.2–II.8.5; [84]: 1.1.–1.1.2, 1.14–1.16, 1.27, 1.1.28, 1.30.

1.3 Relációk

A relációk a függvényfogalom általánosításai, és a függvénykapcsolatnál általánosabb kapcsolatok leírására is alkalmasak. Részletesebben az ekvivalenciarelációkkal, a részben rendezésekkel és a rendezésekkel foglalkozunk.

1.3.1. Rendezett pár. Az (x, y) rendezett párfogalmát úgy szeretnénk definiálni, hogy $(x, y) = (u, v)$ akkor és csak akkor teljesüljön, ha $x = u$ és $y = v$. Megtehetnénk, hogy a rendezett párt alapfogalomnak tekintjük, ekkor azonban új axiómákat kellene bevezetnünk, amelyek a rendezett pár fogalmát az eddigi fogalmakhoz kapcsolják. Ezt elkerülendő a rendezett párokat inkább halmazként fogjuk definiálni. Az $\{x, y\}$ halmaz nem alkalmas rendezett párnak, mert bár $x = u$ és $y = v$ fennállása esetén $\{x, y\} = \{u, v\}$, de megfordítva nem, mert abból, hogy $\{x, y\} = \{u, v\}$ csak az következik, hogy $x = u$ és $y = v$ (amit várunk) vagy pedig $x = v$ és $y = u$, amit nem szeretnénk. A „probléma” az, hogy $\{x, y\} = \{y, x\}$.

Bármely x, y esetén legyen $(x, y) := \{\{x\}, \{x, y\}\}$. Ezzel a definícióval $x = u$ és $y = v$ esetén nyilván $(x, y) = (u, v)$. Másrészt, ha $(x, y) = (u, v)$, akkor $\{x, y\} = \cup(x, y) = \cup(u, v) = \{u, v\}$, és így $x = u$ és $y = v$, amit várunk, vagy pedig $x = v$ és $y = u$. Az utóbbi eset azonban $x \neq y$ esetén lehetetlen, mert ekkor $\{\{x\}, \{x, y\}\} \neq \{\{y\}, \{y, x\}\}$,

hiszen a bal oldalon álló halmaznak van olyan eleme, amelynek x az egyetlen eleme, a jobb oldalon állónak pedig nincs.

Az (x, y) rendezett pár *első koordinátája* x , *második koordinátája* y .

◦ **1.3.2. Feladat [3].** A $\wp(\wp(\{1, 2\}))$ halmaz elemeiből melyek a rendezett párok?

1.3.3. Descartes-szorzat. Az X, Y halmazok *Descartes-szorzatán* vagy *direkt szor-
zatán* az

$$X \times Y := \{(x, y) : x \in X, y \in Y\}$$

rendezett párokból álló halmazt értjük (ez létezik, mert $\wp(\wp(X \cup Y))$ részhalmaza, ugyanis $x \in X, y \in Y$ esetén $\{x\}, \{x, y\} \in \wp(X \cup Y)$, így $(x, y) = \{\{x\}, \{x, y\}\} \in \wp(\wp(X \cup Y))$).

→ **1.3.4. Feladat [1].** Mutassuk meg, hogy $X \times Y = \emptyset$ pontosan akkor, ha $X = \emptyset$ vagy $Y = \emptyset$.

→ **1.3.5. Feladat [2].** Milyen X, Y halmazokra igaz, hogy $X \times Y = Y \times X$?

1.3.6. Feladat [3]. Mutassuk meg, hogy ha $X' \times Y' \neq \emptyset$, akkor $X' \times Y' \subset X \times Y$ pontosan akkor teljesül, ha $X' \subset X$ és $Y' \subset Y$.

1.3.7. Feladat [3]. Mutassuk meg, hogy $(X \times Y) \cup (X' \times Y) = (X \cup X') \times Y$ és $(X \times Y) \cup (X \times Y') = X \times (Y \cup Y')$.

1.3.8. Binér relációk. Egy halmazt *binér relációnak* (vagy *kétváltozós relációnak*) nevezzük, ha minden eleme rendezett pár. Ha R egy binér reláció, akkor $(x, y) \in R$ helyett gyakran azt írjuk, hogy xRy , és azt mondjuk, hogy x és y között fennáll az R reláció vagy x az R relációban van y -nal. (Vannak, akik egy reláció *grafikonjáról* vagy *gráfjáról* beszélnek, amikor párok halmazára gondolnak; vannak, akik a binér relációkat *megfeleltetésnek* nevezik.)

Egyszerű példák relációkra a két „szélsőséges eset”: az üres halmaz, illetve két halmaz Descartes-szorzata. Bármely X halmazra az

$$\mathbb{I}_X := \{(x, x) \in X \times X : x \in X\}$$

halmaz reláció (ez az egyenlőség X -en); ezt a relációt $X \times X$ *diagonálisának* is szokás nevezni. Bármely $\mathcal{F}$ halmazrendszerre az

$$\{(X, Y) \in \mathcal{F} \times \mathcal{F} : X \subset Y\}$$

halmaz binér reláció (ez a tartalmazás $\mathcal{F}$ halmazai között). Bármely $\mathcal{F}$ halmazrendszerre az

$$\{(X, Y) \in \mathcal{F} \times \mathcal{F} : X \subsetneq Y\}$$

halmaz binér reláció (ez a valódi tartalmazás $\mathcal{F}$ halmazai között).

Ha valamely X és Y halmazokra $R \subset X \times Y$, akkor azt mondjuk, hogy R reláció X és Y között. Itt X és Y nyilván nem egyértelműek, hiszen $X \subset X'$ és $Y \subset Y'$ esetén $R \subset X' \times Y'$. (Minden relációhoz léteznek ilyen halmazok, például $X = Y = \cup(\cup R)$ megfelelő, mert $(x, y) = \{\{x\}, \{x, y\}\} \in R$ esetén $\{x\}, \{x, y\} \in \cup R$, így $x, y \in \cup(\cup R)$.) Ha $X = Y$, akkor azt mondjuk, hogy R egy X -beli binér reláció (homogén binér reláció). Nyilván minden X és Y közötti binér reláció tekinthető $X \cup Y$ -beli binér relációnak.

◦ **1.3.9. Feladat [10].** Ábrázoljuk azon (x, y) valós számpárok síkbeli halmazát, amelyek eleget tesznek a megadott összefüggésnek:

- (1) $y = x^n$, $n = 1, 2, 3, 4, 5, 6, -1, -2, -3, -4$;
- (2) $y^m = x$, $m = 2, 3, 4, 5$;
- (3) $y^2 = x^3$ (*Neile-féle parabola*);
- (4) $y^m = x^n$, $(m, n) \in \{(2, 1), (2, 3), (3, 1), (3, 2), (3, 4), (4, 2), (4, 3)\}$;
- (5) $xy = 1 + x^2$ (*hiperbola*);
- (6) $xy = 1 + x^3$ (*Newton-féle háromágú szigony*);
- (7) $yx^2 = 1 + x^3$;
- (8) $y(1 + x^2) = 1$ (*Agnesi-görbe*);
- (9) $y(1 + x^2) = 2x$ (*Newton-féle szerpentin*);
- (10) $y(1 - x^2) = 1$;
- (11) $y(1 - x^2) = x$;
- (12) $y^2 = -x - 2$ (*parabola*);
- (13) $4y^2 + x^2 = 100$ (*ellipszis*);
- (14) $y^2 = x^2 - 1$ (*hiperbola*);
- (15) $y^2(1 + x) = 1 - x$;
- (16) $y^2 = x^2(100 - x^2)$;
- (17) $y^2(10 - x) = x^3$ (*cisszois*);
- (18) $|x|^n + |y|^n = 1$, $n = 1, 2, 3, 4, 5, 1/2, 1/3, 1/4$;
- (19) $\max\{|x|, |y|\} = 1$;
- (20) $xy = \lfloor x \rfloor$.

◦ **1.3.10. Feladat [9].** Ábrázoljuk a megadott valós számpárok síkbeli halmazát:

- (1) $\{(1 - t, 1 - t^2): t \in \mathbb{R}\}$;
- (2) $\{(t + 1/t, t + 1/t^2): t \in \mathbb{R}\}$;
- (3) $\{(10 \cos t, \sin t): t \in \mathbb{R}\}$ (*ellipszis*);
- (4) $\{(5 \cos^2 t, 3 \sin^2 t): t \in \mathbb{R}\}$;
- (5) $\{(2(t - \sin t), 2(1 - \cos t)): t \in \mathbb{R}\}$ (*ciklois*);

◦ **1.3.11. Feladat [9].** Paraméterezést bevezetve, ábrázoljuk azon (x, y) valós számpárok síkbeli halmazát, amelyek eleget tesznek a megadott összefüggésnek:

- (1) $x^3 + y^3 = 3xy$ (*Descartes-féle levél*);
- (2) $x^2 + y^2 = x^4 + y^4$;
- (3) $x^2 y^2 = x^3 - y^3$;
- (4) $x^{2/3} + y^{2/3} = 1$ (*astroid*);
- (5) $x^y = y^x$, $x, y > 0$.

° **1.3.12. Feladat [8].** Polár koordinátára áttérve, ábrázoljuk azon (x, y) valós számpárok síkbeli halmazát, amelyek eleget tesznek a megadott összefüggésnek:

- (1) $(x^2 + y^2)^2 = x^2 - y^2$ (Bernoulli lemniszkátája);
- (2) $x^4 + y^4 = 2xy$;
- (3) $(x^2 + y^2 - 6x)^2 = x^2 + y^2$;
- (4) $(x^2 + y^2 - 4x)^2 = 16(x^2 + y^2)$;
- (5) $x^4 + y^4 = 8xy^2$;
- (6) $x^4 + y^4 = x^2 + y^2$;
- (7) $(x^2 + y^2)^2 = 27x^2y^2$;
- (8) $(x^2 + y^2)^2 = xy$.

° **1.3.13. Feladat [8].** Ábrázoljuk az alábbi, (r, φ) polárkoordinátákban megadott síkbeli halmazokat:

- (1) $r = \varphi$ (arkhimédészi spirális);
- (2) $r = \pi/\varphi$ (hiperbolikus spirális);
- (3) $r = \varphi/(1 + \varphi)$;
- (4) $r = 2^{\varphi/(2\pi)}$ (logaritmikus spirális);
- (5) $r = 2(1 + \cos \varphi)$ (kardiod);
- (6) $r = \sin 3\varphi$ (háromlevelű rozetta);
- (7) $r^2 = \cos 2\varphi$ (Bernoulli lemniszkátája).

° **1.3.14. Relációk gráfja.** Gyakran érdemes binér relációkat úgynevezett „nyíldiagrammal” (tulajdonképpen a reláció irányított gráfjával, lásd később) szemléltetni: egy $R \subset X \times Y$ binér reláció szemléltetésére ábrázoljuk pontokkal X és Y elemeit, és vezessen irányított él x -ből y -ba (azaz rajzoljunk egy x -ből y -ba vezető nyilat), ha $(x, y) \in R$. Lásd az 1.3.1 ábrát.

1.3.15. Értelmezési tartomány, értékészlet. Az R binér reláció értelmezési tartományát a

$$\text{dmn}(R) := \{x: \text{van olyan } y, \text{ hogy } (x, y) \in R\},$$

értékészletét pedig a

$$\text{rng}(R) := \{y: \text{van olyan } x, \text{ hogy } (x, y) \in R\}$$

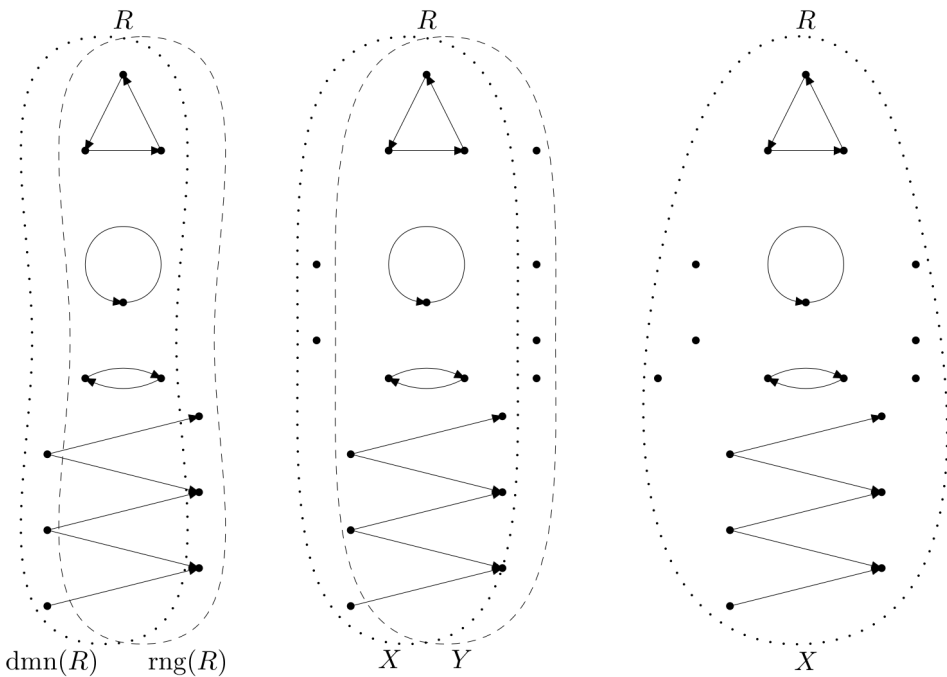
összefüggéssel értelmezzük. A jelölések a „domain”, illetve „range” szóra utalnak; dom vagy $\mathcal{D}$, illetve ran , $\mathcal{R}$ vagy im (az „image” szóból) is szokásosak.

→ **1.3.16. Feladat [0].** Mutassuk meg, hogy egy R relációra $R = \emptyset$, $\text{dmn}(R) = \emptyset$ és $\text{rng}(R) = \emptyset$ ekvivalensek.

1.3.17. Kiterjesztés, leszűkítés. Az R binér relációt az S binér reláció kiterjesztésének, illetve S -et az R leszűkítésének (vagy megszorításának) nevezzük, ha $S \subset R$. Ha A egy halmaz, az R reláció A -ra való leszűkítésén (vagy A -ra való megszorításán) az

$$R|_A := \{(x, y) \in R: x \in A\}$$

relációt értjük. Lásd az 1.3.2 ábrát.



1.3.1 ábra: dmn és rng , reláció X és Y között, X -beli reláció.

1.3.18. Inverz. Egy R binér *inverzén* az

$$R^{-1} := \{(b, a) : (a, b) \in R\}$$

binér relációt értjük. Nyilván $(R^{-1})^{-1} = R$; ha R reláció X és Y között, akkor R^{-1} reláció Y és X között, és $\text{dmn}(R^{-1}) = \text{rng}(R)$, valamint $\text{rng}(R^{-1}) = \text{dmn}(R)$.

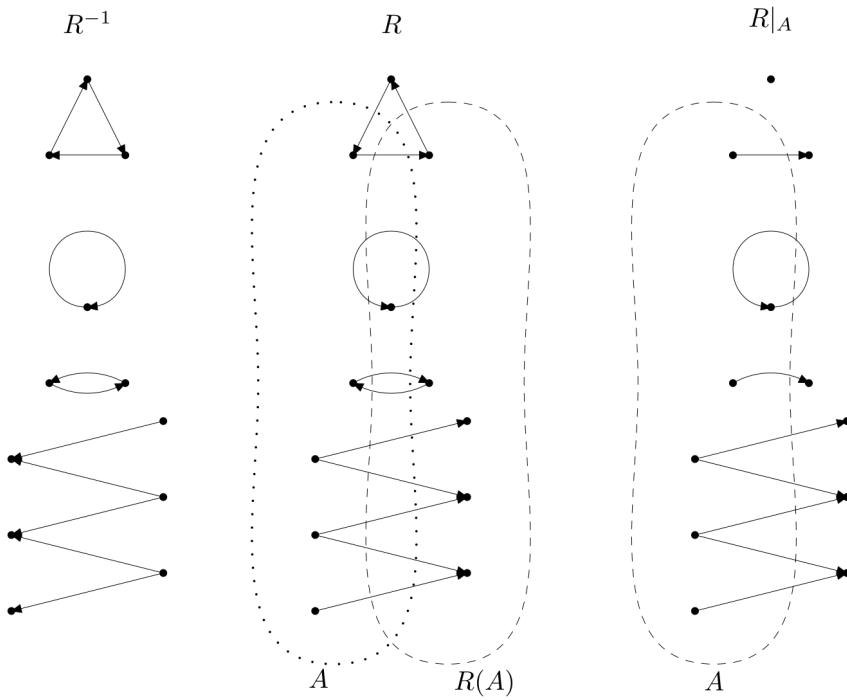
1.3.19. Halmaz képe és inverz képe. Legyen R egy binér reláció és A egy halmaz. Az A *halmaz képe* az R relációnál az

$$R(A) := \{y : \text{van olyan } x \in A, \text{ hogy } (x, y) \in R\}$$

halmaz. Vegyük észre, hogy $R(A)$ pontosan akkor üres, ha A és $\text{dmn}(R)$ diszjunktak. A B halmaz *inverz képe* vagy *ősképe* az R relációnál $R^{-1}(B)$. Ha $A = \{a\}$, akkor $R(\{a\})$ helyett $R(a)$ -t is írhatunk. Ez kényelmes, de néha félreértésekhez vezethet, ha például a és $\{a\}$ is eleme $\text{dmn}(R)$ -nek; ilyen kétes esetekben megmondjuk, hogy hagytunk-e el zárójelet.

→ **1.3.20. Feladat [0].** Ha R binér reláció, mi lesz $R(\emptyset)$, $R^{-1}(\emptyset)$, $R(\text{dmn}(R))$ és $R^{-1}(\text{rng}(R))$?

→° **1.3.21. Feladat [5].** Az $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y^2 = 2 - x - x^2\}$ relációra határozzuk meg a $\{0\}$ halmaz képét és teljes inverz képét. Mely $A \subset \mathbb{R}$ halmazokra lesz $R(A)$ illetve $R^{-1}(A)$ egyelemű?



1.3.2 ábra: Reláció inverze, halmaz képe, reláció megszorítása.

→° **1.3.22. Feladat [3].** Írjuk fel intervallumokkal az $x \mapsto |x|$ leképezésnél az alábbi halmazok teljes inverz képét: $[-1, 2]$, $]1, 4[$, $[-1, 2[$.

→ **1.3.23. Feladat [2].** Mutassuk meg, hogy bármely R relációra és A halmazra $A \subset R^{-1}(R(A))$ pontosan akkor, ha $A \subset \text{dmn}(R)$.

1.3.24. Kompozíció. Az R és S binér relációk *összetételén* (*kompozícióján*, *szorzatán*) az

$$R \circ S := \{(x, y) : \text{van olyan } z, \text{ hogy } (x, z) \in S \text{ és } (z, y) \in R\}$$

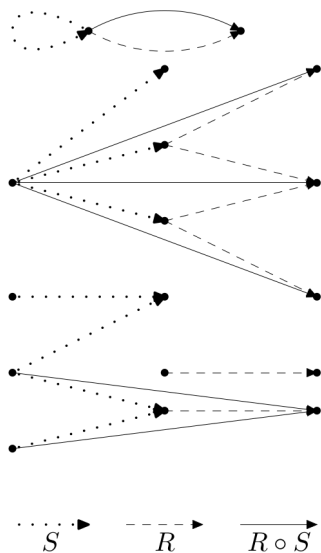
relációt értjük. Lásd a 1.3.3 ábrát. (Egyesek fordítva, $S \circ R$ -et írnak; a fenti jelölés előnye, hogy ezzel bármely A halmazra $R(S(A)) = (R \circ S)(A)$.)

Két reláció kompozíciója lehet üres: ez a helyzet, ha $\text{rng}(S)$ és $\text{dmn}(R)$ diszjunktak.

° **1.3.25. Feladat [3].** Határozzuk meg az $R \cap S$ relációt, ha R az m osztója n -nek reláció $\mathbb{N}^+$ -on, S pedig az $n = m + 6$ reláció $\mathbb{Z}$ -n.

→° **1.3.26. Feladat [7].** Határozzuk meg az $S \circ R$ és $R \circ S$ szorzatot, ha

- (1) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y^2 = x\}$ és $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = 2x\}$;
- (2) $R = \{(x, y) \in \mathbb{R}^+ \times \mathbb{R} : y^3 = x\}$ és $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = \tan x\}$;
- (3) $R = \{(x, y) \in [-\pi, \pi] \times \mathbb{R} : y = \sin x\}$ és $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y + 1/y = x\}$;
- (4) $R = S = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x < y\}$;
- (5) $R = S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x < y\}$;



1.3.3 ábra: két reláció kompozíciója.

- (6) $R = S = \{(x, y) \in \mathbb{N}^+ \times \mathbb{N}^+ : x \text{ osztója } y, \text{ de } x \neq y\}$;
- (7) A tetszőleges halmaz, $R = \{(x, y) \in \wp(A) \times \wp(A) : x \cap y = \emptyset\}$ és $S = \{(x, y) \in \wp(A) \times \wp(A) : x \subset y\}$;
- (8) K és L két körlap a P síkban és $R = \{(x, y) \in P \times P : x = y \text{ vagy } x, y \in K\}$ és $S = \{(x, y) \in P \times P : x = y \text{ vagy } x, y \in L\}$.

1.3.27. Állítás. Legyen R, S és T binér reláció. Ekkor

- (1) ha $\text{rng}(S) \supset \text{dmn}(R)$, akkor $\text{rng}(R \circ S) = \text{rng}(R)$;
- (2) $R \circ (S \circ T) = (R \circ S) \circ T$ (a kompozíció asszociativitása);
- (3) $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$. $\square$

1.3.28. Állítás. Ha R reláció X és Y között, akkor $\mathbb{I}_Y \circ R = R$ és $R \circ \mathbb{I}_X = R$. $\square$

1.3.29. Definíció. Legyen R egy X -beli binér reláció. Azt mondjuk, hogy R

- (1) *transzítív*, ha minden x, y, z -re $(x, y) \in R$ és $(y, z) \in R$ esetén $(x, z) \in R$;
- (2) *szimmetrikus*, ha minden x, y -ra $(x, y) \in R$ esetén $(y, x) \in R$;
- (3) *antiszimmetrikus*, ha minden x, y -ra $(x, y) \in R$ és $(y, x) \in R$ esetén $x = y$;
- (4) *szigorúan antiszimmetrikus*, ha minden x, y -ra $(x, y) \in R$ esetén $(y, x) \notin R$;
- (5) *irreflexív*, ha (x, x) alakú pár nincs R -ben;
- (6) *reflexív*, ha minden $x \in X$ esetén $(x, x) \in R$;
- (7) *trichotom*, ha minden $x, y \in X$ esetén $x = y$, $(x, y) \in R$ és $(y, x) \in R$ közül pontosan egy teljesül;
- (8) *dichotom*, ha minden $x, y \in X$ esetén $(x, y) \in R$ vagy $(y, x) \in R$ (esetleg mindkettő), amire azt is mondjuk, hogy bármely két elem „összehasonlítható”.

Vegyük észre, hogy az első öt tulajdonság csak R -től, míg az utolsó három R -től és X -től is függ, így ezek az (X, R) pár tulajdonságai.

A binér reláció definíciójánál mindegyik tulajdonság teljesülésére találunk példát, és a (2)–(8) tulajdonságok nem teljesülésére is. Nem tranzitív az egyenes pontjai között az a reláció, hogy legfeljebb 1 távolságra vannak. között az a reláció, hogy legfeljebb 1 távolságra vannak.

→ **1.3.30. Feladat [5].** Legyen X kételemű halmaz. Határozzuk meg az összes X -beli binér relációt. Keressünk példát a tanult relációtulajdonságok (tranzitív, stb.) mindegyikének teljesülésére és nem teljesülésére is.

→ **1.3.31. Feladat [5].** Hogyan tükröződnek egy R reláció gráján az előző definícióban megfogalmazott tulajdonságok?

° **1.3.32. Feladat [4].** Milyen tulajdonságokkal rendelkezik a sík egyenesei közötti párhuzamosság illetve merőlegesség?

→ **1.3.33. Feladat [6].** Az emberek halmazán tekintve, milyen tulajdonságokkal rendelkeznek az apja, szülője, anyja, testvére, féltestvére, gyermeke, nagyszülője, unokája, nagyapja, nagyanyja, anyai nagyszülője relációk?

1.3.34. Feladat [6]. Az emberek halmazán fejezzük ki az előző feladatban szereplő összes relációt az apja és a szülője relációk segítségével.

→ **1.3.35. Feladat [6].** Az emberek halmazán tekintve, milyen tulajdonságokkal rendelkeznek az egyenesági leszármazottja és egyenesági rokona relációk?

1.3.36. Feladat [6]. Bizonyítsuk be, hogy egy X -beli R binér relációra

- (1) R pontosan akkor tranzitív, ha $R \circ R \subset R$;
- (2) R pontosan akkor szimmetrikus, ha $R^{-1} = R$;
- (3) R pontosan akkor antiszimmetrikus, ha $R \cap R^{-1} \subset \mathbb{I}_X$;
- (4) R pontosan akkor szigorúan antiszimmetrikus, ha $R \cap R^{-1} = \emptyset$;
- (5) R pontosan akkor irreflexív, ha $\mathbb{I}_X \cap R = \emptyset$;
- (6) R pontosan akkor reflexív, ha $\mathbb{I}_X \subset R$;
- (7) R pontosan akkor trichotom, ha R , R^{-1} és $\mathbb{I}_X$ páronként diszjunktak és egyesítésük $X \times X$;
- (8) R pontosan akkor dichotom, ha $R \cup R^{-1} = X \times X$.

Próbáljuk meg ezekből az összefüggésekből leolvasni, hogy egy vagy két tulajdonságból következik-e egy másik.

° **1.3.37. Reflexív, szimmetrikus, illetve tranzitív relációk grájának egyszerűsítése.** Reflexív relációk irányított gráját egyszerűsíthetjük, ha nem rajzoljuk meg az úgynevezett hurokéleket, amelyeknek a kezdőpontja és a végpontja ugyanaz. Szimmetrikus relációk irányított gráját egyszerűsíthetjük, ha az (x, y) és (y, x) pároknak megfelelő irányított élek („nyilak”) helyett csak egy x -et és y -t összekötő élt („ívet”) rajzolunk, azaz irányítatlan gráfot használunk. Tranzitív relációk (irányított vagy irányítatlan) gráját egyszerűsíthetjük, ha elhagyunk a grájból olyan éleket, amelyek létezése a tranzitivitás miatt a már berajzolt élekből következik.

1.3.38. Ekvivalenciareláció, osztályozás. Legyen X egy halmaz. Az X -beli binér relációt *ekvivalenciareláció*nak nevezzük, ha reflexív, szimmetrikus és tranzitív. Az X részhalmazainak egy $\mathcal{O}$ rendszerét X *osztályozásának* nevezzük, ha $\mathcal{O}$ páronként diszjunkt nem üres halmazokból álló halmazrendszer, amelyre $\cup \mathcal{O} = X$.

Fontos kapcsolat áll fenn az X halmazbeli ekvivalenciarelációk és X osztályozásai között.

1.3.39. Tétel. Valamely X halmazon értelmezett $\sim$ ekvivalenciareláció esetén az $\tilde{x} = \{y \in X: y \sim x\}$, $x \in X$ ekvivalenciaosztályok X -nek egy $\tilde{X} = X / \sim$ osztályozását adják. Megfordítva, az X halmaz bármely $\mathcal{O}$ osztályozása esetén az $\cup \{Y \times Y: Y \in \mathcal{O}\}$ reláció ekvivalenciareláció, amelyhez tartozó ekvivalenciaosztályok halmaza $\mathcal{O}$. Hasonlóan, ha egy ekvivalenciarelációra képezzük az ekvivalenciaosztályokat, majd ebből a hozzá tartozó ekvivalenciarelációt, akkor az eredeti relációt kapjuk vissza.

Bizonyítás. Legyen $\sim$ egy X -beli ekvivalenciareláció, és legyen $\tilde{x} = \{y \in X: y \sim x\}$ az X halmaz x elemének ekvivalenciaosztálya. Azt kell megmutatnunk, hogy az $\tilde{X} = \{\tilde{x}: x \in X\}$ halmaz az X egy osztályozása. Mivel $\sim$ reflexív, $x \in \tilde{x}$, vagyis az $\tilde{x}$ részhalmaz nem üres, és az X halmaz minden x eleme benne van a $\tilde{X}$ valamely elemében, például $\tilde{x}$ -ban. Már csak azt kell belátnunk, hogy a különböző ekvivalenciaosztályok metszete üres. Ha $\tilde{x} \cap \tilde{y} \neq \emptyset$, akkor legyen z a metszet egy eleme. Ekkor $z \sim x$ és $z \sim y$, amiből a szimmetria és a tranzitivitás miatt $x \sim y$. Ha most $w \in \tilde{x}$, akkor a tranzitivitás miatt $w \in \tilde{y}$. Hasonlóan, a szimmetria és a tranzitivitás miatt, ha $w \in \tilde{y}$, akkor $w \in \tilde{x}$. Azt kaptuk tehát, hogy $\tilde{x} = \tilde{y}$, azaz ha két részhalmaznak van közös eleme, akkor azonosak, vagyis a különböző $\tilde{x}$ részhalmazok diszjunktak, ezért valóban az X egy osztályozását kaptuk, és $\tilde{x}$ az x -et tartalmazó osztály.

Megfordítva, legyen $\mathcal{O}$ az X egy osztályozása, és legyen $R = \cup \{Y \times Y: Y \in \mathcal{O}\}$. Nyilván $(x, y) \in R$ pontosan akkor teljesül, ha x és y az $\mathcal{O}$ ugyanazon halmazának elemei. Ez az R nyilván reflexív, szimmetrikus és mivel az osztályok páronként diszjunktak, tranzitív is, tehát ekvivalenciareláció. Az is nyilvánvaló, hogy ha egy osztályozásból képezzük a hozzá tartozó ekvivalenciarelációt, majd ebből a megfelelő ekvivalenciaosztályokat, akkor az eredeti osztályozást kapjuk vissza, és fordítva, ha egy ekvivalenciarelációból képezzük a fentiek szerint hozzá tartozó osztályozást, majd abból a hozzá tartozó ekvivalenciarelációt, akkor az eredeti relációt kapjuk vissza. $\square$

1.3.40. Példa. Egyenesek párhuzamossága ekvivalenciareláció, az ekvivalenciaosztályok az *irány* fogalmához vezetnek. Egy irányt az osztály bármely elemével reprezentálhatunk.

→ **1.3.41. Feladat [0].** Mi a hiba a következő okoskodásban? Szimmetrikus és tranzitív R reláció reflexív is, mert ha xRy akkor yRx is, és a tranzitivitás miatt ebből xRx .

→ **1.3.42. Feladat [2].** Adjunk példát olyan binér relációra, amely

- (1) reflexív és szimmetrikus, de nem tranzitív;
- (2) reflexív és tranzitív, de nem szimmetrikus;
- (3) tranzitív és szimmetrikus, de nem reflexív.

→ **1.3.43. Feladat [6].** Hány különböző osztályozása van egy 0, 1, 2, 3, illetve 4 elemű halmaznak?

1.3.44. Részbenrendezés, rendezés. Egy X halmazbeli *részbenrendezés* (parciális rendezés, féligrendezés, más szerzőknél *rendezés*) egy tranzitív, reflexív és antiszimmetrikus X -beli reláció. A részbenrendezés jelölésére rendszerint $\leq$ jelet vagy valamilyen hasonló jelet (például $\leq, \leqslant, \leqslant, \preceq, \prec, \preceq$ stb.) használunk. Ha $x, y \in X$, és $x \leq y$ vagy $y \leq x$ (esetleg mindkettő), akkor azt mondjuk, hogy a két elem *összehasonlítható*. Ha a $\leq$ részbenrendezési reláció dichotom is, azaz ha X bármely két eleme összehasonlítható, akkor *rendezésnek* (teljes rendezésnek, lineáris rendezésnek) nevezzük. Egy X *részbenrendezett halmaz*, illetve *rendezett halmaz* tulajdonképpen az $(X, \leq)$ pár. Egy X részbenrendezett halmaz minden Y részhalmaza is részbenrendezett, ha a $\leq$ relációt csak ennek az elemei között tekintjük, azaz a $\leq \cap (Y \times Y)$ relációval. Ha az Y részhalmaz ezzel a relációval rendezett, akkor *láncknak* nevezzük.

A legegyszerűbb példa részbenrendezésre egy halmazrendszer a tartalmazással.

° **1.3.45. Példa.** A valós számok halmaza — és így a természetes, egész és racionális számok halmaza is — rendezett a szokásos rendezéssel. A természetes számok körében az „ n osztja m -et” reláció részbenrendezés, de nem rendezés.

1.3.46. Szigorú és gyenge reláció. Egy X -beli R relációhoz definiálhatunk egy X -beli S relációt úgy, hogy xSy akkor álljon fenn, ha xRy de $x \neq y$, ez az R -nek megfelelő *szigorú reláció*. Megfordítva, egy X -beli R relációhoz a megfelelő T *gyenge relációt* úgy definiáljuk, hogy legyen xTy , ha xRy vagy $x = y$. Megjegyezzük, hogy tulajdonképpen $\mathbb{I}_X$ elvétele vagy hozzátétele történik: $S = R \setminus \mathbb{I}_X$ és $T = R \cup \mathbb{I}_X$.

1.3.47. Szigorú és gyenge rendezés. Egy $\leq$ részbenrendezés esetén a megfelelő szigorú relációt $<$ -el jelöljük; ez nyilván irreflexív és tranzitív is: Ha $x < y$ és $y < z$, akkor $x < y$ és $y < z$, ahonnan $x < z$. Ha $x = z$ lenne, akkor teljesülne $y \leq x$, így $x = y$ is, ellentmondás. A tranzitivitásból és az irreflexivitásból következik a szigorú antiszimmetria: $x < y$ esetén $y < x$ nem teljesülhet, mert ebből $x < x$ következne. Megfordítva, ha $<$ egy X -beli *szigorú részbenrendezés*, amin egy tranzitív és szigorúan antiszimmetrikus (tehát szükségképpen irreflexív) relációt értünk, akkor a megfelelő gyenge reláció egy részbenrendezés. Egy részbenrendezésből kapott szigorú részbenrendezésből ily módon az eredeti részbenrendezést kapjuk vissza, ha pedig egy szigorú részbenrendezésből készítünk egy részbenrendezést, majd abból a megfelelő szigorú részbenrendezést, akkor az eredeti szigorú részbenrendezést kapjuk vissza.

Ha $\leq$ rendezés, akkor a megfelelő $<$ reláció trichotom is, és megfordítva, ha a $<$ reláció trichotom, akkor a megfelelő $\leq$ reláció rendezés. Megjegyezzük, hogy egy trichotom és tranzitív reláció irreflexív és szigorúan antiszimmetrikus.

Az $x \leq y$ helyett azt is írjuk, hogy $y \geq x$, az $x < y$ helyett pedig, hogy $y > x$. Tulajdonképpen a $\geq$ reláció a $\leq$ reláció inverze, $>$ pedig a $<$ reláció inverze. Ha $x < y$, akkor azt mondjuk, hogy x *kisebb*, mint y vagy y *nagyobb*, mint x , illetve hogy x *megelőzi* y -t vagy y *követi* x -et. A gyenge reláció esetén hozzátesszük, hogy „vagy egyenlő”.

Ha a részbenrendezés jelölésére más jelet használunk, akkor a *szigorú párja* jelölésére a jel megfelelő nyomdai párja szolgál. Ha tehát például $\preceq$ egy részbenrendezés, akkor a szigorú párja $\prec$, ha viszont $\prec$ jelöli a részbenrendezést, akkor a szigorú párja $\precneq$.

Egy halmazrendszeren a tartalmazás szigorú párja a valódi tartalmazás.

→ **1.3.48. Feladat [0].** Mutassuk meg, hogy ha egy részben rendezett halmazban $x < y$ és $y \leq z$, akkor $x < z$.

→ **1.3.49. Feladat** [1]. Lehet-e $\emptyset$ ekvivalencia reláció, részbenrendezés, rendezés, szigorú részbenrendezés, illetve szigorú rendezés?

1.3.50. Intervallumok. Legyen X egy részbenrendezett halmaz. Ha $x \leq z$ és $z \leq y$, akkor azt mondjuk, hogy z az x és y közé esik, ha pedig $x < z$ és $z < y$, akkor azt mondjuk, hogy z szigorúan x és y közé esik. Az összes ilyen elemek halmazát $[x, y]$, illetve $]x, y[$ jelöli. Az utóbbi halmaz jelölésére (x, y) is szokásos; hátránya, hogy megegyezik a rendezett pár jelölésével. A $]x, y[$ és $[x, y[$ halmazok definíciója analóg; itt is használatos a kerek zárójeles változat. Ha $x < y$, de ugyanakkor nem létezik szigorúan x és y közé eső elem, akkor azt mondjuk, hogy x közvetlenül megelőzi y -t, vagy y közvetlenül követi x -et. Egy x elemhez tartozó kezdőszeletnek a $\{y \in X : y < x\}$ részhalmazt nevezzük. A kezdőszelet logikus, de nem elterjedt jelölése $]\leftarrow, x[$. A $]\leftarrow, x[$, $]x, \rightarrow[$, $[x, \rightarrow[$ jelöléseket analóg módon értelmezzük. Az itt definiált halmazokat közös néven *intervallumoknak* nevezzük. Szokás az $[x, y]$, $]x, y[$, $[x, y[$ illetve $]x, y]$ intervallumokat rendre *zárt*, *nyílt*, *alulról zárt*, *felülről nyílt* illetve *alulról nyílt*, *felülről zárt* intervallumoknak nevezni; az elnevezés az analízisből jön.

° **1.3.51. Részbenrendezések Hasse-diagramja.** Ha egy részbenrendezett halmaz elemeit pontokkal ábrázoljuk, és csak azon x, y párok esetén rajzolunk egy irányított élt, amelyekre x közvetlenül megelőzi y -t, a részbenrendezett halmaz *Hasse-diagramját* kapjuk. (Néha irányított élek helyett irányítatlan éleket rajzolunk, de úgy, hogy a kisebb elem „lejjebb” legyen.) A részbenrendezés a Hasse-diagramból általában (véges halmaz esetén mindig) reprodukálható.

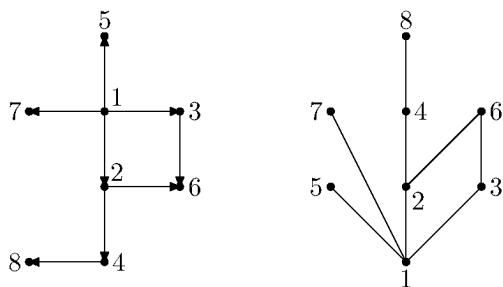
1.3.52. Legkisebb, legnagyobb, minimális és maximális elem. Az X részbenrendezett halmaz *legkisebb* (vagy *első*) elemén egy olyan $x \in X$ elemet értünk, amelyre $x \leq y$ minden $y \in X$ -re. Nem biztos, hogy van ilyen elem, de ha van, akkor egyértelmű. Hasonlóan, X *legnagyobb* (vagy *utolsó*) elemén egy olyan x elemet értünk, amelyre $y \leq x$ minden $y \in X$ -re. Nem biztos, hogy van ilyen elem, de ha van, akkor egyértelmű.

Az x -et *minimálisnak* nevezzük, ha nincs nála kisebb elem, *maximálisnak* pedig akkor, ha nincs nála nagyobb elem. Figyeljük meg, hogy minimális, illetve maximális elem több is lehet, és hogy ha X rendezett, akkor a legkisebb és a minimális elem fogalma, illetve a legnagyobb és a maximális elem fogalma egybeesik, de egyébként nem feltétlenül.

Ha X -nek egyetlen minimális eleme létezik, akkor azt $\min X$ -szel, ha pedig egyetlen maximális eleme létezik, akkor azt $\max X$ -szel jelöljük. Ha van legkisebb elem, akkor az $\min X$; ha van legnagyobb elem akkor az $\max X$.

° **1.3.53. Példa.** Tekintsük az $\{1, 2, 3, 4, 5, 6, 7, 8\}$ halmazon az „osztója” részbenrendezést. A 1.3.4 ábrán ennek Hasse-diagramja látható két alakban. Itt 1 legkisebb és minimális elem, 5, 6, 7 és 8 maximális elemek, de egyik sem legnagyobb; $\{1, 2, 4, 8\}$ lánc, így például $\{2, 8\}$ is, de $\{1, 2, 3, 6\}$ nem; a 2 közvetlenül megelőzi 4-et, de 8-at nem.

1.3.54. Korlátok. Egy X részbenrendezett halmaz egy x elemét az Y részhalmaz *alsó korlátjának* nevezzük, ha minden $y \in Y$ -ra $x \leq y$. Ha minden $y \in Y$ -ra $y \leq x$, akkor x az Y *felső korlátja*. Ha létezik alsó illetve felső korlát, akkor azt mondjuk, hogy Y *alulról korlátos* illetve *felülről korlátos*. Lehet, hogy egy részhalmaznak nincs alsó vagy felső korlátja, de az is lehet, hogy több van. Ha egy Y részhalmaznak van egy vagy akár több alsó korlátja, akkor is előfordulhat, hogy egyik sem eleme Y -nak. Ha mégis van az alsó korlátok között eleme Y -nak, akkor csak egy van, és ez Y legkisebb eleme; hasonló állítás érvényes a felső



1.3.4 ábra: Hasse-diagram két alakban.

korlátokra. Ha az alsó korlátok halmazában van legnagyobb elem, akkor azt *Y legnagyobb alsó korlátjának*, *pontos alsó korlátjának* vagy *alsó határának*, idegen szóval *infimumának* nevezzük, és $\inf Y$ -nal jelöljük. Hasonlóan, ha Y felső korlátjai halmazában van legkisebb elem, akkor azt *Y legkisebb felső korlátjának*, *pontos felső korlátjának* vagy *felső határának*, idegen szóval *szuprémumának* nevezzük, és $\sup Y$ -nal jelöljük.

Ha az X részbenrendezett halmaz bármely nem üres, felülről korlátos részhalmazának van felső határa, akkor *felső határ tulajdonságúnak* nevezzük, ha pedig bármely nem üres, alulról korlátos részhalmazának van alsó határa, akkor X -et *alsó határ tulajdonságúnak* nevezzük. A 1.3.4 ábrán a $\{2, 3\}$ halmaznak 6 a legkisebb felső korlátja, de $\{4, 5\}$ nem korlátos felülről. Az alaphalmaz is fontos: $\{4, 5\}$ az $\mathbb{N}$ -ben korlátos felülről.

→ **1.3.55. Feladat [2].** Bizonyítsuk be, hogy egy részben rendezett halmaz bármely nem üres részhalmazának bármely alsó korlátja kisebb vagy egyenlő bármely felső korlátjánál.

→ **1.3.56. Feladat [2].** Mutassuk meg, hogy egy részbenrendezés inverze is részbenrendezés. Mi a kapcsolat a két Hasse-diagram között?

→° **1.3.57. Feladat [5].** Tekintsük az $\{1, 2, 3, 4, 5, 6, 7, 8\}$ halmazon az „osztója” részbenrendezést. A megfelelő szigorú relációt írjuk fel párok halmazaként. Keressünk intervallumokat, részhalmazokra alsó és felső korlátokat, infimumot és szuprémumot.

° **1.3.58. Feladat [5].** Mely $n \in \mathbb{N}^+$ számokra alkotnak az n -nek az $\mathbb{N}^+$ -beli osztói rendezett halmazt az oszthatóságra nézve?

° **1.3.59. Feladat [1].** Hol a hiba a következő okoskodásban? Megmutatjuk, hogy 1 a legnagyobb természetes szám. Bármely n természetes számra, amely nem 0 és nem 1, teljesül, hogy $n^2 > n$. Mivel $1 > 0$, az 1 a legnagyobb természetes szám.

→° **1.3.60. Feladat [5].** Legyen $H \subset \mathbb{R}$. A H halmaz milyen tulajdonságát fejezik ki az alábbi formulák? A kvantorok, x és y valamint $\mathbb{R}$ és H cserélgetésével keressünk további formulákat és fejtjük meg jelentésüket.

- (1) $\forall x \in \mathbb{R} \exists y \in H (x < y);$
- (2) $\exists x \in \mathbb{R} \forall y \in H (x < y);$
- (3) $\forall x \in H \exists y \in \mathbb{R} (x < y);$
- (4) $\forall x \in H \exists y \in H (x < y).$

1.3.61. Feladat [6]. Mutassuk meg, hogy ha egy rendezett halmaz minden nem üres és felülről korlátos halmazának van pontos felső korlátja, akkor minden nem üres alulról korlátos részhalmazának van pontos alsó korlátja.

→° **1.3.62. Feladat [5].** Határozzuk meg az $\{1, 2, 3, 4, 5, 6\}$ halmazon az „osztója” reláció egy olyan kiterjesztését, amely rendezés.

bg	\$65,\$43,\$55	#e2
bg	\$64,\$42,\$54	#e2
bg	\$63,\$41,\$53	#e2
bg	\$62,\$40,\$52	#e2
sf	\$43,\$43,\$55	#e2
sf	\$42,\$42,\$54	#e2
sf	\$41,\$41,\$53	#e2
sf	\$40,\$40,\$52	#e2
shlqbyi	\$60,\$56,0	#e2
shufb	\$56,\$18,\$65,\$24	#o4
shufb	\$66,\$18,\$65,\$24	#o4
shufb	\$55,\$65,\$64,\$24	#o4
shufb	\$65,\$65,\$64,\$24	#o4
shufb	\$54,\$64,\$63,\$24	#o4
shufb	\$64,\$64,\$63,\$24	#o4
shufb	\$53,\$63,\$62,\$24	#o4
shufb	\$63,\$63,\$62,\$24	#o4
shufb	\$52,\$62,\$18,\$24	#o4
shufb	\$62,\$62,\$18,\$24	#o4
bgx	\$66,\$20,\$60	#e2
bgx	\$65,\$20,\$43	#e2
bgx	\$64,\$20,\$42	#e2
bgx	\$63,\$20,\$41	#e2
bgx	\$62,\$20,\$40	#e2
sfx	\$56,\$20,\$60	#e2
sfx	\$55,\$20,\$43	#e2
sfx	\$54,\$20,\$42	#e2
sfx	\$53,\$20,\$41	#e2
sfx	\$52,\$20,\$40	#e2
and	\$61,\$66,\$65	#e2
and	\$61,\$61,\$64	#e2
and	\$61,\$61,\$63	#e2
and	\$61,\$61,\$62	#e2
xor	\$60,\$61,\$18	#e2
gb	\$60,\$60	#o4
brnz	\$60,subkarasqrb	#o

1.3.5 tábla: IBM Cell program részlet.

→ **1.3.63. Feladat:** program futási sebességének optimalizálása részbenrendezés kiterjesztéseinek segítségével [13]. A 1.3.5 táblázatban egy, az IBM Cell processzorra írt assembly programrészlet van megadva. Minden utasítás az eredményt az elsőként megadott célregiszterbe teszi, az operandusokat pedig a többi regiszterből veszi, kivéve az x -re végződő bgx és sfx utasításokat, ezeknél a célregiszter is operandus. Minden utasításnál megadtuk, hogy e vagy o típusú, és hogy a végrehajtása hány órajelig tart. A processzor két utasítást is el tud kezdeni minden órajelben, de csak ha az első e , a második pedig o típusú, egyébként csak egyet, és csak akkor, ha az operandusai „elkészültek”. (A programrészlet elején minden operandus, amit megváltoztatás előtt használunk, „kész van” és nem „szemét”.) Optimalizáljuk a programrészletet: adjuk meg a sorok egy olyan részbenrendezését, amelynek rendezéssé történő kiterjesztései között csupa olyan sorrend szerepel, amelyre igaz, hogy ugyanezt az eredményt adja minden regiszterben, és programmal keressük meg a minimális futásidejű sorrendet. (Ehhez nem kell megérteni a programrészletet.) Az utolsó, ugró utasításnak utolsónak kell maradnia!

1.3.64. Jólrendezés. Egy X rendezett halmazt *jólrendezettnek*, a rendezését pedig *jólrendezésnek* nevezzük, ha X bármely nem üres részhalmazának van legkisebb eleme.

° **1.3.65. Példa.** A természetes számok halmaza jólrendezett, de az egész, racionális és valós számok halmaza nem jólrendezett a szokásos rendezéssel.

→ **1.3.66. Feladat** [1]. Jólrendezett-e $\mathbb{N}$ a szokásos rendezés inverzével?

→ **1.3.67. Feladat** [1]. Jólrendezett-e a $\{1 - 1/n : n \in \mathbb{N}^+\}$ halmaz a szokásos rendezéssel?

→° **1.3.68. Feladat** [1]. Ki lehet-e választani jólrendezett halmazban elemek végtelen, szigorúan csökkenő sorozatát?

→ **1.3.69. Feladat** [0]. Mutassuk meg, hogy jólrendezett halmaz bármely részhalmaza is jólrendezett.

1.3.70. Példák. Legyen X és Y részbenrendezett halmaz. Az $X \times Y$ -ban legyen $(x, y) \leq (x', y')$, ha $x \leq x'$ az X -ben és $y \leq y'$ az Y -ban. Így egy részbenrendezést kapunk. Figyeljük meg, hogy $X \times Y$ nem feltétlenül rendezett ezzel a relációval, még akkor sem, ha X és Y rendezettek, továbbá, hogy $X \times Y$ -on az így definiált $\leq$ -höz tartozó szigorú reláció nem feltétlenül a

$$\left\{ ((x, y), (x', y')) : x < x' \text{ és } y < y' \right\}$$

reláció.

Legyen most $(x, y) \leq (x', y')$, ha $x < x'$, vagy ha $x = x'$ és $y \leq y'$. Az $X \times Y$ -nak ezt a részbenrendezését *lexikografikus rendezésnek* nevezzük. Ha X és Y rendezettek illetve jólrendezettek, akkor $X \times Y$ is rendezett illetve jólrendezett a lexikografikus (részben)rendezéssel.

→ **1.3.71. Feladat** [2]. Egészítsük ki az előző pontot bizonyítással.

1.3.72. Feladat [5]. Tanulmányozzuk $\mathbb{N} \times \mathbb{N}$ -en a lexikografikus rendezést. Adjunk példát olyan végtelen jólrendezett halmazra, amelyben van legnagyobb elem.

→ **1.3.73. Feladat** [4]. Bizonyítsuk be, hogy egy jólrendezett halmazban (kivéve esetleg a legnagyobb elemet, ha van olyan) minden elemnek van közvetlen rákövetkezője.

° **1.3.74. Feladat** [6]. Tanulmányozzuk $\mathbb{R} \times \mathbb{R}$ -en az előző példában megadott két rendezést. Van-e minden felülről korlátos halmaznak pontos felső korlátja a lexikografikus rendezésnél?

° **1.3.75. Feladat** [6]. Ha A részben rendezett halmaz, definiáljuk a lexikografikus rendezést az A^* halmazon. Ha A rendezett, illetve jólrendezett volt, rendezett, illetve jólrendezett lesz-e A^* ?

1.3.76. További feladatok részletes megoldással. [5]: 1–19.

1.3.77. További feladatok. [3]: I.17–I.24; [56]: 2.0-1.– 2.0-9; [59]: I.2.1–I.2.3, I.2.5, I.2.7–I.2.11, I.2.13, I.2.18, I.3.1–I.3.24, I.3.26–I.3.44, I.3.46–I.3.72; [36]: 2.1–2.12, 3.1, 3.2, 3.7, 3.8, 3.11–3.15, 3.17, 3.21, 3.23, 3.26–3.35, 9.1–9.8, 9.10–9.13, 11.1, 11.4, 11.5, 11.7; [83]: II.8.7–II.8.9, III.5.1–III.5.15, III.5.17; [84]: 4.1–4.3, 4.6, 4.7, 4.42–4.44, 4.53, 4.54, 4.77, 4.91, 4.92, 4.95.

1.4 Függvények

1.4.1. Függvény. Egy *függvény* (leképezés, transzformáció, hozzárendelés, operáció vagy operátor) egy olyan f reláció, amelyre ha $(x, y) \in f$ és $(x, y') \in f$, akkor $y = y'$, más szóval minden x -hez legfeljebb egy olyan y létezik, amelyre $(x, y) \in f$. Így tehát minden $x \in \text{dmn}(f)$ -re $f(x) = \{y\}$ valamely y -ra. Az általános szokás itt is elhagyni a kapcsos zárójelet, azaz $f(x) = y$ -t írni. Az y elemet az f függvény x helyen (*argumentumban*) felvett értékének nevezzük, és gyakran f_x -szel is jelöljük. (Vannak, akik a függvény *grafikonjáról* beszélnek, amikor párok halmazára gondolnak.) Legegyszerűbb példa függvényre $\mathbb{I}_X$, amelyet X *identikus* leképezésének nevezünk.

Annak kifejezésére, hogy az f függvénynek az x helyen y az értéke, azt is szokás írni, hogy $f: x \mapsto y$. (Régebbi könyvekben $f: x \rightarrow y$ szerepel.) Ennél a jelölésnél néha nem is jelöljük semmivel a függvényt. Például az $X \times Y$ Descartes-szorzat elemeihez első, illetve második koordinátájukat rendelő függvények $(x, y) \mapsto x$, illetve $(x, y) \mapsto y$.

Az összes olyan függvény halmazát, amelynek értelmezési tartománya része az X halmaznak, értékkészlete pedig az Y halmaznak, $X \rightarrow Y$ fogja jelölni (a jelölés nem túl elterjedt). Annak kifejezésére, hogy az f függvény értelmezési tartománya a teljes X halmaz, értékkészlete pedig az Y halmaznak részhalmaza, az $f: X \rightarrow Y$ jelölés szolgál, amit úgy olvasunk ki, hogy f az X -et Y -ba képező függvény. Ez nem ugyanaz, mint $f \in X \rightarrow Y$, mert ez utóbbi esetben $\text{dmn}(f) \subsetneq X$ is lehetséges. Szokás az $f \in X \rightarrow Y$ függvényeket az X -et Y -ba képező *parciális függvényeknek* is nevezni. Mi az $f \in X \rightarrow Y$ jelölést fogjuk használni, vagy azt mondjuk, hogy f az X valamely részhalmazát Y -ba képező függvény. Ha azt mondjuk, hogy f az X -et Y -ra képező *függvény*, akkor ez alatt azt értjük, hogy f olyan függvény, amelynek értelmezési tartománya X , értékkészlete pedig Y .

Az f függvényt *kölcsönösen egyértelműnek* nevezzük, ha $f(x) = y$ és $f(x') = y$ esetén $x = x'$. Ez nyilván azzal ekvivalens, hogy az f^{-1} reláció függvény. Szokás a kölcsönösen egyértelmű függvényeket *injektívnek* is nevezni. Ha egy $f: X \rightarrow Y$ függvény az egész Y -ra képez, azaz $f(X) = \{f_x: x \in X\} = Y$, akkor szokás *szürjektívnek* vagy *szuperjektívnek* is nevezni, ha pedig injektív és szürjektív, akkor *bijektívnek*. Ennek a szóhasználatnak az a

veszélye, hogy egy függvény szűrjektivitása, illetve bijektivitása nem csak a függvénytől, hanem az Y halmaz választásától is függ. Például, $\mathbb{I}_X$ szűrjektív, ha $Y = X$, de nem, ha $X \subsetneq Y$; ilyenkor az X -nek Y -ba való *injekciójának* szokás nevezni.

Egy X halmaz önmagára való kölcsönösen egyértelmű leképezéseit az X *permutációinak* nevezzük.

→ **1.4.2. Feladat [1].** Milyen X és Y halmazok esetén lesz $X \times Y$ függvény?

→ **1.4.3. Feladat [0].** Mutassuk meg, hogy ha X, Y halmazok, $c \in Y$, akkor az $X \times \{c\}$ konstans leképezés függvény.

→° **1.4.4. Feladat [4].** Adjunk példát olyan függvényre, amely

- (1) $\mathbb{N}$ -et $\mathbb{N}$ valódi részére képezi le, de nem injektív;
- (2) $\mathbb{N}$ -et $\mathbb{N}$ valódi részére képezi le és injektív;
- (3) $\mathbb{Z}$ -t $\mathbb{Z}$ valódi részére képezi le, de nem injektív;
- (4) $\mathbb{Z}$ -t $\mathbb{Z}$ valódi részére képezi le és injektív;
- (5) $\mathbb{R}$ -et $\mathbb{N}$ -be képezi le;
- (6) $\mathbb{R}$ -et $\mathbb{N}$ -be képezi le, de egyetlen elem képe sem saját maga.

→ **1.4.5. Feladat [3].** Ha $f, g \in X \rightarrow Y$ függvények, függvény lesz-e $f \cup g$, $f \cap g$, $f \setminus g$, illetve $f \triangle g$?

1.4.6. Feladat [5]. Mutassuk meg, hogy ha R reláció az X és Y halmazok között, akkor az alábbi feltételek ekvivalensek:

- (1) R függvény;
- (2) bármely $B \subset Y$ -ra $R(R^{-1}(B)) \subset B$;
- (3) bármely $A, B \subset Y$ -ra $R^{-1}(A \cap B) = R^{-1}(A) \cap R^{-1}(B)$;
- (4) ha $A, B \subset Y$ diszjunktak, akkor $R^{-1}(A) \cap R^{-1}(B) = \emptyset$.

→ **1.4.7. Feladat [7].** Legyen $R \subset X \times Y$ egy reláció. Vizsgáljuk meg, hogy tetszőleges $A, B \subset X$ esetén milyen kapcsolat áll fenn az alábbi halmazpárok között (egyenlőség, egyik vagy másik irányú tartalmazás). Ha találtunk összefüggést, bizonyítsuk be, egyébként adjunk ellenpéldát. Mi a helyzet, ha $R: X \rightarrow Y$ függvény? Mi a helyzet, ha R egy $f: Y \rightarrow X$ függvény inverze?

- (1) $R(A \cup B)$ és $R(A) \cup R(B)$;
- (2) $R(A \cap B)$ és $R(A) \cap R(B)$;
- (3) $R(\text{dmn}(R) \setminus A)$ és $\text{rng}(R) \setminus R(A)$;
- (4) $R(A \setminus B)$ és $R(A) \setminus R(B)$;
- (5) $R(A \triangle B)$ és $R(A) \triangle R(B)$.

1.4.8. Feladat [5]. Mutassuk meg, hogy ha R reláció az X és Y halmazok között, S pedig reláció az Y és X halmazok között, továbbá $S \circ R = \mathbb{I}_X$ és $R \circ S = \mathbb{I}_Y$, akkor R és S bijektív leképezések és $S = R^{-1}$.

1.4.9. Feladat [5]. Legyenek A, B, C és D halmazok, $f: A \rightarrow B$, $g: B \rightarrow C$ és $h: C \rightarrow D$ leképezések. Mutassuk meg, hogy ha $g \circ f$ és $h \circ g$ bijektívek, akkor f , g és h bijektív.

1.4.10. Feladat [6]. Legyenek A, B , és C halmazok, $f: A \rightarrow B$, $g: B \rightarrow C$ és $h: C \rightarrow A$ leképezések. Mutassuk meg, hogy ha a $h \circ g \circ f$, $g \circ f \circ h$ és $f \circ h \circ g$ leképezések közül kettő szürjektív, a harmadik pedig injektív, vagy kettő injektív, a harmadik pedig szürjektív, akkor f , g és h is bijektív.

1.4.11. Állítás. Ha f és g függvény, akkor $g \circ f$ is. Ha f és g kölcsönösen egyértelmű függvény, akkor $g \circ f$ is az. Ha az f függvény X -et Y -ra, a g függvény pedig Y -t Z -re képezi le, akkor $g \circ f$ az X -et Z -re képezi le. $\square$

1.4.12. Kanonikus leképezés. Ha az X halmazon adott egy ekvivalenciareláció, akkor az x elemhez az ekvivalenciaosztályát rendelő leképezést *kanonikus leképezésnek* nevezzük. Megfordítva, ha $f: X \rightarrow Y$ egy függvény, akkor az $x \sim x'$, ha $f(x) = f(x')$ reláció egy ekvivalenciareláció.

$\rightarrow^\circ$ **1.4.13. Feladat [9].** Határozzuk meg az alábbi relációk értelmezési tartományát, értékkészletét, döntsük el, hogy függvény-e, és hogy az inverze függvény-e.

- (1) $\{(x, y) \in \mathbb{R}^2: a < x < b, x < y < 2x\}$, ahol $a, b \in \mathbb{R}$ adott számok;
- (2) $\{(x, y) \in \mathbb{R}^2: y(1 - x^2) = x - 1\}$;
- (3) $\{(x, y) \in \mathbb{R}^2: y = (x - 1)/(1 - x^2)\}$;
- (4) $\{(x, y) \in \mathbb{R}^2: |x| + |y| \leq 1\}$;
- (5) $\{(x, y) \in \mathbb{R}^2: x^2 = 1 + y^2, y > 0\}$;
- (6) $\{(x, y) \in \mathbb{R}^2: x^2 + y^2 - 2y < 0\}$;
- (7) $\{(x, y) \in \mathbb{R}^2: |x| = |y|\}$;
- (8) $\{(x, y) \in \mathbb{R}^2: y(\lfloor x \rfloor - 2) = 1\}$;
- (9) $\{(x, y) \in \mathbb{R}^2: y = x - \lfloor x \rfloor\}$;
- (10) $\{(x, y) \in \mathbb{R}^2: y = \lfloor x \rfloor^2\}$;
- (11) $\{(x, y) \in \mathbb{R}^2: y = x^2\}$;
- (12) $\{(x, y) \in \mathbb{R}^2: y = x^4, 0 < x < 2\}$;
- (13) $\{(x, y) \in \mathbb{R}^2: y = x^2, \text{ ha } x \in \mathbb{N}\}$;
- (14) $\{(x, y) \in \mathbb{R}^2: y = x, \text{ ha } x \in \mathbb{Q}, \text{ egyébként } y = 1 - x\}$.

1.4.14. Feladat [5]. Abból, hogy az $f: X \rightarrow Y$ és $g: Y \rightarrow Z$ függvényekre $g \circ f$ inverze függvény, következik-e, hogy f és g inverze is függvény?

1.4.15. Feladat [4]. Mutassuk meg, hogy bármely f függvényre és B halmazra $f(f^{-1}(B)) = B \cap \text{rng}(f)$. Mutassuk meg, hogy az állítás nem marad érvényben, ha f csak reláció.

1.4.16. Feladat [5]. Legyen $f: X \rightarrow Y$ függvény. Mutassuk meg, hogy az alábbi feltételek ekvivalensek:

- (1) f injektív;
- (2) minden $A \subset X$ halmazra $f^{-1}(f(A)) = A$;
- (3) bármely $A, B \subset X$ halmazokra $f(A \cap B) = f(A) \cap f(B)$;
- (4) bármely diszjunkt $A, B \subset X$ halmazokra $f(A) \cap f(B) = \emptyset$;
- (5) ha $A \subset B \subset X$, akkor $f(A \setminus B) = f(A) \setminus f(B)$.

°* **1.4.17. Feladat [8].** Legyen $f: \mathbb{R} \rightarrow \mathbb{R}$ egy függvény és $a, \varepsilon, \delta \in \mathbb{R}$. Milyen tulajdonságát fejezik ki a függvénynek az alábbi formulák? Adjunk meg olyan függvényt, amely rendelkezik a megfelelő tulajdonsággal.

- (1) $\forall \varepsilon > 0 \forall \delta > 0 \forall x \left(|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon \right);$
- (2) $\exists \varepsilon > 0 \forall \delta > 0 \forall x \left(|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon \right);$
- (3) $\exists \varepsilon > 0 \exists \delta > 0 \forall x \left(|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon \right);$
- (4) $\forall \delta > 0 \exists \varepsilon > 0 \forall x \left(|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon \right);$
- (5) $\exists \delta > 0 \forall \varepsilon > 0 \forall x \left(|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon \right);$
- (6) $\forall \varepsilon > 0 \exists \delta > 0 \forall x \left(|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon \right).$

1.4.18. Monoton függvények. Legyenek X és Y részbenrendezett halmazok. Az $f: X \rightarrow Y$ függvény

- (1) *monoton növekedő*, ha $x, y \in X$, $x \leq y$ esetén $f(x) \leq f(y)$;
- (2) *szigorúan monoton növekedő*, ha $x, y \in X$, $x < y$ esetén $f(x) < f(y)$;
- (3) *monoton csökkenő*, ha $x, y \in X$, $x \leq y$ esetén $f(x) \geq f(y)$;
- (4) *szigorúan monoton csökkenő*, ha $x, y \in X$, $x < y$ esetén $f(x) > f(y)$.

Szigorúan monoton növekedő (illetve csökkenő) függvény nyilván monoton növekedő (illetve csökkenő) is.

Ha X és Y rendezett, akkor szigorúan monoton növekedő (illetve csökkenő) függvény nyilván kölcsönösen egyértelmű is. Megfordítva, ha X és Y rendezettek, akkor egy $f: X \rightarrow Y$ kölcsönösen egyértelmű monoton növekedő (illetve csökkenő) leképezés szigorúan monoton növekedő (illetve csökkenő) is, és az inverze is szigorúan monoton növekedő (illetve csökkenő) $f(X)$ -en: Valóban, ha $x < y$, akkor $f(x) \leq f(y)$, de $f(x) = f(y)$ nem lehetséges, és ha $u, v \in f(X)$, $u < v$, $x = f^{-1}(u)$, $y = f^{-1}(v)$, akkor $x \geq y$ nem lehetséges, mert ebből $f(x) \geq f(y)$, azaz $u = f(x) > f(y) = v$ következne. A másik eset hasonlóan bizonyítható.

→ **1.4.19. Feladat [6].** Két részbenrendezett halmazt *használnak* nevezünk, ha létezik közöttük bijekció, amely monoton növekedő és az inverze is monoton növekedő. Mi a kapcsolat hasonló halmazok Hasse-diagramja között?

→ **1.4.20. Feladat [6].** Hány olyan részbenrendezése van egy 0, 1, 2, 3, illetve 4 elemű halmaznak, amelyek nem hasonlóak? Hány van ezek között, amely rendezés? Minden esetben keressük meg a minimális, maximális, legkisebb és legnagyobb elemeket, és a láncokat.

1.4.21. Indexelt családok. Mint említettük, egy x függvény i helyen felvett értékét néha x_i -vel jelöljük. Ilyenkor gyakran a függvény I értelmezési tartományát *indexhalmaznak*, elemeit *indexeknek*, értékkészletét *indexelt halmaznak*, az x függvényt magát pedig *indexelt családnak* nevezzük.

Ha az értékkészlet elemei halmazok, akkor *indexelt halmazcsaládról* beszélünk. Egy X_i , $i \in I$ indexelt halmazcsalád *unióját* az $\cup_{i \in I} X_i := \cup \{X_i : i \in I\}$ összefüggéssel értelmezzük. Ha nem okozhat félreértést, akkor a rövidebb $\cup_i X_i$ jelölést is használjuk. Ha $I \neq \emptyset$,

akkor az indexelt halmazcsalád *metszetét* definiáljuk a $\cap_{i \in I} X_i := \cap \{X_i : i \in I\}$ összefüggéssel, és erre is használjuk a rövidebb $\cap_i X_i$ jelölést. Indexelt halmazcsaládokra is igaz marad számos halmazelméleti azonosság, például a metszet és az unió kommutativitása, asszociativitása, disztributivitása. Csak eggyel foglalkozunk részletesen.

1.4.22. De Morgan-szabályok. Ha $X_i, i \in I$ az X halmaz részhalmazainak egy nem üres indexelt családja (azaz $I \neq \emptyset$), akkor az X -re vonatkozó komplementert vesszővel jelölve

- (1) $(\cup_{i \in I} X_i)' = \cap_{i \in I} X_i';$
- (2) $(\cap_{i \in I} X_i)' = \cup_{i \in I} X_i'. \square$

1.4.23. Megjegyzés. Ha az X „alaphalmaz” részhalmazai egy $X_i, i \in I$ indexelt családjának a metszetét a $\cap_{i \in I} X_i := \{x \in X : \text{minden } i \in I\text{-re } x \in X_i\}$ összefüggéssel értelmezzük, a De Morgan-szabályok üres család esetén (azaz ha $I = \emptyset$) is érvényben maradnak, mert $\cap_{i \in I} X_i = X$ megegyezik az $\{X_i : i \in I\} \cup \{X\}$ nem üres halmazrendszer metszetével, azaz $\cap_{i \in \emptyset} X_i = X$, míg $\cup_{i \in \emptyset} X_i = \emptyset$.

Számos olyan összefüggés érvényes, amely egy adott függvény (vagy akár egy adott binér reláció) esetén az értelmezési tartomány, illetve az értékkészlet részhalmazainak indexelt családjai, valamint a család halmazainak képei, illetve inverz képei között teremt kapcsolatot. Mivel ezek az összefüggések általában könnyen kitalálhatók és bizonyíthatók, csak annyit emelünk ki, hogy ebből a szempontból legjobban egy függvény inverze viselkedik:

1.4.24. Tétel. Legyen $f: X \rightarrow Y$ egy függvény, $B, B_i \subset Y$, ha $i \in I \neq \emptyset$. Ekkor

- (1) $f^{-1}(\cup_i B_i) = \cup_i f^{-1}(B_i);$
- (2) $f^{-1}(\cap_i B_i) = \cap_i f^{-1}(B_i);$
- (3) $f^{-1}(Y \setminus B) = X \setminus f^{-1}(B). \square$

1.4.25. Feladat [6]. Legyenek $A_i, B_i, i \in I$ nem üres indexelt halmazcsaládok. Mutassuk meg, hogy

$$(\cup_{i \in I} A_i) \triangle (\cup_{i \in I} B_i) \subset \cup_{i \in I} (A_i \triangle B_i).$$

Mutassuk meg, hogy a tartalmazás lehet valódi. Mi a helyzet, ha unió helyett metszet van?

$\rightarrow$ **1.4.26. Feladat [5].** Ha $r \in \mathbb{R}$, legyen $K_r = \{x \in \mathbb{R} : |x| < r\}$. Mi lesz $\cup_{i \in I} K_i$ és $\cap_{i \in I} K_i$, ha $I = \mathbb{R}^+$?

1.4.27. Feladat [4]. Bizonyítsuk be, hogy bármely R relációra és $A_i (i \in I)$ indexelt halmazcsaládra $R(\cup_{i \in I} A_i) = \cup_{i \in I} R(A_i)$.

$\circ$ **1.4.28. Feladat [6].** Legyenek $f, g: \mathbb{R} \rightarrow \mathbb{R}$ függvények, és

$$H_r = \{x \in \mathbb{R} : f(x) > r\} \cap \{x \in \mathbb{R} : g(x) < r\}, \quad \text{ha } r \in \mathbb{R}.$$

Mutassuk meg, hogy $\{x \in \mathbb{R} : f(x) > g(x)\} = \cup_{r \in \mathbb{Q}} H_r$.

1.4.29. Reláció és Descartes-szorzat általános esetben. Sokfajta kapcsolatot írhatunk le relációkkal, ezért az általános relációfogalom fontos szerepet játszik nem csak a matematikában, hanem az adatbázis-kezelő rendszerekben is. Tekintsük bizonyos „jellemzők” vagy „nevek” („attribútumok”) egy (véges) I halmazát. Például egy személyi törzsállomány esetén egy ember leírására az alábbi jellemzők halmazát használhatjuk:

$$I = \{\text{személyi_szám, név, lakcím, végzettség}\}.$$

Minden $i \in I$ -hez hozzárendeljük az adott attribútumhoz rendelhető értékek X_i halmazát, például $X_{\text{személyi_szám}}$ lehet a 11 jegyű decimális számok halmaza. Tekintsünk egy

$$x: I \mapsto \cup_{i \in I} X_i$$

függvényt, amelyre $x_i \in X_i$ minden $i \in I$ -re. Egy ilyen függvényt az informatikában az X_i ($i \in I$) indexelt családhoz tartozó rekordnak nevezzük: I elemei a mezőnevek, x_i pedig a rekordnak az i nevű mezője. Az X_i ($i \in I$) indexelt családhoz tartozó rekordoknak egy tetszőleges halmazát az adott X_i ($i \in I$) indexelt családhoz tartozó adattáblának nevezzük. A gyakorlatban a mezőneveket persze csak egyszer tároljuk le valamilyen sorrendben, és ugyanebben a sorrendben tároljuk az egyes rekordok mezőit. Az alábbi táblázat egy adattáblát mutat:

személyi_szá	név	lakcím	végzettség
15106111888	Vass Oxid	Arad	egyetem
17806111888	Czink Szulfid	Budapest	egyetem
17809171888	Arany Klorid	Budapest	szakiskola
18809151888	Radon Fluorid	Debrecen	szakiskola
⋮	⋮	⋮	⋮

Általánosabban, a matematika nyelvén fogalmazva, legyen X_i , $i \in I$ egy tetszőleges indexelt halmazcsalád. A halmazcsaládhoz tartozó kiválasztási függvény minden olyan $x: I \rightarrow \cup_{i \in I} X_i$ függvény, amelyre $x_i \in X_i$ minden $i \in I$ -re. Az X_i ($i \in I$) halmazcsaládhoz tartozó reláción kiválasztási függvények egy tetszőleges halmazát értjük. Legyen a halmazcsalád $\times_{i \in I} X_i$ Descartes-szorzata a halmazcsaládhoz tartozó összes kiválasztási függvények halmaza. Ha nem okozhat félreértést, csak $\times_i X_i$ -t írunk. Kételemű I esetén a binér reláció fogalmát, illetve két halmaz Descartes-szorzatát kapjuk vissza, ha az I egyik eleméhez rendelt értéket első koordinátának, a másikhoz rendelt értéket pedig második koordinátának tekintjük.

Világos, hogy ha van olyan $i \in I$, amelyre $X_i = \emptyset$, akkor nincs kiválasztási függvény, így $\times_i X_i = \emptyset$. Ha $I = \emptyset$, akkor viszont az üres függvény az egyetlen kiválasztási függvény, így $\times_i X_i = \{\emptyset\}$. Ha minden $i \in I$ -re $X_i = X$, akkor X^I -t is írhatunk $\times_{i \in I} X_i$ helyett. Így X^I az összes I -t X -be képező függvények halmaza. (Ezt a jelölést tetszőleges X és I halmazok esetén használjuk a továbbiakban.) Ennek a halmaznak a részhalmazait X -beli relációknak vagy homogén relációknak nevezzük. Most is, ha $I = \emptyset$, akkor $X^I = \{\emptyset\}$. Ha I egyelemű, $I = \{i\}$, akkor $\{(i, x)\} \mapsto x$ egy természetes, kölcsönösen egyértelmű leképezése X^I -nek X -re, pontatlanul fogalmazva X^I azonosítható X -szel.

Ha $J \subset I$, akkor az $x \in \times_i X_i$ kiválasztási függvényekre értelmezett $x \mapsto x|_J$ leképezést $\times_{i \in I} X_i$ -nek $\times_{j \in J} X_j$ -be való vetítésének, idegen szóval projekciójának nevezzük.

Ha J egyelemű, $J = \{j\}$, akkor ez a $p_j: x \mapsto x_j$ leképezéssel azonosítható, amit j -edik projekciónak nevezünk. Egy $\times_{i \in I} X_i$ -be képező f függvényre $f_j = p_j \circ f$ az f függvény j -edik koordinátafüggvénye.

Ha $I = J \cup K$, akkor gyakran hasznos az x kiválasztási függvényt az $(x|_J, x|_K)$ rendezett párral azonosítani, mert ekkor tetszőleges relációból binér reláció lesz, és használhatjuk binér relációk kompozícióját (összetételét) tetszőleges relációk *kompozíciójának* (összetételének) képzésére. Ha egy $R \subset \times_{i \in I} X_i$ reláció esetén az $\{(x|_J, x|_K): x \in R\}$ binér reláció függvény, akkor azt mondjuk, hogy $x|_J$ az x kiválasztási függvénynek az R relációban a J -beli indexekhez tartozó (illetve az x rekordnak az R adattáblában a J -beli mezőnevekhez tartozó) *kulcsa*. A kulcsok segítségével vett összetétel a halmazműveletek, a részhalmazképzés és a projekció mellett az egyik leggyakoribb művelet relációs adatbáziskezelőknél.

→ **1.4.30. Feladat [0].** Mutassuk meg, hogy $Y^X = \emptyset$ pontosan akkor teljesül, ha $Y = \emptyset$ és $X \neq \emptyset$.

→ **1.4.31. Feladat [5].** Határozzuk meg az X^Y összes elemét, ha X -nek illetve Y -nak nulla, egy, két illetve három eleme van. Melyek lesznek invertálhatóak?

1.4.32. Feladat [3]. Mutassuk meg, hogy ha $X^Y \cap Y^X \neq \emptyset$, akkor $X = Y$.

→ **1.4.33. Feladat [5].** Legyen $X_0 = \{A\}$, $X_1 = \{a, b\}$, $X_2 = \{\alpha, \beta, \gamma\}$, és $I = \{0, 1, 2\}$, $J = \{1, 2\}$. Adjuk meg $\cup_{i \in I} X_i$ -t és $\times_{i \in I} X_i$ -t. Adjuk meg $X_1 \times X_2$ -t és $\times_{i \in J} X_i$ -t. Adjunk meg $\times_{i \in I} X_i$ projekcióját $\times_{i \in J} X_i$ -be. Mi a helyzet, ha $X_0 = \emptyset$?

→ **1.4.34. Feladat [5].** Egy személyi törzsadattárból, amely a vállalat dolgozóinak adatait tartalmazza, és minden rekordja 7 mezőt tartalmaz, egy listát készítünk, amely az összes dolgozóra a nevét és a beosztását tartalmazza. Mi köze ennek a Descartes-szorzatok projekciójához?

→ **1.4.35. Feladat [12].** Tervezzünk egy Mini Tanulmányi Rendszert. Egy oktatónk megbetegedett, egy adott napon nem tud órát tartani. Szeretnénk e-mailt küldeni mindenkinek, akit ez érint. Milyen relációműveletek segítségével tudjuk a szükséges adatokat kinyerni?

1.4.36. Műveletek. Legyen X egy halmaz. Egy X -beli *binér műveleten* vagy *kétváltozós műveleten* egy $*$: $X \times X \rightarrow X$ leképezést értünk. Ha $x, y \in X$, akkor $*(x, y)$ a *művelet eredménye*, x és y pedig az *operandusai* vagy *argumentumai*. Rendszerint a binér művelet jelét az operandusok közé írjuk: $x*y$. Ha $A, B \subset X$, akkor $*(A \times B) = \{x*y: x \in A, y \in B\}$ helyett $A*B$ -t, az $A = \{a\}$, illetve $B = \{b\}$ esetben pedig $a*B$ -t, illetve $A*b$ -t is írhatunk. A legszokásosabb műveleti jelek $+$ és $\cdot$, az utóbbit gyakran ki sem írjuk.

Egy X -beli *unér művelet* vagy *egyváltozós művelet* egy $*$: $X \rightarrow X$ leképezés. Mivel $X^0 = \{\emptyset\}$, egy *nullér művelet* vagy *nullváltozós művelet* egy $*$: $\{\emptyset\} \rightarrow X$ leképezés, ami tulajdonképpen X egy elemének a kijelölését jelenti: operandusa nincs, csak eredménye, tehát azonosítható X egy elemével.

Ha műveletek eredményeire újabb műveleteket alkalmazunk, akkor zárójelekkel kell jelezniük, hogy milyen sorrendben kell elvégezniük a műveleteket. Szokás megállapodni a műveletek *precedenciájában*, például a nullér műveletek után az unér műveleteket, majd a binér műveletek közül előbb a „hatványozásszerű”, majd a „szorzásszerű”, végül az „összeadásszerű” műveleteket végezzük el, stb. Ilyen megállapodással a zárójelek egy

része megtakarítható. Megjegyezzük azonban, hogy a zárójelek teljesen elhagyhatók, ha a műveleti jeleket mindig az operandusok elé írjuk. Ezt a jelölésmódot Jan Łukasiewicz vezette be, és *lengyel jelölés*nek szokás nevezni. Az informatikában még elterjedtebb a *fordított lengyel jelölés* (szokásos rövidítése: *RPN*, Reverse Polish Notation), amelynél a műveleti jelek az operandusok után következnek. Néhány zsebszámológép mellett a FORTH programozási nyelv és a belőle kifejlesztett PostScript® nyomtatóvezérlő nyelv és szinte minden fordítóprogram ezt használja, mert ezzel a jelöléssel a kifejezések kiértékelése egyszerűen balról jobbra történhet.

° **1.4.37. Példa.** A természetes, egész, racionális, illetve valós számok esetén $+$ és $\cdot$ binér (kétfváltozós) művelet. A természetes számokon a kivonás nem művelet, a többi esetben igen. Az osztás egyik esetben sem művelet, mert nincs mindenütt definiálva. Az $x \rightarrow -x$ ellentettképzés a természetes számokon nem, a többi esetben unér (egyváltozós) művelet, míg a reciprokképzés nem művelet, mert nincs mindenütt definiálva. A 0 illetve az 1 kijelölése nullér (nullváltozós) művelet.

1.4.38. Példák. (1) Ha X egy halmaz, akkor az $\cup$, $\cap$, $\setminus$ és $\triangle$ binér műveletek, a ' (komplementerképzés) pedig unér művelet $\wp(X)$ -en.

(2) Ha X egy halmaz, a $\circ$ összetétel művelet az X -beli binér relációk között.

° **1.4.39. Példák: művelet megadása táblázattal.** Egy véges halmazon egy binér műveletet (vagy általánosabban, bármely, két véges halmaz Descartes-szorzatán értelmezett függvényt) *műveleti táblával* is megadhatunk: az első oszlopba a baloldali operandus, az első sorba pedig a jobboldali operandus kerül. Például az alábbi táblázatok a logikai jeleknek megfelelő binér *logikai műveleteket* definiálják (nevük itt is rendre konjunkció, diszjunkció, implikáció, ekvivalencia, kizáró vagy, sem-sam, összeférhetetlen vagy):

$\wedge$	$\uparrow$	$\downarrow$
$\uparrow$	$\uparrow$	$\downarrow$
$\downarrow$	$\downarrow$	$\downarrow$

$\vee$	$\uparrow$	$\downarrow$
$\uparrow$	$\uparrow$	$\uparrow$
$\downarrow$	$\uparrow$	$\downarrow$

$\Rightarrow$	$\uparrow$	$\downarrow$
$\uparrow$	$\uparrow$	$\downarrow$
$\downarrow$	$\uparrow$	$\uparrow$

$\Leftrightarrow$	$\uparrow$	$\downarrow$
$\uparrow$	$\uparrow$	$\downarrow$
$\downarrow$	$\downarrow$	$\uparrow$

$\oplus$	$\uparrow$	$\downarrow$
$\uparrow$	$\downarrow$	$\uparrow$
$\downarrow$	$\uparrow$	$\downarrow$

	$\uparrow$	$\downarrow$
$\uparrow$	$\downarrow$	$\downarrow$
$\downarrow$	$\downarrow$	$\uparrow$

$\parallel$	$\uparrow$	$\downarrow$
$\uparrow$	$\downarrow$	$\uparrow$
$\downarrow$	$\uparrow$	$\uparrow$

Hasonlóan egy véges halmazon egy unér műveletet (vagy általánosabban, bármely, véges halmazon értelmezett függvényt) is megadhatunk táblázattal. Például az alábbi

táblázat a „nem” logikai jelnek megfelelő függvényt adja meg:

	$\uparrow$	$\downarrow$
$\neg$	$\downarrow$	$\uparrow$

Általánosabban, az informatikában véges sok véges halmaz Descartes-szorzatán értelmezett függvényt egy tömbbel adhatunk meg.

→ **1.4.40. Feladat [3].** Hány nullér, unér illetve binér művelet definiálható egy 0, 1, 2, illetve 3 elemű halmazon?

→ **1.4.41. Feladat [7].** Keressük meg az összes binér logikai műveletet (azaz az összes műveletet az $\{\uparrow, \downarrow\}$ halmazon). Fejezzük ki mindet a tanult logikai műveletekkel, minél kevesebbrel. Keressünk olyan binér műveletet, amellyel minden más binér logikai művelet kifejezhető.

° **1.4.42. Feladat [7].** Milyen logikai műveletek találhatók például az MMIX vagy az IBM Cell processzor utasításkészletében? Vajon miért pontosan ezek?

1.4.43. Műveletek függvényekkel. Legyen X tetszőleges halmaz, Y pedig egy halmaz a $*$ binér művelettel. Ekkor az X -et Y -ba képező függvények között is értelmezhetünk „pontonként” egy binér műveletet (amelyet ugyanazzal a jellel szokás jelölni) az

$$(f * g)(x) := f(x) * g(x) \text{ minden } x \in X\text{-re, ha } f, g: X \rightarrow Y$$

összefüggéssel. Hasonlóan definiálhatók unér, illetve nullér műveletek függvényekkel. Sőt, ha csak egy $*$ $Y \times Y \rightarrow Y$ *parciális művelet* adott és $f, g \in X \rightarrow Y$, akkor is tekinthetjük az $x \mapsto *(f(x), g(x))$ leképezést, de ez már nem biztos, hogy mindenütt értelmezve lesz X -en, még akkor sem, ha f és g mindenütt értelmezve vannak X -en.

° **1.4.44. Példa.** Egy adott X halmazon értelmezett egész, racionális, illetve valós értékű függvények esetén az összeadást, kivonást és a szorzást „pontonként” értelmezzük függvényekre is, de két függvény hányadosa nincs mindenütt definiálva. Függvény ellentettjét is pontonként definiáljuk. A 0 illetve az 1 kijelöléséből mint nullér műveletből az azonosan 0, illetve azonosan 1 függvény adódik.

° **1.4.45. Példák.** Egy n -bites számítógépen rendszerint rendelkezésre állnak a logikai műveletek az n -bites szavakon, azaz a $\{0, 1, \dots, n-1\}$ halmazt a $\{\uparrow, \downarrow\}$ halmazba képező függvények halmazán. Szokásosan az $\uparrow$ értéket 1, a $\downarrow$ értéket pedig 0 reprezentálja. Áramkörökben $\uparrow$ reprezentációja magas feszültség- vagy áramérték (H, mint high), $\downarrow$ reprezentációja pedig alacsony feszültség- vagy áramérték (L, mint low), vagy pedig fordítva. Az első esetben *pozitív logikáról*, a második esetben pedig *negatív logikáról* beszélünk.

1.4.46. Művelettartó leképezések. Legyen $*$ binér művelet az X , és legyen $*$ ' binér művelet az X' halmazon. Egy $\varphi: X \rightarrow X'$ leképezést *művelettartónak* nevezünk, ha $\varphi(x * y) = \varphi(x) *' \varphi(y)$ minden $x, y \in X$ -re. Hasonlóan értelmezzük a művelettartást unér és nullér műveletre is.

A művelettartás jelentősége, hogy ha φ kölcsönösen egyértelmű, akkor X és $\varphi(X)$ között nem tudunk különbséget tenni a művelet alapján, „algebrailag megkülönböztethetetlenek”.

◦ **1.4.47. Példa.** Ha $a > 1$, az $x \mapsto a^x$ leképezés művelettartó és kölcsönösen egyértelmű leképezése az összeadással tekintett valós számoknak a szorzással tekintett pozitív valós számokra. Ez a leképezés művelettartó leképezése az ellentettképzéssel tekintett valós számoknak a reciprokképzéssel tekintett pozitív valós számokra, valamint a 0-t 1-be viszi át, így ezen unér műveletekre is művelettartó.

→◦ **1.4.48. Feladat [5].** Mi köze a kilences illetve a tizenegyes-próbának a művelettartó leképezésekhez?

1.4.49. További feladatok. [3]: I.25–I.52, I.54–I.90; [36]: 4.2–4.6, 4.10, 4.12–4.14, 4.18–4.20, 4.22–4.30, 5.2–5.6, 5.9–5.11; 6.1–6.9, 9.9, 12.3–12.22; [56]: 2.0–10.–2.0–19; [59]: I.1.22, I.1.29, I.1.36–39, I.2.4, I.2.6, I.2.12, I.2.15, I.2.16, I.2.19, I.2.20, I.2.21, I.2.25, I.2.28, I.2.30–I.2.43, I.2.46–49, I.2.51; [83]: II.8.10–II.8.25, II.8.33; [84]: 1.13, 1.17, 1.32–1.36.

Természetes számok

Ebben a fejezetben a természetes számokat tárgyaljuk a Peano-axiómákból kiindulva. A részletes axiomatikus tárgyalás célja egy példával előkészíteni a logika és a logikai programozási nyelvek tanítását.

2.1 Peano-axiómák

2.1.1. Peano-axiómák. Legyen $\mathbb{N}$ egy halmaz és $+$ egy $\mathbb{N}$ -en értelmezett függvény. Az alábbi feltételeket *Peano-axiómáknak* nevezzük:

- (1) $0 \in \mathbb{N}$;
- (2) ha $n \in \mathbb{N}$, akkor $n^+ \in \mathbb{N}$;
- (3) ha $n \in \mathbb{N}$, akkor $n^+ \neq 0$;
- (4) ha $n, m \in \mathbb{N}$ és $n^+ = m^+$, akkor $n = m$;
- (5) ha $S \subset \mathbb{N}$, $0 \in S$, továbbá $n \in S$ esetén $n^+ \in S$, akkor $S = \mathbb{N}$.

Tulajdonképpen egy $(\mathbb{N}, (0, +))$ párt tekintünk, ahol $\mathbb{N}$ egy halmaz. (1) azt fejezi ki, hogy kijelöltünk egy speciális elemet, azaz 0 egy nullér művelet $\mathbb{N}$ -en. (2) azt fejezi ki, hogy $+$ egy unér művelet $\mathbb{N}$ -en. (3) azt fejezi ki, hogy 0 nincs a $+$ értékészletében. (4) azt fejezi ki, hogy a $+$ leképezés kölcsönösen egyértelmű (injektív). A 0 elemet *nullának*, a $+$ unér műveletet *rákövetkezésnek*, az n^+ elemet az n *rákövetkezőjének* nevezzük. (5) a *matematikai indukció elve*, vagy röviden az *indukció elve* (a *teljes indukció elve* elnevezés is használatos, de a teljes indukció elnevezést mi a szokásosnál szűkebb értelemben fogjuk használni); szemléletesen azt jelenti, hogy $\mathbb{N}$ minden eleme 0-ból *rákövetkezéssel* elérhető, más természetes szám nincs.

Ha $n \in \mathbb{N}$, akkor $n^+ \neq n$: valóban, az $S = \{n \in \mathbb{N} : n^+ \neq n\}$ halmaz (3) szerint tartalmazza 0-t, és (4) szerint, ha tartalmazza n -et, akkor n^+ -t is, mert $(n^+)^+ = n^+$ -ből $n^+ = n$ következne, így (5) szerint $S = \mathbb{N}$, azaz minden $n \in \mathbb{N}$ -re $n^+ \neq n$. (Az ilyen bizonyításokat *matematikai indukcióval* vagy röviden *indukcióval* való bizonyításoknak szokás nevezni, és nagyon gyakran szerepelnek természetes számokra vonatkozó állítások bizonyításánál.)

Minden $0 \neq n \in \mathbb{N}$ -hez van egy ((4) szerint egyértelmű) $m \in \mathbb{N}$, amelyre $m^+ = n$; ezt is indukcióval bizonyítjuk. Valóban, az

$$S = \{0\} \cup \{n \in \mathbb{N} : \text{van olyan } m \in \mathbb{N}, \text{ amelyre } m^+ = n\}$$

halmazra $0 \in S$, és ha $n \in S$, akkor $n^+ = (m^+)^+ \in S$, így (5) szerint $S = \mathbb{N}$. Az $n \mapsto n^+$ leképezés értékészletét, az $\mathbb{N} \setminus \{0\}$ halmazt, a *pozitív természetes számok* halmazát $\mathbb{N}^+$ -szal jelöljük, a leképezés inverze pedig az $\mathbb{N}^+$ -szon értelmezett $n \mapsto n^-$ leképezés.

Ezt az apró trükköt, amelyet az előző bekezdésben használtunk, azaz hogy a nullát bevettük S -be, mindig alkalmazhatjuk, ha az indukciót nem 0-tól akarjuk kezdeni.

Legyen $1: = 0^+$, $2: = 1^+$, $3: = 2^+$, $4: = 3^+$, $5: = 4^+$, $6: = 5^+$, $7: = 6^+$, $8: = 7^+$, $9: = 8^+$. (Ha további számjegyekre van szükségünk, például hexadecimális (tizenhatos) számszerben, akkor így folytatjuk: $A: = 9^+$, $B: = A^+$, stb.)

Az $\mathbb{N}$ halmazt (vagy pontosabban az $(\mathbb{N}, (0, ^+))$ párt) *természetes számoknak* nevezzük. (Vannak, akik a természetes számokat 1-gyel kezdik.)

Több természetes kérdés merül fel. Az első, hogy a Peano-axiómáknak nevezett feltételek egyértelműen meghatározzák-e $\mathbb{N}$ -et? A válasz igen, egy pontosan meghatározott értelemben. A második, hogy létezik-e $\mathbb{N}$? Erre is igen a válasz, a halmazelmélet szokásos axiómarendszerében. Mindkét állítást be fogjuk bizonyítani. Egy további, hogy szükség van-e mind az öt axiómára a fenti két igen válaszhoz? Igen, mint a következő megjegyzés példái mutatják.

*** 2.1.2. Megjegyzés.** Peano öt axiómája (bizonyos értelemben) egyértelműen meghatározza a természetes számokat (lásd 2.1.5), de ezek közül bármelyiket elhagyva már nem teljesül az egyértelműség: a természetes számokon kívül más struktúrák is megfelelnek. Peano az egyes esetekre a következő példákat adta:

(1) Legyen N a pozitív egész számok halmaza. Ekkor az első axióma nem teljesül (a harmadik és az ötödik pedig értelmetlenné válik).

(2) Legyen $N = \{0, 1, 2\}$, és $0^+ = 1$, $1^+ = 2$, de nem értelmezzük 2^+ -t. Ekkor a második axióma nem teljesül.

(3) Legyen $N = \{0, 1, 2, \dots, 23\}$, és a rákövetkezőt definiáljuk az óránál szokásos értelemben, tehát $0^+ = 1$, $1^+ = 2$, $\dots$, $23^+ = 0$. Ekkor a harmadik axióma nem teljesül.

(4) Legyen $N = \{0, 1\}$, és $0^+ = 1$, $1^+ = 1$. Ekkor a negyedik axióma nem teljesül.

(5) Legyen N a nem negatív racionális számok halmaza, és minden elem rákövetkezője legyen a nála 1-gyel nagyobb racionális szám. Ekkor az ötödik axióma nem teljesül.

Ezek a példák azt is mutatják, hogy az öt axióma mindegyike független a másik négytől.

*** 2.1.3. Megjegyzés.** Peano nem halmazok, hanem tulajdonságok segítségével fogalmazta meg axiómáit. Bár jelöléseink hasonlóak az övéhez, számára azok egészen mást jelentettek. Számára $0 \in N$ a „zero es numero” mondat rövidítése, ahol az „ $\in$ ” az olasz „es” (németül: „ist”, angolul: „is”) jele. Ez pontosan nem adható vissza magyarul, mert (jelen időben) nem használunk segédigét, vö.: „Peter is happy”. Peano szerint $\text{Peter} \in \text{happy}$ azt fejezi ki, hogy Péter rendelkezik a „happy” tulajdonsággal, és nem halmazhoz tartozást jelent.

Peano híres munkája megírásakor még nem tudhatta, hogy tetszőleges tulajdonság alapján nem képezhetünk összességet, halmazt (lásd 1.2.7), hiszen Russell paradoxona pár évvel későbből származik. Ennek ellenére Peano axiómarendszere szolgált mintául Zermelonak a halmazelmélet axiomatikus felépítéséhez. Manapság Peano axiómáit halmazok nyelvén szokás megfogalmazni, ahogy mi is tettük.

Mielőtt a természetes számok létezésére és egyértelműségére vonatkozó tételt bebizonyítanánk, az $\mathbb{N}$ -en értelmezett függvények rekurzióval való definíciójának módszerét tárgyaljuk. Az $\mathbb{N}$ -en értelmezett függvényeket *végtelen sorozatoknak* nevezzük. (Az $\mathbb{N}^+$ halmazon értelmezett függvényeket is szokás végtelen sorozatnak nevezni.) Érezzük, hogy egy sorozatot megadhatunk úgy, hogy megadjuk a 0 helyen felvett értékét, és megadunk egy képzési szabályt, amelynek alapján megkapjuk a sorozat n helyen felvett értékéből az n^+ helyen felvett értékét. Erről szól a következő tétel.

2.1.4. Rekurziótétel. Legyen X egy halmaz, $a \in X$ és $f: X \rightarrow X$ egy függvény. Ha $\mathbb{N}$ -re a Peano-axiómák teljesülnek, akkor egy és csak egy olyan $\mathbb{N}$ -et X -be képező g függvény létezik, amelyre $g(0) = a$ és $g(n^+) = f(g(n))$ minden $n \in \mathbb{N}$ -re.

* **Bizonyítás.** Vegyük észre, hogy ha g és g^* is a tétel feltételeit kielégítő függvény, akkor indukcióval adódik, hogy $g = g^*$.

Csak g létezését kell tehát belátnunk. Tekintsük $\mathbb{N} \times X$ mindazon A részhalmazainak $\mathcal{A}$ rendszerét, amelyekre $(0, a) \in A$, és ha $(n, x) \in A$, akkor $(n^+, f(x)) \in A$. Mivel az egész $\mathbb{N} \times X$ rendelkezik ezekkel a tulajdonságokkal, az $\mathcal{A}$ halmazrendszer nem üres. Indukcióval kapjuk, hogy minden $A \in \mathcal{A}$ reláció értelmezési tartománya $\mathbb{N}$.

Tekintsük az $\mathcal{A}$ -beli halmazok metszetét, jelölje ezt g . Mivel $\mathcal{A}$ zárt a metszetképzésre, nyilván $g \in \mathcal{A}$, csak azt kell bizonyítanunk, hogy g függvény. Más szóval, azt kell igazolnunk, hogy minden $n \in \mathbb{N}$ -re, ha $(n, x) \in g$ és $(n, y) \in g$, akkor $x = y$. Indukcióval bizonyítunk. Legyen S azoknak az $n \in \mathbb{N}$ -eknek a halmaza, amelyekre $(n, x) \in g$ és $(n, y) \in g$ esetén $x = y$.

Ha $0 \notin S$ teljesülne, akkor valamilyen $a \neq b \in X$ -re $(0, a), (0, b) \in g$ állna fenn. De ekkor $g \setminus \{(0, b)\}$ még mindig $\mathcal{A}$ -beli, mert tartalmazza $(0, a)$ -t, és ha tartalmazza (n, x) -et, akkor $(n^+, f(x))$ -et is, hiszen $n^+ \neq 0$, tehát $((n^+, f(x))) \neq ((0, f(x)))$. Ez ellentmond annak, hogy $g = \cap \mathcal{A}$, tehát $0 \in S$.

Most tegyük fel, hogy $n \in S$. Ez azt jelenti, hogy pontosan egy olyan $x \in X$ létezik, hogy $(n, x) \in g$. Mivel $(n, x) \in g$, teljesül, hogy $(n^+, f(x)) \in g$. Ha n^+ nem tartozna S -hez, akkor $(n^+, y) \in g$ teljesülne valamely $f(x)$ -től különböző y -ra. A $g \setminus \{(n^+, y)\}$ reláció még mindig $\mathcal{A}$ -beli, mert nyilván tartalmazza $(0, a)$ -t, hiszen $0 \neq n^+$, és ha tartalmazza például (m, z) -t, akkor tartalmazza $(m^+, f(z))$ -t is; valóban, ha $m = n$ akkor ez fennáll, ha pedig $m \neq n$, akkor $m^+ \neq n^+$. Ez megint ellentmond annak, hogy $g = \cap \mathcal{A}$. Ebből az ellentmondásból következik, hogy $n^+ \in S$. De akkor az indukció elve szerint $S = \mathbb{N}$. $\square$

2.1.5. A természetes számok egyértelműsége. Tegyük fel, hogy $\mathbb{N}$ és $\mathbb{N}'$ is eleget tesz a Peano-axiómáknak. Ekkor létezik olyan φ kölcsönösen egyértelmű leképezése $\mathbb{N}$ -nek $\mathbb{N}'$ -re, amelyre $\varphi(0) = 0'$ és $\varphi(n^+) = (\varphi(n))^{+'}$ minden $n \in \mathbb{N}$ -re. (Itt $\mathbb{N}'$ -ben 0 helyett $0'$ -t és $+$ helyett $+'$ -t írtunk.)

A későbbiekben a természetes számokra további műveleteket (összeadás, szorzás, stb.) fogunk bevezetni. Mivel ezeket mindig a rákövetkezés segítségével definiáljuk, mindig könnyen bizonyítható, hogy φ ezeket is „tartja”. Ennek bizonyításával nem foglalkozunk.

Bizonyítás. A rekurziótételt alkalmazva $X = \mathbb{N}'$ -re, $a = 0' \in \mathbb{N}'$ -re és $f = +'$ -re kapjuk φ -t, mint a tételbeli g -t. Mivel az értékészlet tartalmazza $0'$ -t, és ha tartalmazza n' -t, akkor $n'^{+'}$ -t is, φ az $\mathbb{N}'$ -re képez az indukció elve miatt. Jelölje S az $\mathbb{N}'$ azon elemeit, amelyek csak egyetlen $n \in \mathbb{N}$ képeként lépnek fel. Nyilván $0' \in S$, mert az értékészlet minden más eleme valaminek a rákövetkezője. Ha $n' \in S$, akkor egyetlen olyan $n \in \mathbb{N}$ létezik, amelyre $\varphi(n) = n'$. Definíció szerint $\varphi(n^+) = n'^{+'}$. Ha valamely m -re $\varphi(m) = n'^{+'}$, akkor ez az m nem lehet 0 , így $m = k^+$. De $\varphi(k^+) = (\varphi(k))^{+'}$, így $\varphi(k) = n'$, amiből $k = n$, tehát $m = n^+$ következik, vagyis $n'^{+'} \in S$. Tehát $S = \mathbb{N}'$, azaz φ kölcsönösen egyértelmű. $\square$

2.1.6. A természetes számok létezése. Van olyan $(\mathbb{N}, (0, +))$ pár, amely eleget tesz a Peano-axiómáknak.

* **Bizonyítás.** Azt fogjuk megmutatni, hogy az ω halmaz az $\emptyset$ -zal mint nullával és a $^+ : x \mapsto x \cup \{x\}$ unér művelettel eleget tesz a Peano-axiómáknak. Ennek alapján a halmazelméletben rendszerint ω -t azonosítják $\mathbb{N}$ -nel.

A Peano-axiómák közül (1) és (2) következik ω definíciójából. (5) ugyancsak következik ω definíciójából, mert ω a legszűkebb olyan halmaz, amelynek az üres halmaz eleme és zárt az $x \mapsto x \cup \{x\}$ rákövetkezésre. (3) nyilván teljesül, mert $x^+ = x \cup \{x\}$ nem üres. Így csak (4)-et kell belátni.

Legyen

$$S = \{x \in \omega : \text{ha } y \in x, \text{ akkor } x \not\subset y\}.$$

Az S halmaz ω azon elemeit tartalmazza, amelyek nem részhalmazai egyetlen elemüknek sem. Indukcióval megmutatjuk, hogy $S = \omega$. Nyilván $\emptyset \in S$. Tegyük fel, hogy $x \in S$. Mivel $x \subset x$, az S definíciójából kapjuk, hogy $x \notin x$. Így $x^+ = x \cup \{x\}$ nem részhalmaza x -nek. Minek lehet részhalmaza x^+ ? Ha $x^+ \subset y$, akkor $x \subset y$, így $y \notin x$. Tehát x^+ nem részhalmaza x egyetlen elemének sem. Így x^+ sem x -nek, sem x elemeinek nem lehet részhalmaza, tehát x^+ az x^+ egyetlen elemének sem lehet részhalmaza. Innen $x^+ \in S$ adódik. Ez azt jelenti, hogy $S = \omega$.

Nevezzünk egy halmazt *transzitivnak*, ha bármely eleme halmaz, és annak minden eleme az eredeti halmaznak is eleme; azaz x transzitiv halmaz, ha $y \in x$ esetén y halmaz, és $z \in y$ esetén $z \in x$. Legyen

$$T = \{x \in \omega : \text{minden } y\text{-ra, amelyre } y \in x, \text{ teljesül } y \subset x\},$$

azaz ω transzitiv elemeinek halmaza. Indukcióval megmutatjuk, hogy $T = \omega$. Nyilván $\emptyset \in T$. Tegyük fel, hogy $x \in T$. Ha $y \in x^+$, akkor $y \in x$ vagy $y = x$. Az első esetben az $x \in T$ feltevés miatt y halmaz, és $y \subset x \subset x^+$. A második esetben y nyilván halmaz, és $y \subset x^+$, azaz $y \subset x^+$. Ezzel megmutattuk, hogy x^+ minden eleme halmaz és részhalmaza x^+ -nak, így $x^+ \in T$. Ez azt jelenti, hogy $T = \omega$.

Most bebizonyítjuk (4)-et. Tegyük fel, hogy $x, y \in \omega$ és $x^+ = y^+$. Mivel $x \in x^+$, kapjuk hogy $x \in y^+$, amiből x halmaz, és $x \in y$ vagy $x = y$. Hasonlóképpen y is halmaz, és $y \in x$ vagy $y = x$. Ha $x \neq y$, akkor $x \in y$ és $y \in x$ is teljesül. Mivel ω minden eleme transzitiv, ezért $x \in x$. De akkor a transzitivitás miatt $x \subset x$, ami viszont S definíciója szerint ellentmond annak, hogy $S = \omega$. $\square$

2.1.7. Karakterisztikus függvények. Legyen X egy halmaz, és ha $Y \subset X$, legyen $\chi_Y(x) = 1$, ha $x \in Y$ és $\chi_Y(x) = 0$, ha $x \in X \setminus Y$. A χ_Y függvényt az Y halmaz (X -en értelmezett) *karakterisztikus függvényének* nevezzük. Az $Y \mapsto \chi_Y$ leképezés nyilván kölcsönösen egyértelmű leképezése $\wp(X)$ -nek az X -en értelmezett karakterisztikus függvények $\{0, 1\}^X$ halmazára. (Emiatt szokás $\wp(X)$ -et 2^X -szel is jelölni.)

→° **2.1.8. Feladat [5].** Indukcióval bizonyítsuk be az alábbi összefüggéseket:

(1)

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2};$$

(2)

$$1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6};$$

(3)

$$1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3};$$

(4)

$$\begin{aligned} 1 \cdot 2 \cdots m + 2 \cdot 3 \cdots (m+1) + \cdots + n(n+1) \cdots (n+m-1) \\ = \frac{n(n+1) \cdots (n+m)}{m+1}; \end{aligned}$$

(5)

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2 = \frac{n^2(n+1)^2}{4};$$

(6)

$$1 \cdot 4 + 2 \cdot 7 + \cdots + n(3n+1) = n(n+1)^2;$$

(7)

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(n-1)n} = \frac{n-1}{n};$$

(8)

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} < \frac{2n-1}{n}, \quad \text{ha } n > 1;$$

(9)

$$2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1;$$

(10)

$$1 + q + q^2 + \cdots + q^n = \frac{q^{n+1} - 1}{q - 1}, \quad \text{ha } q \neq 1.$$

2.1.9. Feladat [8]. Bizonyítsuk be Nikomakhosz tételét: $1^3 = 1$, $2^3 = 3 + 5$, $3^3 = 7 + 9 + 11$, $4^3 = 13 + 15 + 17 + 19$ stb. Vezessük le ebből az előző feladat (6) összefüggését.

→° **2.1.10. Feladat [1].** Hol a hiba a következő okoskodásban? Bebizonyítjuk, hogy minden egész szám egyenlő. Azt látjuk be, hogy bármely egész szám megegyezik a rákövetkezőjével, azaz $n = n + 1$. Tegyük fel, hogy ez igaz n -re. Ekkor $n + 1$ -re is, mert $n = n + 1$ -ből $n + 1 = (n + 1) + 1$.

→° **2.1.11. Feladat [4].** Hol a hiba a következő okoskodásban? Bebizonyítjuk, hogy a sík rajta van egyetlen egyenesen. Elég megmutatni, hogy akárhogy veszünk véges sok pontot, azok egy egyenesen vannak. Egy és két pontra ez igaz. Tegyük fel, hogy bármely n pont egy egyenesen van. Vegyünk $n + 1$ pontot. Az első n pont egy egyenesen van. Vegyünk el ezek közül egyet, és adjuk hozzá az $n + 1$ -edik pontot. Ez az n pont is egy egyenesen van, tehát az $n + 1$ pont egy egyenesen van.

→° **2.1.12. Feladat [4].** Hol a hiba a következő okoskodásban? Bebizonyítjuk, hogy adott a pozitív valós számra és bármely $n \in \mathbb{N}^+$ természetes számra $a^{n-1} = 1$. Az állítás igaz, ha $n = 1$. Ha igaz bármely $n + 1$ -nél kisebb számra, akkor

$$a^{(n+1)-1} = a^n = \frac{a^{n-1} \cdot a^{n-1}}{a^{(n-1)-1}} = \frac{1 \cdot 1}{1} = 1.$$

→° **2.1.13. Feladat [4].** Hol a hiba a következő okoskodásban? Bebizonyítjuk, hogy

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(n-1)n} = \frac{3}{2} - \frac{1}{n}.$$

Ha $n = 1$, akkor $3/2 - 1/n = 1/(1 \cdot 2)$, és ha n -re igaz, akkor

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(n-1)n} + \frac{1}{n(n+1)} = \frac{3}{2} - \frac{1}{n} + \frac{1}{n} - \frac{1}{n+1} = \frac{3}{2} - \frac{1}{n+1}.$$

° **2.1.14. Feladat [5].** Indukcióval bizonyítsuk be az alábbi összefüggéseket:

(1)

$$1 - \frac{1}{2} + \frac{1}{3} - \cdots - \frac{1}{2n} = \frac{1}{n+1} + \cdots + \frac{1}{2n};$$

(2)

$$\frac{1}{1 \cdot 2} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{(2n-1)2n} = \frac{1}{n+1} + \cdots + \frac{1}{2n};$$

(3)

$$1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{n(4n^2-1)}{3};$$

(4)

$$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! = (n+1)! - 1.$$

(5)

$$0 \cdot 1^2 + 1 \cdot 2^2 + 2 \cdot 3^2 + \cdots + (n-1)n^2 = \frac{n(n^2-1)(3n+2)}{12};$$

(6)

$$\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right)\left(1 - \frac{1}{16}\right) \cdots \left(1 - \frac{1}{(n+1)^2}\right) = \frac{n+2}{2n+2};$$

(7)

$$(1+1)\left(1 + \frac{1}{2}\right)\left(1 + \frac{1}{3}\right) \cdots \left(1 + \frac{1}{n}\right) = n+1;$$

(8)

$$(2^{2^0} + 1)(2^{2^1} + 1)(2^{2^2} + 1) \cdots (2^{2^n} + 1) = 2^{2^{n+1}} - 1.$$

→° **2.1.15. Feladat [6].** Fejezzük ki egyszerűbb alakban az alábbi összegeket:

(1)

$$1 + 3 + 5 + \cdots + 2n - 1 = n^2;$$

(2)

$$1^2 - 2^2 + 3^2 - \cdots + (-1)^{n-1}n^2.$$

° **2.1.16. Feladat [9].** Fejezzük ki egyszerűbb alakban az alábbi összegeket:

$$(1) \quad \frac{1}{1 \cdot 5} + \frac{1}{2 \cdot 6} + \frac{1}{3 \cdot 7} + \cdots + \frac{1}{(n-3)(n+1)};$$

$$(2) \quad \frac{1}{1 \cdot 2 \cdot 3} + \frac{1}{2 \cdot 3 \cdot 4} + \cdots + \frac{1}{n(n+1)(n+2)};$$

$$(3) \quad 1^4 + 2^4 + \cdots + n^4.$$

◦ **2.1.17. Feladat [8].** Bizonyítsuk be, hogy minden $k \in \mathbb{N}$ -re

$$1^k + 2^k + 3^k + \cdots + n^k$$

egy $k+1$ -ed fokú polinomja n -nek.

◦ **2.1.18. Feladat [11].** Fejezzük ki egyszerűbb alakban az alábbi összegeket:

$$(1) \quad \frac{1^3}{1^4+4} - \frac{3^3}{3^4+4} + \frac{5^3}{5^4+4} + \cdots + \frac{(-1)^n(2n+1)^3}{(2n+1)^4+4};$$

$$(2) \quad 1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + n \cdot 2^n;$$

$$(3) \quad 1x^1 + 2x^2 + 3x^3 + \cdots + nx^n, \quad \text{ha } x \in \mathbb{R}, \quad x \neq 1.$$

→◦ **2.1.19. Feladat [6].** Bizonyítsuk be, hogy minden $n \in \mathbb{N}^+$ -ra

$$(1) \quad \sqrt{n} \leq 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} < 2\sqrt{n};$$

$$(2) \quad \frac{n}{2} \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^n - 1} \leq n.$$

◦ **2.1.20. Feladat [6].** Igazoljuk, hogy

$$(1) \quad \sqrt{n} \leq 1 + \frac{1}{2\sqrt{2}} + \frac{1}{3\sqrt{3}} + \cdots + \frac{1}{n\sqrt{n}} \leq 3 - \frac{2}{\sqrt{n}}, \quad \text{ha } n \in \mathbb{N}^+;$$

$$(2) \quad \sqrt{n} \leq 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} < 2\sqrt{n}, \quad \text{ha } n \in \mathbb{N}^+;$$

$$(3) \quad \frac{(n+1)^n}{n^n} > 2, \quad \text{ha } n \in \mathbb{N}, \quad n > 1;$$

$$(4) \quad \frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n} > \frac{13}{24}, \quad \text{ha } n \in \mathbb{N}, \quad n > 1;$$

$$(5) \quad \frac{1}{2\sqrt{n}} < \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdots \frac{2n-1}{2n} < \frac{1}{\sqrt{3n+1}}, \quad \text{ha } n \in \mathbb{N}, n > 1;$$

$$(6) \quad n^{6/7} \leq \frac{1}{\sqrt[7]{1}} + \frac{1}{\sqrt[7]{2}} + \frac{1}{\sqrt[7]{3}} + \cdots + \frac{1}{\sqrt[7]{n}} \leq \frac{7}{6} n^{6/7}, \quad \text{ha } n \in \mathbb{N}^+;$$

$$(7) \quad 2^n > 1 + n\sqrt{2^{n-1}}, \quad \text{ha } n \in \mathbb{N}, n > 1;$$

$$(8) \quad 2^n > n^2, \quad \text{ha } n \in \mathbb{N}, n > 4;$$

$$(9) \quad 3^n > n^3, \quad \text{ha } n \in \mathbb{N}, n > 3;$$

$$(10) \quad 2^n > n^3, \quad \text{ha } n \in \mathbb{N}, n > 9;$$

$$(11) \quad 3^n > 2^n + 7n, \quad \text{ha } n \in \mathbb{N}, n > 3.$$

◦ **2.1.21. Feladat [5].** Indukcióval bizonyítsuk be, hogy ha $n \in \mathbb{N}^+$, akkor 2^n osztja az $(n+1)(n+2) \cdots (2n)$ szorzatot.

◦ **2.1.22. Feladat [5].** Bizonyítsuk be a *Bernoulli-egyenlőtlenséget*: $x > -1$, $n \in \mathbb{N}^+$ esetén fennáll az $(1+x)^n \geq 1+nx$ egyenlőtlenség és egyenlőség csak $n=1$ vagy $x=0$ esetén teljesül.

◦ **2.1.23. Feladat [5].** Bizonyítsuk be az *általánosított Bernoulli-egyenlőtlenséget*:

$$(1+x_1)(1+x_2) \cdots (1+x_n) \geq 1+x_1+x_2+\cdots+x_n,$$

ahol $x_1, \dots, x_n$ azonos előjelű és -1 -nél nagyobb valós számok.

◦ **2.1.24. Feladat [6].** Fejben: hány jegyű 2^{300} tizes számrendszerben?

◦ **2.1.25. Feladat [6].** Fejben: hány jegyű 10^{60} kettes számrendszerben?

◦ **2.1.26. Feladat [3].** Igazoljuk, hogy $(1+1/n)^n > 2$, ha $n \in \mathbb{N}$, $n > 2$.

◦ **2.1.27. Feladat [5].** Igazoljuk, hogy

$$\frac{3}{2} \cdot \frac{5}{2} \cdot \frac{7}{2} \cdots \frac{2n+1}{2} < \left(\frac{n+1}{2}\right)^{n+1},$$

ha $n \in \mathbb{N}$, $n > 2$.

◦ **2.1.28. Feladat [5].** A k szerinti indukcióval bizonyítsuk be, hogy ha $k, n \in \mathbb{N}^+$ és $k \leq n$, akkor $(1+1/n)^k < 1+k/n+k^2/n^2$. Ezt felhasználva mutassuk meg, hogy

$$(1) \quad (1+1/n)^n < 3, \quad \text{ha } n \in \mathbb{N}^+;$$

$$(2) \quad n^n < (n!)^2, \quad \text{ha } n \in \mathbb{N}, n > 2;$$

$$(3) \quad n^{n+1} > (n+1)^n, \quad \text{ha } n \in \mathbb{N}, n > 2.$$

* **2.1.29. Feladat [10].** Bizonyítsuk be, hogy van olyan $N \in \mathbb{N}$, hogy

$$2! \cdot 4! \cdots (2n)! > (n!)^2 ((n+1)!)^n, \quad \text{ha } n > N.$$

° **2.1.30. Feladat [7].** Hány részre osztja a síkot n egyenes, ha „általános helyzetűek”, azaz közülük semelyik kettő nem párhuzamos és semelyik három nem megy át egy ponton?

° **2.1.31. Feladat [9].** Bizonyítandó, hogy véges sok egyenes (vagy kör) a síkot olyan tartományokra bontja, amelyek kiszínezhetők két színnel úgy, hogy azonos színű tartományoknak nincs közös határvonaluk.

* **2.1.32. Feladat [9].** Írjunk a $\dots \varepsilon > 0 \dots N \dots n \geq N$ ($|a_n - A| < \varepsilon$) kifejezésbe, amelyben $a: \mathbb{N} \rightarrow \mathbb{R}$ egy sorozat, $A, \varepsilon \in \mathbb{R}$ és $n, N \in \mathbb{N}$, a kipontozott részek helyére kvantorokat az összes lehetséges módon. Milyen tulajdonságát fejezik ki a sorozatnak a kapott formulák? Ha van, adjunk meg olyan sorozatot, amely rendelkezik a megfelelő tulajdonsággal.

* **2.1.33. Feladat [8].** Az előző feladat jelöléseivel, adott $A \in \mathbb{R}$ -re milyen tulajdonságát fejezik ki az $a: \mathbb{N} \rightarrow \mathbb{R}$ egy sorozatnak az alábbi formulák? Ha van, adjunk meg olyan sorozatot, amely rendelkezik a megfelelő tulajdonsággal.

$$(1) \quad \exists N \forall \varepsilon > 0 \forall n \geq N (|a_n - A| < \varepsilon);$$

$$(2) \quad \exists N \forall \varepsilon > 0 \exists n \geq N (|a_n - A| < \varepsilon);$$

$$(3) \quad \forall N \exists \varepsilon > 0 \forall n \geq N (|a_n - A| < \varepsilon);$$

$$(4) \quad \forall N \exists \varepsilon > 0 \exists n \geq N (|a_n - A| < \varepsilon).$$

* **2.1.34. Feladat [10].** Írjunk a $\dots A \dots N \dots n \geq N$ ($a_n > A$) kifejezésbe, amelyben $a: \mathbb{N} \rightarrow \mathbb{R}$ egy sorozat, $A \in \mathbb{R}$ és $n, N \in \mathbb{N}$, a kipontozott részek helyére kvantorokat az összes lehetséges módon, illetve permutáljuk a kvantoros részeket. Milyen tulajdonságát fejezik ki a sorozatnak a kapott formulák? Ha van, adjunk meg olyan sorozatot, amely rendelkezik a megfelelő tulajdonsággal.

→° **2.1.35. Feladat [3].** Ha Y és Z az X alaphalmaz részhalmazai, fejezzük ki az $X \setminus Y$, $Y \cap Z$, $Y \cup Z$, $Y \setminus Z$ és $Y \triangle Z$ halmazok karakterisztikus függvényeit χ_Y és χ_Z segítségével.

→° **2.1.36. Feladat [3].** Az informatikában elterjedt az *Iverson-konvenció*: ha

$$Y = \{x \in X: \mathcal{F}(x)\}$$

az X részhalmaza, akkor karakterisztikus függvényét $[\mathcal{F}(x)]$ jelöli. Adjuk meg másként az $x \mapsto [x \neq 0]/(x + [x = 0])$, $x \in \mathbb{R}$ függvényt.

2.1.37. További feladatok. [59]: I.2.44, I.2.45; [64]: 2.1.1–2.1.13, 2.2.1, 2.2.2, 2.5.1–2.5.4; [84]: 1.37.

2.2 Műveletek természetes számokkal

2.2.1. Természetes számok összeadása. A rekurziótétel alapján minden $m \in \mathbb{N}$ -re egyértelműen létezik olyan $s_m: \mathbb{N} \rightarrow \mathbb{N}$ függvény (az m -mel növelés), amelyre $s_m(0) = m$ és minden $n \in \mathbb{N}$ -re $s_m(n^+) = (s_m(n))^+$. Az $s_m(n)$ számot $m + n$ -nel fogjuk jelölni, és az m és az n összegének nevezzük, + az *összeadás*. Megjegyezzük, hogy az összeadásból visszakaphatjuk a rákövetkezést, hiszen $m^+ = m + 1 = s_m(1)$.

2.2.2. Tétel. Ha $k, m, n \in \mathbb{N}$, akkor

- (1) $(k + m) + n = k + (m + n)$ (asszociativitás);
- (2) $0 + n = n + 0 = n$ (a 0 nullelem);
- (3) $m + n = n + m$ (kommutativitás);
- (4) ha $m + k = n + k$ vagy $k + m = k + n$, akkor $m = n$ (egyszerűsítési szabály vagy törlési szabály).

Bizonyítás. Az asszociativitást n szerinti indukcióval bizonyítjuk. Felhasználjuk, hogy $k = s_k(0) = k + 0$ minden $k \in \mathbb{N}$ -re. Az $n = 0$ esetben

$$(k + m) + 0 = k + m = k + (m + 0).$$

Tegyük fel, hogy $n \in \mathbb{N}$ -re igaz az állítás. Belátjuk, hogy akkor $n^+ \in \mathbb{N}$ -re is igaz. Valóban,

$$\begin{aligned} (k + m) + n^+ &= s_{k+m}(n^+) = ((k + m) + n)^+ = (k + (m + n))^+ \\ &= k + (m + n)^+ = k + (m + n^+); \end{aligned}$$

az indukciós feltevést a harmadik egyenlőségnél használtuk fel.

(2) bizonyítása is n szerinti indukcióval történik. $0 + n = s_0(n) = n$ az $n = 0$ esetben nyilvánvaló. Tegyük fel, hogy $n \in \mathbb{N}$ -re igaz az állítás. Ekkor $0 + n^+ = s_0(n^+) = s_0(n)^+ = (0 + n)^+ = n^+$, így az állítás minden $n \in \mathbb{N}$ -re teljesül.

A jobb oldali egyszerűsítési szabály bizonyítása k szerinti indukcióval történik: a $k = 0$ eset s_m és s_n definíciója miatt nyilvánvaló, és ha k -ra teljesül az állítás, akkor $m + k^+ = n + k^+$ -ből $(m + k)^+ = (n + k)^+$, így $m + k = n + k$, amiből az indukciós feltevés miatt $m = n$. A bal oldali egyszerűsítési szabály következni fog ebből az esetből, ha belátjuk a kommutativitást.

A kommutativitást két indukcióval bizonyítjuk. Először n szerinti indukcióval belátjuk, hogy rögzített $m \in \mathbb{N}$ esetén $m^+ + n = (m + n)^+$ minden $n \in \mathbb{N}$ -re. Az $n = 0$ eset (2) miatt teljesül: $m^+ + 0 = m^+ = (m + 0)^+$. Tegyük fel, hogy $m^+ + n = (m + n)^+$ valamilyen $n \in \mathbb{N}$ -re. Ekkor s_{m^+} és s_m definíciója valamint az indukciós feltevés miatt

$$m^+ + n^+ = (m^+ + n)^+ = ((m + n)^+)^+ = (m + n^+)^+,$$

vagyis a segédállítás tényleg minden $n \in \mathbb{N}$ -re igaz. Most megmutatjuk, hogy $m + n = n + m$ minden $n \in \mathbb{N}$ -re. Az $n = 0$ eset (2)-ből következik. Indukcióval bizonyítva tegyük fel, hogy valamilyen $n \in \mathbb{N}$ -re igaz az állítás. Ekkor a segédállítás és az indukciós feltevés miatt

$$m + n^+ = (m + n)^+ = (n + m)^+ = n^+ + m,$$

vagyis $m + n = n + m$ minden $n \in \mathbb{N}$ -re teljesül. $\square$

2.2.3. Természetes számok szorzása. A rekurziótétel alapján minden $m \in \mathbb{N}$ -re egyértelműen létezik olyan $p_m: \mathbb{N} \rightarrow \mathbb{N}$ függvény (az m -mel való szorzás), amelyre $p_m(0) = 0$ és minden $n \in \mathbb{N}$ -re $p_m(n^+) = p_m(n) + m$. A $p_m(n)$ számot $m \cdot n$ -el fogjuk jelölni, és az m és az n szorzatának nevezzük; $\cdot$ a szorzás.

2.2.4. Tétel. Ha $k, m, n \in \mathbb{N}$, akkor

- (1) $(k \cdot m) \cdot n = k \cdot (m \cdot n)$ (asszociativitás);
- (2) $0 \cdot n = n \cdot 0 = 0$;
- (3) $1 \cdot n = n \cdot 1 = n$ (az 1 egységelem);
- (4) $m \cdot n = n \cdot m$ (kommutativitás);
- (5) $k \cdot (m + n) = k \cdot m + k \cdot n$ és $(m + n) \cdot k = m \cdot k + n \cdot k$ (disztributivitás).

Az egyszerűsítési szabályt később bizonyítjuk.

Bizonyítás. (2) bizonyítása n szerinti indukcióval történik. A szorzás definíciójából következik, hogy $n \cdot 0 = 0$ minden $n \in \mathbb{N}$ -re, így $n = 0$ esetén $0 \cdot n = 0$ is teljesül. Tegyük fel, hogy $n \in \mathbb{N}$ -re $0 \cdot n = 0$. Ekkor

$$0 \cdot n^+ = 0 \cdot n + 0 = 0 \cdot n = 0.$$

(3) bizonyítása is n szerinti indukcióval történik. Nyilván $n \cdot 1 = n \cdot 0 + n = n$. Az, hogy $1 \cdot 0 = 0$, definíció szerint teljesül. Tegyük fel, hogy $n \in \mathbb{N}$ -re $1 \cdot n = n$. Ekkor

$$1 \cdot n^+ = 1 \cdot n + 1 = n + 1 = n^+.$$

A bal oldali disztributivitást n szerinti indukcióval bizonyítjuk. Ha $n = 0$, akkor

$$k \cdot (m + 0) = k \cdot m = k \cdot m + 0 = k \cdot m + k \cdot 0.$$

Tegyük fel, hogy $n \in \mathbb{N}$ -re igaz az állítás. Ekkor

$$\begin{aligned} k \cdot (m + n^+) &= k \cdot (m + n)^+ = k \cdot (m + n) + k \\ &= (k \cdot m + k \cdot n) + k = k \cdot m + (k \cdot n + k) \\ &= k \cdot m + k \cdot n^+. \end{aligned}$$

A jobb oldali disztributivitás ebből következik, ha belátjuk majd a kommutativitást. Az asszociativitást is n szerinti indukcióval bizonyítjuk. Az $n = 0$ esetben

$$(k \cdot m) \cdot 0 = 0 = k \cdot 0 = k \cdot (m \cdot 0).$$

Tegyük fel, hogy $n \in \mathbb{N}$ -re igaz az állítás. Ekkor

$$\begin{aligned} (k \cdot m) \cdot n^+ &= (k \cdot m) \cdot n + k \cdot m = k \cdot (m \cdot n) + k \cdot m = k \cdot (m \cdot n + m) \\ &= k \cdot (m \cdot n^+). \end{aligned}$$

A kommutativitáshoz először bebizonyítjuk, hogy

$$m^+ \cdot n = m \cdot n + n$$

minden $n \in \mathbb{N}$ -re. Indukcióval bizonyítva az $n = 0$ eset $m^+ \cdot 0 = 0 = m \cdot 0 + 0$ miatt nyilvánvaló. Tegyük fel, hogy valamilyen $n \in \mathbb{N}$ -re igaz az állítás. Ekkor

$$\begin{aligned} m^+ \cdot n^+ &= m^+ \cdot n + m^+ = (m \cdot n + n) + m^+ = ((m \cdot n + n) + m)^+ \\ &= (m \cdot n + (n + m))^+ = (m \cdot n + (m + n))^+ = ((m \cdot n + m) + n)^+ \\ &= (m \cdot n^+ + n)^+ = m \cdot n^+ + n^+. \end{aligned}$$

Ebből az $m \cdot n = n \cdot m$ kommutativitás bizonyítása n szerinti indukcióval történik. Az $n = 0$ eset (2) miatt teljesül. Tegyük fel, hogy $n \in \mathbb{N}$ -re igaz az állítás. Ekkor

$$m \cdot n^+ = m \cdot n + m = n \cdot m + m = n^+ \cdot m. \quad \square$$

→ **2.2.5. Feladat [3].** Bizonyítsuk be, hogy természetes számokra

- (1) $m + n = 0$ esetén $m = 0$ és $n = 0$;
- (2) $mn = 0$ esetén $m = 0$ vagy $n = 0$;
- (3) $m + n = 1$ esetén $m = 1$ vagy $n = 1$;
- (4) $mn = 1$ esetén $m = 1$ és $n = 1$.

→° **2.2.6. Feladat [6].** Az alábbi, képlettel megadott sorozatokat definiáljuk rekurzióval. (Hasonló rekurziókat használt Babbage első számítógépe polinomok értékeinek kiszámítására, és ezáltal trigonometrikus függvények értékeinek közelítésére.)

- (1) $a_n = (-1)^n$;
- (2) $a_n = n^2$;
- (3) $a_n = (2n + 3)^2$;
- (4) $a_n = n^3$;
- (5) $a_n = n^3 - n^2 - 2n + 3$;
- (6) $a_n = n$, ha n páros, és $a_n = 1$, ha n páratlan.

2.2.7. Félcsoport, csoport, kommutativitás. Legyen $*$ egy binér művelet a G halmazon. A G halmazt a $*$ művelettel, (azaz, ha pontosak akarunk lenni, a $(G, *)$ párt) szokás *grupoid*-nak is nevezni. A G egy s elemét *bal*, illetve *jobb oldali semleges elem*nek nevezzük, ha $s * g = g$, illetve $g * s = g$ minden $g \in G$ -re. Ha s bal és jobb oldali semleges elem is, akkor *semleges elem*nek nevezzük. A G -ben létezhet akárhány bal oldali vagy jobb oldali semleges elem. (Például a $(g, h) \mapsto h$ műveletnél minden elem bal oldali semleges elem, a $(g, h) \mapsto g$ műveletnél pedig minden elem jobb oldali semleges elem.) Ha azonban van egy bal oldali s_b és egy jobb oldali s_j semleges elem, akkor $s_b = s_b * s_j = s_j$, így bármely bal oldali semleges elem megegyezik bármely jobb oldali semleges elemmel, azaz csak egy bal és jobb oldali semleges elem van.

Ha a $*$ binér művelet a G halmazon *asszociatív*, azaz $x, y, z \in G$ esetén $(x * y) * z = x * (y * z)$, akkor G -t (pontosabban a $(G, *)$ párt) *félcsoport*-nak nevezzük. Semleges elemes félcsoport neve *monoid*. Ha a G félcsoportban s semleges elem, és $g, g^* \in G$ -re $g * g^* = s$, akkor azt mondjuk, hogy g a g^* *balinverze*, g^* pedig a g *jobbinverze*. Ha g^* a g bal- és jobbinverze is, akkor azt mondjuk, hogy a g *inverze*. Ekkor nyilván g meg a g^* inverze. Ha g^* a g egy balinverze, g^{**} pedig a g egy jobbinverze, akkor

$$g^* = g^* * s = g^* * (g * g^{**}) = (g^* * g) * g^{**} = s * g^{**} = g^{**}.$$

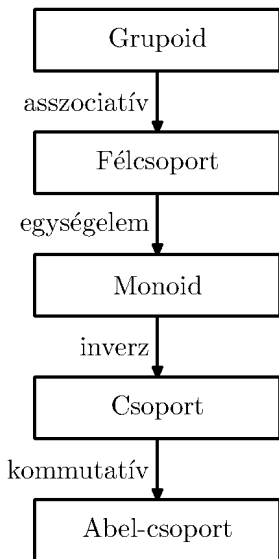
Speciálisan, ha g -nek van inverze, az egyértelmű. Az inverzképzést unér műveletnek is tekinthetjük. Vegyük észre, hogy ha h -nak h^* az inverze, akkor $g * h$ inverze $h^* * g^*$, mert

$$(g * h) * (h^* * g^*) = g * (h * (h^* * g^*)) = g * ((h * h^*) * g^*) = g * (s * g^*) = g * g^* = s,$$

és hasonlóan $(h * g) * (g * h) = s$. Ha egy semleges elemes félcsoporth minden elemének van inverze, akkor *csoporthnak* nevezzük.

Egy G monoid azon elemeinek halmazát, amelyeknek van inverze, $G^\times$ -szel jelöljük (függetlenül attól, hogy mivel jelöljük a műveletet). Bármely G monoidra $(G^\times, *)$ csoport. (Ha két művelet van, és a struktúra az egyikre csoport, akkor a másikra értendő a jelölés, például $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$.)

Ha a $*$ binér művelet a G halmazon, $g, h \in G$ és $g * h = h * g$, akkor azt mondjuk, hogy g és h *felcserélhetőek*. Ha G bármely két eleme felcserélhető, akkor a $*$ műveletet *kommutatívnak* nevezzük. Kommutatív esetben a műveletet gyakran $+$ -szal jelöljük (*additív jelölés*), a semleges elemet *nullelemnek* nevezzük, és n -nel vagy 0 -val (ha nagyon precízek vagyunk, n_G -vel vagy 0_G -vel) jelöljük, a g inverzét pedig $-g$ -vel jelöljük és g *ellentettjének* nevezzük. A kommutatív csoportokat *Abel-csoportnak* szokás nevezni, mert Niels Henrik Abel norvég matematikus vizsgálta őket először. Gyakran $h + (-g)$ helyett $h - g$ -t írunk. Nem kommutatív esetben a műveletet rendszerint $\cdot$ -tal jelöljük (*multiplikatív jelölés*). Multiplikatív jelölés esetén általában is a semleges elemet *egységelemnek* nevezzük, és e -vel vagy 1 -gyel (ha nagyon precízek vagyunk, akkor e_G -vel vagy 1_G -vel) jelöljük. A g inverzét általában g^{-1} -el, néha $1/g$ -vel jelöljük. Ha kommutatív esetben multiplikatív jelölést használunk, akkor $h \cdot g^{-1}$ helyett gyakran h/g -t írunk. A nem kommutatív esetben ez nem célszerű, mert $h \cdot g^{-1}$ nem feltétlenül egyenlő $g^{-1} \cdot h$ -val, holott mindkettőt írhatjuk h/g alatt. A 2.2.1 ábra szemlélteti az összefüggéseket.



2.2.1 ábra: egyműveletes algebrai struktúrák.

2.2.8. Megjegyzés. Az előző két tétel mutatja, hogy $(\mathbb{N}, +)$ kommutatív félcsoporth a 0 nullelemmel (belátható, hogy csak a 0 -nak van additív inverze, a 0 , tehát $(\mathbb{N}, +)$ nem csoport), valamint $(\mathbb{N}, \cdot)$ és $(\mathbb{N}^+, \cdot)$ is kommutatív félcsoporth az 1 egységelemmel

(belátható, hogy csak az 1-nek van multiplikatív inverze, az 1, tehát $(\mathbb{N}, \cdot)$ és $(\mathbb{N}^+, \cdot)$ sem csoport).

2.2.9. Példák. (1) Ha X tetszőleges halmaz, akkor $(\wp(X), \cap)$ és $(\wp(X), \cup)$ kommutatív egységelemes félcsoporthok (az egységelem X illetve $\emptyset$), továbbá $(\wp(X), \Delta)$ Abel-csoport, amelyben az egységelem az üres halmaz, az inverz pedig a halmaz maga, míg $(\wp(X), \setminus)$ -ben általában nincs egységelem, a művelet nem asszociatív és nem is kommutatív.

(2) Ha X egy halmaz, akkor az X -beli binér relációk a $\circ$ összetétellel egységelemes félcsoporthot alkotnak, amelyben az identikus leképezés az egységelem, de amely általában nem kommutatív és nem is csoport, bár vannak invertálható elemei.

(3) Ha X egy halmaz, akkor az X -et önmagába képező függvények a $\circ$ összetétellel mint művelettel egységelemes félcsoporthot alkotnak, amelyben az identikus leképezés az egységelem. Ha csak az összes injektív, illetve az összes szürjektív leképezéseket tekintjük, akkor is egy-egy egységelemes félcsoporthot kapunk ugyanazzal az egységelemmel. Az összes bijektív leképezések (vagyis a permutációk) csoportot alkotnak. Ezt a csoportot S_X -szel jelöljük, és X szimmetrikus csoportjának nevezzük. Ha az összes nem injektív leképezéseket, illetve az összes nem szürjektív leképezéseket tekintjük, akkor is félcsoporthot kapunk, de ez már nem lesz egységelemes. Mindezen példákban a művelet általában nem kommutatív.

2.2.10. Feladat [10]. Egészítsük ki az előző pontot bizonyítással.

◦ **2.2.11. Feladat [5].** Mutassuk meg, hogy az $\mathbb{R} \setminus \{0, 1\}$ halmaz $t \mapsto t$, $t \mapsto 1/(1-t)$, $t \mapsto (t-1)/t$, $t \mapsto 1/t$, $t \mapsto 1-t$ és $t \mapsto t/(t-1)$ leképezései a függvényösszetétellel nemkommutatív csoportot alkotnak.

◦ **2.2.12. Példák.** $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Z}^\times, \cdot)$, $(\mathbb{Q}^\times, \cdot)$ és $(\mathbb{R}^\times, \cdot)$ Abel-csoportok.

2.2.13. Példák. Ha $X = \{\uparrow, \downarrow\}$, akkor $(X, \wedge)$ és $(X, \vee)$ kommutatív egységelemes félcsoporthok, $(X, \iff)$ Abel-csoport, míg $(X, \Rightarrow)$ -ben nincs egységelem, a művelet nem asszociatív és nem is kommutatív. (Lásd 1.4.39)

→ **2.2.14. Feladat [3].** Egészítsük ki az előző pontot bizonyítással.

→ **2.2.15. Feladat [3].** Defináljuk a természetes számok hatványozását természetes szám kitevőre. Vizsgáljuk meg a tulajdonságait.

→ **2.2.16. Feladat [3].** Hány kommutatív binér művelet definiálható egy 0, 1, 2, illetve 3 elemű halmazon?

→ **2.2.17. Feladat [5].** Adjunk példát semleges elemes grupoidra, amelyben egy elemnek több inverze is van.

→ **2.2.18. Feladat [5].** Hány olyan binér művelet van a $\{\uparrow, \downarrow\}$ halmazon, amellyel semleges elemes félcsoporth?

→ **2.2.19. Feladat [5].** Hány olyan binér művelet van a $\{\uparrow, \downarrow\}$ halmazon, amellyel félcsoporth, amelyben nincs semleges elem, de van jobb illetve bal oldali semleges elem?

→ **2.2.20. Feladat [6].** Hány olyan binér művelet van a $\{\uparrow, \downarrow\}$ halmazon, amellyel félcsoporth? A műveleteket fejezzük ki $\neg$, $\wedge$, $\vee$, $\oplus$, $|$, $\parallel$, $\Rightarrow$ és $\iff$ segítségével.

→ **2.2.21. Feladat [8].** Hányféleképpen tudunk műveletet definiálni egy háromelemű halmazon úgy, hogy azzal egységelemes félcsoporth legyen?

→ **2.2.22. Feladat [8].** Hányféleképpen tudunk műveletet definiálni egy 0, 1, 2, 3 illetve 4 elemű halmazon úgy, hogy azzal Abel-csoport legyen?

→ **2.2.23. Feladat [9].** Hányféleképpen tudunk műveletet definiálni egy 0, 1, 2, 3 illetve 4 elemű halmazon úgy, hogy azzal csoport legyen?

° **2.2.24. Feladat [6].** Vizsgáljuk meg, teljesül-e az asszociativitás, kommutativitás, van-e egységelem, illetve mely elemeknek van inverze az alábbi esetekben:

- (1) $(\mathbb{N}^+, \star)$, ahol $x \star y = xy - x + y$;
- (2) $(\mathbb{N}^+, \star)$, ahol $x \star y = xy + x + y$;
- (3) $(\mathbb{N}, \star)$, ahol $x \star y = xy + x + y$;
- (4) $(\mathbb{Z}, \star)$, ahol $x \star y = x$;
- (5) $(\mathbb{R}, \star)$, ahol $x \star y = ax + by$, $a, b \in \mathbb{R}$ rögzített;
- (6) $(A \times B, \star)$, ahol $(x, x') \star (y, y') = (x, y')$, A, B nem üres halmazok.

2.2.25. Feladat [6]. Az alábbi állítások mikor igazak minden csoportban, minden a, b, x, y elemre? Az érvényeseket bizonyítsuk be, a többire adjunk ellenpéldát:

- (1) ha $axb = ayb$, akkor $x = y$;
- (2) ha $x^{-1} = y^{-1}$, akkor $x = y$;
- (3) ha $xa = ay$, akkor $x = y$;
- (4) ha $xy = 1$, akkor $y = x^{-1}$;
- (5) ha $abx = 1$, akkor $x = a^{-1}b^{-1}$;
- (6) ha $(xy)^2 = x^2y^2$, akkor $xy = yx$.

2.2.26. Feladat [8]. Legyen G kommutatív félcsoporth, amelyben $x^2 = x$ minden $x \in G$ -re. (Például bármely X halmazra $(\wp(X), \cap)$, illetve $(\wp(X), \cup)$ ilyen.) Mutassuk meg, hogy $\{(x, y) \in G \times G : xy = y\}$ olyan részbenrendezés, amelyre minden $\{x, y\} \subset G$ halmaznak van szuprémuma. Megfordítva, mutassuk meg, hogy ha adott egy olyan részbenrendezés a G halmazon, amelyre minden $\{x, y\} \subset G$ halmaznak van szuprémuma, akkor az $(x, y) \mapsto \sup\{x, y\}$ művelettel G kommutatív félcsoporth, amelyben $x^2 = x$ minden $x \in G$ -re.

2.3 A természetes számok rendezése

2.3.1. A természetes számok rendezése. Ha $n, m \in \mathbb{N}$, akkor azt mondjuk, hogy $m \leq n$, ha van olyan k természetes szám, hogy $m + k = n$.

2.3.2. Tétel. A természetes számok halmaza $a \leq$ relációval rendezett.

Bizonyítás. Nyilvánvaló, hogy $\leq$ reflexív és tranzitív. Megmutatjuk, hogy antiszimmetrikus. Ha $m \leq n$ és $n \leq m$, akkor $n = m + x$ és $m = n + y$ valamely (az egyszerűsítési szabály szerint egyértelműen meghatározott) $x, y \in \mathbb{N}$ -re. De ebből $n + 0 = n = m + x = (n + y) + x = n + (y + x)$. Az egyszerűsítési szabály szerint $y + x = 0$. Ha $x \neq 0$, az összeg definíció szerint rákövetkezője valaminek, így nem lehet 0. Tehát $x = 0$. Innen $n = m$.

Meg kell még mutatnunk, hogy $\mathbb{N}$ bármely két eleme összehasonlítható. Jelölje $S(n)$ azon elemek halmazát, amelyek egy adott $n \in \mathbb{N}$ -nel összehasonlíthatók, S pedig azon $n \in \mathbb{N}$ -ek halmazát, amelyekre $S(n) = \mathbb{N}$. Azt kell megmutatnunk, hogy $S = \mathbb{N}$. Először megmutatjuk, hogy $S(0) = \mathbb{N}$, azaz $0 \in S$. Valóban, $m = 0 + m$, így $0 \leq m$ minden $m \in \mathbb{N}$ -re. Most feltéve, hogy $S(n) = \mathbb{N}$, megmutatjuk, hogy $S(n^+) = \mathbb{N}$. Legyen $m \in \mathbb{N}$. Ha $m \leq n$, akkor $n = m + k$, így $n^+ = m + k^+$, tehát $m \leq n^+$, azaz $m \in S(n^+)$. Ha $m > n$, akkor $m = n + k$ valamely, az egyszerűsítési szabály szerint egyértelműen meghatározott $k \in \mathbb{N}$ -re, amelyre $k \neq 0$. Legyen $k = j^+$, akkor $m = n + k = n + j^+ = n^+ + j$, így $m \geq n^+$. Ezzel beláttuk, hogy $S(n^+) = \mathbb{N}$, így ha $n \in S$, akkor $n^+ \in S$. Indukcióval kapjuk, hogy $S = \mathbb{N}$. $\square$

2.3.3. Tétel. Legyen $k, m, n \in \mathbb{N}$. Ekkor

- (1) n^+ közvetlenül követi n -et;
- (2) $m \leq n$ akkor és csak akkor, ha $m + k \leq n + k$;
- (3) $k \neq 0$ esetén $m \leq n$ akkor és csak akkor, ha $m \cdot k \leq n \cdot k$;
- (4) $m < n$ akkor és csak akkor, ha $m + k < n + k$;
- (5) $k \neq 0$ esetén $m < n$ akkor és csak akkor, ha $m \cdot k < n \cdot k$;
- (6) $k \neq 0$ esetén, ha $m \cdot k = n \cdot k$, akkor $m = n$ (egyszerűsítési szabály vagy törlési szabály $k \neq 0$ -ra).

Bizonyítás. (1)-hez, ha $n < m$, akkor $m = n + x$. Mivel $x \neq 0$, van olyan y , amelyre $x = y^+$. De ekkor $m = n + y^+ = n^+ + y$, azaz $m \geq n^+$, így nincs olyan m , amelyre $n < m < n^+$. (2) és (4) a definíció és az összeadásra vonatkozó egyszerűsítési szabály alapján adódnak. A definícióból és a disztributivitásból adódik, hogy $m \leq n$ esetén $m \cdot k \leq n \cdot k$, illetve hogy $m < n$ esetén $m \cdot k < n \cdot k$, amivel beláttuk (3) illetve (5) egyik irányát. A másik irány indirekten adódik, (3) esetén az (5), az (5) esetén pedig (3) már bizonyított részének felhasználásával. (6) következik (3)-ból. $\square$

2.3.4. Tétel. A természetes számok halmaza $a \leq$ relációval jólrendezett.

Bizonyítás. Legyen $A \subset \mathbb{N}$ nem üres halmaz. Legyen

$$B = \{m \in \mathbb{N} : m \leq n \text{ minden } n \in A\text{-ra}\}.$$

Nyilván $0 \in B$. Ha $n \in A$, akkor $n^+ \notin B$. Tehát van olyan $m \in B$ is, amelyre $m^+ \notin B$, mert egyébként indukcióval azt kapnánk, hogy $B = \mathbb{N}$. Megmutatjuk, hogy m az A legkisebb eleme. Az világos, hogy alsó korlát, csak azt kell belátnunk, hogy $m \in A$. Ha $m \notin A$ teljesülne, akkor minden $n \in A$ -ra $m < n$ lenne, amiből $m^+ \leq n$ következne, mert m^+ közvetlenül követi m -et, ez azonban $m^+ \notin B$ miatt ellentmondás. $\square$

2.3.5. Sorozatok. Mint már említettük, az $\mathbb{N}$ -en vagy $\mathbb{N}^+$ -on értelmezett függvényeket *végtelen sorozatnak* nevezzük. Az x végtelen sorozatot úgy is jelöljük, hogy $x_0, x_1, x_2, \dots$ (vagy $x_i, i = 0, 1, 2, \dots$), illetve $x_1, x_2, x_3, \dots$ (vagy $x_i, i = 1, 2, 3, \dots$). Ha $n \in \mathbb{N}$, akkor a $[0, n[\subset \mathbb{N}$ vagy $[1, n] \subset \mathbb{N}^+$ halmazon értelmezett függvényeket *véges sorozatnak* nevezzük. Az x véges sorozatot úgy is jelöljük, hogy $x_0, x_1, \dots, x_{n-1}$ (vagy $x_i, i = 0, 1, 2, \dots, n-1$), illetve $x_1, x_2, \dots, x_n$ (vagy $x_i, i = 1, 2, \dots, n$). Az $x_1, x_2, \dots, x_n$ véges sorozatot *rendezett*

n -esnek is nevezzük; ekkor rendszerint $(x_1, x_2, \dots, x_n)$ -nel jelöljük. Ha a szövegösszefüggésből kiderül, hogy véges vagy végtelen sorozatról van szó, akkor egyszerűen csak *sorozatról* beszélünk.

Végtelen halmazsorozat uniójára a

$$\bigcup_{i=0}^{\infty} A_i \quad \text{vagy} \quad A_0 \cup A_1 \cup \dots,$$

metszetére a

$$\bigcap_{i=0}^{\infty} A_i \quad \text{vagy} \quad A_0 \cap A_1 \cap \dots,$$

Descartes-szorzatára pedig a

$$\bigtimes_{i=0}^{\infty} A_i \quad \text{vagy} \quad A_0 \times A_1 \times \dots$$

jelölést használjuk. Véges sorozatok esetén a megfelelő jelölések

$$\begin{aligned} \bigcup_{i=0}^n A_i & \quad \text{vagy} \quad A_0 \cup A_1 \cup \dots \cup A_n, \\ \bigcap_{i=0}^n A_i & \quad \text{vagy} \quad A_0 \cap A_1 \cap \dots \cap A_n, \\ \bigtimes_{i=0}^n A_i & \quad \text{vagy} \quad A_0 \times A_1 \times \dots \times A_n. \end{aligned}$$

Persze mindegyiknél kezdetünk 1-el is.

→ **2.3.6. Feladat [5].** Mutassuk meg, hogy tetszőleges $A_0, A_1, \dots$ halmazsorozat diszjunktá tehető: adjunk meg hozzá olyan, páronként diszjunkt halmazokból álló $B_0, B_1, \dots$ halmazsorozatot, amelyre $\bigcup_{i=0}^n A_i = \bigcup_{i=0}^n B_i$ minden $n \in \mathbb{N}$ -re. Mutassuk meg, hogy $B_i \subset A_i$ minden i -re és $\bigcup_{i=0}^{\infty} A_i = \bigcup_{i=0}^{\infty} B_i$.

→ **2.3.7. Feladat: tranzitív lezárt [5].** Mutassuk meg, hogy tetszőleges X -beli R reláció esetén az X -beli

$$\overline{R} = R \cup (R \circ R) \cup (R \circ R \circ R) \cup \dots$$

reláció, az R *tranzitív lezártja* tranzitív, és minden olyan S tranzitív relációra, amelyre $R \subset S$, teljesül, hogy $\overline{R} \subset S$.

→ **2.3.8. Feladat [3].** Mi a kapcsolat egy X -beli R relációnak és a tranzitív lezártjának a gráfja között?

→ **2.3.9. Feladat [3].** Mi az emberek közötti „gyermek” illetve „szülője” reláció tranzitív lezártja?

2.3.10. Példa. Legyen X egy tetszőleges halmaz, amelyet *ábécének* fogunk nevezni. Az összes, X elemeiből képzett véges sorozatok (ezeket *szavaknak* fogjuk hívni) egységelemes félcsoportot alkotnak az egymás után írásra nézve: ha $f = f_1 f_2 \dots f_n$ egy szó, $g = g_1 g_2 \dots g_m$ pedig egy másik szó, akkor legyen $fg = f_1 f_2 \dots f_n g_1 g_2 \dots g_m$. (Szavaknál nem szokás kiírni a sorozat tagjait elválasztó vesszőket.) Az egységelem az üres sorozat. Ez a félcsoport nem kommutatív, ha X legalább kételemű.

2.3.11. Többváltozós függvények. Egy $X_1 \times X_2 \times \cdots \times X_n$ Descartes-szorzaton vagy annak egy részhalmazán értelmezett függvényt szokás *többváltozós függvénynek* is nevezni. Többváltozós függvények esetén is előfordul, hogy a változókat alsó indexként írjuk. Például a *Kronecker-féle δ -függvényt* a $\delta_{x,y} = 1$, ha $x = y$ és $\delta_{x,y} = 0$, ha $x \neq y$ összefüggésekkel definiáljuk ($x, y \in X$). Megjegyezzük, hogy a Kronecker-delta nem más, mint az $\mathbb{I}_X$ identikus leképezés (a diagonális) karakterisztikus függvénye.

2.3.12. Motiváció: további rekurzív definíciók. A Fibonacci-sorozatot a következőképpen „defináljuk”: legyen $F_0 = 0$, $F_1 = 1$, és legyen $F_{n++} = F_n + F_{n+}$. Érezzük, hogy ez a feltétel egyértelműen definiálja a sortozatot, de ennek bizonyítására a rekurziótétel nem használható, mert a sorozat általános tagja nem csak az előzőtől, hanem az előző kettőtől függ.

Másik példaként tekintsük azt a problémát, hogy az $n + 1$ tényezős $x_0 x_1 \cdots x_n$ szorzatot hányféleképpen lehet zárójelezni, azaz a szorzások sorrendjét hányféleképpen lehet kijelölni. Jelölje c_n ezt a számot. (Ezek az úgynevezett *Catalan-számok*; számos informatikai problémánál előkerülnek.) Ha $n = 0$, akkor nyilván $c_n = 1$. Egyébként gyűjtsük össze azokat a zárójelezéseket, amelyekben a legkülső szorzás x_k után áll. Ezek száma $c_k c_{n-k-1}$, így azt kapjuk, hogy

$$c_n = c_0 c_{n-1} + c_1 c_{n-2} + \cdots + c_{n-1} c_0.$$

Ha a c_n számot ennek az összefüggésnek az alapján akarjuk kiszámítani, akkor az összes előző számra szükség van.

A rekurziótétel alábbi általánosabb változata lehetővé teszi, hogy egy sorozat egy tagját az összes előző tag függvényeként adjuk meg.

2.3.13. Általános rekurziótétel. Legyen adott egy X halmaz és egy X -be képező f függvény, amelynek értelmezési tartománya az X -beli (nullától indexelt) véges sorozatok halmaza. (Az f adja a rekurziót.) Ekkor egyértelműen létezik egy $g: \mathbb{N} \rightarrow X$ függvény, amely „ f -zárt”, azaz $g(n) = g_n = f(g_0, g_1, \dots, g_{n-1})$ minden $n \in \mathbb{N}$ -re.

A tétel szemléletesen fogalmazva azt mondja, hogy ha adott egy függvényünk, amely egy sorozat esetén kiszámítja a sorozat már megadott részéből, hogy a következő helyre mit kell írunk, akkor ennek segítségével a sorozatot akármeddig folytathatjuk.

A tétel és a bizonyítás érvényes marad akkor is, ha $\mathbb{N}$ helyett tetszőleges N jólrendezett halmaz szerepel. Ezt az általánosabb változatot szokás *transzfinit rekurziótételnek* nevezni. Ekkor f értelmezési tartománya az összes, N valamely kezdőszeletéből X -be képező függvény halmaza, és azt állítjuk, hogy egyértelműen létezik egy $g: N \rightarrow X$ függvény, amely „ f -zárt”, azaz $g(n) = f(g|_{\leftarrow, n}]$ minden $n \in N$ -re. (Itt $\leftarrow, n[$ az $n \in N$ -hez tartozó kezdőszelet.)

* **Bizonyítás.** Az egyértelműség bizonyítása $\mathbb{N}$ jólrendettségén múlik. (Az ilyen bizonyításokat *teljes indukcióval* való bizonyításnak, tetszőleges jólrendezett halmazon *transzfinit indukcióval* történő bizonyításnak nevezzük.) Tegyük fel, hogy g és g^* is eleget tesz a tétel feltételeinek. Legyen $S = \{x \in \mathbb{N}: g(x) \neq g^*(x)\}$. Ha S nem üres, akkor létezik legkisebb eleme, legyen ez n . Mivel g és g^* megegyeznek az $\leftarrow, n[$ intervallumon, azt kapjuk, hogy

$$g(n) = f(g|_{\leftarrow, n}] = f(g^*|_{\leftarrow, n}] = g^*(n),$$

ami ellentmond annak, hogy $n \in S$.

A g létezésének bizonyítása hasonlít a rekurziótétel megfelelő részének bizonyítására. Nevezzük $\mathbb{N} \times X$ egy A részhalmazát f -zártnak, ha minden $n \in \mathbb{N}$ -re és minden

$$h:]\leftarrow, n[\rightarrow X$$

függvényre, amelyre $h \subset A$, az is teljesül, hogy $(n, f(h)) \in A$. Maga $\mathbb{N} \times X$ egy f -zárt halmaz, ilyen halmaz tehát létezik. Legyen g az összes f -zárt halmaz metszete. Mivel nyilván g is f -zárt, csak azt kell megmutatnunk, hogy g az egész $\mathbb{N}$ -en értelmezett függvény. Más szóval, azt fogjuk bizonyítani, hogy ha $k \in \mathbb{N}$, akkor van olyan $x \in X$, hogy $(k, x) \in g$, továbbá ha $(k, y) \in g$, akkor $x = y$. A bizonyítás megint indirekt, transzfinit indukcióval történik. Legyen S azon $\mathbb{N}$ -beli k elemek halmaza, amelyekre ez nem igaz. Legyen n az S legkisebb eleme. Ekkor $g|_{]\leftarrow, n[}$ egy $]\leftarrow, n[$ -en értelmezett függvény, és mivel a g halmaz f -zárt, ha $x = f(g|_{]\leftarrow, n[})$, akkor $(n, x) \in g$. Mivel $n \in S$, ez csak úgy lehet, hogy van olyan $y \in X$, hogy $(n, y) \in g$ és $y \neq x$. Megmutatjuk, hogy $g \setminus \{(n, y)\}$ is f -zárt. Ez azt jelenti, hogy $m \in \mathbb{N}$ és $h:]\leftarrow, m[\rightarrow X$, $h \subset g \setminus \{(n, y)\}$ esetén $(m, f(h)) \in g \setminus \{(n, y)\}$. Ez nyilvánvaló akkor is, ha $m = n$, és akkor is, ha $m \neq n$. Viszont ez ellentmond annak, hogy g a legszűkebb f -zárt halmaz. $\square$

2.3.14. Példa: Fibonacci-számok. Példaként megmutatjuk, hogyan definiálhatók a Fibonacci-számok az előző tétel segítségével pontosan. Legyen $X = \mathbb{N}$. Először az $f(\emptyset) = 0$, $f(\{(0, k)\}) = 1$ bármely $k \in \mathbb{N}$ -re definíciókkal előírjuk, hogy az előző tétel szerint adódó g -re $g(0) = 0$ és $g(1) = 1$ legyen. Most ha $n > 1$, $h:]\leftarrow, n[\rightarrow \mathbb{N}$ egy függvény, akkor legyen $f(h) = h(n^-) + h(n^{--})$. (Vegyük észre, hogy $n = \min(\mathbb{N} \setminus \text{dmn}(h))$, így a h meghatározza n -et.) Ezzel előírtuk, hogy g -re $g(n^{++}) = g(n^+) + g(n)$ teljesüljön minden $n \in \mathbb{N}$ -re. Így g a Fibonacci-számok sorozata lesz. Az első néhány Fibonacci-szám:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
F_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610

2.3.15. Szorzatok és összegek. Legyen G egy (multiplikatív) félcsoporth, $x: \mathbb{N}^+ \rightarrow G$ egy sorozat. Az általános rekurziótételt alkalmazva definiálhatjuk a $\prod_{k=1}^n x_k$, $n \in \mathbb{N}^+$ szorzatokat úgy, hogy $\prod_{k=1}^1 x_k = x_1$ és $\prod_{k=1}^{n+1} x_k = \left(\prod_{k=1}^n x_k\right) \cdot x_{n+1}$, azaz az általános esetben a szorzat az előző részletszorzat és a sorozat aktuális tagjának szorzata. Ha G egységelemes félcsoporth e egységelemmel, akkor érdemes úgy megállapodni, hogy $\prod_{k=1}^0 x_k = e$. Ha $x_k = g$ minden k -ra, akkor $\prod_{k=1}^n x_k$ helyett g^n -et írunk, és a g elem n -edik hatványáról beszélünk, g az *alap*, n a *kitevő*. Ha G egységelemes, akkor $g^0 = e$ is definiálva van. Vegyük észre, hogy a hatványozás általában nem művelet, mert az alap és a kitevő nem ugyanannak a halmaznak az elemei. A szorzatok tulajdonságait indukcióval bizonyíthatjuk, ezt nem részletezzük. A szorzatok tulajdonságaiból következik, vagy indukcióval közvetlenül is bizonyítható, hogy $g^{m+n} = g^m \cdot g^n$ és $(g^m)^n = g^{mn}$ minden $m, n \in \mathbb{N}^+$ -ra (ha G egységelemes félcsoporth, akkor minden $m, n \in \mathbb{N}$ -re). Gyakran $\prod_{k=1}^n x_k$ helyett azt írjuk, hogy $x_1 \cdot x_2 \cdots x_n$; ez a felírás már felhasználja azt az állítást, hogy az asszociativitás miatt a szorzat bármely zárójelzése esetén az eredmény ugyanaz. (Ez az *általános asszociativitás tétele*; indukcióval könnyen belátható.) Ha g, h a G félcsoporth felcserélhető elemei,

akkor indukcióval $(gh)^n = g^n h^n$ minden $n \in \mathbb{N}^+$ -ra (ha G egységelemes félsoport, akkor minden $n \in \mathbb{N}$ -re).

Ha G kommutatív, akkor additív írásmódot is használhatunk, ilyenkor szorzat helyett $\sum_{k=1}^n x_k$ összeget írunk. Ha G kommutatív félsoport a 0 nullelemmel, akkor érdemes úgy megállapodni, hogy $\sum_{k=1}^0 x_k = 0$. Ha $x_k = g$ minden n -re, akkor $\sum_{k=1}^n x_k$ helyett ng -t írunk, n az *együttható*. (Természetesen itt is az együtthatóval való szorzás általában nem művelet, mert az együttható általában nem eleme G -nek.) Gyakran $\sum_{k=1}^n x_k$ helyett azt írjuk, hogy $x_1 + x_2 + \cdots + x_n$. Ha $x: A \rightarrow G$ egy tetszőleges függvény, és van olyan $\varphi: \{k \in \mathbb{N}: 1 \leq k \leq n\} \rightarrow A$ kölcsönösen egyértelmű leképezés, amely A -ra képez, akkor a kommutativitást és asszociativitást felhasználva indukcióval belátható, hogy minden ilyen leképezésre $\sum_{k=1}^n x_{\varphi(k)}$ ugyanaz. (Ez az *általános kommutativitás tétele*.) Ezt a közös értéket $\sum_{a \in A} x_a$ -val is jelöljük.

→° **2.3.16. Feladat [5].** Az alábbi, általános rekurzióval megadott sorozatokat hozzuk zárt alakra:

$$(1) \quad a_0 = -1, a_1 = 2, a_n = (a_{n-1} + a_{n-2})/2;$$

$$(2) \quad a_0 = 1, a_1 = 3, a_n = \sqrt[n]{a_1 a_2 \cdots a_n}.$$

° **2.3.17. Feladat [9].** Az alábbi sorozatokat adjuk meg általános rekurzióval:

$$(1) \quad a_n \text{ az } n\text{-edik prímszám};$$

$$(2) \quad a_n \text{ a } \sqrt{2} \text{ tizedes kifejtésének } n\text{-edik jegye}.$$

→° **2.3.18. Feladat [7].** Bizonyítsuk be, hogy az n -edik Fibonacci-számmra

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2} \right)^n.$$

° **2.3.19. Feladat [2].** Határozzuk meg az F_{1000} Fibonacci-szám közelítő értékét.

° **2.3.20. Feladat [4].** Mennyi $\cos 36^\circ$? Szerkesszünk szabályos ötszöget.

° **2.3.21. Feladat [5].** Fejezzük ki az alábbi, rekurzióval adott sorozatokat a Fibonacci-számok segítségével, $(r, s, c \in \mathbb{R}$ tetszőleges):

$$(1) \quad a_0 = r, a_1 = s, a_{n+2} = a_{n+1} + a_n, \text{ ha } n \in \mathbb{N};$$

$$(2) \quad b_0 = r, b_1 = s, b_{n+2} = b_{n+1} + b_n + c, \text{ ha } n \in \mathbb{N}.$$

2.3.22. Feladat [5]. Jelölje F_n az n -edik Fibonacci-számot. Bizonyítsuk be az alábbi azonosságokat:

$$(1) \quad F_{n+1} F_{n-1} - F_n^2 = (-1)^n, \text{ ha } n \in \mathbb{N}^+;$$

$$(2) \quad F_0^2 + F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1}, \text{ ha } n \in \mathbb{N}.$$

° **2.3.23. Feladat [7].** Jelölje F_n az n -edik Fibonacci-számot. Fejezzük ki egyszerűbb alakban az alábbi összegeket:

$$(1) \quad F_0 + F_2 + F_4 + \cdots + F_{2n};$$

$$(2) \quad F_1 + F_3 + F_5 + \cdots + F_{2n+1};$$

$$(3) \quad F_0 + F_3 + F_6 + \cdots + F_{3n};$$

$$(4) \quad F_1 F_2 + F_2 F_3 + F_3 F_4 + \cdots + F_{2n-1} F_{2n}.$$

◦ **2.3.24. Feladat** [6]. Jelölje F_n az n -edik Fibonacci-számot. Bizonyítsuk be az alábbi azonosságokat:

- (1) $F_m F_{n-1} + F_{m-1} F_n = F_{n+m}$, ha $n \in \mathbb{N}$, $m \in \mathbb{N}^+$;
- (2) $F_{n+k} F_{m-k} - F_n F_m = (-1)^n F_{m-n-k} F_k$, ha $k, m, n \in \mathbb{N}$, $m \geq n+k$.

◦ **2.3.25. Feladat** [2]. Keressük meg az összes olyan F_n Fibonacci-számot, amelyre $F_n = n$, illetve $F_n = n^2$.

◦ **2.3.26. Feladat** [9]. Jelölje F_n az n -edik Fibonacci-számot. Fejezzük ki a Fibonacci-számok segítségével az alábbi összegeket:

- (1)
$$\sum_{k=0}^n \binom{n-k}{k}, \quad k, n \in \mathbb{N};$$
- (2)
$$\sum_{k=0}^n F_k;$$
- (3)
$$\sum_{k=0}^n \binom{n}{k} F_{m+k}, \quad k, m, n \in \mathbb{N};$$
- (4)
$$\sum_{k=0}^n \binom{n}{k} F_{r+1}^k F_r^{n-k} F_{m+k}, \quad k, m, n, r \in \mathbb{N}.$$

→◦ **2.3.27. Feladat** [5]. Legyen $p(x) = x^k - c_1 x^{k-1} - c_2 x^{k-2} - \dots - c_k$, tegyük fel, hogy $\lambda_1, \dots, \lambda_m$ gyökei a p polinomnak, $\alpha_1, \dots, \alpha_m$ pedig tetszőleges számok. Mutassuk meg, hogy az $a_n = \alpha_1 \lambda_1^n + \dots + \alpha_m \lambda_m^n$ sorozat eleget tesz az $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_{n-k}$ rekurzióknak minden $n \geq k$ -ra.

→◦ **2.3.28. Feladat** [5]. Adjunk zárt formulát az alábbi, általános rekurzióval definiált sorozatok n -edik tagjára:

- (1) $a_0 = 0$, $a_1 = 1$, $a_n = a_{n-1} + a_{n-2}$, ha $n > 1$;
- (2) $a_0 = 0$, $a_1 = 1$, $a_n = a_{n-1} + 2a_{n-2}$, ha $n > 1$;
- (3) $a_0 = 0$, $a_1 = 1$, $a_n = 2a_{n-1} + a_{n-2}$, ha $n > 1$;
- (4) $a_1 = 1$, $a_2 = 3$, $a_n = 4a_{n-1} - 3a_{n-2}$, ha $n > 2$.

◦* **2.3.29. Feladat** [6]. Legyen $p(x) = x^k - c_1 x^{k-1} - c_2 x^{k-2} - \dots - c_k$, tegyük fel, hogy λ a p polinomnak kétszeres gyöke, azaz p felírható $p(x) = (x - \lambda)^2 q(x)$ alakban valamely q polinommal. Mutassuk meg, hogy az $a_n = n\lambda^n$ sorozat eleget tesz az $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_{n-k}$ rekurzióknak minden $n \geq k$ -ra.

◦ **2.3.30. Feladat** [5]. Adjunk zárt formulát az $a_0 = 0$, $a_1 = 0$, $a_2 = 1$, és $a_n = a_{n-1} + a_{n-2} + a_{n-3}$, ha $n \geq 3$ általános rekurzióval definiált sorozat n -edik tagjára.

◦ **2.3.31. Feladat** [5]. Adjunk zárt formulát az $u_1 = a$, $u_2 = b$, és $u_n = 2u_{n-1} - u_{n-2}$, ha $n > 2$ általános rekurzióval definiált sorozat n -edik tagjára.

◦ **2.3.32. Feladat [5].** Adjunk zárt formulát az $u_1 = a$, $u_2 = b$, és

$$u_n = -(2u_{n-1} + u_{n-2}), \quad \text{ha } n > 2$$

általános rekurzióval definiált sorozat n -edik tagjára. Külön vizsgáljuk meg az $a = 1$, $b = -1$ és $a = 1$, $b = -2$ speciális eseteket.

◦ **2.3.33. Feladat [5].** Adjunk zárt formulát az $u_1 = a$, $u_2 = b$, és $u_n = 2u_{n-1} + 3u_{n-2}$, ha $n > 2$ általános rekurzióval definiált sorozat n -edik tagjára.

2.3.34. Feladat: Catalan-számok [11]. Egy kártyacsomag kezdetben n különböző lapot tartalmaz. Minden időpontban két dolog között választhatunk: vagy leveszünk a csomag tetejéről egy lapot (ha még van), és egy „veremre” tesszük, vagy a verem tetején levő lapot kiadjuk (ha a verem nem üres). Mutassuk meg, hogy a lehetséges lépéssorozatok száma c_n , az n -edik Catalan-szám.

◦* **2.3.35. Feladat: Catalan-számok [12].** Az előző feladat jelöléseivel bizonyítsuk be, hogy

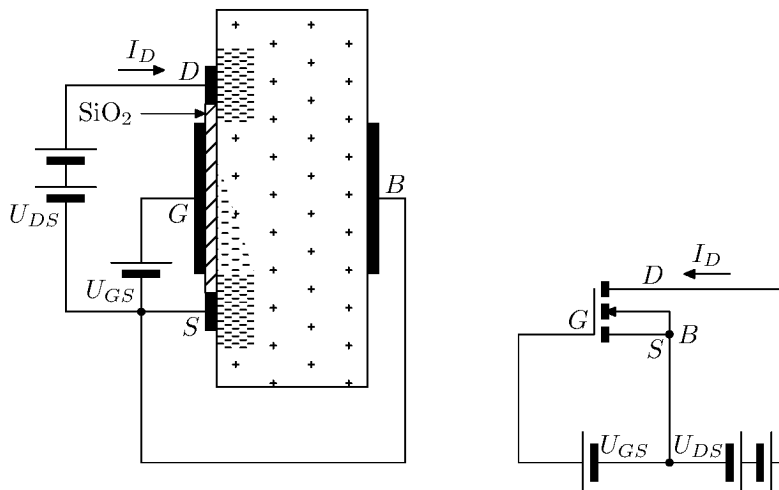
$$c_n = \frac{1}{n+1} \binom{2n}{n}.$$

2.3.36. Logikai függvények. *Logikai függvény* (vagy *Boole-függvény*) alatt az $\{\uparrow, \downarrow\}^n$ halmazt az $\{\uparrow, \downarrow\}^m$ halmazba leképező függvényt értünk, ahol $m, n \in \mathbb{N}$. A számítógép központi egysége, de a központi tár is lényegében logikai függvényeket megvalósító áramkörökből és (órjelvezérelt) tárolókból áll. A logikai jeleknek megfelelő logikai műveletek közül néhányat (hogyan melyeket, az a használt technológiától függ, manapság például a „nem”, angol rövidítése NOT, és az „összeférhetetlen vagy”, angol rövidítése NAND) közvetlenül meg tudunk valósítani hardver alapelemként, a többi logikai függvényt ezek segítségével kell megvalósítani.

Tekintsünk $X_1, X_2, \dots, X_n$ nullváltozós predikátumokat, amelyeknél az egyszerűség kedvéért nem írtuk ki a predikátum jele után az üres zárójelet. Minden, ezen predikátumokkal felírt formula, amely nem tartalmaz kvantort (ez itt most természetes feltevés, hiszen nincsenek változók), egy $\{\uparrow, \downarrow\}^n$ -et $\{\uparrow, \downarrow\}$ -ba képező logikai függvényt ad meg: minden $X_1, X_2, \dots, X_n$ helyére az $\uparrow$ illetve $\downarrow$ jelek valamelyikét helyettesítve, majd a logikai jeleknek megfelelő logikai műveleteket elvégezve, $\uparrow$ vagy $\downarrow$ értéket kapunk. Például az $(X_1, X_2, X_3) \mapsto \neg(X_1 \wedge X_2) \vee X_3$ logikai függvény értéke $X_1 = X_2 = X_3 = \downarrow$ esetén $\uparrow$, míg $X_1 = X_2 = \uparrow$, $X_3 = \downarrow$ esetén $\downarrow$.

A következő tétel azt mutatja, hogy az $m = 1$ esetben minden logikai függvényt megkaphatunk így, már a $\neg$, $\wedge$ és $\vee$ felhasználásával is. Az $m > 1$ esetben a koordinátafüggvényeket állíthatjuk elő így. Természetesen a hardvertervezők egyrészt arra törekednek, hogy a szükséges logikai függvényeket minél kevesebb hardver logikai alapelem segítségével valósítsák meg, mert annál kisebb lesz az áramkör, másrészt, hogy minél kevesebb hardver logikai alapelem kapcsolódjon egymás után, mert annál kisebb lesz a késleltetés, így annál gyorsabb lesz az áramkör működése.

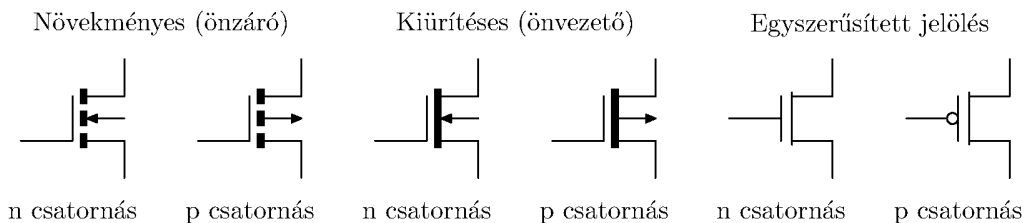
A mai számítógépekben a *kapcsolóelemek* rendszerint *térvezérlésű tranzisztorok*, *FET*-ek (*field effect transistor*), amelyek számunkra elektromos térrel vezérelt kapcsolónak tekinthetők. A 2.3.1 ábrán egy ilyen eszköz szerkezetét és működését, valamint a kapcsolási rajzokon használt jelét mutatjuk be. Az elektródák jól vezető anyagból,



2.3.1 ábra: MOSFET működése és rajzjele.

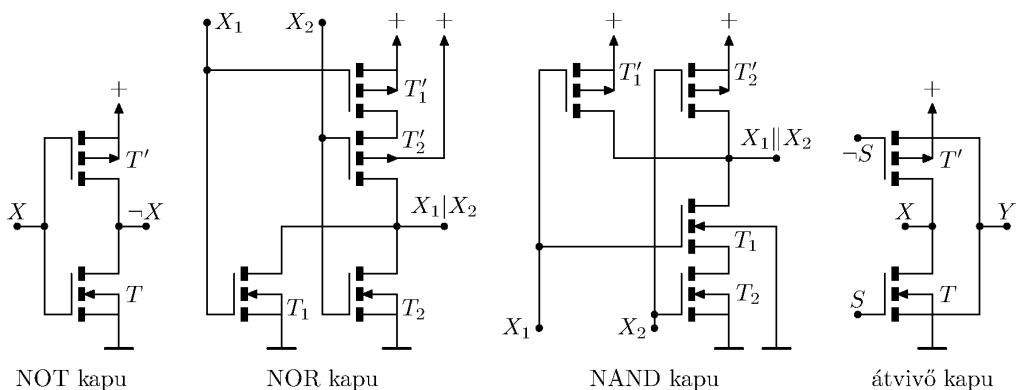
rendszerint fémből készülnek (az ábrán fekete). A *p* típusú félvezető szilícium alaplemezen (amelyben tehát a vezetést a kristályrács elektronhiányos helyei, a pozitív töltésű „lyukak” biztosítják) diffúzióval az S *forrás* (*source*) és D *nyelő* (*drain*) elektródák alatt olyan szigeteket hoznak létre, amelyekben sok vezetésre képes elektron van. Az alaplemezről szigetelő réteggel elválasztott G *kapu* (*gate*) elektródára pozitív U_{GS} feszültséget adva S-hez képest, az elektronok egy része beáramlik a szigetelő réteg alá, létrehozva az n típusú, elektronokat tartalmazó *csatornát*. Növelve a feszültséget, a csatorna végül eléri a D elektróda alatti szigetig, és ekkor a D-re adott, S-hez képes pozitív U_{DS} feszültség hatására I_G áram indul meg, az eszköz vezet. Csökkentve az U_{GS} feszültséget, az eszköz lezár. (Az alaplemez kivezetését, a B *bázis* (*base*) elektródát általában az S elektródához kötik.) Az eszközt *szigetelt kapus* FET-nek, *IGFET*-nek (*insulated gate FET*), vagy — mivel legtöbbször a kapu fém, a szigetelő pedig szilícium-dioxid — *MOSFET*-nek (*MOS: metall-oxid-semiconductor*) nevezzük. A rajzon szereplő változat $U_{GS} = 0$ esetén zárva van, ezért *önzáró*nak vagy *növekményes*nek illetve *dúsításos*nak (*enhancement*) nevezzük. (A bázis a kapcsolásban a forráshoz van kötve.) Készíthető olyan változat is, amelyben a gyártás során a szigetelő réteg alatt eleve létrehozunk egy n típusú csatornát, amely csak negatív U_{GS} feszültség hatására ürül ki, és zár le az eszköz, ezt *önvezető*nek vagy *kiürítési*nek (*depletion*) nevezzük. Végül mindkét típus elkészíthető n típusú alaplemezen p típusú szigetekkel és csatornával is; ezt röviden *p csatornás MOSFET*-nek fogjuk nevezni (míg az előzőleg tárgyalt eszközt *n csatornás MOSFET*-nek); ennek működtetéséhez a telepfeszültségeket meg kell fordítani, és az áramirány is megfordul. A felsorolt típusok rajzjelét a 2.3.2 ábrán láthatjuk. Az egyszerűsített jelölés önzáró típus jelent.

A 2.3.3 ábra a legegyszerűbb, de gyakran használt *statikus CMOS* (*CMOS: complementer MOS*) kapuk kapcsolási rajzát mutatja. A bal oldali, komplementálást végző *nem kapu* (*NOT kapu, inverter*) működése a következő: Ha a bemenet alacsony feszültségen van, a *T* tranzisztor, amely n csatornás önzáró MOSFET, zárva van, a komplementer *T'* tranzisztor, amely p csatornás önzáró MOSFET, viszont kinyit, mert a kapuelektrodája

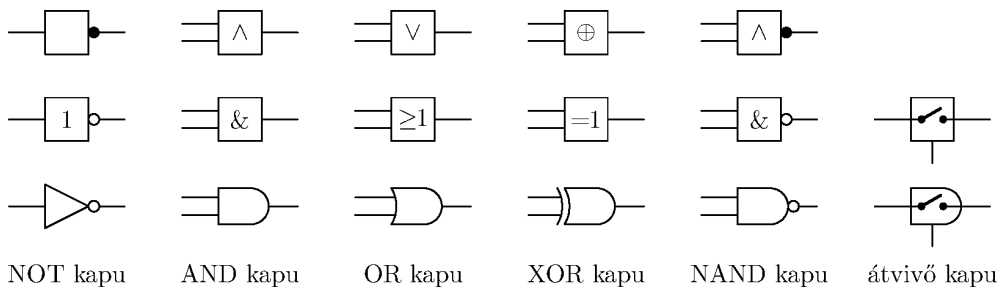


2.3.2 ábra: MOSFET típusok rajzjele.

a pozitív tápfeszültséghez kötött S elektródához képest negatív feszültségen van. Így a kimenet össze van kötve a tápfeszültséggel, de nincs összekötve a földdel, tehát nagy feszültségű. Ha a bemenet nagy feszültségen van, a helyzet megfordul: T kinyit, T' lezár, és a kimenet alacsony feszültségű lesz.



2.3.3 ábra: statikus CMOS kapuáramkörök.

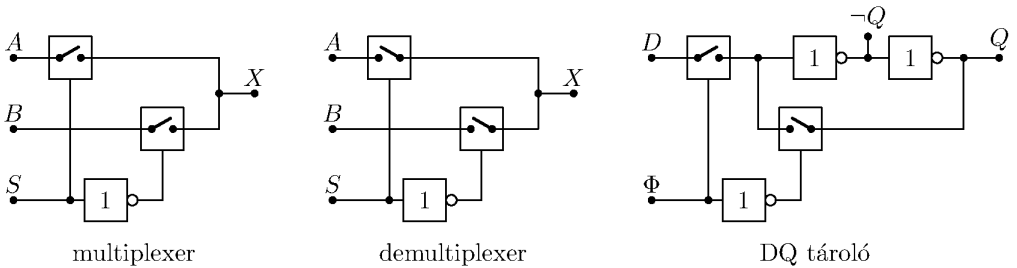


2.3.4 ábra: logikai kapuk rajzjele.

Hasonlóan működik a mellette látható *sem-sem kapu* (*not or*, *NOR*): ha valamelyik bemenet magas feszültségen van, akkor a neki megfelelő T tranzisztor kinyit, T' tranzisztor pedig lezár, így a kimenet alacsony feszültségű lesz, egyébként pedig magas

feszültségű. A következő *összeférhetetlen vagy* (*not and*, *NAND*) kapunál, ha mindkét bemenet magas feszültségen van, a T_1 és T_2 tranzisztorok kinyitnak, a T'_1 és T'_2 tranzisztorok pedig lezárnak, így a kimenet alacsony feszültségre kerül, minden más esetben pedig magas feszültségre. Mindkét kapufajta három, négy, sőt több bemenettel is készülhet (több bemenet növeli a szükséges tápfeszültséget). A számítógépekben használnak még *átvivő kapukat*, ilyen látható a jobb oldalon; ez feszültségvezérelt kapcsolónak tekinthető.

Figyeljük meg, hogy az első három kapunál akármilyen bemenetnél a kimenet vagy a földdel, vagy a tápfeszültséggel van csak összekötve, így állandósult állapotban áram gyakorlatilag nem folyik, csak kapcsoláskor. A negyedik, az átvivő kapunál az S vezérlő bemenet szintjétől függően kerül az X bemenet szintje az Y kimenetre; ha S szintje alacsony, mindkét tranzisztor le van zárva, és a kimenet nem kap áramot, „*lebeg*”. A CMOS áramkörtípusnak a fő előnye: kis sebességnél igen keveset fogyaszt. Hátránya, hogy a kapcsolási idők nem elég kicsik. Nagy sebességű áramköröknél bonyolultabb kapcsolásokat használnak. A kapuk rajzjelei a 2.3.4 ábrán láthatók.



2.3.5 ábra: multiplexer, demultiplexer, DQ-tároló.

Az átvivő kapu főleg a RAM memóriákban használatos, de a processzoroknak is fontos alkatrésze. A 2.3.5 ábrán bal oldalon egy úgynevezett *multiplexer* látható. Az egyik kapcsolót az S bemenet közvetlenül, a másikat egy *inverteren* (NOT kapun) keresztül vezérli. Ha az S bemenet 1, azaz magas feszültségű, akkor az A , egyébként a B kerül az X kimenetre. A középen látható *demultiplexer* ennek a kapcsolásnak a megfordítása: X a bemenet, szintje S -től függően A -ra vagy B -re kerül. A jobb oldalt látható *DQ-tároló* működése a következő: Ha Φ 1, akkor beírás történik: a felső kapcsoló kinyit, az alsó lezár, és a két inverteren keresztül a D bemenet szintje megjelenik Q -n (a komplementere pedig a másik kimeneten). Ha most Φ 0-ra vált, a felső kapcsoló lezár, az alsó kinyit, és Q (valamint a másik kimenet is) tartja a beírt értéket.

2.3.37. Logikai függvények normálalakja. Az előző pont jelöléseivel, minden

$$f: \{\uparrow, \downarrow\}^n \rightarrow \{\uparrow, \downarrow\}$$

logikai függvény felírható

$$f(X_1, X_2, \dots, X_n) = \mathcal{A}_1 \vee \mathcal{A}_2 \vee \dots \vee \mathcal{A}_m$$

alakban, ahol $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_m$ különböző logikai formulák, de mindegyik

$$\mathcal{B}_1 \wedge \mathcal{B}_2 \wedge \dots \wedge \mathcal{B}_{n_k}$$

alakú, ahol $\mathcal{B}_j$ vagy X_{i_j} , vagy $\neg X_{i_j}$ és $1 \leq i_1 < i_2 < \dots < i_{n_k} \leq n$.

Emlékeztetünk rá, hogy $\wedge$ illetve $\vee$ asszociatív logikai műveletek a $\{\uparrow, \downarrow\}$ halmazon, így ha nulla tényezőre hajtjuk végre őket, akkor az eredmény az egységelemük, $\uparrow$ illetve $\downarrow$ lesz.

Bizonyítás. Direkt módon konstruáljuk meg a normálalakot: ha valamilyen

$$(x_1, x_2, \dots, x_n) \in \{\uparrow, \downarrow\}^n$$

sorozatra f igaz értéket vesz fel, akkor képezzünk egy $\mathcal{A}$ tagot, amelyben $\mathcal{B}_j = X_j$, ha a sorozatban x_j igaz, és $\mathcal{B}_j = \neg X_j$, ha a sorozatban x_j hamis. Az összes így adódó (legfeljebb 2^n) tagot kapcsoljuk össze diszjunkcióval. $\square$

2.3.38. Normálalakok. Az előző tétel bizonyításában adódó *normálalakot teljes diszjunktív normál alaknak* nevezzük, mert benne $n_k = n$ minden k -ra. Egyes $\mathcal{A}$ logikai részformulák összevonásával, vagy bármilyen más módon kapható, a tétel állításában szereplő alakot *diszjunktív normál alaknak* nevezünk. (Részletesebben lásd Knuth [46], Vol. 4., Fas. 0.) Ha az $(x_1, x_2, \dots, x_n) \mapsto \neg f(x_1, x_2, \dots, x_n)$ logikai függvényt állítjuk elő diszjunktív normál alakban, majd mindkét oldalt negáljuk, akkor az f logikai függvény

$$f(X_1, X_2, \dots, X_n) = \mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \dots \wedge \mathcal{A}_m$$

alakban való felírását kapjuk, ahol $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_m$ különböző logikai formulák, de mindegyik

$$\mathcal{B}_1 \vee \mathcal{B}_2 \vee \dots \vee \mathcal{B}_{n_k}$$

alakú, ahol $\mathcal{B}_j$ vagy X_{i_j} , vagy $\neg X_{i_j}$ és $1 \leq i_1 < i_2 < \dots < i_{n_k} \leq n$. Ezt az alakot *konjunktív normál alaknak* nevezzük, ha pedig $n_k = n$ minden k -ra, akkor *teljes konjunktív normál alaknak*.

Megjegyezzük, hogy készülnek olyan integrált áramkörök, úgynevezett *programozható logikai síkok* (angolul *programmable logical array*, PLA), amelyek programozhatók bármely logikai függvény megvalósítására, ha annak koordinátafüggvényei normálalakban adóttak.

2.3.39. A maradékos osztás tétele. Legyen $n > 0$ rögzített természetes szám. Minden m természetes szám egyértelműen felírható $m = qn + r$ alakban, ahol $q, r \in \mathbb{N}$ és $r < n$.

Bizonyítás. Mivel $kn \geq k$, van olyan k , amelyre $kn > m$, például $k = m^+$. Legyen k a legkisebb természetes szám, amelyre $kn > m$. Nyilván $k \neq 0$, így $k = q^+$ valamely $q \in \mathbb{N}$ -re. Mivel $qn \leq m$, van olyan r természetes szám, amelyre $m = qn + r$. Ha $r \geq n$ lenne, akkor $m \geq qn + n = (q+1)n > m$ adódna. Az egyértelműség bizonyításához tegyük fel, hogy $m = q'n + r'$, ahol $r' < n$. Ha például $q' > q$, akkor $m = q'n + r' \geq q'n \geq (q+1)n > qn + r = m$, ellentmondás, és hasonlóan $q' < q$ is ellentmondásra vezet. Így $q = q'$, amiből már az egyszerűsítési szabály alapján $r = r'$ következik. $\square$

2.3.40. Hányados és maradék. Az előző tétel szerint egyértelműen létező q számot *hányadosnak*, r számot pedig *maradéknak* nevezzük az m szám n -nel való maradékos osztásánál. Ha az m természetes szám 2-vel való maradékos osztásánál a maradék 0, akkor m -et *párosnak*, egyébként *páratlannak* nevezzük. A páros és páratlan számok összegére és szorzatára vonatkozó ismert szabályok (páros és páratlan összege páratlan egyébként az összeg páros; páratlanszor páratlan páratlan, egyébként a szorzat páros) azonnal következnek a maradékos osztás egyértelműségéből.

2.3.41. Tétel: számrendszerek. Legyen $q > 1$ természetes szám. Minden $m > 0$ természetes számhoz egy és csak egy olyan n természetes szám és

$$a_0, a_1, \dots, a_n \in [0, q[\subset \mathbb{N}$$

sorozat létezik, amelyre $a_n \neq 0$ és $m = \sum_{i=0}^n a_i \cdot q^i$.

A valós számok helyiértékes előállításáról analízisből tanulunk. A kettes, hármas, négyes, ötös, stb. alapú számrendszer latin szóval bináris, ternáris, kvaternáris, kvináris, stb.

Bizonyítás. Úgynevezett teljes indukcióval bizonyítunk: feltesszük, hogy $0 < m' < m$ esetén igaz az állítás, és bebizonyítjuk, hogy m -re is. Ebből következik, hogy az állítás minden pozitív természetes számra teljesül. (Az ilyen típusú bizonyításokat fogjuk *teljes indukció*val való bizonyításoknak nevezni; ezek a természetes számok jólrendezettségén múlnak. Ha ugyanis lenne olyan pozitív természetes szám, amelyre az állítás nem teljesül, az ilyenek között lenne legkisebb. Ezt választva m -nek ellentmondást kapnánk. Arra is gondolnunk kell, hogy az m lehet az egész halmaz első eleme, ekkor a nála kisebb elemek halmaza üres.) Osszuk maradékosan m -et q -val, azaz írjuk fel $m = m'q + r$ alakban, ahol $m', r \in \mathbb{N}$ és $r < q$. Ha $m' = 0$, akkor $n = 0$, $a_0 = r$ választással készen is vagyunk (az egyértelműség a maradékos osztás egyértelműségéből következik). Ha $m' \neq 0$, akkor $m' < m$, és az indukciós feltevés szerint egyértelműen felírható $m' = a_1 + a_2q + \dots + a_{n+1}q^n$ alakban. A maradékos osztás egyértelműségéből következik a_0 egyértelműsége, és teljes indukcióval az állítás. $\square$

2.3.42. Természetes számok számítógépes ábrázolása. A mai számítógépek mindegyike alapvetően *kettes számrendszerben* dolgozik: a *bináris jegy*, a *binary digit* angol kifejezésből *bit* 0 vagy 1 lehet. A természetes számokat (*előjel nélküli*, angolul *unsigned* számokat) a számítógép kettes számrendszerben ábrázolja. Történeti érdekesség, hogy készítettek *hármas számrendszerben* működő *ternáris* gépet is. (Természetesen, ha rögzített hosszúságú, például 8, 16, 32 vagy 64 bites számábrázolást használunk, az eredmény *túlcsordulhat*, és csak az alacsonyabb helyiértékű bitjeit kapjuk meg.) Számunkra jóval kényelmesebb a biteket kettesével, hármasával vagy négyesével csoportosítva *négyes* (*kvadrális*), *nyolcas* (*oktális*) vagy *tizenhatos* (kicsit hibásan *hexadecimális*: a latin kifejezés szedecimális, a görög hexadekadikus lenne) számrendszert használni. A byteszervezésű gépek (IBM 360-as sorozat) elterjedése óta a memória legkisebb címezhető egysége rendszerint 8 bit, azaz 1 *bájt* (az angol *byte* elnevezést az IBM Stretch gép tervezői vezették be 1956-ban). Mivel egy fél bájt (angolul *nybble*) egy hexadecimális jegynek felel meg, leggyakrabban hexadecimális számrendszert használunk. Néhány üzleti alkalmazás tízes számrendszert kíván: ekkor a számjegyeket ASCII-kódjukkal ábrázoljuk, vagy *binárisan kódolt decimális* (angolul *binary coded decimal*, *BCD*) kódot használunk, melyben a tízes számrendszerbeli egy-egy jegy egy-egy félbájtot foglal el, binárisan kódolva.

* **2.3.43. Hash-transzformáció.** A számrendszerek és a maradékos osztás felhasználható úgynevezett *hash-transzformációra* vagy *kulcs-cím transzformációra*: egy R rekord K kulcsát — például 256 alapú számrendszerben — számnak tekintjük, és egy adott M számmal (amelyet érdemes olyan prímnek választani, amely egyetlen kettőhatványhoz sem esik nagyon közel) maradékosan osztjuk. A kapott $0 \leq h(K) < M$ érték megmondja, hogy egy tömbben hol van az R rekord címe. Persze több R_i rekord K_i kulcsára lehet

$h(K_i)$ ugyanaz: ezeket a rekordokat egy listában helyezük el. Ha a keresés jóval gyakoribb, mint új rekordok bejegyzése, a listákat tarthatjuk rendezetten is. Belső tárbán a listák ne legyenek túl hosszúak: ha hosszuk jóval 1 fölé megy, érdemes új, nagyobb M -et választani, és az összes rekordot „újrahashelni”. Például ha semmit nem tudunk az elhelyezendő rekordok számáról, kezdhetünk $M = 5$ -tel, és ha növelni kell M -et, az előző M kétszerese utáni első prímet választjuk a következő M -nek. A módszer mágneslemezen is használható, itt $h(K)$ egy szektor relatív címét adja, amelyben a rekord van. Ha egy újabb rekord esetleg már nem fér az adott szektorba, rakhatjuk egyszerűen a következő szektorba is.

* **2.3.44. Feladat [13].** Adjunk használható algoritmust tetszőlegesen nagy természetes számok maradékos osztására bináris számítógépen.

→ **2.3.45. Feladat [4].** Adjunk használható algoritmust tetszőlegesen nagy természetes számok decimális ábrázolásról binárisra való konverziójára bináris számítógépen.

→ **2.3.46. Feladat [4].** Adjunk használható algoritmust tetszőlegesen nagy természetes számok bináris ábrázolásról decimálisra való konverziójára bináris számítógépen.

→ **2.3.47. Feladat [4].** Adjunk használható algoritmust BCD ábrázolású, tetszőlegesen nagy természetes számok összeadására, szorzására és maradékos osztására bináris számítógépen.

2.3.48. Feladat [8]. Adjunk gyors algoritmust tetszőlegesen nagy természetes számok decimális ábrázolásról binárisra való konverziójára bináris számítógépen, ha a szorzásra van olyan algoritmusunk, amelynek futásideje „majdnem arányos” a szám hosszával.

2.3.49. Feladat [8]. Adjunk gyors algoritmust tetszőlegesen nagy természetes számok bináris ábrázolásról decimálisra való konverziójára bináris számítógépen, ha a szorzásra és a maradékos osztásra van olyan algoritmusunk (szubrutinként), amelynek futásideje „majdnem arányos” a szám hosszával.

° **2.3.50. Feladat [9].** Jelölje F_n az n -edik Fibonacci-számot. Mutassuk meg, hogy bármely $n \in \mathbb{N}^+$ egyértelműen felírható „a Fibonacci-számrendszerben 0-1-együtthatókkal”, pontosabban $n = F_{k_1} + F_{k_2} + \dots + F_{k_m}$ alakban, ahol $m \in \mathbb{N}^+$ és a $0, k_1, k_2, \dots, k_m$ sorozat szigorúan monoton növekedő és nem tartalmaz egymás melletti számokat.

2.3.51. Feladat [8]. Tervezzünk CMOS áramkört

- (1) két bit összeadására, kimenet az összeg alsó és felső bitje;
- (2) három bit összeadására, kimenet az összeg alsó és felső bitje;
- (3) két bájt összeadására, kimenet az összeg és az *átvitel* (*carry*) bit.

°* **2.3.52. Feladat [9].** Írjunk programot hash-transzformációra és kísérletezzünk vele különböző adattáblákra (például programok változóinak nevei, stb.)

° **2.3.53. Feladat [12].** Teljes indukcióval bizonyítsuk be a számtani és a mértani közép közötti egyenlőtlenséget: ha $x_1, x_2, \dots, x_n$ nemnegatív valós számok, akkor

$$\sqrt[n]{x_1 x_2 \cdots x_n} \leq \frac{x_1 + x_2 + \cdots + x_n}{n},$$

és egyenlőség pontosan akkor áll fenn, ha $x_1 = x_2 = \dots = x_n$.

◦ **2.3.54. Feladat [4].** Igazoljuk, hogy ha $n \in \mathbb{N}^+$ és $x > 1$ valós szám, akkor $\sqrt[n]{x} - 1 < (x - 1)/n$.

◦ **2.3.55. Feladat [6].** Igazoljuk, hogy

$$n! < \left(\frac{n+1}{2}\right)^n,$$

ha $n \in \mathbb{N}^+$.

◦ **2.3.56. Feladat [9].** A számtani és mértani közép közötti egyenlőtlenséget felhasználva bizonyítsuk be, hogy

(1)

$$\left(1 + \frac{1}{n}\right)^n < \left(1 + \frac{1}{n+1}\right)^{n+1},$$

ha $n \in \mathbb{N}^+$;

(2) az előző egyenlőtlenség ekvivalens az $(n+1)^{2n+1} < n^n(n+2)^{n+1}$ egyenlőtlenséggel, és megfordul, ha a bal oldalról egy $n+1$, a jobb oldalról pedig egy $n+2$ tényezőt elhagyunk;

(3)

$$\left(1 - \frac{1}{n}\right)^n > \left(1 - \frac{1}{n+1}\right)^{n+1},$$

ha $n \in \mathbb{N}^+$;

(4)

$$\left(1 + \frac{1}{n}\right)^{n+1} > \left(1 + \frac{1}{n+1}\right)^{n+2},$$

ha $n \in \mathbb{N}^+$.

2.3.57. További feladatok. [36]: 8.9, 8.11–8.15, 12.1, 12.2; [59]: I.1.34, I.1.35, I.1.40, I.1.41; [64]: 4.1.1–4.1.3, 4.2.1–4.2.9, 4.3.1–4.3.16; [69]: 4.5.1–4.1.13; [84]: 1.38–1.44.

A számfogalom bővítése

Ebben a fejezetben a számfogalom bővítésével foglalkozunk. Bevezetjük az egész számokat, a racionális számokat, a valós számokat, a komplex számokat és a kvaterniókat. A definíció általában a programozási nyelvek adattípus-definíciójával analóg.

Megjegyezzük, hogy a számköröket tárgyalhatjuk a valós számokból kiindulva is, a 3.3.15 pontra alapozva. Ekkor a 2. fejezetből csak a félcsoport, csoport és kommutativitás fogalmát bevezető 2.2.7 definíciót és a hozzá tartozó 2.2.9 és 2.2.13 példákat, valamint a gyűrűk fogalmát, tulajdonságait, azaz a 3.1. pontot a gyűrű definíciójától a pont végéig, a 3.2. pontból pedig a test, ferdetest, rendezett test 3.2.3 definícióját tárgyaljuk, majd a 3.3.2, 3.3.3 és 3.3.6 stb., pontok tárgyalásával folytatjuk a 3.3. pont végéig. Ezután térhetünk vissza a kimaradt részek tárgyalásához, de a 2.1.5, 2.1.6, 2.2.1–2.2.4, 2.3.1–2.3.3, 3.1.4–3.1.9, 3.2.1, 3.2.2 pontok kimaradnak, a művelet osztályozással való kompatibilitását és a rá vonatkozó példát (3.1.1, 3.1.2) pedig elég a 6.2. pont elején tárgyalni. Természetesen ez a felépítés jóval egyszerűbb, mégsem javasoljuk, mivel a logika tanítása ekkor nem támaszkodhat egyetlen konkrét axiomatikus tárgyalásra sem, ami nyilvánvalóan helytelen.

3.1 Egész számok

A természetes számok körében az összeadásra nézve csak a nullának van inverze, másként szólva, a kivonás általában nem végezhető el. Ez indokolja az egész számok bevezetését. Az alapgondolat az, hogy „kettős könyvelést” vezetünk, külön egy „követel” és egy „tartozik” oldalt, és alkalmas ekvivalenciát vezetünk be.

3.1.1. Osztályozás kompatibilitása művelettel. Legyen $*$ egy binér művelet X -en, és legyen adott X egy osztályozása, illetve a megfelelő $\sim$ ekvivalencia-reláció. Azt mondjuk, hogy a $*$ művelet kompatibilis az osztályozással, illetve az ekvivalenciarelációval, ha $x \sim x'$ és $y \sim y'$ esetén $x * y \sim x' * y'$. Az ekvivalenciareláció tulajdonságai miatt nyilván elég azt megkövetelni, hogy $x * y \sim x' * y$ és $x * y \sim x * y'$ teljesüljön.

Ha a művelet kompatibilis az osztályozással, akkor az ekvivalenciaosztályok terén, $\tilde{X}$ -on bevezethetünk egy $\tilde{*}$ műveletet az $\tilde{x}\tilde{*}\tilde{y} = \widetilde{x*y}$ definícióval, mert a kompatibilitás miatt az eredmény független a reprezentánsválasztástól. Általában $\tilde{*}$ helyett $*$ -ot írunk. A már definiált $x \mapsto \tilde{x}$ kanonikus leképezés az így definiált műveletre nézve művelettartó.

3.1.2. Példa. A természetes számok halmazán soroljuk egy osztályba azokat a számokat, amelyek kettővel osztva ugyanazt a maradékot adják. A két osztály a páros, illetve páratlan számok osztálya. Az összeadás és a szorzás is kompatibilis az osztályozással.

° 3.1.3. Feladat [4]. Soroljuk egy osztályba $\mathbb{N}^+$ azon elemeit, amelyekre az a legnagyobb $n \in \mathbb{N}^+$ kitevő, amelyre 5^n osztja a számot, ugyanannyi. Mutassuk meg, hogy ez az osztályozás kompatibilis a szorzással. Mi a helyzet, ha 5 helyett 6-ot veszünk?

3.1.4. Osztályozás kompatibilitása relációval. Legyen R egy X -beli binér reláció, és legyen adott X egy osztályozása, illetve a megfelelő $\sim$ ekvivalenciareláció. Azt mondjuk, hogy az R reláció kompatibilis az osztályozással, illetve az ekvivalenciarelációval, ha $x \sim x'$ és $y \sim y'$ esetén xRy -ből következik, hogy $x'Ry'$. Az ekvivalenciareláció tulajdonságai miatt nyilván most is elég azt megkövetelni, hogy xRy -ből következzen, hogy $x'Ry$ és xRy' teljesül.

Ha az R reláció kompatibilis az osztályozással, akkor az ekvivalenciaosztályok tén, $\tilde{X}$ -on bevezethetünk egy $\tilde{R}$ relációt az $\tilde{x}\tilde{R}\tilde{y}$, ha xRy definícióval, mert az R reláció fennállása független a reprezentánsválasztástól. Általában $\tilde{R}$ helyett R -et írunk.

3.1.5. Példa. A természetes számokat soroljuk kételemű osztályokba: minden osztályban egy páros szám és a rákövetkezője van. A rendezés kompatibilis az osztályozással.

3.1.6. Tétel. Tekintsük $\mathbb{N} \times \mathbb{N}$ -en az $(m, n) \sim (m', n')$, ha $m + n' = m' + n$ relációt és az $(m, n) + (m', n') = (m + m', n + n')$ összeadást. A $\sim$ reláció ekvivalenciareláció. Az ekvivalenciosztályok halmazát $\mathbb{Z}$ -vel fogjuk jelölni, és elemeit egész számoknak nevezük. Az összeadás kompatibilis a $\sim$ ekvivalenciarelációval, így az egész számok között értelmezve van az összeadás és $\mathbb{Z}$ az összeadásra nézve Abel-csoport.

Bizonyítás. A $\sim$ reláció nyilván reflexív és szimmetrikus. Ha $(m, n) \sim (m', n')$ és $(m', n') \sim (m'', n'')$, akkor $m + n' = m' + n$ és $m' + n'' = m'' + n'$. Innen $m + n' + m' + n'' = m' + n + m'' + n'$. Felhasználva az összeadás kommutativitását, asszociativitását és a természetes számok összeadásának egyszerűsítési szabályát, azt kapjuk, hogy $m + n'' = m'' + n$, azaz $(m, n) \sim (m'', n'')$, vagyis a reláció tranzitív is. Ezzel beláttuk, hogy ekvivalenciareláció.

Megmutatjuk, hogy a párok összeadása kompatibilis az ekvivalenciarelációval. Mint azt a kompatibilitás definíciójánál megjegyeztük, elég megmutatni, hogy külön-külön az összeg első, illetve második tagját helyettesíthetjük vele ekvivalenssel, az összeg az eredetivel ekvivalens marad. Mivel a párok összeadása kommutatív, ezért elég azt megmutatni, hogy ha $(m, n) \sim (m', n')$, akkor $(m, n) + (m'', n'') \sim (m', n') + (m'', n'')$. Az, hogy $(m, n) \sim (m', n')$, azt jelenti, hogy $m + n' = m' + n$. Ebből $m + m'' + n' + n'' = n + n'' + m' + m''$, ami viszont azt jelenti, hogy

$$(m, n) + (m'', n'') = (m + m'', n + n'') \sim (m' + m'', n' + n'') = (m', n') + (m'', n'').$$

Mivel a párok összeadása kommutatív és asszociatív, az ekvivalenciosztályoké is. A $(0, 0)$ pár osztálya (az (m, m) alakú párok halmaza) nyilván nullelem. Az (m, n) pár osztályának additív inverze nyilván létezik, az (n, m) pár osztálya. Így $\mathbb{Z}$ az összeadással Abel-csoport. $\square$

3.1.7. Tétel: $\mathbb{N}$ beágyazása $\mathbb{Z}$ -be. Az előző tétel jelöléseivel, a $\varphi: n \mapsto \widetilde{(n, 0)}$ leképezésre $\mathbb{N}$ -nek $\mathbb{Z}$ -be $\varphi(n) = n\varphi(1)$ minden $n \in \mathbb{N}$ -re, a leképezés kölcsönösen egyértelmű (injektív) és összeadástartó. Így $\varphi(\mathbb{N})$ -et azonosíthatjuk $\mathbb{N}$ -el. Ezzel az azonosítással $\mathbb{N} \cup (-\mathbb{N}) = \mathbb{Z}$ és $\mathbb{N} \cap (-\mathbb{N}) = \{0\}$, ahol $-\mathbb{N} = \{-n: n \in \mathbb{N}\}$.

Bizonyítás. Mivel megállapodás szerint, ha semmit sem adunk össze, az összeg a nullelem, $0\varphi(1) = \widetilde{(0, 0)} = \varphi(0)$. Az egytagú összeg definíciója szerint $1\varphi(1) = \widetilde{(1, 0)} = \varphi(1)$. Indukcióval

$$n^+\varphi(1) = n\varphi(1) + \varphi(1) = \widetilde{(n, 0)} + \widetilde{(1, 0)} = \widetilde{(n+1, 0)} = \varphi(n^+)$$

minden $n \in \mathbb{N}$ -re. A leképezés nyilván kölcsönösen egyértelmű és összeadástartó, mert $\varphi(m+n) = (m+n)\varphi(1) = m\varphi(1) + n\varphi(1) = \varphi(m) + \varphi(n)$. Az állítás többi része adódik, ha belátjuk, hogy $\mathbb{Z}$ minden eleme, azaz minden ekvivalenciaosztály pontosan egyet tartalmaz a $(k, 0)$ illetve $(0, k)$ alakú elemek közül, ahol $k \in \mathbb{N}$ (általában ezzel az elemmel reprezentáljuk az osztályt). Legyen $m, n \in \mathbb{N}$. Ha $n \geq m$, akkor van olyan $k \in \mathbb{N}$, amelyre $n = m + k$; ekkor $(m, n) \sim (k, 0)$. Hasonlóan, ha $n \leq m$, akkor van olyan $k \in \mathbb{N}$, hogy $n + k = m$; ekkor $(m, n) \sim (0, k)$. Másrészt, ha $(k, 0) \sim (k', 0)$, akkor $k = k'$; ha $(0, k) \sim (0, k')$, akkor is $k = k'$; végül ha $(k, 0) \sim (0, k')$, akkor $k = k' = 0$. $\square$

3.1.8. Az egész számok rendezése. Ha $m, n \in \mathbb{Z}$, akkor legyen $m \leq n$, ha van olyan $k \in \mathbb{N}$, amelyre $m + k = n$. Ez persze ugyanazt jelenti, mint hogy $n - m \in \mathbb{N}$. Ugyanúgy, mint a természetes számoknál, adódik, hogy így egy részbenrendezést kapunk. Az egész számok körében $-\mathbb{N}$ elemeit az jellemzi, hogy kisebb vagy egyenlőek, mint nulla: ha $n \in \mathbb{N}$, akkor $(-n) + n = 0$, így $-n \leq 0$, másrészt ha $m \leq 0$, akkor valamely $n \in \mathbb{N}$ -re $m + n = 0$, azaz $m = -n$. Innen következik, hogy $-\mathbb{N}$ bármely eleme kisebb vagy egyenlő, mint $\mathbb{N}$ bármely eleme. Megmutatjuk, hogy $-\mathbb{N}$ elemei is összehasonlíthatók: mivel $m, n \in \mathbb{N}$, $m \leq n$ esetén $n - m \in \mathbb{N}$, azt kapjuk, hogy $(-n) + (n - m) = -m$, azaz $-n \leq -m$. Ezzel beláttuk, hogy $\mathbb{Z}$ rendezett. Megmutatjuk, hogy ha $k, m, n \in \mathbb{Z}$ és $m \leq n$, akkor $m + k \leq n + k$; valóban, $(n + k) - (m + k) = n - m \in \mathbb{N}$. Ezt a tulajdonságot úgy hívjuk, hogy az *összeadás monoton*.

3.1.9. Az egész számok szorzása. Ha $m, n \in \mathbb{Z}$, akkor az $m, n \in \mathbb{N}$ esetben legyen mn a természetes számokra definiált szorzat, ha $m, -n \in \mathbb{N}$, akkor legyen $mn = nm = -m(-n)$, és ha $-m, -n \in \mathbb{N}$, akkor legyen $mn = (-m)(-n)$. Esetszétválasztással azonnal adódik, hogy a szorzat pontosan akkor lesz nulla, ha valamelyik tényezője nulla, ezzel a szorzással $\mathbb{Z}$ kommutatív félcsoport az 1 egységelemmel, valamint ha $k, m, n \in \mathbb{Z}$, akkor $k \cdot (m+n) = k \cdot m + k \cdot n$, azaz a szorzás *disztributív* az összeadásra nézve. (Rövidesen belátjuk az úgynevezett előjelszabályt, amelyből következik, hogy a szorzást nem is definiálhattuk volna másként, ha azt akarjuk, hogy disztributív legyen az összeadásra nézve.)

3.1.10. Egész számok számítógépes ábrázolása. Egyik mód a számot az abszolút értékével és az előjelével megadni: tetszőleges pontosságú aritmetikánál, például [komputer]algebra rendszer]ekben általában ezt használjuk. Egy másik mód a „*többlletes kód*”: választunk egy $T \in \mathbb{N}^+$ „többltet” és egy $n \in \mathbb{Z}$, $n \geq -T$ szám helyett az $n + T$ természetes számot tároljuk. Ha az ábrázolás m biten történik, akkor a többltet rendszerint $T = 2^{m-1}$ vagy $T = 2^{m-1} - 1$. (Például $m = 11$ esetén a többltet 1024 vagy 1023, és például -3 kódja 1021 illetve 1020.) Ennek megfelelően az ábrázolható számtartomány $-2^{m-1} \leq n < 2^{m-1}$ vagy $-2^{m-1} < n \leq 2^{m-1}$. Ennek a számaábrázolásnak a hátránya, hogy összeadáskor a többltetet az összegből le kell vonni, kivonáskor hozzá kell adni, stb. A sokkal gyakoribb komplementus ábrázolásról lásd a 6.2.4 pontot.

3.1.11. Hatványozás egész kitevővel. Ha G egységelemes félcsoport, $g \in G$ -nek van inverze, akkor az $n \mapsto g^n$ leképezést a $g^n = (g^{-1})^{-n}$, ha $-n \in \mathbb{N}^+$ definícióval kiterjeszthetjük egy $\mathbb{Z}$ -n értelmezett leképezéssé; most is g az *alap*, n pedig a *kitevő*.

Mint esetszétválasztással nem nehéz belátni, erre a leképezésre $g^{m+n} = g^m g^n$ és $(g^m)^n = g^{mn}$ minden $m, n \in \mathbb{Z}$ -re, továbbá ha $g, h \in G$ felcserélhető elemek amelyeknek van inverze, akkor $(gh)^n = g^n h^n$ minden $n \in \mathbb{Z}$ -re.

Persze, ha G csoport, akkor minden elemének van inverze, és így minden elemének minden egész kitevős hatványa értelmezve van.

Ha G Abel-csoport additív írásmóddal, akkor g^n helyett ng -t írunk, és n -et *együtt-hatónak* nevezzük. Figyelem, $(n, g) \mapsto ng$, $g \in G$, $n \in \mathbb{Z}$ most sem művelet, hanem a fenti összefüggéssel van definiálva. A fenti összefüggések ezzel a jelöléssel: $(m+n)g = mg + ng$, $m(ng) = (mn)g$ és $n(g+h) = ng + nh$ minden $m, n \in \mathbb{Z}$, $g, h \in G$ esetén.

° **3.1.12. Példa.** A kétszer kettes valós elemű mátrixok a szorzással egységelemes félcsoporthot alkotnak, amelyben pontosan a nem nulla determinánsú elemeknek van inverze; ezeknek minden egész kitevős hatványa értelmezve van, a többinek csak az $\mathbb{N}$ -beli kitevős hatványai.

3.1.13. Gyűrűk. Egy R halmazt egy $(+, \cdot)$ binér műveletekből álló párral *gyűrűnek* nevezzük, ha az összeadással Abel-csoport (a nullelemet 0 fogja jelölni), a szorzással félcsoporthot, és teljesül mindkét oldali disztributivitás, azaz ha $x, y, z \in R$, akkor

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{és} \quad (y + z) \cdot x = y \cdot x + z \cdot x.$$

Ha a szorzás kommutatív, akkor a gyűrűt *kommutatív gyűrűnek* nevezzük. Ha a szorzásnak van egységeleme, akkor a gyűrűt *egységelemes gyűrűnek* nevezzük.

Tetszőleges gyűrűben $x0 = x(0+0) = x0 + x0$. Mindkét oldalhoz hozzáadva $-x0$ -t, kapjuk, hogy $x0 = 0$. Hasonlóan adódik, hogy $0x = 0$. Érvényes az úgynevezett „előjelszabály” is: $(-x)y = x(-y) = -xy$ és $(-x)(-y) = xy$ minden x, y elemre. Például $xy + (-x)y = (x + (-x))y = 0y = 0$, amiből az inverz egyértelmősége miatt $(-x)y = -xy$; a többi összefüggés hasonlóan adódik. Az is teljesül, hogy $n(xy) = (nx)y = x(ny)$ minden x, y gyűrűbeli elemre és $n \in \mathbb{Z}$ -re. (Figyelem, $(n, x) \mapsto nx$ most sem a gyűrűbeli szorzás, hanem ismételt összeadással van definiálva!) Ha $n \in \mathbb{N}$, ekkor ez az összefüggés indukcióval adódik, felhasználva a disztributivitást; innen az általános esetet az előjelszabály felhasználásával kapjuk.

A legegyszerűbb példa a *nullgyűrű*, amely csak egy elemet tartalmaz, ez nyilván a 0 . Másik triviális példa egy (additív) Abel-csoport, amelyben bármely két elem szorzatát nullának értelmezzük; ezeket a gyűrűket *zérógyűrűnek* nevezzük. Fontosabb példa $\mathbb{Z}$. Ezek a gyűrűk mind kommutatívak, $\mathbb{Z}$ és a nullgyűrű (amelyben $1 = 0$) egységelemesek.

3.1.14. Példa. Bármely X halmazra $\wp(X)$ a $(\triangle, \cap)$ műveletekkel kommutatív egységelemes gyűrű ($\emptyset$ a nulla), amelyben $X \neq \emptyset$ esetén két nem nulla elem „szorzata” lehet nulla.

→ **3.1.15. Feladat [6].** Egészítsük ki az előző pont bizonyítását.

° **3.1.16. Példák.** További példák gyűrűkre a racionális és a valós számok, a páros egész számok, a racionális együtthatós polinomok, a valós vagy komplex együtthatós polinomok, tetszőleges halmazon értelmezett valós értékű függvények a pontonkénti műveletekkel. Általában nem kommutatív gyűrű például az $n \times n$ -es mátrixok (egész, racionális, valós vagy komplex elemekkel).

→° **3.1.17. Feladat [6].** Az előző pontban megadott gyűrűk között keressünk olyat, amelyik egységelemes, amelyik nem egységelemes, amelyik kommutatív, amelyik nem kommutatív, amelyik nullosztómentes, és amelyikben vannak nullosztók.

→ **3.1.18. Feladat [6].** Hányféleképpen értelmezhetünk olyan összeadást és szorzást a $\{0, a, b\}$ halmazon, amelyekkel gyűrű? Minden esetben határozzuk meg az elemek többszöröseit és hatványait.

→ **3.1.19. Feladat [6].** Hányféleképpen értelmezhetünk olyan összeadást és szorzást a $\{0, 1, a, b\}$ halmazon, amelyekkel egységelemes gyűrű? Minden esetben határozzuk meg az elemek többszöröseit és hatványait.

3.1.20. Az általános disztributivitás tétele. Egy R gyűrűben

(1) ha $m, n \in \mathbb{N}$, valamint $a_1, a_2, \dots, a_m$ és $b_1, b_2, \dots, b_n$ a gyűrű tetszőleges elemei, akkor

$$\left(\sum_{i=1}^m a_i\right) \left(\sum_{j=1}^n b_j\right) = \sum_{i=1}^m \sum_{j=1}^n a_i b_j;$$

(2) általánosabban, ha $m \in \mathbb{N}^+$, $n_1, \dots, n_m \in \mathbb{N}$, valamint $a_{i,j_i} \in R$, ha $1 \leq i \leq m$, $1 \leq j_i \leq n_i$, akkor

$$\prod_{i=1}^m \left(\sum_{j_i=1}^{n_i} a_{i,j_i}\right) = \sum_{j_1=1}^{n_1} \dots \sum_{j_m=1}^{n_m} \prod_{i=1}^m a_{i,j_i}.$$

A tételt egyszerűen úgy szoktuk megfogalmazni, hogy többtagok szorzásánál minden tagot minden taggal kell szorozni.

Bizonyítás. (1) triviális, ha $m = 0$ vagy $n = 0$. Az $n = 1$ eset m szerinti indukcióval következik a jobb oldali disztributivitásból. Végül az általános esetet n szerinti indukcióval kapjuk:

$$\begin{aligned} \left(\sum_{i=1}^m a_i\right) \left(\sum_{j=1}^n b_j\right) &= \left(\sum_{i=1}^m a_i\right) \left(\sum_{j=1}^{n-1} b_j + b_n\right) \\ &= \left(\sum_{i=1}^m a_i\right) \left(\sum_{j=1}^{n-1} b_j\right) + \left(\sum_{i=1}^m a_i\right) b_n \\ &= \sum_{i=1}^m \sum_{j=1}^{n-1} a_i b_j + \sum_{i=1}^m a_i b_n \\ &= \sum_{i=1}^m \sum_{j=1}^n a_i b_j. \end{aligned}$$

(2) triviális, ha $m = 1$ és (1)-el ekvivalens, ha $m = 2$. Utolsó lépésként az általános esetet (1) felhasználásával m szerinti indukcióval bizonyítjuk:

$$\begin{aligned} \prod_{i=1}^m \left(\sum_{j_i=1}^{n_i} a_{i,j_i}\right) &= \prod_{i=1}^{m-1} \left(\sum_{j_i=1}^{n_i} a_{i,j_i}\right) \cdot \left(\sum_{j_m=1}^{n_m} a_{i,j_m}\right) \\ &= \left(\sum_{j_1=1}^{n_1} \dots \sum_{j_{m-1}=1}^{n_{m-1}} \prod_{i=1}^{m-1} a_{i,j_i}\right) \cdot \left(\sum_{j_m=1}^{n_m} a_{i,j_m}\right) \\ &= \sum_{j_1=1}^{n_1} \dots \sum_{j_m=1}^{n_m} \prod_{i=1}^m a_{i,j_i}. \quad \square \end{aligned}$$

3.1.21. Nullosztók, integritási tartomány, rendezett integritási tartomány.

Mint a zérógyűrűk példája mutatja, két nem nulla elem szorzata lehet nulla egy gyűrűben. Ha x, y egy R gyűrű nullától különböző elemei, és $xy = 0$, akkor azt mondjuk, hogy x és y egy nullosztópár, x bal oldali nullosztó, y pedig jobb oldali nullosztó (lásd a 3.1.14

példát). A nullgyűrűben nyilván nincsenek ilyenek, de ez a gyűrű érdektelen. Ezért egy legalább kételemű gyűrűt *nullosztómentesnek* nevezünk, ha nincsenek benne nullosztópárok. Ez nyilván azzal ekvivalens, hogy $R \setminus \{0\}$ egy nem üres félcsoport a szorzással. Nullosztómentes gyűrűben nem nulla elemmel való szorzásnál lehet balról is, jobbról is egyszerűsíteni: ha $xy = xz$, akkor $x(y - z) = 0$, és ha $x \neq 0$, akkor $y - z = 0$, tehát $y = z$. Hasonlóan adódik, hogy ha $yx = zx$ és $x \neq 0$, akkor $y = z$. Az nyilvánvaló, hogy ha van nullosztópár, akkor a bal oldali nullosztóval balról, a jobb oldali nullosztóval pedig jobbról nem lehet egyszerűsíteni. Ha x -nek van multiplikatív inverze, akkor x nem lehet sem bal, sem jobb oldali nullosztó, hiszen $xy = 0$ -ból illetve $yx = 0$ -ból $y = x^{-1}xy = 0$, illetve $y = yxx^{-1} = 0$ következik.

Kommutatív nullosztómentes gyűrűt *integritási tartománynak* nevezünk. Nyilván $\mathbb{Z}$ egységelemes integritási tartomány. Az R -et *rendezett integritási tartománynak* nevezzük, ha rendezett halmaz, integritási tartomány, és

- (1) ha $x, y, z \in R$ és $x \leq y$, akkor $x + z \leq y + z$ (az összeadás monoton);
- (2) ha $x, y \in R$ és $x, y \geq 0$, akkor $x \cdot y \geq 0$ (kissé furcsa, de az mondjuk, hogy a szorzás monoton).

Rendezett integritási tartományban ha $x > 0$, akkor x -et *pozitív*nak, ha $x < 0$, akkor x -et *negatív*nak nevezzük.

Az egész számok tulajdonságait röviden úgy foglalhatjuk össze, hogy $\mathbb{Z}$ rendezett integritási tartomány.

3.1.22. Tétel. *Egy rendezett halmaz, amely integritási tartomány, akkor és csak akkor rendezett integritási tartomány, ha az alábbi feltételek fennállnak:*

- (1') ha $x, y, z \in R$ és $x < y$, akkor $x + z < y + z$ (az összeadás szigorúan monoton);
- (2') ha $x, y \in R$ és $x, y > 0$, akkor $x \cdot y > 0$ (a monoton szorzás szigorúan monoton).

Bizonyítás. Ha a definícióból (1) teljesül, $x < y$, akkor $x \leq y$, és így $x + z \leq y + z$, de egyenlőség nem teljesülhet, mert akkor $x = x + z - z = y + z - z = y$ következne, így kapjuk (1')-t. (1')-ből nyilván következik (1), mert az egyenlőség esete triviális.

Ha a definícióból (2) teljesül, és $x, y > 0$, akkor $x, y \geq 0$, így $xy \geq 0$. Ha $xy = 0$ lenne, akkor x és y egy nullosztópár lenne, ami lehetetlen, így kapjuk (2')-t. (2')-ből nyilván következik (2), mert gyűrűben $x0 = 0y = 0$. $\square$

3.1.23. Tétel. *Legyen R rendezett integritási tartomány. Ekkor teljesülnek a szokásos „egyenlőtlenségekkel való számolási szabályok”:*

- (1) ha $x > 0$, akkor $-x < 0$, és ha $x < 0$, akkor $-x > 0$;
- (2) ha $x < y$ és $z > 0$, akkor $xz < yz$;
- (3) ha $x < y$ és $z < 0$, akkor $xz > yz$;
- (4) ha $x \neq 0$, akkor $x^2 > 0$; speciálisan, ha van egységelem, akkor az pozitív;
- (5) ha 1 az egységelem, $0 < x < y$, és x -nek is, y -nak is van multiplikatív inverze, akkor $0 < 1/y < 1/x$.

Bizonyítás. Ha $x > 0$, akkor $0 = -x + x > -x + 0 = -x$. Ha $x < 0$, akkor $0 = -x + x < -x + 0 = -x$. Ezzel beláttuk (1)-et. (2) abból következik, hogy $y - x > x - x = 0$, így $(y - x)z > 0$, amiből $yz - xz > 0$, így $yz > xz$. (3)-at megkapjuk (1)-ből és (2)-ből, mert $-((y - x)z) = (y - x)(-z) > 0$, így $(y - x)z < 0$, tehát $yz < xz$. Ha $x > 0$, akkor

$x^2 > 0$, ha viszont $x < 0$, akkor $-x > 0$, így $x^2 = (-x)^2 > 0$. Speciálisan, $1 = 1^2 > 0$. Végül (5)-höz: ha $y > 0$ és $v \leq 0$, akkor $yv \leq 0$. De $y(1/y) = 1 > 0$. Ezért $1/y > 0$, és hasonlóan $1/x > 0$. Ha az $x < y$ egyenlőtlenség mindkét oldalát megszorozzuk a pozitív $(1/x)(1/y)$ -nal, akkor azt kapjuk, hogy $1/y < 1/x$. $\square$

→ **3.1.24. Feladat [3].** Mutassuk meg, hogy a $\{m + n\sqrt{5} : m, n \in \mathbb{Z}\}$ halmaz rendezett integritási tartomány a szokásos összeadással, szorzással és rendezéssel.

→ **3.1.25. Feladat [4].** Mutassuk meg, hogy a $\{m/3^n : m \in \mathbb{Z}, n \in \mathbb{N}^+\}$ halmaz rendezett integritási tartomány a szokásos összeadással, szorzással és rendezéssel. Mely elemeknek van (multiplikatív) inverze?

3.2 Racionális számok

Az egész számok körében a nem nulla elemek közül csak 1-nek és -1 -nek van multiplikatív inverze, másként szólva, az osztás általában nem végezhető el. Ez indokolja a racionális számok bevezetését. Az alapgondolat, hogy „számláló–nevező” párokat tekintünk, és alkalmas ekvivalenciát vezetünk be.

3.2.1. Tétel. Tekintsük $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ -n az $(m, n) \sim (m', n')$, ha $mn' = nm'$ relációt, az $(m, n) + (m', n') = (mn' + nm', nn')$ összeadást és az $(m, n) \cdot (m', n') = (mm', nn')$ szorzást, valamint az $(m, n) \leq (m', n')$, ha $(m'n - n'm)nn' \geq 0$ relációt. A $\sim$ reláció ekvivalenciareláció. Az ekvivalenciaosztályok halmazát $\mathbb{Q}$ -val fogjuk jelölni, és elemeit racionális számoknak nevezzük. Az összeadás, a szorzás és a $\leq$ reláció kompatibilis az ekvivalenciával, így a racionális számok között értelmezve van az összeadás, a szorzás és a $\leq$ reláció, amely rendezés, továbbá

- (1) $\mathbb{Q}$ az összeadással és a szorzással egységelemes integritási tartomány;
- (2) $\mathbb{Q}$ nem nulla elemei a szorzással Abel-csoportot alkotnak;
- (3) ha $x, y, z \in \mathbb{Q}$ és $x \leq y$, akkor $x + z \leq y + z$ (az összeadás monoton);
- (4) ha $x, y \in \mathbb{Q}$ és $x, y \geq 0$, akkor $x \cdot y \geq 0$ (a szorzás monoton).

(1), (3) és (4) azt jelenti, hogy $\mathbb{Q}$ rendezett integritási tartomány.

Bizonyítás. Triviális, hogy $\sim$ reflexív és szimmetrikus. Ha $(m, n) \sim (m', n')$ és $(m', n') \sim (m'', n'')$, akkor $mn' = nm'$ és $m'n'' = n'm''$. A két összefüggést összeszorozva $mm'n'n'' = nm'n'm''$. Ha $m' \neq 0$, akkor $m'n' \neq 0$, így egyszerűsítve azt kapjuk, hogy $mn'' = nm''$, azaz $(m, n) \sim (m'', n'')$. Ha $m' = 0$, akkor $n' \neq 0$ miatt $m = 0$ és $m'' = 0$, és ekkor is $(m, n) \sim (m'', n'')$.

Az összeadás kompatibilis az ekvivalenciarelációval, mert ha $(m, n) \sim (m', n')$, akkor $mn' = nm'$, amiből $mn'n''n'' = nm'n''n''$, innen viszont

$$\begin{aligned} (mn'' + nm'')n'n'' &= mn'n''n'' + nm'm''n'' = nm'n''n'' + nm'm''n'' \\ &= (m'n'' + n'm'')nn'', \end{aligned}$$

tehát

$$\begin{aligned} (m, n) + (m'', n'') &= (mn'' + nm'', nn'') \sim (m'n'' + n'm'', n'n'') \\ &= (m', n') + (m'', n''), \end{aligned}$$

és a párok összeadása triviálisan kommutatív, így elég ezt belátni. Mivel a párok összeadása könnyen kiszámolhatóan asszociatív is, az ekvivalenciosztályok összeadása is kommutatív és asszociatív. A $(0, 1)$ pár osztálya, a $(0, n)$ alakú párok halmaza nullelem, ezt jelöljük nullával. Az (m, n) pár osztályának additív inverze a $(-m, n)$ pár osztálya. Így $\mathbb{Q}$ az összeadással Abel-csoport.

A szorzás is kompatibilis az osztályozással, mert ha $(m, n) \sim (m', n')$, akkor $mn' = nm'$, amiből $mm''n'n'' = nm'm''n''$, így

$$(m, n) \cdot (m'', n'') = (m \cdot m'', n \cdot n'') \sim (m' \cdot m'', n' \cdot n'') = (m', n') \cdot (m'', n'').$$

Mivel a párok szorzása láthatóan kommutatív, beláttuk a szorzás kompatibilitását az osztályozással. Mivel a párok szorzása asszociatív is, az osztályoké is asszociatív. Egyszerű számolás mutatja, hogy $(m, n) \cdot ((m', n') + (m'', n''))$ és $(m, n) \cdot (m', n') + (m, n) \cdot (m'', n'')$ ekvivalens párok, így az osztályok szorzása disztributív. Ezzel beláttuk, hogy $\mathbb{Q}$ kommutatív gyűrű.

Az $(1, 1)$ pár nyilván multiplikatív egységelem a párok halmazában, így osztálya, az (n, n) alakú párok halmaza a multiplikatív egységelem az osztályok halmazában. Ha $(m, n) \sim (0, 1)$, akkor $m \neq 0$, ekkor viszont az (m, n) pár osztályának multiplikatív inverze az (n, m) pár osztálya. Ezzel (1) és (2) bizonyítását befejeztük.

Következő lépésként a rendezéssel fogunk foglalkozni. Először is vegyük észre, hogy $(0, 1) \leq (m, n)$ akkor és csak akkor teljesül, ha $mn \geq 0$. Megmutatjuk, hogy ha $(m, n) \sim (m', n')$, akkor $(0, 1) \leq (m', n')$: Valóban, ha $(m, n) \sim (m', n')$, azaz $mn' = nm'$, akkor $m = 0$ esetén $mn' = 0$, azaz $nm' = 0$, amiből $n \neq 0$ miatt (például az előző tétel felhasználásával) $m' = 0$, így $m'n' = 0$, azaz $(0, 1) \leq (m', n')$. Ha $m > 0$, akkor az előző tétel szerint $n > 0$. Ha $mn' > 0$, akkor ebből $n' > 0$ és $m' > 0$ következik, így $m'n' > 0$, amiből $(0, 1) \leq (m', n')$. Az $mn' < 0$, valamint az $m < 0$ esetén adódó további esetek vizsgálata hasonló. Most vegyük észre, hogy $(m, n) \leq (m'', n'')$ azzal ekvivalens, hogy $(0, 1) \leq (m'', n'') + (-m, n)$. Mivel az eddig bizonyítottak szerint a jobb oldalon $(m', n') \sim (m'', n'')$ esetén (m'', n'') helyére (m', n') -t írva, vagy $(m', n') \sim (m, n)$ esetén $(-m, n)$ helyére $(-m', n')$ -t írva, az összeg ekvivalens összegbe megy át, kapjuk, hogy $\leq$ reláció kompatibilis az osztályozással.

Az előző bekezdésben bizonyítottakból (4) könnyen adódik. A disztributivitást és az előjelszabályt használva kapjuk (3)-at is, de be kell még látnunk, hogy $\leq$ rendezés az osztályokon. A reflexivitás és a szimmetria azonnal adódik $\leq$ definíciójából. Az, hogy bármely két osztály összehasonlítható, következik abból, hogy vagy $(m, n) = (m', n') - (m'', n'')$ -re vagy a $(-m, n)$ ellentettjére $(0, 1) \leq (m, n)$. Végül a tranzitivitáshoz elég belátnunk, hogy ha $(0, 1) \leq (m, n)$ és $(0, 1) \leq (m', n')$, akkor $(0, 1) \leq (m, n) + (m', n')$. Ez azonban teljesül, mert $(mn' + m'n)nn' = mnn'^2 + m'n'n^2 \geq 0$. $\square$

3.2.2. Tétel: $\mathbb{Z}$ beágyazása $\mathbb{Q}$ -ba. Az előző tétel jelöléseivel, a $\mathbb{Z}$ -nek $\mathbb{Q}$ -ba való $\varphi: n \mapsto \widetilde{(n, 1)}$ leképezése kölcsönösen egyértelmű, összeadás- és szorzástartó, monoton növekedő, valamint $\varphi(n) = n\varphi(1)$ minden $n \in \mathbb{Z}$ -re. Így $\varphi(\mathbb{Z})$ -t azonosíthatjuk $\mathbb{Z}$ -vel. A $\mathbb{Q}$ minden eleme m/n alakban írható, ahol $m, n \in \mathbb{Z}$ és $n \neq 0$.

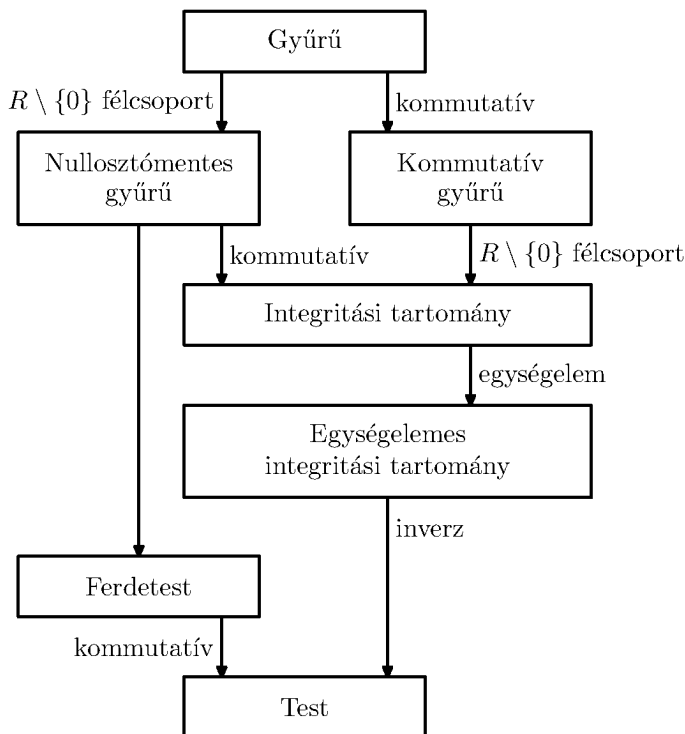
A felírás természetesen nem egyértelmű, mert $m/n = (mk)/(nk)$ minden $k \in \mathbb{Z}$ -re. Számítógépben való ábrázolásnál azt a felírást szoktuk választani, amelyre $n > 0$, de a lehető legkisebb.

Bizonyítás. Ugyanúgy, mint $\mathbb{N}$ -nek $\mathbb{Z}$ -be való beágyazásánál, indukcióval adódik, hogy $\varphi(n) = n\varphi(1) = \overline{(n, 1)}$ minden $n \in \mathbb{N}$ -re, és $n\varphi(1)$ definíciója alapján, hogy $n \in \mathbb{Z}$, $n < 0$ esetén is. Az állítás többi része az előző tétel bizonyításában tett észrevételek segítségével könnyen belátható. $\square$

3.2.3. Ferdetest, test, rendezett test. Egy F gyűrűt *ferdetest*nek nevezünk, ha a nullelemet 0-val jelölve $F \setminus \{0\}$ a szorzással csoport. A szorzás egységelemét rendszerint 1-gyel jelöljük. Ha a szorzás kommutatív, akkor a ferdetestet *test*nek nevezzük. Természetesen minden test egységelemes integritási tartomány, hiszen testben minden nem nulla elemnek van inverze, invertálható elem pedig nem lehet nullosztó. Az eddig tanult számkörök közül példa testre $\mathbb{Q}$. A legegyszerűbb példa a *kételemű test*: $\{0, 1\}$ a $0+0 = 1+1 = 0$, $0+1 = 1+0 = 1$ összefüggésekkel megadott összeadással és a $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$ összefüggésekkel megadott kommutatív szorzással.

Egy testet *rendezett test*nek nevezünk, ha test és rendezett integritási tartomány. Az előző tétel szerint $\mathbb{Q}$ rendezett test. Megjegyezzük, hogy a kételemű testen nincs olyan rendezés, amellyel rendezett test lenne, mert rendezett testben $1 > 0$ és $-1 < 0$, de a kételemű testben $-1 = 1$.

Az eddig tanult kétműveles algebrai struktúrák közötti kapcsolatokat a 3.2.1 ábra mutatja.



3.2.1 ábra: kétműveletes algebrai struktúrák.

◦ **3.2.4. Példák.** További példák testre a valós, illetve a komplex számok, a modulo p maradékosztályok, ha p prímszám, ferdetestre pedig a kvaterniók, mint azt később látni fogjuk. Ezek közül a valós számok rendezett testet alkotnak. A többin nincs olyan rendezés, amellyel rendezett integritási tartomány lenne, mert bennük -1 előáll négyzetösszegként.

3.2.5. Tétel: $\mathbb{Q}$ beágyazása rendezett testbe. Legyen F rendezett test e egységelemmel. Ekkor egyértelműen létezik egy kölcsönösen egyértelmű, összeadás- és szorzástartó $\varphi: \mathbb{Q} \rightarrow F$ leképezés. Ez a leképezés monoton növekedő is, és $\varphi(m/n) = (me)/(ne)$, ha $m, n \in \mathbb{Z}$ és $n \neq 0$. Így $\mathbb{Q}$ azonosítható $\varphi(\mathbb{Q})$ -val.

* **Bizonyítás.** A φ leképezés egyértelműségének bizonyításával kezdjük. Tegyük fel, hogy $\varphi: \mathbb{Q} \rightarrow F$ kölcsönösen egyértelmű és összeadástartó. Ekkor $\varphi(0) = \varphi(0+0) = \varphi(0)+\varphi(0)$, kapjuk hogy $\varphi(0)$ az F nulleleme. Innen $\varphi(0) = \varphi(r-r) = \varphi(r)+\varphi(-r)$ miatt $\varphi(-r) = -\varphi(r)$ minden $r \in \mathbb{Q}$ -ra. Mivel $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$ és $\varphi(1)$ már nem lehet a nullelem, így mindkét oldalt szorozva $\varphi(1)$ multiplikatív inverzával, $e = \varphi(1)$. Indukcióval $\varphi(mr) = m\varphi(r)$, ha $r \in \mathbb{Q}$, $m \in \mathbb{N}$. Felhasználva, hogy $\varphi(-mr) = -\varphi(mr)$, ez minden $m \in \mathbb{Z}$ -re teljesül. Ha $n \in \mathbb{N}^+$, akkor $e = \varphi(n \cdot 1/n) = n\varphi(1/n)$ miatt $\varphi(1/n) = e/(ne)$, és hasonlóan, mint az előbb kapjuk, hogy ez $0 \neq n \in \mathbb{Z}$ esetén is igaz. Végül

$$\varphi(m/n) = m\varphi(1/n) = m(e/(ne)) = m(e^2/(ne)) = (me)(e/(ne)) = (me)/(ne).$$

Ezzel a keresett leképezés egyértelműségét beláttuk.

A fentiek alapján világos, hogyan kell a létezését bizonyítani: ha $m, n \in \mathbb{Z}$, $n \neq 0$, legyen $\varphi(m/n) = (me)/(ne)$. Mivel e pozitív, indukcióval ne is pozitív, ha n pozitív, ha pedig n negatív, akkor ne is negatív, tehát nem lehet nulla. Ha $m', n' \in \mathbb{Z}$, $n' \neq 0$ és $m/n = m'/n'$, akkor $(me)(n'e) = (mn')ee = (m'n)ee = (m'e)(ne)$, tehát $(me)/(ne) = (m'e)/(n'e)$, azaz $\varphi(m/n)$ nem függ m és n választásától, csak m/n -től. Ez a leképezés nyilván multiplikatív is, és $\varphi(m+m') = (m+m')e = me + m'e = \varphi(m) + \varphi(m')$, ha $m, m' \in \mathbb{Z}$, amiből

$$\begin{aligned} \varphi(m/n + m'/n') &= \varphi((mn' + m'n)/(nn')) = \varphi(mn' + m'n)/\varphi(nn') \\ &= (\varphi(mn') + \varphi(m'n))/(nn'e) = (me)/(ne) + (m'e)/(n'e) \\ &= \varphi(m/n) + \varphi(m'/n'), \end{aligned}$$

azaz a leképezés additív. Végül, ha $m, n \in \mathbb{N}^+$, akkor $\varphi(m/n)$ is pozitív, amiből már adódik a szigorú monotonitás, és így az is, hogy φ kölcsönösen egyértelmű. $\square$

→ **3.2.6. Feladat [6].** Adjunk meg olyan összeadást és szorzást a $\{0, 1, a, b\}$ halmazon, amelyekkel test.

→ **3.2.7. Feladat [6].** Bizonyítsuk be, hogy véges test nem tehető rendezett testté.

→ **3.2.8. Feladat [7].** Ellenőrizzük, hogy a racionális számok halmaza Abel-csoport az $(a, b) \rightarrow a+b+1$ művelettel. Mi lesz a nullelem? Adjunk meg olyan szorzást, amellyel testet kapunk. Igaz-e hasonló állítás minden testre, illetve egységelemes gyűrűre?

3.2.9. Feladat [9]. Legyen K a racionális számok egy olyan részhalmaza, amelynek legalább három eleme van és tartalmazza az 1-et. Tegyük fel, hogy ha $a, b \in K$ és $a \neq 0$, akkor $(1/a) - b \in K$. Mutassuk meg, hogy K test.

3.3 Valós számok

Pythagoras iskolájának matematikusai észrevették, hogy egy egységnyi oldalú négyzet átlójának hossza nem racionális szám. Fokozatosan kidolgozták az új számokkal való számolás szabályait, racionális számokkal való közelítéseik felhasználásával. Módszerük az volt, hogy egy valós számot az összes nála kisebb racionális szám halmazával azonosítottak. Ezt az alapgondolatot fogjuk felhasználni a valós számok bevezetésére. A görögök geometriai megfontolásokat használtak. A valós számok tisztán halmazelméleti bevezetése Dedekindtől, illetve Cantortól származik 1872-ből.

3.3.1. Állítás. *Nincs olyan racionális szám, amelynek a négyzete 2.*

Bizonyítás. Ha lenne, akkor $(-m/n)^2 = (m/n)^2$ miatt lenne olyan is, amely felírható m/n alakban, ahol $m, n \in \mathbb{N}^+$. Válasszuk azt a felírást, amelyre a számláló minimális. Mivel $m^2 = 2n^2$, m páros kell legyen. Legyen $m = 2k$, $k \in \mathbb{N}^+$. Ekkor $4k^2 = 2n^2$, ahonnan $2k^2 = n^2$. Innen n is páros. Ez ellentmond annak, hogy a számláló minimális. $\square$

3.3.2. Arkhimédészi tulajdonság. Egy F rendezett testet *arkhimédészien rendezettnek* nevezzük, ha $x, y \in F$, $x > 0$ esetén van olyan $n \in \mathbb{N}$, amelyre $nx \geq y$.

3.3.3. Állítás. *Egy felső határ tulajdonságú rendezett test mindig arkhimédészien rendezett.*

Bizonyítás. Ellenkező esetben $A = \{nx : n \in \mathbb{N}\}$ -nek az y felső korlátja lenne. Legyen $z = \sup A$. Mivel $z - x < z$, a $z - x$ már nem felső korlát, így van olyan $n \in \mathbb{N}$, amelyre $nx > z - x$. De ebből $(n + 1)x > z$, ami ellentmondás. $\square$

A megfordítás nem igaz:

3.3.4. Állítás. *A racionális számok rendezett teste arkhimédészien rendezett, de nem felső határ tulajdonságú.*

* **Bizonyítás.** Legyen $x > 0$. Ha $y \leq 0$, akkor $n = 0$ választással, ha pedig $x = i/j$, $y = k/m$, $i, j, k, m \in \mathbb{N}^+$, akkor $n \geq kj$ választással $nx \geq y$, így kapjuk, hogy $\mathbb{Q}$ arkhimédészien rendezett.

Legyen A az összes olyan $r > 0$ racionális számok halmaza, amelyekre $r^2 < 2$, és legyen B az összes olyan $r > 0$ racionális számok halmaza, amelyekre $r^2 > 2$. Legyen

$$s = r - \frac{r^2 - 2}{r + 2} = \frac{2r + 2}{r + 2}.$$

Ekkor

$$s^2 - 2 = \frac{2(r^2 - 2)}{(r + 2)^2}.$$

Ha $r \in A$, akkor $s > r$, de $s^2 < 2$, azaz $s \in A$, így A -nak nincs legnagyobb eleme. Ha $r \in B$, akkor $s < r$, de $s^2 > 2$, azaz $s \in B$, így B -nek nincs legkisebb eleme. Innen következik, hogy A -nak nincs $\mathbb{Q}$ -ban legkisebb felső korlátja: ha lenne, nem lehetne A -ban, mert akkor A legnagyobb eleme lenne, így B -ben kellene lennie, de B -nek nincs legkisebb eleme. (Hasonlóan adódik, hogy B -nek nincs legnagyobb alsó korlátja $\mathbb{Q}$ -ban.) $\square$

* **3.3.5. Tétel.** Egy arkhimédészien rendezett test bármely $a < b$ elemeihez van olyan $r \in \mathbb{Q}$, amelyre $a < r < b$. (A racionális számokat azonosítjuk a test egy részhalmazával a beágyazásról szóló tétel alapján.)

Bizonyítás. Mivel $b - a > 0$, van olyan $n \in \mathbb{N}^+$, hogy $n(b - a) > 1$, továbbá ezen n -hez vannak olyan m_1 és m_2 egészek, amelyekre $m_1 > na$ és $m_2 > -na$. Így $-m_2 < na < m_1$. Legyen k az a legkisebb természetes szám, amelyre $m = -m_2 + k > na$. Így m olyan $-m_2 \leq m \leq m_1$ egész, amelyre $m - 1 \leq na < m$. Innen $na < m \leq 1 + na < nb$, és mivel $n > 0$, azt kapjuk, hogy $a < m/n < b$. $\square$

3.3.6. Tétel: a valós számok egyértelműsége. Legyen $\mathbb{R}'$ és $\mathbb{R}''$ két felső határ tulajdonságú rendezett test. Ekkor létezik egy φ kölcsönösen egyértelmű leképezése $\mathbb{R}'$ -nek $\mathbb{R}''$ -re, amely monoton növekedő, összeadás- és szorzástartó.

* **Bizonyítás.** A jelölések egyszerűsítésére mindjárt feltesszük, hogy $\mathbb{R}' \supset \mathbb{Q} \subset \mathbb{R}''$. Ha $x' \in \mathbb{R}'$, legyen $S_{x'}$ az x' -höz $\mathbb{R}'$ -ben tartozó kezdőszelet metszete $\mathbb{Q}$ -val. (Ha $x'' \in \mathbb{R}''$, akkor $S_{x''}$ hasonlóan van definiálva, persze az $\mathbb{R}''$ -beli $<$ relációval.) Az $S_{x'}$ (illetve $S_{x''}$) halmazok sohasem üresek, van racionális felső korlátjuk, és nincs legnagyobb elemük, mert az előző tétel szerint van olyan $r \in \mathbb{Q}$, amelyre $x' - 1 < r < x'$, emiatt $r + 1$ felső korlát, és bármely $p \in S_{x'}$ -re van olyan $q \in \mathbb{Q}$, amelyre $p < q < x'$. Továbbá x' az $S_{x'}$ legkisebb felső korlátja $\mathbb{R}'$ -ben: nyilván felső korlát, és nála kisebb y' nem lehet felső korlát, mert van olyan $r \in \mathbb{Q}$, amelyre $y' < r < x'$. Legyen $\varphi(x') = x''$ az $S_{x'} \subset \mathbb{Q}$ halmaz legkisebb felső korlátja, de most $\mathbb{R}''$ -ben.

Ha $x', y' \in \mathbb{R}'$, $x' < y'$, akkor van olyan $r \in \mathbb{Q}$, amelyre $x' < r < y'$, és van olyan $s \in \mathbb{Q}$, amelyre $x' < s < r < y'$. Innen $\varphi(x') \leq s$ és $\varphi(y') \geq r$, azaz $\varphi(x') < \varphi(y')$, tehát φ szigorúan monoton növekedő, így kölcsönösen egyértelmű is.

Legyen $x'' \in \mathbb{R}''$, és x' az $S_{x''}$ legkisebb felső korlátja, most viszont $\mathbb{R}'$ -ben. Megmutatjuk, hogy $S_{x'} = S_{x''}$, amiből már következik $\varphi(x') = x''$, azaz φ szürjektív. Nyilván $x' \notin S_{x''}$, mert egyébként $S_{x''}$ -nek lenne legnagyobb eleme. Így $S_{x''} \subset S_{x'}$. Másrészt, ha $S_{x'}$ egy r eleme nem lenne $S_{x''}$ -ben, akkor egy x' -nél kisebb felső korlátja lenne $S_{x''}$ -nek, így $S_{x'} \subset S_{x''}$.

Annak igazolására, hogy φ művelettartó az összeadásra nézve, megmutatjuk, hogy $S_{x'} + S_{y'} = S_{x'+y'}$ minden $x', y' \in \mathbb{R}'$ -re; a jobb oldal, mint tudjuk, elemenkénti összegként van értelmezve. Csak azt kell megmutatni, hogy $S_{x'} + S_{y'} \supset S_{x'+y'}$, mert a másik irányú tartalmazás nyilvánvaló. Legyen $r < x' + y'$ racionális szám és $\varepsilon = x' + y' - r$. Legyen p olyan racionális szám, amelyre $x' - \varepsilon < p < x'$. Ekkor $q = r - p < r - (x' - \varepsilon) = r - (r - y') = y'$, így $q \in S_{y'}$, tehát $r = p + q \in S_{x'} + S_{y'}$. Innen már következik a művelettartás az összeadásra nézve, mert ha $\varphi(x') = x''$ és $\varphi(y') = y''$, akkor $S_{x'+y'} = S_{x'} + S_{y'} = S_{x''} + S_{y''} = S_{x''+y''}$, ahonnan $\varphi(x' + y') = x'' + y''$.

Végül megmutatjuk, hogy ha $x' > 0$ és $y' > 0$, akkor $S_{x'y'}$ az összes olyan r racionális számok $S_{x',y'}$ halmaza, amelyekhez van olyan $p, q \in \mathbb{Q}$, hogy $0 < p \in S_{x'}$, $0 < q \in S_{y'}$ és $r \leq pq$. Csak azt kell megmutatnunk, hogy $S_{x'y'} \subset S_{x',y'}$, mivel a másik irányú tartalmazás nyilvánvaló, hiszen $r \leq pq < x'y'$. Legyen $r \in S_{x'y'}$, és válasszuk úgy az $s \in \mathbb{Q}$ racionális számot, hogy $0 < s \leq (x'y' - r)/(x' + y')$, $s < x'$ és $s < y'$ teljesüljön. Ha p -re illetve q -ra $x' - s < p < x'$, illetve $y' - s < q < y'$, akkor $p \in S_{x'}$, illetve $q \in S_{y'}$,

továbbá

$$\begin{aligned} pq &> (x' - s)(y' - s) = x'y' - s(x' + y') + s^2 > x'y' - s(x' + y') \\ &\geq x'y' - \frac{x'y' - r}{x' + y'}(x' + y') = r. \end{aligned}$$

Mivel $\varphi(x') = x''$, $\varphi(y') = y''$ esetén $S_{x',y'}$ definíciójában $S_{x'}$ helyére $S_{x''}$ -t, $S_{y'}$ helyére $S_{y''}$ -t helyettesíthetünk, és az így kapott $S_{x'',y''}$ halmaz megegyezik $S_{x',y'}$ -vel, azt kapjuk, hogy $S_{x'y'} = S_{x''y''}$. Innen következik, hogy $x', y' > 0$ esetén $\varphi(x'y') = x''y'' = \varphi(x')\varphi(y')$. Felhasználva a nullával való szorzás tulajdonságait és az előjelszabályt, kapjuk, hogy φ művelettartó a szorzásra is. $\square$

3.3.7. Valós számok. Egy felső határ tulajdonságú rendezett testet a *valós számok* testének nevezünk. Az előző tétel szerint lényegében legfeljebb egy ilyen van. A következő tételben megmutatjuk, hogy van ilyen. A valós számok testét $\mathbb{R}$ -rel fogjuk jelölni. Ha x valós szám, legyen $|x| = x$, ha $x \geq 0$, és legyen $|x| = -x$, ha $x < 0$. Legyen $\text{sgn}(x) = 0$, ha $x = 0$ és $\text{sgn}(x) = x/|x|$ egyébként; sgn az *előjel függvény*. Legyen $[x]$, az x *alsó egész része* az a legnagyobb eleme $\mathbb{Z}$ -nek, amely nem nagyobb, mint x , és legyen $\lceil x \rceil$, az x *felső egész része* az a legkisebb eleme $\mathbb{Z}$ -nek, amely nem kisebb, mint x : ha $x = 0$, akkor nyilvánvaló, hogy ezek léteznek (ekkor mindkettő nulla). Ha $x > 0$, az arkhimédészi rendezettségéből és $\mathbb{N}$ jólrendezettségéből következik, hogy van az x -nél nagyobb vagy egyenlő természetes számok között egy legkisebb n természetes szám, ez éppen $\lceil x \rceil$. Nyilván $n > 0$. Ha $n = x$, akkor $\lceil x \rceil = \lfloor x \rfloor = n$, egyébként $\lceil x \rceil = n + 1$. Végül, ha $x < 0$, akkor $\lceil x \rceil = -\lfloor -x \rfloor$ és $\lfloor x \rfloor = -\lceil -x \rceil$.

Ha x valós szám, akkor legyen $x \bmod 0 = x$ és $x \bmod y = x - \lfloor x/y \rfloor \cdot y$, ha $0 \neq y \in \mathbb{R}$. Nyilván, ha $y > 0$, akkor $0 \leq x \bmod y < y$, ha pedig $y < 0$, akkor $y < x \bmod y \leq 0$. Az $x \bmod 1 = x - \lfloor x \rfloor$ értéket x *törtrészének* nevezzük.

3.3.8. Bővített valós számok. Néha szükségünk lesz a *bővített valós számok* $\bar{\mathbb{R}} = \mathbb{R} \cup \{+\infty, -\infty\}$ halmazára. A valós számok rendezését úgy terjesztjük ki $\bar{\mathbb{R}}$ -ra, hogy $-\infty < x < +\infty$ teljesüljön minden $x \in \mathbb{R}$ -re. A bővített valós számok körében bármely részhalmaznak van szuprémuma és infimuma (de $\sup \emptyset = -\infty$ és $\inf \emptyset = +\infty$). Az ellentettképzésnél $-(+\infty) = -\infty$ és $-(-\infty) = +\infty$. Az összeadást is értelmezzük, ha nem is mindenütt: $x + (+\infty) = (+\infty) + x = +\infty$, ha $x \in \bar{\mathbb{R}}$, $x > -\infty$ és $x + (-\infty) = (-\infty) + x = -\infty$, ha $x \in \bar{\mathbb{R}}$, $x < +\infty$, de $(+\infty) + (-\infty)$ és $(-\infty) + (+\infty)$ nincs értelmezve.

3.3.9. Valós számok kerekítése és fixpontos ábrázolása számítógépben. Valós számok általában pontosan nem ábrázolhatók számítógépben, de közelítőleg igen. Egyik mód erre a *fixpontos ábrázolás*. Kettes számrendszert használva rögzítünk egy N egész számot, a törtrész hosszát. Az $n/2^N$, $n \in \mathbb{Z}$ alakú valós számok pontosan ábrázolhatók, ha n -et tároljuk. Egy tetszőleges x valós szám helyett a hozzá legközelebb eső pontosan ábrázolható számot tároljuk; ha két ilyen van, akkor azt, amelyben n páros (ez kiküszöböli, hogy ebben az esetben mindig egyirányban történjen a kerekítés); ez a *szabályos kerekítés*. Más *kerekítés* mellett is dönthetünk: $-\infty$ felé való kerekítés esetén az x -nél nem nagyobb pontosan ábrázolható számok közül választjuk ki az x -hez legközelebbit (lefelé); ha $+\infty$ felé kerekítünk, akkor az x -nél nem kisebb pontosan ábrázolható számok közül választjuk ki az x -hez legközelebbit (felfelé). Ezek a kerekítési módok az intervallumaritmetikánál fontosak. Végül *csonkítás* esetén az $|x|$ -nél nem nagyobb abszolút értékű pontosan ábrázolható számok közül választjuk ki az x -hez legközelebbit. Az ábrázolásnál *kerekítési*

hiba lép fel. Műveletek után is ezeket a *kerekítési szabályokat* alkalmazhatjuk a (pontos) eredményre, így természetesen általában a műveleteknél is kerekítési hiba lép fel. Ha n biteinek száma korlátozott, akkor csak egy intervallum elemei ábrázolhatók aránylag kis (szabályos kerekítésnél 2^{-N-1} , a többi kerekítésnél 2^{-N}) hibával, ezen kívüli számoknál *túlsordulás* lép fel.

3.3.10. Valós számok lebegőpontos ábrázolása számítógépben. Fixpontos számábrázoláskor a hiba a szám abszolút értékéhez képest nagy lehet, ha a szám abszolút értéke kicsi. A *lebegőpontos számábrázolás* ezt küszöböli ki, a hiba és a szám értéke hányadosának abszolút értéke, a *relatív hiba* nagyon sok nagyságrenden keresztül kicsi marad. Csak bináris ábrázolással, azon belül is csak az *IEEE 754* szabvány által leírt, ma szinte kizárólagosan használt ábrázolással foglalkozunk. Ennél a pontosan ábrázolható számok $n \cdot 2^{k-N}$ alakúak, ahol $n, k \in \mathbb{Z}$ és $1 - 2^K < k < 2^K$, $-2^{N+1} < n < 2^{N+1}$; a K és N konstansoknak a szabvány által megengedett értékeit az 3.3.1 táblázat tartalmazza.

pontosság	bájtok száma	$K + 1$	N
egyszeres	4	8	23
kétszeres	8	11	52
kiterjesztett kétszeres	≥ 10	≥ 15	≥ 63
négyszeres	16	15	112

3.3.1 táblázat: Lebegőpontos szabvány I.

Az egyszeres pontosság használatos például képfeldolgozásnál. A kétszeres pontosság az általános a legtöbb más esetben. A négyszeres pontosság tulajdonképpen nem szerepel a szabványban, de egyre terjed. A kisebb pontosságról nagyobbra való konverzió csak nullákkal való kiegészítéssel jár, míg fordított irányban kerekítés történik.

Az $n \cdot 2^{k-N}$ alakban való felírás általában nem egyértelmű, mert ha n páros, akkor $(n/2) \cdot 2^{k+1-N}$ ugyanannak a számnak egy másik felírása. Úgy tesszük egyértelművé, hogy k -t a lehető legkisebbnek választjuk. Ha ekkor $|n| \geq 2^N$, akkor $n \cdot 2^{k-N} = \pm 2^k \cdot (1 + f)$, ahol $f = (|n| - 2^N)/2^N < 1$ a szám *törtrésze*; ha $|n| < 2^N$, akkor csak $k = 2 - 2^K$ lehet, ekkor $n \cdot 2^{k-N} = \pm 2^k \cdot (0 + f)$, ahol $f = |n|/2^N < 1$ a szám *törtrésze*; ez utóbbi esetben ha $n \neq 0$, akkor a szám *szubnormális lebegőpontos szám*, minden más esetben *normális lebegőpontos szám*. A pontosan ábrázolható lebegőpontos számok esetén az ábrázolás a következő: a legfelső bit az előjelbit (0 pozitív, 1 negatív), ezután jön a $K + 1$ bites exponens, ami $|n| \geq 2^N$ esetén $k + 2^K - 1$, azaz k értéke $2^K - 1$ -többletes kódban, egyébként pedig 0, ezután pedig a törtrész N biten. Két nulla is van, ± 0 , de a hardver (általában) egyenlőnek tekinti őket. A speciális $2^{K+1} - 1$ exponens érték 0 törtrésszel $\pm\infty$ ábrázolására szolgál (ha az exponens túl nagy lenne, akkor is ez az ábrázolás); ha a törtrész nem nulla, akkor a tartalom nem szám (*NaN*, Not any Number), mégpedig ha a törtrész legfelső bite 0, akkor jelző nem szám (*SNaN*, Signaling Not any Number), ami megszakítást is okoz. A további részleteket lásd a [40] cikkben. Az egyes eseteket a 3.3.2 táblázat foglalja össze.

3.3.11. Tétel: a valós számok létezése. *Létezik felső határ tulajdonságú rendezett test.*

szám típus	előjel bit	exponens	implicit bit	tötrész
$\pm\infty$	$\pm$	$111\dots111_2$	1	$000\dots000_2$
NaN	?	$111\dots111_2$	1	$1??\dots??_2$
SNaN	?	$111\dots111_2$	1	$0??\dots??_2$
normális	$\pm$	$k + 2^K - 1$	1	$ n - 2^N$
szubnormális	$\pm$	0	0	$ n $
nulla	$\pm$	0	0	0

3.3.2 táblázat: Lebegőpontos szabvány II.

* **Bizonyítás.** I. A bizonyítás alapgondolata, hogy a valós számokat mint a racionális számok bizonyos részhalmazait, úgynevezett *Dedekind-szeleteit* vagy röviden csak *szeleteit* definiáljuk. A $\mathbb{Q}$ egy α részhalmazát *szeletnek* nevezzük, ha

- (1) $\emptyset \neq \alpha \neq \mathbb{Q}$;
- (2) ha $r \in \alpha$, $s \in \mathbb{Q}$ és $s < r$, akkor $s \in \alpha$;
- (3) ha $r \in \alpha$, akkor van olyan $s \in \alpha$, amelyre $s > r$.

A valós számok $\mathbb{R}$ halmazát mint $\mathbb{Q}$ szeleteinek halmazát definiáljuk. Megjegyezzük, hogy $\mathbb{Q}$ kezdőszeletei mind szeletek, ezek felelnek majd meg az $\mathbb{R}$ racionális számainak. Egy $r \in \mathbb{Q}$ racionális számhoz tartozó kezdőszeletet r^* -gal fogunk jelölni.

II. Ha $\alpha, \beta \in \mathbb{R}$, akkor legyen $\alpha \leq \beta$, ha $\alpha \subset \beta$. Ez a reláció nyilván reflexív, antiszimmetrikus és tranzitív. Meg kell mutatni, hogy dichotom. Tegyük fel, hogy $\alpha \not\subset \beta$. Ekkor van olyan $r \in \alpha$, amelyre $r \notin \beta$. Ha $s \in \beta$, akkor $s < r$, hiszen $r \notin \beta$, így (2) szerint $s \in \alpha$. Tehát $\beta \subset \alpha$, azaz $\mathbb{R}$ rendezett halmaz $\leq$ -vel.

III. Megmutatjuk, hogy az $\mathbb{R}$ rendezett halmaz felső határ tulajdonságú. Legyen A az $\mathbb{R}$ egy nem üres részhalmaza, és tegyük fel, hogy $\beta \in \mathbb{R}$ az A egy felső korlátja. Legyen γ az $\alpha \in A$ szeletek egyesítése. Megmutatjuk, hogy $\gamma \in \mathbb{R}$ és $\gamma = \sup A$. Mivel A nem üres, van $\alpha \in A$, és mivel α nem üres, γ sem üres. Továbbá $\gamma \subset \beta$, hiszen $\alpha \subset \beta$ minden $\alpha \in A$ esetén, ezért $\gamma \neq \mathbb{Q}$. (2) és (3) bizonyításához válasszunk ki egy $r \in \gamma$ elemet. Ekkor $r \in \alpha$ valamely $\alpha \in A$ esetén. Ha $s < r$, akkor $s \in \alpha$, így $s \in \gamma$, tehát (2) teljesül. Most legyen $s \in \alpha$ olyan, hogy $s > r$. Ekkor $s \in \gamma$, így (3) is teljesül. Tehát $\gamma \in \mathbb{R}$. Világos, hogy $\alpha \leq \gamma$ minden $\alpha \in A$ esetén, tehát γ felső korlátja A -nak. Megmutatjuk, hogy a legkisebb. Tegyük fel, hogy $\delta < \gamma$. Ekkor van olyan $r \in \gamma$, amelyre $r \notin \delta$. Mivel $r \in \gamma$, ezért $r \in \alpha$ valamely $\alpha \in A$ esetén. Így $\delta < \alpha$ és δ nem felső korlátja A -nak. Így $\gamma = \sup A$.

IV. Ha $\alpha, \beta \in \mathbb{R}$, legyen $\alpha + \beta$ a két halmazból összeadással nyert racionális számok halmaza, azaz az összes $r + s$ alakú összegek halmaza, ahol $r \in \alpha$ és $s \in \beta$. Megmutatjuk, hogy a szeletek ezzel az összeadással Abel-csoportot alkotnak, amelyben a nullelem szerepét 0^* , a nullához tartozó kezdőszelet játssza, és az összeadás monoton.

Először meg kell mutatnunk, hogy a nyilván nem üres $\alpha + \beta$ szelet. Ha $r' \in \mathbb{Q} \setminus \alpha$, $s' \in \mathbb{Q} \setminus \beta$, akkor $r' + s' > r + s$ minden $r \in \alpha$, $s \in \beta$ esetén, így (1) teljesül. Válasszunk egy $r \in \alpha + \beta$ elemet. Ekkor $r = p + q$ valamely $p \in \alpha$, $q \in \beta$ elemekkel. Ha $s < r$, akkor $s - p < q$, így $s - p \in \beta$ és $s = p + (s - p) \in \alpha + \beta$, tehát (2) teljesül. Válasszuk most

r -hez az $s \in \alpha$ elemet úgy, hogy $s > p$ teljesüljön. Ekkor $s + q > r$ és $s + q \in \alpha + \beta$, tehát (3) is teljesül.

Másodszor vegyük észre, hogy az összeadás kommutatív és asszociatív, és mutassuk meg, hogy 0^* nullelem. Ha $r \in \alpha$ és $s \in 0^*$, akkor $r + s < r$, így $r + s \in \alpha$, tehát $\alpha + 0^* \subset \alpha$. A másik irányú tartalmazás bizonyításához válasszunk egy tetszőleges $r \in \alpha$ elemet, és legyen $s \in \alpha$, $s > r$. Ekkor $r - s \in 0^*$ és $r = s + (r - s) \in \alpha + 0^*$. Ezzel beláttuk, hogy $\alpha + 0^* = \alpha$.

Harmadszor az additív inverz létezését mutatjuk meg. Legyen $\alpha \in \mathbb{R}$ rögzített, és legyen β azon $r \in \mathbb{Q}$ racionális számok halmaza, amelyekhez van olyan $p > 0$ racionális szám, hogy $-r - p \notin \alpha$, más szóval, amelyekhez van olyan $-r$ -nél kisebb racionális szám, amely nincs α -ban. Megmutatjuk, hogy $\beta \in \mathbb{R}$ és $\alpha + \beta = 0^*$. Ha $s \notin \alpha$ és $r = -s - 1$, akkor $s = -r - 1 \notin \alpha$, így $r \in \beta$, tehát β nem üres. Ha $r \in \alpha$, akkor $-r \notin \beta$, így $\beta \neq \mathbb{Q}$. Ezért β -ra teljesül (1). Legyen $r \in \beta$ tetszőleges, és válasszuk meg a $p > 0$ elemet úgy, hogy $-r - p \notin \alpha$ teljesüljön. Ha $s < r$, akkor $-s - p > -r - p$, így $-s - p \notin \alpha$. Tehát $s \in \beta$, és (2) teljesül. Legyen most $s = r + p/2$. Ekkor $s > r$, és $-s - p/2 = -r - p \notin \alpha$, így $s \in \beta$. Tehát (3) is teljesül β -ra, amivel beláttuk, hogy $\beta \in \mathbb{R}$. Ha $r \in \alpha$ és $s \in \beta$, akkor van olyan p pozitív racionális szám, hogy $-s - p \notin \alpha$, ahonnan $-s \notin \alpha$, ezért $r < -s$, azaz $r + s < 0$. Tehát $\alpha + \beta \subset 0^*$. Az ellenkező irányú tartalmazás bizonyításához legyen $r \in 0^*$, és legyen $p = -r/2$. Ekkor $p > 0$, és van olyan n egész, amelyre $np \in \alpha$, de $(n+1)p \notin \alpha$. (Itt az arkhimédészi tulajdonságot használtuk ki.) Legyen $s = -(n+2)p$. Most $s \in \beta$, hiszen $-s - p \notin \alpha$, és $r = np + s \in \alpha + \beta$. Tehát $0^* \subset \alpha + \beta$. Ezzel beláttuk, hogy $\alpha + \beta = 0^*$.

Az összeadás monotonitása nyilvánvaló a rendezés és az összeadás definíciójából.

V. A szorzás némileg nehezebben kezelhető, mint az összeadás, mert szeleteket elemenként összeszorozva nem kapunk szeletet. Ezért először azoknak az α szeleteknek a halmazára szorítkozunk, amelyekre $\alpha > 0^*$. Ha $\alpha > 0^*$ és $\beta > 0^*$, akkor legyen definíció szerint $\alpha\beta$ azon r racionális számok halmaza, amelyekhez vannak olyan $p \in \alpha$ és $q \in \beta$ pozitív racionális számok, hogy $r \leq pq$. Ezzel a definícióval pozitív szeletek szorzata is szelet, és a pozitív szeletek szorzása kommutatív, asszociatív, disztributív, 1^* egységelem, és erre vonatkozóan minden pozitív szeletnek van (pozitív) inverze: ezen tulajdonságok bizonyítása hasonló a IV. pont bizonyításaihoz. Figyeljük meg, hogy az is teljesül, hogy ha $\alpha > 0^*$ és $\beta > 0^*$, akkor $\alpha\beta > 0^*$, azaz teljesül a szorzás monotonitása.

VI. A szorzás definícióját a következőképpen tesszük teljessé: legyen $\alpha 0^* = 0^* \alpha = 0^*$, továbbá

$$\alpha\beta = \begin{cases} (-\alpha)(-\beta), & \text{ha } \alpha < 0^*, \beta < 0^*, \\ -((-\alpha)\beta), & \text{ha } \alpha < 0^*, \beta > 0^*, \\ -(\alpha(-\beta)), & \text{ha } \alpha > 0^*, \beta < 0^*. \end{cases}$$

A definíció alapján a szorzás tulajdonságai és a disztributivitás esetszétválasztással beláthatók.

VII. Végül vegyük észre, hogy a racionális számokat beágyazva $\mathbb{R}$ -be, nullához a nullelem, azaz 0^* , 1-hez az egységelem, azaz 1^* rendelődik, és egy $r = m/n$, $m, n \in \mathbb{Z}$, $n \neq 0$ racionális számhoz az $(m1^*)/(n1^*)$ szelet, ami nem más, mint r^* . $\square$

* **3.3.12. A valós számok más bevezetései.** Némely könyv a rendezett test fogalmát a nemnegatív elemek kijelölése segítségével definiálja: egy F test rendezett test, ha adott egy olyan P részhalmaza, a *nemnegatív elemek halmaza*, amelyből nem vezet ki az

összeadás és a szorzás, és amelyre $F = P \cup (-P)$, $P \cap (-P) = \{0\}$. Könnyű látni, hogy ez a definíció ekvivalens az itt szereplővel.

A valós számok rendezett teste rendelkezik az alábbi *intervallumskatulyázási tulajdonsággal*: ha a_n, b_n , $n = 1, 2, \dots$ valós számsorozatok, $a_n < b_n$, $a_n \leq a_{n+1}$ és $b_n \geq b_{n+1}$, ha $n = 1, 2, \dots$ akkor $\bigcap_{n=1}^{\infty} [a_n, b_n] \neq \emptyset$. (Lásd Rudin [75] könyvét: 2.38 tétel.) Továbbá, a valós számok rendezett teste teljes: benne minden *Cauchy-sorozat* konvergens. (Lásd Rudin [75] könyvét: 3.11 tétel és 3.12 definíció.)

A valós számok teste ezen tulajdonságok segítségével is definiálható: vagy mint olyan arkhimédészien rendezett test, amely rendelkezik az intervallumskatulyázási tulajdonsággal (lásd a Leindler–Schip [60] jegyzetet; ekkor a felső határ tulajdonság és a teljesség tételek), vagy mint olyan arkhimédészien rendezett test, amely teljes (lásd a Hewitt–Stromberg [38] könyvet; ekkor a felső határ tulajdonság és az intervallumskatulyázási tulajdonság tételek). Ezekben az esetekben a valós számok halmazát mint a racionális számok Cauchy-sorozatának ekvivalenciaosztályait szokás definiálni. Ennek a felépítésnek a részletes tárgyalását lásd a Hewitt–Stromberg [38] könyvben.

3.3.13. Tétel: gyökvonás. Minden $x \geq 0$ valós számhoz és $n \in \mathbb{N}^+$ természetes számhoz pontosan egy olyan $y \geq 0$ valós szám található, amelyre $y^n = x$.

Az y számot az x szám n -edik gyökének nevezzük és $\sqrt[n]{x}$ -el ($n = 2$ esetén $\sqrt{x}$ -el is) vagy $x^{1/n}$ -el jelöljük.

* **Bizonyítás.** Világos, hogy legfeljebb egy ilyen y létezik, hiszen $y_1 < y_2$ esetén $y_1^n < y_2^n$. Ha $x = 0$, akkor $y = 0$. Legyen E azoknak a t pozitív valós számoknak a halmaza, amelyekre $t^n < x$. Ha $t = x/(1+x)$, akkor $0 < t < 1$, így $t^n \leq t < x$, így E nem üres. Ha $t > 1+x$, akkor $t^n \geq t > 1+x$, így $1+x$ az E felső korlátja. Legyen $y = \sup E$. Meg fogjuk mutatni, hogy $y^n = x$. A bizonyítás indirekt: megmutatjuk, hogy az $y^n < x$ és $y^n > x$ egyenlőtlenségek mindegyike ellentmondásra vezet.

A

$$b^n - a^n = (b-a)(b^{n-1} + b^{n-2}a + \dots + a^{n-1})$$

azonosság alapján $b^n - a^n \leq (b-a)nb^{n-1}$, ha $0 < a < b$.

Tegyük fel, hogy $y^n < x$. Válasszunk olyan h számot, amelyre $0 < h < 1$ és

$$h < \frac{x - y^n}{n(y+1)^{n-1}}.$$

Legyen $a = y$, $b = y + h$. Ekkor

$$(y+h)^n - y^n \leq hn(y+h)^{n-1} \leq hn(y+1)^{n-1} < x - y^n,$$

így $(y+h)^n < x$, és ezért $y+h \in E$. Ez ellentmond y felső határ voltának.

Tegyük fel, hogy $y^n > x$. Legyen

$$k = \frac{y^n - x}{ny^{n-1}}.$$

Ekkor $0 < k < y$. Ha $t \geq y - k$, akkor

$$y^n - t^n \leq y^n - (y-k)^n \leq kny^{n-1} = y^n - x,$$

így $t^n \geq x$, és $t \notin E$. Így $y - k$ az E egy felső korlátja. Ez ellentmond y felső határ voltának. $\square$

3.3.14. Következmény. Ha a és b nemnegatív valós számok és $n \in \mathbb{N}^+$, akkor $\sqrt[n]{ab} = \sqrt[n]{a} \sqrt[n]{b}$.

Bizonyítás. Legyen $\alpha = \sqrt[n]{a}$ és $\beta = \sqrt[n]{b}$. Ekkor $(\alpha\beta)^n = ab$, így az egyértelműségből következik az állítás. $\square$

*** 3.3.15. A természetes, az egész és a racionális számok bevezetése a valós számok segítségével.** Az $x^+ := x + 1$, ha $x \in \mathbb{R}$ jelöléssel, jelölje $\mathbb{N}$ az $\mathbb{R}$ mindazon N részhalmainak a metszetét, amelyek rendelkeznek az alábbi két tulajdonsággal:

- (1) $0 \in N$;
- (2) ha $n \in N$, akkor $n^+ \in N$.

Az $\mathbb{N}$ halmaz elemeit *természetes számoknak* nevezzük. (Vannak, akik a természetes számokat 1-gyel kezdik.)

Megmutatjuk, hogy $\mathbb{N}$ rendelkezik az alábbi tulajdonságokkal, amelyeket történeti okokból *Peano-axiómáknak* nevezzük:

- (1) $0 \in \mathbb{N}$;
- (2) ha $n \in \mathbb{N}$, akkor $n^+ \in \mathbb{N}$;
- (3) ha $n \in \mathbb{N}$, akkor $n^+ \neq 0$;
- (4) ha $n, m \in \mathbb{N}$ és $n^+ = m^+$, akkor $n = m$;
- (5) ha $S \subset \mathbb{N}$, $0 \in S$ és $n \in S$ esetén $n^+ \in S$, akkor $S = \mathbb{N}$.

Mivel $\mathbb{N}$ olyan halmazok metszete, amelyek rendelkeznek az (1) és (2) tulajdonságokkal, $\mathbb{N}$ is rendelkezik ezekkel a tulajdonságokkal, így (P1) és (P2) teljesül. (P5) a *matematikai indukció elve* vagy röviden az *indukció elve* (a *teljes indukció elve* elnevezés is használatos, de mi ezt szűkebb értelemben fogjuk használni); abból következik, hogy az S halmaz rendelkezik az (1) és (2) tulajdonságokkal, így $\mathbb{N} \subset S$. (P4) következik az egyszerűsítési szabályból. Végül (P3) fennállását (P5) segítségével bizonyítjuk. (Az ilyen bizonyításokat *matematikai indukcióval* vagy röviden *indukcióval* való bizonyításoknak szokás nevezni, és nagyon gyakran szerepelnek természetes számokra vonatkozó állítások bizonyításánál.) Legyen $S = \{n \in \mathbb{N} : n^+ > 0\}$. Nyilván $0 \in S$, és ha $n \in S$, akkor $(n^+)^+ > 0 + 1 > 0$, így $n^+ \in S$. Innen (P5) miatt $S = \mathbb{N}$, azaz teljesül (P3).

Megjegyezzük, hogy ha $m, n \in \mathbb{N}$, akkor (n szerinti indukcióval) $m + n \in \mathbb{N}$. Hasonlóan, mivel $mn^+ = mn + m$, az n szerinti indukcióval kapjuk, hogy $mn \in \mathbb{N}$, ha $m, n \in \mathbb{N}$. Ugyancsak n szerinti indukcióval, ha $m, n \in \mathbb{N}$ és $m \leq n$, akkor $n - m \in \mathbb{N}$.

A természetes számok körében az összeadásra nézve csak a 0-nak van inverze, másrészt szólva, a kivonás általában nem végezhető el. Ez indokolta az egész számok bevezetését. A $\mathbb{Z} = -\mathbb{N} \cup \mathbb{N} \subset \mathbb{R}$ halmaz elemeit *egész számoknak* nevezzük. A definíció alapján adódik, hogy $\mathbb{Z}$ -ből nem vezet ki az összeadás és az additív inverz képzése, az előjelszabály alapján pedig, hogy a szorzás sem.

Az egész számok körében a nem nulla elemek közül csak 1-nek és -1 -nek van multiplikatív inverze, másképp szólva, az osztás általában nem végezhető el. Ez indokolta a racionális számok bevezetését. A $\mathbb{Q} = \{m/n \in \mathbb{R} : m, n \in \mathbb{Z}, n \neq 0\}$ halmaz elemeit *racionális számoknak* nevezzük; $\mathbb{R} \setminus \mathbb{Q}$ elemeit *irracionális számoknak* szokás nevezni. A racionális számok rendezett testet alkotnak: $0 = 0/1 \in \mathbb{Q}$, $1 = 1/1 \in \mathbb{Q}$, ha $m/n \in \mathbb{Q}$ és $m'/n' \in \mathbb{Q}$, akkor $(-m)/n = -m/n \in \mathbb{Q}$, $m/n + m'/n' = (mn' + m'n)/(nn') \in \mathbb{Q}$ és $(m/n)(m'/n') = (mm')/(nn') \in \mathbb{Q}$, valamint ha $0 \neq m/n$, akkor $m \neq 0$, így $1/(m/n) = n/m \in \mathbb{Q}$.

→ **3.3.16. Feladat [4].** Bizonyítsuk be, hogy ha $x \in \mathbb{R}$ racionális, $y \in \mathbb{R}$ pedig irracionális, akkor $x + y$ irracionális. Igaz-e, hogy irracionálisok összege irracionális?

→ **3.3.17. Feladat [4].** Bizonyítsuk be, hogy ha $0 \neq x \in \mathbb{R}$ racionális, $y \in \mathbb{R}$ pedig irracionális, akkor xy irracionális. Igaz-e, hogy irracionálisok szorzata irracionális?

3.3.18. Feladat [6]. Bizonyítsuk be, hogy ha $a, b \in \mathbb{R}$, $a < b$ akkor van köztük racionális és irracionális szám is.

3.3.19. Feladat [6]. Bizonyítsuk be, hogy ha $n \in \mathbb{N}$, akkor $\sqrt{n}$ vagy egész, vagy irracionális.

3.3.20. Feladat [6]. Bizonyítsuk be, hogy $\sqrt{2} + \sqrt{3}$ irracionális.

3.3.21. Feladat [7]. Bizonyítsuk be, hogy ha $n, k \in \mathbb{N}^+$, akkor $\sqrt[k]{n}$ vagy egész, vagy irracionális.

→ **3.3.22. Feladat [3].** Bizonyítsuk be, hogy $\{p + q\sqrt{2}: p, q \in \mathbb{Q}\}$ test a valós számok szokásos műveleteivel.

3.3.23. Feladat [6]. Bizonyítsuk be, hogy $\sqrt[3]{2} \notin \{p + q\sqrt{2}: p, q \in \mathbb{Q}\}$.

3.3.24. Feladat [8]. Bizonyítsuk be, hogy $\{p + q\sqrt{2} + r\sqrt{3} + s\sqrt{6}: p, q, r, s \in \mathbb{Q}\}$ test a valós számok szokásos műveleteivel.

3.3.25. Feladat [8]. Bizonyítsuk be, hogy ha a, b pozitív racionális számok, akkor $\{p + q\sqrt{a} + r\sqrt{b} + s\sqrt{ab}: p, q, r, s \in \mathbb{Q}\}$ test a valós számok szokásos műveleteivel. Általánosítsuk az állítást akárhány pozitív racionális számra.

→ **3.3.26. Feladat [3].** Bizonyítsuk be, hogy ha $a, b \in \mathbb{R}$, akkor

$$\max\{a, b\} = \frac{|a - b| + a + b}{2}, \quad \min\{a, b\} = \frac{-|a - b| + a + b}{2}.$$

→ **3.3.27. Feladat [0].** Határozzuk meg az alábbi maradékok értékét:

- (1) $100 \bmod 3$;
- (2) $100 \bmod 7$;
- (3) $(-100) \bmod 7$;
- (4) $(-100) \bmod 0$;
- (5) $5 \bmod -3$;
- (6) $18 \bmod -3$;
- (7) $(-2) \bmod -3$;
- (8) $1,1 \bmod 1$;
- (9) $0,11 \bmod 0,1$;
- (10) $0,11 \bmod -0,1$.

→ **3.3.28. Feladat [1].** Bizonyítsuk be, hogy ha $x \in \mathbb{R}$, $n \in \mathbb{Z}$, akkor

- (1) $\lfloor x \rfloor < n$ pontosan akkor, ha $x < n$;
- (2) $n \leq \lfloor x \rfloor$ pontosan akkor, ha $n \leq x$;

- (3) $\lceil x \rceil \leq n$ pontosan akkor, ha $x \leq n$;
- (4) $n < \lceil x \rceil$ pontosan akkor, ha $n < x$;
- (5) $\lfloor x \rfloor = n$ pontosan akkor, ha $x - 1 < n \leq x$;
- (6) $\lfloor x \rfloor = n$ pontosan akkor, ha $n \leq x < n + 1$;
- (7) $\lceil x \rceil = n$ pontosan akkor, ha $x \leq n < x + 1$;
- (8) $\lceil x \rceil = n$ pontosan akkor, ha $n - 1 < x \leq n$.

→ **3.3.29. Feladat [3].** A modern processzorokban négyféle egészre kerekítési mód állítható be (az *IEEE 754* szabvány szerint): $+\infty$ felé, $-\infty$ felé, 0 felé, és a legközelebbi egészre (ha két ilyen van, akkor a párosra). Írjuk fel adott x valós számra mindegyiknek az eredményét a tanult jelölésekkel.

→ **3.3.30. Feladat [4].** Mely összefüggések teljesülnek az alábbiak közül bármely $x \in \mathbb{R}^+$ -ra:

- (1) $\lfloor \sqrt{\lceil x \rceil} \rfloor = \lfloor \sqrt{x} \rfloor$;
- (2) $\lceil \sqrt{\lceil x \rceil} \rceil = \lceil \sqrt{x} \rceil$;
- (3) $\lceil \sqrt{\lfloor x \rfloor} \rceil = \lceil \sqrt{x} \rceil$.

3.3.31. Feladat [4]. Mutassuk meg, hogy minden $x, y \in \mathbb{R}$ -re $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$ és egyenlőség pontosan akkor teljesül, ha $x \bmod 1 + y \bmod 1 < 1$. Teljesül-e hasonló összefüggés a felső egész részre?

3.3.32. Feladat [4]. Mutassuk meg, hogy ha az $m \in \mathbb{N}^+$ számot q alapú számrendszerben írjuk fel, ahol $q \in \mathbb{N}$, $q > 1$, akkor q^j együtthatója $\lfloor m/q^j \rfloor - q\lfloor m/q^{j+1} \rfloor$, ha $j \in \mathbb{N}$.

3.3.33. Feladat [9]. Mutassuk meg, hogy

- (1) minden $n \in \mathbb{N}^+$ -ra $\lfloor \sqrt{n} + \sqrt{n+1} \rfloor = \lfloor \sqrt{n} + \sqrt{n+2} \rfloor$;
- (2) van olyan $n \in \mathbb{N}^+$, amelyre $\lfloor \sqrt[3]{n} + \sqrt[3]{n+1} \rfloor \neq \lfloor \sqrt[3]{n} + \sqrt[3]{n+2} \rfloor$.

3.3.34. Feladat: öröknaptár [8]. Mutassuk meg, hogy ha d, m és y rendre a nap, hónap és év, akkor az 1582. évet követő időpontokra (azóta használatos a Gergely-naptár)

- (1) $h = [y \bmod 4 = 0] - [y \bmod 100 = 0] + [y \bmod 400 = 0]$ szökőév esetén 1, egyébként 0;
- (2) $x = (d + [2,6n - 0,2] + r + [r/4] + [h/4] - 2h - (1+s)[n/11]) \bmod 7$ vasárnap 0, hétfőn 1, stb., szombaton 6; itt $h = [y/100]$ az év „évszázad-része”, $r = y \bmod 100$ pedig a maradék része, $n = 1 + ((m - 3) \bmod 12)$ pedig a hónap „módosított sorszáma”, márciust véve elsőnek (mert február a szökőhónap).

3.3.35. Feladat [4]. Határozzuk meg az alábbi feltételt kielégítő valós számok halmazát:

- (1) $|x + 1| < 1/4$;
- (2) $|x - 2| > 5$;
- (3) $|x| > |x - 1|$;
- (4) $|2x - 1| < |x - 1|$;

$$(5) \quad |x+2| + |x-2| \leq 12;$$

$$(6) \quad |x+2| - |x| > 1;$$

$$(7) \quad ||x+1| - |x-1|| < 1;$$

$$(8) \quad |x(1-x)| < 3.$$

→ **3.3.36. Feladat [4].** Határozzuk meg az alábbi valós számhalmazok felső és alsó határát, minimumát és maximumát, ha létezik:

$$(1) \quad \{1/n: n \in \mathbb{N}^+\};$$

$$(2) \quad \{x \in \mathbb{Q}: -1 < x < 1\};$$

$$(3) \quad \{x \in \mathbb{R}: -\sqrt{2} \leq x \leq \sqrt{2}\};$$

$$(4) \quad \{(-1)^n/n: n \in \mathbb{N}^+\};$$

$$(5) \quad \{(-1)^n + 1/n: n \in \mathbb{N}^+\};$$

$$(6) \quad \{1/2^n + 1/2^m: n, m \in \mathbb{N}^+\}.$$

→ **3.3.37. Feladat [4].** Bizonyítsuk be, hogy egy rendezett test pontosan akkor felső határ tulajdonságú, ha alsó határ tulajdonságú, azaz ha minden nem üres alulról korlátos részhalmazának van legnagyobb eleme, továbbá A pontosan akkor felülről korlátos, ha $-A$ alulról korlátos, és ekkor $\inf(-A) = -\sup A$, valamint ha értelmezve van $\max A$, akkor $\min(-A)$ is és $\min(-A) = -\max A$.

3.3.38. Feladat [4]. Legyenek $A, B \subset \mathbb{R}$ nem diszjunkt halmazok. Mit tudunk mondani $\sup A$, $\sup B$, $\sup(A \cup B)$ és $\sup(A \cap B)$ kapcsolatáról?

3.3.39. Feladat [4]. Legyenek $A, B \subset \mathbb{R}$ nem üres halmazok. Mutassuk meg, hogy $\sup(A + B) = \sup A + \sup B$ és $\inf(A + B) = \inf A + \inf B$.

3.3.40. Feladat [4]. Legyenek $A, B \subset \mathbb{R}$ nem üres halmazok. Mit tudunk mondani $\sup A$, $\sup B$, $\inf A$, $\inf B$ és $\sup(AB)$, $\inf(AB)$ kapcsolatáról? És ha feltesszük, hogy $A, B \subset \mathbb{R}^+$?

3.3.41. Feladat [4]. Legyen $A \subset \mathbb{R}$ nem üres halmaz. Mit tudunk mondani $\sup A$, $\inf A$ és $\sup(1/A)$, $\inf(1/A)$ kapcsolatáról?

3.3.42. Feladat [4]. Legyen X nem üres halmaz, $f, g: X \rightarrow \mathbb{R}$ függvények. Mutassuk meg, hogy ha $f(X)$ és $g(X)$ felülről korlátosak, akkor $f+g$ értékkészlete is felülről korlátos, és $\sup f(X) + \sup g(X) \geq \sup(f+g)(X)$, valamint ha $f(X)$ és $g(X)$ alulról korlátosak, akkor $f+g$ értékkészlete is alulról korlátos, és $\inf f(X) + \inf g(X) \leq \inf(f+g)(X)$. Mutassunk példát, amikor nem teljesül egyenlőség.

3.3.43. Feladat [4]. Legyen X nem üres halmaz, $f, g: X \rightarrow \mathbb{R}^+$ függvények. Mutassuk meg, hogy $\inf f(X) \inf g(X) \leq \inf(fg)(X)$, és $\sup f(X) \sup g(X) \geq \sup(fg)(X)$. Mutassunk példát, amikor nem teljesül egyenlőség.

3.3.44. Feladat [6]. Legyen X nem üres halmaz, $f, g: X \rightarrow \mathbb{R}$ függvények. Mit tudunk mondani $\inf f(X)$, $\inf g(X)$, $\sup f(X)$ és $\sup g(X)$ valamint az $\inf(fg)(X)$, $\sup(fg)(X)$, $\inf(1/g)(X)$ és $\sup(1/g)(X)$ kapcsolatáról?

3.3.45. Feladat [4]. Legyen A_i , $i \in I$ az $\mathbb{R}$ felülről korlátos, nem üres részhalmazainak egy nem üres családja. Mutassuk meg, hogy $\cup_{i \in I} A_i$ pontosan akkor felülről korlátos, ha a $B = \{\sup A_i: i \in I$ halmaz felülről korlátos, és ekkor $\sup A = \sup B$.

3.3.46. Feladat [7]. Ellenőrizzük, hogy a pozitív valós számok halmaza Abel-csoport az $(a, b) \rightarrow a \cdot b$ művelettel. Mi lesz a semleges elem? Adjunk meg ehhez az „összeadáshoz” olyan szorzást, amellyel testet kapunk.

3.3.47. Feladat [9]. Ellenőrizzük, hogy a pozitív racionális számok halmaza Abel-csoport az $(a, b) \rightarrow a \cdot b$ művelettel. Mi lesz a semleges elem? Bizonyítsuk be, hogy ehhez az „összeadáshoz” nincs olyan szorzás, amellyel testet kapunk.

* **3.3.48. Feladat [6].** Bizonyítsuk be az intervallumskatulyázási „axiómát” $\mathbb{R}$ általunk megadott definíciójából.

3.3.49. Feladat [6]. Az intervallumskatulyázási axiómában megköveteljük, hogy az egymásba skatulyázott intervallumok zártak, korlátosak és nem üresek. Mutassuk meg ellenpéldákkal, hogy az állítás nem marad igaz, ha bármelyik feltételt elhagyjuk.

* **3.3.50. Feladat [12].** Tekintsük $\mathbb{Q}(x)$ -et azzal a rendezéssel, amelyben $r > s$, ha $r - s$ számlálójának és nevezőjének főegyütthatója azonos előjelű. Ellenőrizzük, hogy $\mathbb{Q}(x)$ rendezett test. Mutassuk meg, hogy nem arkhimédészien rendezett. Mutassuk meg, hogy nem teljesül az intervallumskatulyázási tulajdonság.

3.3.51. További feladatok. [69]: 4.1.3, 4.1.4, 4.1.6–4.1.8, 4.1.10, 4.1.15, 4.1.16, 4.1.18, 4.1.22, 4.1.24;

3.4 Komplex számok

A görög matematikán, amelynek szabatosága a tudományok mintájául szolgált (Eukleidész műve 2000 évig volt tankönyv!), először a reneszánsz számolóművészeinek sikerült túllépniük, amikor Scipione del Ferro és Niccolo Fontana „Tartaglia” harmadfokú egyenleteket oldottak meg. Felfedezéseiket Gerolamo Cardano és tanítványa, Lodovico Ferrari fejlesztették tovább, megtalálva az általános harmad- és negyedfokú egyenletek megoldásának módját. Éppen olyan esetekben azonban, amikor három különböző valós gyöke van egy harmadfokú egyenletnek, a Cardano-képletben a négyzetgyökkel alatt negatív szám szerepelt, és így nem adta meg a megoldást: ez a „casus irreducibilis”. Észrevették azonban, hogy negatív számok négyzetgyökeire is bevezethetők megfelelő számolási szabályok. Fokozatosan tisztázódtak a „képzetes” számokkal való számolás szabályai, és a trigonometrikus függvényekkel való kapcsolat. A komplex számok fogalmát Carl Friedrich Gauss tisztázta véglegesen, és ezután bebizonyította az algebra alaptételét.

3.4.1. Komplex számok. A *komplex számok* halmaza $\mathbb{C} = \mathbb{R} \times \mathbb{R}$, azaz a valós számpárok halmaza, az $(x, y) + (x', y') = (x + x', y + y')$ összeadással és az $(x, y) \cdot (x', y') = (xx' - yy', yx' + yy')$ szorzással mint műveletekkel. Egyszerű számolás mutatja, hogy $\mathbb{C}$ test a fenti műveletekkel: a nullelem a $(0, 0)$ pár, az (x, y) pár additív inverze a $(-x, -y)$ pár, egységelem az $(1, 0)$ pár, és a nullelemtől különböző (x, y) pár multiplikatív inverze az $(x/(x^2 + y^2), -y/(x^2 + y^2))$ pár. Vegyük észre, hogy ha $x, x' \in \mathbb{R}$, akkor $(x, 0) + (x', 0) = (x + x', 0)$, $(x, 0) \cdot (x', 0) = (xx', 0)$, így az $x \mapsto (x, 0)$ leképezés kölcsönösen egyértelmű, összeadás- és szorzástartó leképezése $\mathbb{R}$ -nek $\mathbb{C}$ -be, ezért az összes $(x, 0)$, $x \in \mathbb{R}$ alakú komplex számok halmazát azonosítjuk $\mathbb{R}$ -rel.

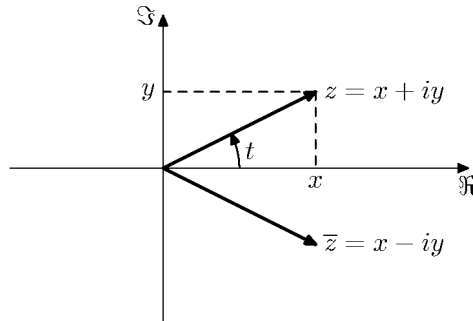
Jelölje i a $(0, 1)$ komplex számot (villamosmérnökök ezt a számot j -vel jelölik). Vegyük észre, hogy $i^2 = -1$, az i segítségével az (x, y) komplex számot $x + iy$ alakban

írhatjuk, és ez a felírás természetesen egyértelmű. Ezt a szám *algebrai alakjának* nevezzük. Ha $z = x + iy \in \mathbb{C}$, ahol $x, y \in \mathbb{R}$, akkor x -et a z *valós részének*, az y -t pedig a z *képzetes részének* nevezzük. Jelölésük: $\Re(z)$, illetve $\Im(z)$ (vagy $\operatorname{Re}(z)$, illetve $\operatorname{Im}(z)$). A z *konjugáltja* a $\bar{z} = x - iy$ komplex szám. Egy komplex szám pontosan akkor valós, ha megegyezik a konjugáltjával. Ha egy komplex szám valós része nulla, akkor *képzetesnek* nevezzük.

A definíció alapján azonnal következnek a $\bar{\bar{z}} = z$, $\overline{z+w} = \bar{z} + \bar{w}$, $\overline{zw} = \bar{z}\bar{w}$, $1/\bar{z} = 1/\overline{z}$, $z + \bar{z} = 2\Re(z)$, $z - \bar{z} = 2i\Im(z)$ összefüggések.

Megjegyezzük, hogy nincs olyan rendezés, amellyel a komplex számok teste rendezett test lenne, mert rendezett testben $1 > 0$ és $-1 < 0$, és $\mathbb{C}$ -ben $i^2 = -1$, ami ellentmond annak, hogy rendezett testben minden nem nulla elem négyzete pozitív.

Néha szükségünk van a *bővített komplex számok* $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ halmazára. A ∞ szimbólumot számítógépen például a $(+\infty, +\infty)$ párként ábrázolhatjuk.



3.4.1 ábra: Komplex szám, valós és képzetes rész, konjugált, argumentum.

3.4.2. Példa. A $z = 64/(\sqrt{3}+i)$ komplex szám algebrai alakját a nevező konjugáltjával való bővítéssel kapjuk:

$$z = \frac{64}{\sqrt{3}+i} \cdot \frac{\sqrt{3}-i}{\sqrt{3}-i} = \frac{64 \cdot (\sqrt{3}-i)}{3+1} = 16\sqrt{3} - 16i.$$

Innen a z valós része $\Re(z) = 16\sqrt{3}$, képzetes része $\Im(z) = -16$, konjugáltja $16\sqrt{3} + 16i$.

3.4.3. Komplex szám abszolút értéke. A komplex számok a sík pontjainak, vagyis az origóból kiinduló vektoroknak is tekinthetők. A komplex számok összeadása megfelel a vektorok szokásos összeadásának. Egy komplex szám abszolút értéke ennek a vektornak a hossza: legyen az $(x, y) \in \mathbb{R} \times \mathbb{R}$ komplex szám *abszolút értéke* $|(x, y)| = \sqrt{x^2 + y^2}$. (Ezzel a jelöléssel $z\bar{z} = |z|^2$, és így $1/z = \bar{z}/|z|^2$, ha $0 \neq z \in \mathbb{C}$.) A valós számokra a szokásos abszolút értéket kapjuk vissza: $|(x, 0)| = |x|$. Nyilván $|0| = 0$ és $z \neq 0$ esetén $|z| > 0$, $|\bar{z}| = |z|$, $|zw| = |z||w|$ (mert mindkét oldal négyzete ugyanannyi), $|\Re(z)| \leq |z|$ és $|\Im(z)| \leq |z|$. Teljesül a $|z+w| \leq |z| + |w|$ *háromszög-egyenlőtlenség* is:

$$\begin{aligned} |z+w|^2 &= (z+w)\overline{(z+w)} = (z+w)(\bar{z}+\bar{w}) = z\bar{z} + z\bar{w} + w\bar{z} + w\bar{w} \\ &= z\bar{z} + z\bar{w} + \overline{z\bar{w}} + w\bar{w} = |z|^2 + 2\Re(z\bar{w}) + |w|^2 \\ &\leq |z|^2 + 2|z\bar{w}| + |w|^2 = |z|^2 + 2|z||w| + |w|^2 = (|z| + |w|)^2, \end{aligned}$$

ahonnan négyzetgyökvonással következik az egyenlőtlenség. A háromszög-egyenlőtlenség-ből $||z| - |w|| \leq |z - w|$ minden $z, w \in \mathbb{C}$ -re, ugyanis egyrészt $|z| \leq |z - w| + |w|$, ahonnan $|z| - |w| \leq |z - w|$, másrészt z és w szerepét felcserélve $|w| - |z| \leq |z - w|$.

Legyen $\operatorname{sgn}(0) = 0$, és legyen $\operatorname{sgn}(z) = z/|z|$, ha $0 \neq z \in \mathbb{C}$. Nyilván $\operatorname{sgn}(\bar{z}) = \overline{\operatorname{sgn}(z)}$ és $|\operatorname{sgn}(z)| = 1$, ha $z \neq 0$. A valós számokra visszakapjuk az ott definiált sgn függvényt.

→ **3.4.4. Feladat [3].** Bizonyítsuk be, hogy tetszőleges $z_1, z_2, \dots, z_n$ komplex számokra $|z_1 + z_2 + \dots + z_n| \leq |z_1| + |z_2| + \dots + |z_n|$.

→ **3.4.5. Feladat [3].** Bizonyítsuk be, hogy tetszőleges z, w komplex számokra fennáll a *paralelogramma-azonosság*: $|z + w|^2 + |z - w|^2 = 2|z|^2 + 2|w|^2$. Honnan eredhet a neve?

→ **3.4.6. Feladat [6].** Hozzuk algebrai alakra:

$$\frac{2}{(1-i)(3+i)}, \quad \frac{1}{(3+4i)^2}, \quad \frac{2+i}{i(-3+4i)},$$

$$\frac{\sqrt{3}+i}{(1-i)(\sqrt{3}-i)}, \quad \frac{1}{i(3-2i)(1+i)}, \quad \frac{i}{(1-i)(1-2i)(1+2i)}.$$

→ **3.4.7. Feladat [6].** Ha $z = 1 - 5i$ és $w = 3 + 4i$, akkor mennyi z/w , $\bar{z}/w$, $z/\bar{w}$, $\bar{z}/\bar{w}$, $z/|w|$, $|z/w|$?

3.4.8. Feladat [6]. Ha $z = 1 + i$ és $w = 1 - 2i$, akkor mennyi $z - z/w$, $(z - 1)/w$, $z^2 - iz/w$, $z/(iw)$, $z/|w|$?

3.4.9. Feladat [6]. Legyen $z_1 = 2 + i$, $z_2 = 3 - 2i$ és $z_3 = -1/2 + \sqrt{3}i/2$. Mennyi $|3z_1 - 4z_2| + z_3\bar{z}_3$, $z_1^3 + 3z_1^2 + 4z_1 - 8$, $|(2z_2 + z_1 - 5 - i)/(2z_1 - z_2 + 3 - i)|$?

° **3.4.10. Komplex szám argumentuma és trigonometrikus alakja.** A komplex számokat origóból kiinduló vektoroknak tekintve, a vektor koordinátái felírhatók a vektor hossza és a vektornak az „ x tengely pozitív felével” bezárt szöge, annak szinusza és koszinusza segítségével. Ennek az úgynevezett trigonometrikus alaknak (a geometriára való hivatkozás nélkül történő) bevezetéséhez fel fogjuk használni a $\cos$ és $\sin$ függvények, továbbá a π szám definícióját, és számos ezekre vonatkozó (a középiskolából ismert) összefüggést, amelyet az analízis tárgyalása során szokás bizonyítani.

Ha $0 \neq z \in \mathbb{C}$, akkor van olyan t valós szám, amelyre $\operatorname{sgn}(z) = \cos t + i \sin t$. Ha ez az összefüggés fennáll t -re, akkor a $t + 2k\pi$, $k \in \mathbb{Z}$ számokra is, és csak ezekre. Ekkor $z = |z|(\cos t + i \sin t)$, ez a komplex szám *trigonometrikus alakja*. Ha $z = 0$, akkor akármilyen $t \in \mathbb{R}$ választható. Ha $0 \neq z \in \mathbb{C}$, akkor legyen a z *argumentuma*, $\arg(z)$ az az egyetlen t valós szám, amelyre $-\pi < t \leq \pi$ és $\operatorname{sgn}(z) = \cos t + i \sin t$; ez az egyetlen t valós szám, amelyre $-\pi < t \leq \pi$ és $z = |z|(\cos t + i \sin t)$. Nyilván, ha $z = |z|(\cos t + i \sin t)$, akkor $\bar{z} = |z|(\cos t - i \sin t) = |z|(\cos(-t) + i \sin(-t))$, összhangban azzal a geometriai képpel, hogy $\bar{z}$ a z vektor „ x tengelyre” történő tükrözésével kapható.

Legyen $z, w \in \mathbb{C}$, $z = |z|(\cos t + i \sin t)$ és $w = |w|(\cos s + i \sin s)$, ahol $t, s \in \mathbb{R}$. Ekkor zw trigonometrikus alakja

$$\begin{aligned} zw &= |z| \cdot (\cos t + i \sin t) \cdot |w| \cdot (\cos s + i \sin s) \\ &= |z| \cdot |w| \cdot (\cos t + i \sin t) \cdot (\cos s + i \sin s) \\ &= |zw|(\cos t \cos s - \sin t \sin s + i(\cos t \sin s + \cos s \sin t)) \\ &= |zw|(\cos(t + s) + i \sin(t + s)). \end{aligned}$$

Ezt az összefüggést *Moivre-azonosságnak* nevezzük. Figyelembe véve, hogy ha $w \neq 0$, akkor $1/w = \overline{w}/|w|^2$, ebből

$$\frac{z}{w} = \frac{|z|}{|w|}(\cos(t-s) + i \sin(t-s)).$$

Ha tehát z, w nem nulla komplex számok, akkor zw argumentuma $\arg(z) + \arg(w)$, ha ez nagyobb, mint $-\pi$, de nem nagyobb, mint π . Ha $\arg(z) + \arg(w) \leq -\pi$, akkor $\arg(zw) = \arg(z) + \arg(w) + 2\pi$, ha pedig $\arg(z) + \arg(w) > \pi$, akkor $\arg(zw) = \arg(z) + \arg(w) - 2\pi$. Tehát a komplex számok szorzásának geometriai jelentése, hogy a hosszak összeszoródnak, az „ x tengely pozitív felével” bezárt szögek pedig összeadódnak. (A komplex számok osztásánál az eredmény hossza a hosszak hányadosa, az „ x tengely pozitív felével” bezárt szögek pedig kivonódnak.)

Indukcióval azt kapjuk, hogy $z^n = |z|^n(\cos(nt) + i \sin(nt))$, ha $n \in \mathbb{N}$; ha $z \neq 0$, akkor ez az összefüggés minden $n \in \mathbb{Z}$ -re teljesül.

3.4.11. Példa. $A z = 16\sqrt{3} - 16i$ komplex szám trigonometrikus alakja, mivel $|z| = \sqrt{16^2 \cdot 3 + 16^2} = 32$,

$$z = 16\sqrt{3} - 16i = 32 \left(\frac{\sqrt{3}}{2} - \frac{1}{2}i \right) = 32(\cos(-\pi/6) + i \sin(-\pi/6)).$$

° **3.4.12. Gyökvonás komplex számból.** Legyen $n \in \mathbb{N}^+$, és vizsgáljuk a $z \mapsto z^n$, $z \in \mathbb{C}$ hatványozás inverzét. Ha $n = 1$, akkor a $z \mapsto z$ az $\mathbb{C}$ identikus leképezés, és inverze saját maga. Ha $n > 1$, $z, w \in \mathbb{C}$ és $z^n = w$, akkor (indukcióval) $|w| = |z|^n$. Ebből $w = 0$ esetén $z = 0$. Egyébként, ha $t = \arg(w)$, akkor a

$$z_k = \sqrt[n]{|w|} \left(\cos\left(\frac{t + 2k\pi}{n}\right) + i \sin\left(\frac{t + 2k\pi}{n}\right) \right), \quad k = 0, 1, \dots, n-1$$

különböző komplex számok, és csak ezek azok, amelyeknek n -edik hatványa w . Vegyük észre, hogy ha $n = 2$, akkor $z_1 = -z_0$. Így tehát $n > 1$ esetén $z \mapsto z^n$ inverze nem függvény, de persze $\mathbb{C}$ -beli reláció. Néha mégis szokás az inverzet $\sqrt[n]{}$ -kel jelölni. Ezzel a jelöléssel $\sqrt[n]{0} = \{0\}$ és $\sqrt[n]{w} = \{z_k : k = 0, 1, \dots, n-1\}$; ha $n = 2$, akkor $\sqrt{w} = \{z_0, -z_0\}$. Mivel nagy a veszélye az (egyértelművé tett) valós gyökvonással való összetévesztésnek, ezt a jelölést a továbbiakban nem használjuk.

Speciálisan, ha $w = 1$, akkor az $\varepsilon^n = 1$ feltételnek az

$$\varepsilon_k = \cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right), \quad k = 0, 1, \dots, n-1$$

komplex számok tesznek eleget. Ezeket n -edik *komplex egységgyököknek* nevezzük, halmazukat $\mathbb{U}_n$ jelöli, a szorzással Abel-csoport. Bizonyos n -edik egységgyökök hatványaiként az összes többi előáll (például $\varepsilon_k = \varepsilon_1^k$, $k = 0, 1, \dots, n-1$), ezeket n -edik *primitív egységgyököknek* nevezzük. Az $\varepsilon_0 = 1$ nyilván nem n -edik primitív egységgyök, ha $n \neq 1$.

Ha $z^n = w$, akkor z és az n -edik komplex egységgyökök segítségével megkaphatjuk az összes komplex számot, amelyek n -edik hatványa w , ezek $z\varepsilon_0, z\varepsilon_1, \dots, z\varepsilon_{n-1}$. Innen

következik, hogy ha $n > 1$, akkor az összes olyan komplex számok összege, amelyek n -edik hatványa w , nulla. Valóban,

$$\sum_{k=0}^{n-1} z \varepsilon_k = \sum_{k=0}^{n-1} z \varepsilon_1^k = z \frac{\varepsilon_1^n - 1}{\varepsilon_1 - 1} = z \frac{1 - 1}{\varepsilon_1 - 1} = 0.$$

(Geometriailag, $2\pi/n$ -nel elforgatva a gyököket, az összegük is elfordul $2\pi/n$ -nel. Mivel a gyökök halmaza nem változik, $n > 1$ esetén ez csak úgy lehetséges, hogy az összeg nulla.)

Ugyanúgy, mint a valós esetben, beláthatjuk, hogy ha $a, b, c \in \mathbb{C}$, $a \neq 0$, akkor $az^2 + bz + c = 0$ pontosan akkor teljesül, ha

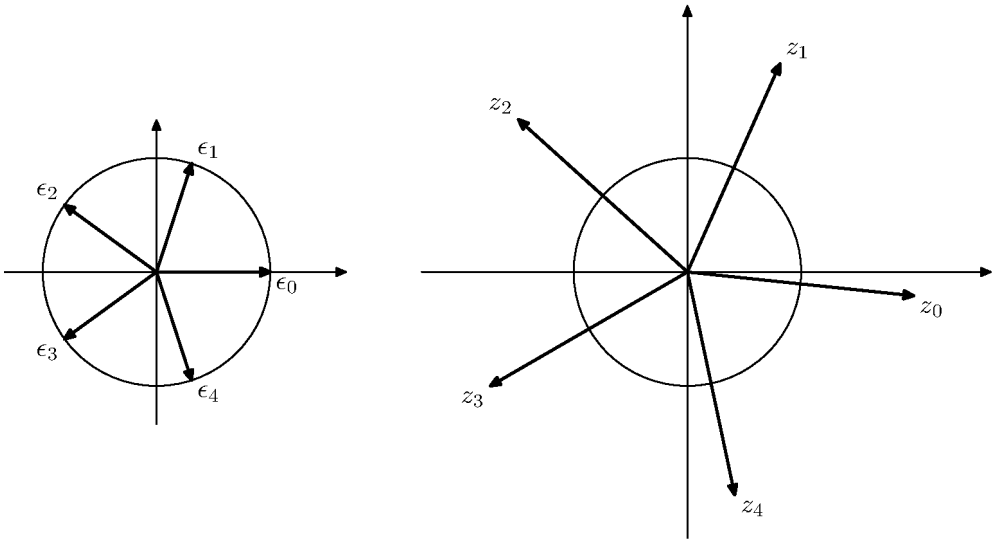
$$z = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

ahol $d \neq 0$ esetén $t = \arg(d)$ jelöléssel $\sqrt{d} = \sqrt{|d|}(\cos(t/2) + i \sin(t/2))$.

3.4.13. Példa. A $w = 16\sqrt{3} - 16i$ komplex szám trigonometrikus alakja $w = 32(\cos(-\pi/6) + i \sin(-\pi/6))$, így az ötödik gyökei a

$$z_k = 2(\cos(-\pi/30 + 2k\pi/5) + i \sin(-\pi/30 + 2k\pi/5)), \quad k = 0, 1, 2, 3, 4$$

komplex számok.



3.4.2 ábra: ötödik egységgyökök és $16\sqrt{3} - 16i$ ötödik gyökei.

3.4.14. Az algebra alaptétele. Ha $n \in \mathbb{N}^+$, valamint $c_0, c_1, \dots, c_n$ komplex számok, $c_n \neq 0$, akkor van olyan z komplex szám, amelyre $\sum_{k=0}^n c_k z^k = 0$.

Másként fogalmazva, minden legalább elsőfokú komplex együtthatós algebrai egyenletnek van komplex gyöke. A gyökökkel a polinomok tárgyalásánál foglalkozunk részletesebben.

Mivel a tétel valamennyi ismert bizonyítása az analízis eszközeit is felhasználja, az analízis tárgyalása során szokás bizonyítani (lásd például Rudin [75] könyvét, 8.8 tétel).

→ **3.4.15. Feladat [2].** Állítsuk elő trigonometrikus alakban az i , $\bar{i}$, $1 + i$, $1 + i\sqrt{3}$ és $\sqrt{3} - i$ komplex számokat.

→ **3.4.16. Feladat [2].** Határozzuk meg i és $-1 + i$ összes harmadik gyökét, valamint 64 és -64 összes hatodik gyökét.

→ **3.4.17. Feladat [6].** Legyen $w = u + iv$, $u, v \in \mathbb{R}$. Mutassuk meg, hogy ha

$$x = \sqrt{\frac{|w| + u}{2}}, \quad y = \sqrt{\frac{|w| - u}{2}},$$

akkor $z = x + iy$ -ra $v \geq 0$ esetén $z^2 = w$, ha pedig $v \leq 0$, akkor $\bar{z}^2 = w$.

3.4.18. Feladat [4]. Számítsuk ki az i , $\bar{i}$, $3 + 4i$ és $-7 + 24i$ komplex számok négyzetgyökeit.

3.4.19. Feladat [0]. Mi annak a szükséges és elégséges feltétele, hogy két komplex szám összege, illetve szorzata valós legyen?

3.4.20. Feladat [4]. Adjuk meg az alábbi komplex számokat algebrai alakban:

(1)

$$\frac{(1 + 2i)^2 - (1 - i)^3}{(3 + 2i)^3 - (2 + i)^2};$$

(2)

$$\frac{(1 - i)^5 - 1}{(1 + i)^5 + 1};$$

(3)

$$\frac{(1 + i)^9}{(1 - i)^7};$$

(4)

$$(1 + i)^{52};$$

(5)

$$\left(\frac{1 + i\sqrt{3}}{1 - i}\right)^{20}.$$

3.4.21. Feladat [3]. Számítsuk ki az alábbi kifejezéseket, ha $a, b, c \in \mathbb{R}$ és $\omega = -1/2 + i\sqrt{3}/2$:

(1) $(a\omega + b\omega^2)(a\omega^2 + b\omega);$

(2) $(a + b + c)(a + b\omega + c\omega^2)(a + b\omega^2 + c\omega);$

(3) $(a + b\omega + c\omega^2)^3 + (a + b\omega^2 + c\omega)^3.$

→ **3.4.22. Feladat [4].** Határozzuk meg azokat a komplex számokat, amelyekre

- (1) $\bar{z} = z^2$;
- (2) $\bar{z} = z^3$;
- (3) $\bar{z} = z^n$ egy adott $n \in \mathbb{N}^+$ -ra.

→ **3.4.23. Feladat [4].** Ábrázoljuk a komplex számsíkon az alábbi feltételt kielégítő komplex számok halmazát:

- (1) $|z - i| < 1$;
- (2) $2 < |z| \leq 3$;
- (3) $|z - 2 - i| < |z|$;
- (4) $|z - 1| < 1$ és $\Re(z) > 0$;
- (5) $|z + i| > 2$ és $\Im(z) < 2$;
- (6) $|z - 1| = 2|z - 2 + i|$.

→ **3.4.24. Feladat [8].** Az alábbi relációkra határozzuk meg értelmezési tartományt, értékészletet, döntsük el, hogy függvény-e, és hogy az inverze függvény-e.

- (1) $\{(z, w) \in \mathbb{C}^2: |z - 1| = |w|\}$;
- (2) $\{(z, w) \in \mathbb{C}^2: z^2 = w\}$;
- (3) $\{(z, w) \in \mathbb{C}^2: z = w^2\}$;
- (4) $\{(z, y) \in \mathbb{C} \times \mathbb{R}: \Re(z) = y\}$;
- (5) $\{(z, y) \in \mathbb{C} \times \mathbb{R}: |z| + y = 0\}$;
- (6) $\{(z, w) \in \mathbb{C}^2: \Re(z) = \Im(w)\}$;
- (7) $\{(z, w) \in \mathbb{C}^2: w(z^2 - 1) = z\}$;
- (8) $\{(z, w) \in \mathbb{C}^2: w = |z|\}$;
- (9) $\{(z, w) \in \mathbb{C}^2: w(z - 1) = z\}$.

→ **3.4.25. Feladat [5].** Határozzuk meg az $f \circ g$ függvényt, ha

- (1) $g(z) = \operatorname{sgn}(z)$, ha $z \in \mathbb{C}$ és $f(x) = 1/(x^2 - 1)$, ha $x \in \mathbb{R}$;
- (2) $g(z) = z^2$, ha $z \in \mathbb{C}$ és $f(x) = 1/(x + 1)$, ha $x \in \mathbb{R}$;
- (3) $g(z) = \Re(z)$, ha $z \in \mathbb{C}$ és $f(x) = x/(x^2 - 1)$, ha $x \in \mathbb{R}$;
- (4) $g(x) = |x|$, ha $x \in \mathbb{R}$ és $f(z) = iz$, ha $z \in \mathbb{C}$.

3.4.26. Feladat [4]. Mutassuk meg, hogy $\mathbb{R} \times \mathbb{R}$ a koordinátánkénti összeadással és szorzással kommutatív egységelemes gyűrű, de nem test.

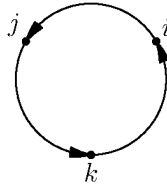
3.4.27. Feladat [6]. Mutassuk meg, hogy ha az $f, g: \mathbb{C} \rightarrow \mathbb{C}$ leképezések mindegyike külön-külön forgatás (valamely pont körül) vagy eltolás, akkor az összetételük is forgatás vagy eltolás.

3.4.28. Kvaterniók. Ha a komplex számok bevezetésénél használt *duplázási eljárást* megismételjük, a William Rowan Hamilton ír matematikus, fizikus és csillagász által bevezetett *kvaterniókhoz* vagy *Hamilton-féle számokhoz* jutunk: ezek halmaza

$$\mathbb{H} = \mathbb{C} \times \mathbb{C},$$

a komplex számpárok halmaza, a $(z, w) + (z', w') = (z + z', w + w')$ összeadással és a $(z, w) \cdot (z', w') = (zz' - \overline{w'}w, w'z + w\overline{z'})$ szorzással mint műveletekkel. (Figyeljük meg, hogy a szorzás hasonló a komplex számoknál bevezetett szorzáshoz, de itt konjugálások is szerepelnek.) Egyszerű számolás mutatja, hogy $\mathbb{H}$ ferdetest a fenti műveletekkel: a nullelem a $(0, 0)$ pár, a (z, w) pár additív inverze a $(-z, -w)$ pár, egységelem az $(1, 0)$ pár, és a nullelemtől különböző (z, w) pár multiplikatív inverze a $(\bar{z}/(z\bar{z} + w\bar{w}), -w/(z\bar{z} + w\bar{w}))$ pár. Vegyük észre, hogy ha $z, z' \in \mathbb{C}$, akkor $(z, 0) + (z', 0) = (z + z', 0)$, $(z, 0) \cdot (z', 0) = (zz', 0)$, így a $z \mapsto (z, 0)$ leképezés kölcsönösen egyértelmű, összeadás és szorzástartó leképezése $\mathbb{C}$ -nek $\mathbb{H}$ -ba, így a $(z, 0)$, $z \in \mathbb{C}$ alakú kvaterniók halmazát azonosítjuk $\mathbb{C}$ -vel, azaz úgy tekinthetjük, hogy $\mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$.

Jelölje j a $(0, 1)$ kvaterniót. Vegyük észre, hogy $j^2 = -1$, a j segítségével a (z, w) kvaterniót $z + wj$ alakba írhatjuk, és ez a felírás természetesen egyértelmű. Ha k a $(0, i)$ kvaterniót jelöli, akkor a (z, w) kvaterniót felírhatjuk $a + bi + cj + dk$ alakban, ahol $a, b, c, d \in \mathbb{R}$, és ez a felírás egyértelmű, mert $a = \Re(z)$, $b = \Im(z)$, $c = \Re(w)$ és $d = \Im(w)$. A definíció alapján $i^2 = j^2 = k^2 = -1$. Míg egy valós szám bármely kvaternióval felcserélhető, a komplex számokra ez már nem igaz; például ha $z \in \mathbb{C}$, akkor $jz = \bar{z}j$. Könnyen ellenőrizhető, hogy $ij = k$, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$, $ik = -j$. A számolási szabályok legegyszerűbben a 3.4.3 ábra alapján jegyezhetők meg: a nyílak mentén ciklikusan körbe haladva, a két kvaternió szorzata a harmadik, míg ellenkező irányba haladva az ellentettje. Ezek alapján legegyszerűbb a kvaterniókat $a + bi + cj + dk$ alakba írni, és a disztributivitást, az asszociativitást, a fenti szorzási szabályokat, valamint a valós számok i, j, k -val való felcserélhetőségét felhasználva számolni velük.



3.4.3 ábra: kvaterniók szorzása.

Ha $p = a + bi + cj + dk$, ahol $a, b, c, d \in \mathbb{R}$, akkor az a valós számot a p valós részének, *időszerű részének* vagy *skalár részének*, a $bi + cj + dk$ kvaterniót pedig a p *képzetes részének*, *térszerű részének* vagy *vektor részének* nevezzük. Jelölésük: $\Re(p)$, illetve $\Im(p)$. (A jelölés eltér a komplex számoknál szokásostól!) A p konjugáltja a $\bar{p} = a - bi - cj - dk$ kvaternió. A komplex számokra a szokásos konjugálást kapjuk vissza. A p kvaternió pontosan akkor valós, ha megegyezik a konjugáltjával, azaz $b = c = d = 0$. Ha egy kvaternió valós része nulla, akkor *tisztán képzetesnek*, *térszerűnek* vagy $-$ ha a szövegösszefüggésből kiderül, hogy a háromdimenziós tér egy vektorára gondolunk – egyszerűen csak *vektornak* nevezzük. A definíció alapján azonnal következnek a $\bar{\bar{p}} = p$, $p + \bar{p} = 2\Re(p)$, $p - \bar{p} = 2\Im(p)$, $\overline{p + q} = \bar{p} + \bar{q}$, $\overline{pq} = \bar{q}\bar{p}$ (sic!) összefüggések, ahol $p, q \in \mathbb{H}$. Osztás nincs, mert a szorzás nem kommutatív.

3.4.29. Kvaterniók abszolút értéke. Egy kvaternió abszolút értéke a hossza (mint négydimenziós vektornak): ha $p = a + bi + cj + dk$, ahol $a, b, c, d \in \mathbb{R}$, akkor legyen a p kvaternió *abszolút értéke* $|p| = \sqrt{a^2 + b^2 + c^2 + d^2}$. (Ezzel a jelöléssel most is $p\bar{p} = |p|^2$, és

ha $p \neq 0$, akkor $1/p = (1/|p|^2)\bar{p}$.) A komplex számokra a szokásos abszolút értéket kapjuk vissza. Nyilván $|0| = 0$ és $p \neq 0$ esetén $|p| > 0$, $|\bar{p}| = |p|$, $|pq| = |p||q|$ (mert mindkét oldal négyzete ugyanannyi). Teljesül a $|p + q| \leq |p| + |q|$ *háromszög-egyenlőtlenség* és a belőle kapható $||p| - |q|| \leq |p - q|$ egyenlőtlenség; mindkettő ugyanúgy kapható, mint a komplex számoknál.

→ **3.4.30. Feladat [3].** Bizonyítsuk be, hogy egy p kvaternióra $|\Re(p)| \leq |p|$, $|\Im(p)| \leq |p|$ és $|p| \leq |\Re(p)| + |\Im(p)|$.

* **3.4.31. Vektoriális szorzás.** A kvaterniószorzás eltérését a kommutativitástól a $p \times q = \frac{1}{2}(pq - qp)$ mennyiséggel mérhetjük. Ez egy új szorzás a kvaterniók között, amelyet *vektoriális szorzásnak* nevezünk, mert a könnyen ellenőrizhető $\Re(pq) = \Re(qp)$ egyenlőség miatt a valós része mindig nulla, azaz háromdimenziós vektor. A vektoriális szorzás mindkét oldalról disztributív az összeadásra nézve és valós szám bármelyik tényezőjéből kiemelhető. Nyilván $p \times p = 0$ bármely $p \in \mathbb{H}$ -ra, ahonnan

$$\begin{aligned} 0 &= (p + q) \times (p + q) = p \times p + p \times q + q \times p + q \times q \\ &= p \times q + q \times p, \end{aligned}$$

tehát tetszőleges $p, q \in \mathbb{H}$ -ra $p \times q = -q \times p$, azaz a vektoriális szorzás nem kommutatív, hanem *antikommutatív*. A definícióból könnyen adódik, hogy $i \times j = k$, $j \times k = i$, $k \times i = j$ és teljesül a *Jacobi-identitás*: tetszőleges $p, q, r \in \mathbb{H}$ -ra

$$(p \times q) \times r + (q \times r) \times p + (r \times p) \times q = 0.$$

A vektoriális szorzás nem asszociatív, például $i \times (i \times j) = i \times k = -j$, míg $(i \times i) \times j = 0$.

* **3.4.32. Kvaterniók és a háromdimenziós euklidészi tér.** A kvaterniók a fentiek alapján $\mathbb{R}^4$ (azaz például a négydimenziós *téridő*) pontjainak is tekinthetők. A kvaterniók összeadása megfelel az $\mathbb{R}^4$ -beli összeadásnak. A tisztán képzetes kvaterniók $\mathbb{R}^3$ -mal, és így a *háromdimenziós tér* pontjaival azonosíthatók: egy derékszögű koordináta-rendszerben az $(x, y, z) \in \mathbb{R}^3$ koordinátákkal rendelkező pontnak az $xi + yj + zk$ tisztán képzetes kvaternió, azaz vektor felel meg, és ily módon i, j és k rendre a koordináta-rendszer három tengelyén vett egységvektoroknak. Ha mást nem mondunk, akkor a koordináta-rendszert úgy választjuk, hogy *jobbsodrású* legyen, azaz egy jobbmenetes csavart az i vektor irányából a j vektor irányába forgatva, a k vektor irányába haladjon, vagy másként, i, j, k rendre a jobb kezünk kifeszített hüvelyk-, mutató- és középső ujjának feleljen meg. A tisztán képzetes kvaterniók összeadása megfelel a térbeli vektorok szokásos összeadásának (paralelogramma-szabály). A $v = xi + yj + zk$ és $v' = x'i + y'j + z'k$ tisztán képzetes kvaterniók szorzatának valós része nyilván $-\langle v, v' \rangle$, ahol $\langle v, v' \rangle = xx' + yy' + zz'$, képzetes része pedig

$$\begin{aligned} \Im(vv') &= \frac{1}{2}\Im(vv') - \frac{1}{2}\Im(\overline{vv'}) = \frac{1}{2}(vv' - \overline{vv'}) = \frac{1}{2}(vv' - \bar{v}'\bar{v}) = \frac{1}{2}(vv' - (-v')(-v)) \\ &= \frac{1}{2}(vv' - v'v) = v \times v', \end{aligned}$$

azaz v és v' vektori szorzata. Erre

$$v \times v' = \Im(vv') = (yz' - zy')i + (zx' - xz')j + (xy' - x'y)k.$$

A $(v, v') \mapsto \langle v, v' \rangle$ leképezést *belső szorzásnak* vagy *skaláris szorzásnak* nevezzük; (bár nem művelet, de) „kommutatív” és „mindkét oldalról disztributív az összeadásra nézve”. (Van általánosabb belső szorzás fogalom is tetszőleges vektortérben; ha tisztán képzetes kvaterniókról, azaz háromdimenziós vektorokról van szó, akkor a fent megadottat fogjuk használni.) Összefoglalva,

$$vv' = -\langle v, v' \rangle + v \times v'.$$

Nyilván $\langle v, v \rangle = |v|^2$. Egy kvaternió pontosan akkor vektor, ha a négyzete valós és kisebb vagy egyenlő nulla: ha s skalár, v vektor, akkor

$$(s + v)^2 = s^2 + v^2 + 2sv = s^2 - \langle v, v \rangle + v \times v + 2sv = s^2 - \langle v, v \rangle + 2sv;$$

ez az $s = 0$ esetben valós és kisebb, vagy egyenlő nulla, és ha valós, akkor $v = 0$ vagy $s = 0$, de a $v = 0$, $s \neq 0$ esetben nagyobb lenne, mint nulla.

Ha v, v', v'' háromdimenziós vektorok, akkor, mint könnyen kiszámolható, $v \times (v' \times v'') = \langle v, v'' \rangle v' - \langle v, v' \rangle v''$. A $(v, v', v'') \mapsto \langle v, v' \times v'' \rangle$ leképezést *vegyes szorzásnak* szokás nevezni.

*** 3.4.33. A szorzások geometriai jelentése.** Ha egy tisztán képzetes kvaterniót, azaz egy háromdimenziós vektort valós számmal (skalárral) szorzunk, az a vektor nyújtásának illetve összehúzásának felel meg, negatív valós szám esetén pedig az irányítás is változik, az ellenkezőjére. Az előző pont szerint, ha v és v' tisztán képzetes kvaterniók, azaz vektorok, akkor $vv' = -\langle v, v' \rangle + v \times v'$, ahonnan mindkét oldal hosszának négyzetét véve

$$(1) \quad \langle v, v' \rangle^2 + |v \times v'|^2 = |v|^2 |v'|^2.$$

Innen $|\langle v, v' \rangle| \leq |v| |v'|$ és $|v \times v'| \leq |v| |v'|$. A koszinusz-tételből, ha a v és v' vektorok által bezárt szög φ , akkor

$$\begin{aligned} 2|v| |v'| \cos \varphi &= |v|^2 + |v'|^2 - |v - v'|^2 \\ &= \langle v, v \rangle + \langle v', v' \rangle - (\langle v, v \rangle - \langle v, v' \rangle - \langle v', v \rangle + \langle v', v' \rangle) \\ &= 2\langle v, v' \rangle, \end{aligned}$$

tehát $\langle v, v' \rangle = |v| |v'| \cos \varphi$. Ha v egységvektor és $v' \neq 0$, akkor $\langle v, v' \rangle$ abszolút értéke a v' vektor v irányú vetületének hossza, előjele pedig pozitív, ha a két vektor hegyesszöget zár be, negatív, ha a két vektor tompaszöget zár be, és nulla, ha merőlegesek.

Ebből az eredményből (1) felhasználásával $|v \times v'| = |v| |v'| |\sin \varphi|$, a v és v' által kifeszített paralelogramma területe. Tehát ha v és v' párhuzamosak, akkor vektoriális szorzatuk nulla lesz. Egyszerű számolással adódik, hogy $\langle v, v \times v' \rangle = 0$ és $\langle v', v \times v' \rangle = 0$, azaz $v \times v'$ merőleges a v és v' vektorokra. Az irányítás meghatározásához forgassuk a v vektort az i irányba, a v' vektort pedig az i és j által adott síkba. Ez kétféleképpen lehetséges; válasszuk azt a forgatást, amelynél v' olyan vektorba megy, amelynek második koordinátája nem negatív. Ekkor az elforgatott vektorok vektori szorzata k irányú, azaz jobbsodrású rendszert kapunk. Ez azt jelenti, hogy v , v' és $v \times v'$ (ebben a sorrendben) ugyanolyan irányítású vektorrendszert alkotnak, mint i , j és k , mert a forgatás során a vektoriális szorzat hossza állandó, mindig merőleges a két vektorra, és a vektorhármás irányítása nem változhat, hiszen a vektoriális szorzat „folytonosan függ a tényezőitől”.

Végül a vegyes szorzat geometriai jelentése a v , v' és v'' vektorok által kifeszített paralelepipedon előjeles térfogata, hiszen ennek alapterülete $|v' \times v''|$, magassága pedig $|v| \cos \varphi$, ahol φ a v és $v' \times v''$ által bezárt szög.

* **3.4.34. Forgatások.** A kvaterniókat a háromdimenziós forgatásokkal való szoros kapcsolatuk miatt felhasználják robotok vezérlésénél. Legyen p egy *egységvektor*, azaz egységnyi abszolút értékű vektor, v pedig először egy tetszőleges p -re merőleges vektor. Megmutatjuk, hogy a $v \mapsto qv$ leképezés, ahol q az egységnyi abszolút értékű $\cos \varphi + p \sin \varphi$ kvaternió, a v vektornak a φ szöggel való elforgatása a p tengely körül, és pedig a p vektor vége felől nézve olyan irányba, mint a k vektor vége felől i -nek j -be való forgatása. Mivel $\langle v, p \rangle = 0$,

$$qv = (\cos \varphi + p \sin \varphi)v = v \cos \varphi + pv \sin \varphi = v \cos \varphi + p \times v \sin \varphi,$$

amiből adódik az állítás, hiszen qv a v és a v -re merőleges, de vele egyenlő hosszúságú $p \times v$ vektorok segítségével van felírva, és mindkettő merőleges p -re.

Most tekintsük a $v \mapsto qvq^{-1}$ leképezést. Megmutatjuk, hogy ez tetszőleges v vektorra a p tengely körüli 2φ szöggel való elforgatás. Először tegyük fel, hogy v merőleges p -re. Mivel $q^{-1} = \bar{q} = \cos \varphi - p \sin \varphi$, a $\tilde{v} = qv$ jelöléssel, mivel $\tilde{v}$ merőleges p -re,

$$\tilde{v}q^{-1} = \tilde{v}(\cos \varphi - p \sin \varphi) = \tilde{v} \cos \varphi - \tilde{v} \times p \sin \varphi = \tilde{v} \cos \varphi + p \times \tilde{v} \sin \varphi,$$

azaz $\tilde{v}q^{-1}$ a $\tilde{v}$ vektor φ szöggel történő továbbforgatásával kapható. Most legyen v tetszőleges, és írjuk fel $v = v' + v''$ alakban, ahol $v' = \alpha p$, $\alpha = \langle v, p \rangle$ és $v'' = v - v'$. Mivel v'' merőleges p -re, most $qv''q^{-1}$ a v'' -nek 2φ szöggel való elforgatásával adódik. Másrészt

$$qv'q^{-1} = (\cos \varphi + p \sin \varphi)\alpha p(\cos \varphi - p \sin \varphi) = \alpha p(\cos^2 \varphi + \langle p, p \rangle \sin^2 \varphi) = \alpha p = v',$$

azaz v' a transzformációnál nem változik. Ezzel az állítást beláttuk.

Az állításból azonnal adódik, hogy két forgatás egymásutánja is forgatás, és ennek tengelye és szöge is meghatározható, mert a $v \mapsto q'vq'^{-1}$ és $v \mapsto q''vq''^{-1}$ leképezések összetétele a $v \mapsto qvq^{-1}$ leképezés, ahol $q = q''q'$ egységnyi abszolút értékű kvaternió. Vegyük észre, hogy φ és $\varphi + \pi$ választással ugyanazt a forgatást kapjuk, hiszen a 2φ és $2\varphi + 2\pi$ szöggel való forgatások megegyeznek, de a $\cos \varphi + p \sin \varphi$ és a $\cos(\varphi + \pi) + p \sin(\varphi + \pi) = -\cos \varphi - p \sin \varphi$ kvaterniók egymás ellentettjei. Általánosabban, bármely $q \neq 0$ kvaternióra és $\alpha \neq 0$ valós számra a $v \mapsto qvq^{-1}$ és a $v \mapsto q'vq'^{-1}$ leképezések megegyeznek, ha $q' = \alpha q$.

* **3.4.35. A skaláris és vektoriális szorzás geometriai alkalmazásai.** A háromdimenziós térben p_0 és p_1 által megadott pontok *távolsága* $|p_1 - p_0|$. Ha $p_0 \neq p_1$, akkor a két ponton átmenő egyenesnek a $v = p_1 - p_0$ vektor egy *irányvektora*; az egyenes bármely p pontjára $p - p_0$ a v vektor egy skalárszorosa, azaz valamely $t \in \mathbb{R}$ -re $p = p_0 + tv$. Ez az *egyenes paraméteres egyenlete*. Ha p_0, p_1 és p_2 három pont, amelyek nem esnek egy egyenesbe, akkor a három ponton átmenő sík tetszőleges p pontjához léteznek olyan t_1 és t_2 valós számok, amelyekkel a $p - p_0 = v$ irányvektorra $v = t_1 v_1 + t_2 v_2$, ahol v_1 , illetve v_2 a $p_1 - p_0$, illetve $p_2 - p_0$ irányvektorok. Innen $p = p_0 + t_1 v_1 + t_2 v_2$, ez a *sík paraméteres egyenlete*. A koordinátákat kiírva, ez három összefüggést jelent. Kettőből kifejezve a t_1 és t_2 paramétereket, és beírva a harmadikba, egy egyenletet kapunk, ez a *sík egyenlete*. Ugyanezt úgy is megkaphatjuk, hogy választunk egy, a v_1 -re és a v_2 -re is merőleges n *normálvektort*, például $v_1 \times v_2$ -t, és észrevesszük, hogy a v vektorokat az

jellemzi, hogy merőlegesek n -re, azaz $\langle p, n \rangle = \langle p_0, n \rangle$. Hasonló módon, az egyenes paraméteres egyenletéből két sík egyenletét kaphatjuk (az egyenes ezek metszete), ez az *egyenes egyenletrendszer*.

A p pont és a p_0 ponton átmenő, n normálvektorú sík távolságát különösen egyszerű számolni, ha n -et egységvektornak választjuk, mivel ez a $p - p_0$ vektor n irányú vetületének hossza, azaz $\langle p - p_0, n \rangle$ abszolút értéke. Egy p pont távolságát a p_0 ponton átmenő, v irányvektorú egyenestől ugyancsak akkor a legegyszerűbb számolni, ha v egységvektor: ez $(p - p_0) \times v$ hossza. A p_1 , illetve p_2 pontokon átmenő, v_1 , illetve v_2 irányvektorú egyenesek távolsága, ha n egységvektor, amely merőleges v_1 -re és v_2 -re is, $\langle p_2 - p_1, n \rangle$ abszolút értéke. Ezen két egyenes hajlásszöge a v_1 és v_2 vektorok által bezárt szög, amelynek koszinusza $\langle v_1, v_2 \rangle$ abszolút értéke, ha v_1 és v_2 egységvektorok. Végül a v irányvektorú egyenes és az n normálvektorú sík hajlásszögének szinusza, ha n és v is egységvektor, $\langle v, n \rangle$ abszolút értéke.

*** 3.4.36. Oktávok vagy Cayley-számok.** Ha a kvaterniók bevezetésénél használt *duplázási eljárást* megismételjük, az Arthur Cayley angol matematikus által bevezetett *oktávokhoz* vagy *Cayley-számokhoz* jutunk: ezek halmaza $\mathbb{O} = \mathbb{H} \times \mathbb{H}$, a kvaterniópárok halmaza, a $(p, q) + (p', q') = (p + p', q + q')$ összeadással és a $(p, q) \cdot (p', q') = (pp' - \overline{q'}q, q'p + q\overline{p'})$ szorzással mint műveletekkel. (Figyeljük meg, hogy a szorzás hasonló a kvaternióknál bevezetett szorzáshoz, de itt a sorrend is fontos, mert a kvaterniók szorzása nem kommutatív.) Az $u = (p, q) \in \mathbb{O}$ pár *konjugáltja* legyen a $(\overline{p}, -q)$ pár, *valós része* $\Re(u) = \Re(p)$, *képzetes része* $\Im(u) = (\Im(p), q)$. (A jelölés eltér a komplex számoknál szokásostól!) A definíció alapján könnyen belátható, hogy ha $u, v \in \mathbb{O}$, akkor $\overline{\overline{u}} = u$, $u + \overline{u} = 2\Re(u)$, $u - \overline{u} = 2\Im(u)$, $\overline{u + v} = \overline{u} + \overline{v}$, $\Re(uv) = \Re(vu)$ és $\overline{uv} = \overline{v}\overline{u}$ (sic!). Egyszerű számolás mutatja, hogy $\mathbb{O}$ Abel-csoport a fenti összeadással: a nullelem a $(0, 0)$ pár, a (p, q) pár additív inverze a $(-p, -q)$ pár. A szorzásra nézve az $(1, 0)$ pár egységelem. Teljesül mindkét oldali disztributivitás is. Vegyük észre, hogy ha $p, p' \in \mathbb{H}$, akkor $(p, 0) + (p', 0) = (p + p', 0)$, $(p, 0) \cdot (p', 0) = (pp', 0)$, így az $p \mapsto (p, 0)$ leképezés kölcsönösen egyértelmű, összeadás- és szorzástartó leképezése $\mathbb{H}$ -nak $\mathbb{O}$ -ba, így a $(p, 0)$, $p \in \mathbb{H}$ alakú oktávok halmazát azonosítjuk $\mathbb{H}$ -val, azaz úgy tekinthetjük, hogy $\mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O}$. A kvaterniókra a szokásos konjugálást, valós és képzetes részt kapjuk vissza.

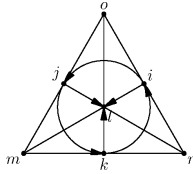
A szorzás nem kommutatív, hiszen már $\mathbb{H} \subset \mathbb{O}$ -ban sem az. Viszont $\mathbb{R}$ -beli elemekkel akár balról, akár jobbról szorozva ugyanazt kapjuk, nevezetesen, ha $x \in \mathbb{R}$, akkor $x \cdot (p, q) = (p, q) \cdot x = (xp, xq)$. Ezt felhasználva, és bevezetve az $l = (0, 1)$, valamint az $m = (0, i) = il$, $n = (0, j) = jl$, $o = (0, k) = kl$ jelöléseket, minden $u \in \mathbb{O}$ egyértelműen felírható $a + bi + cj + dk + el + fm + gn + ho$ alakban, ahol $a, b, c, d, e, f, g, h \in \mathbb{R}$. Ilyen alakban $\Re(u) = a$, $\Im(u) = u - \Re(u)$ és $\overline{u} = \Re(u) - \Im(u)$, azaz $\overline{u}$ -at úgy kapjuk, hogy i, j, k, l, m, n és o együtthatóját az ellentettjével helyettesítjük. Az i, j, k, l, m, n, o elemek mindegyikének a négyzete -1 , egyébként a szorzataikra vonatkozó – a definícióból adódó – számolási szabályok a 3.4.4 ábráról olvashatók le: a körön, illetve az egyeneseken a megjelölt irányban haladva (ciklikusan) az egyik elemtől a másikig az eredmény a harmadik elem lesz, míg ellenkező irányban haladva annak az ellentettje.

A szorzás már nem is asszociatív, mert például

$$(ij)l = kl = o \neq -o = in = i(jl).$$

Az u, v, w elemek szorzásának asszociativitástól való eltérését az

$$[u, v, w] = (uv)w - u(vw)$$



3.4.4 ábra: oktávok szorzása (és a Fano-sík).

mennyiséggel, az úgynevezett *asszociátor*ral mérhetjük. Az asszociátor az u, v, w elemek közül kettőt felcserélve ellenkezőjére változik, ezt *alternatív* tulajdonságnak nevezzük; bár az alternatív tulajdonság közvetlenül is kiszámolható, megmutatjuk, hogy következik a bal és jobb oldali disztributivitásból és a könnyebben kiszámolható

$$(uu)v = u(uv) \quad \text{és} \quad v(uu) = (vu)u,$$

azaz másként $[u, u, v] = 0$ és $[v, u, u] = 0$ két speciális esetből. Valóban, ezekből

$$0 = [u, u + v, u + v] = [u, u, u] + [u, u, v] + [u, v, u] + [u, v, v] = [u, v, u],$$

azaz az asszociativitás mindig teljesül, ha bármely két tényező egyenlő. Innen

$$0 = [u, v + w, v + w] = [u, v, v] + [u, v, w] + [u, w, v] + [u, w, w],$$

azaz $[u, v, w] = -[u, w, v]$. Hasonlóan adódik a többi eset.

Ha $u = a + bi + cj + dk + el + fm + gn + ho$, ahol $a, b, c, d, e, f, g, h \in \mathbb{R}$, akkor legyen

$$|u| = \sqrt{a^2 + b^2 + c^2 + d^2 + e^2 + f^2 + g^2 + h^2}.$$

A kvaterniókra a szokásos abszolút értéket kapjuk vissza. Ha $u, v \in \mathbb{O}$, akkor $u\bar{u} = \bar{u}u = |u|^2$, $|0| = 0$, $u \neq 0$ esetén $|u| > 0$, $|u| = |\bar{u}|$, $|\Re(u)| \leq |u|$, $|\Im(u)| \leq |u|$, és $|uv| = |u||v|$ (mert mindkét oldal négyzete ugyanannyi). Teljesül az $|u + v| \leq |u| + |v|$ *háromszög-egyenlőtlenség* és a belőle kapható $||u| - |v|| \leq |u - v|$ egyenlőtlenség; mindkettő ugyanúgy kapható, mint a komplex számoknál.

Figyeljük meg, hogy bármely $u, v \in \mathbb{O}$, $u \neq 0$ oktávokhoz pontosan egy olyan w oktáv van, amelyre $uw = v$, nevezetesen $w = (1/|u|^2)(\bar{u}v)$; az egyértelműség onnan következik, hogy ha $uw = v = uw'$, akkor $u(w - w') = 0$, ahonnan $|w - w'| = 0$. Hasonlóan egyértelműen oldható meg w -re a $wu = v$ egyenlet is, ha $u \neq 0$, nevezetesen $w = (1/(u\bar{u}))(\bar{v}u)$.

→ **3.4.37. Feladat** [4]. Ha $p = 1 + i + j + k$ és $q = k$ kvaterniók, határozzuk meg a $\bar{p}$, p^2 , $1/p$, $q(1/p)$ és $(1/p)q$ kvaterniókat.

→ **3.4.38. Feladat** [4]. Mutassuk meg, hogy ha q tetszőleges kvaternió, akkor $q - iqi - jqj - kqk = 4\Re(q)$.

* **3.4.39. Feladat** [10]. Mutassuk meg, hogy ha az $f, g: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ leképezések forgatások metsző egyenesek körül, akkor az összetételük is forgatás.

3.4.40. További feladatok megoldásokkal. [53].

3.4.41. További feladatok. [17]: 1–72, 81–126; [20]: 1–48; [83]: VI.4.1–VI.4.25.

Véges halmazok

Ebben a fejezetben a véges halmazok tulajdonságait tárgyaljuk, ide értve a legalapvetőbb kombinatorikai összefüggéseket is. Ezek az ismeretek alapvetőek, ha algoritmusok futásidejét kívánjuk elemezni: lásd például Knuth [46] könyvét, vagy a Cormen–Leiserson–Rivest [8] könyvet.

4.1 Véges halmazok alaptulajdonságai

4.1.1. Halmazok ekvivalenciája. Az X és Y (tetszőleges) halmazokat *ekvivalenseknek* nevezzük, ha létezik X -et Y -ra leképező kölcsönösen egyértelmű leképezés (bijekció). Jelölése: $X \sim Y$.

4.1.2. Állítás. Legyenek X, Y és Z tetszőleges halmazok. Ekkor

- (1) $X \sim X$ (reflexivitás);
- (2) ha $X \sim Y$, akkor $Y \sim X$ (szimmetria);
- (3) ha $X \sim Y$ és $Y \sim Z$, akkor $X \sim Z$ (transzitivitás). $\square$

4.1.3. Megjegyzés. Ha f az X -et X' -re képező kölcsönösen egyértelmű leképezés, g pedig Y -t Y' -re leképező kölcsönösen egyértelmű leképezés, akkor az $(x, y) \mapsto (f(x), g(y))$ kölcsönösen egyértelmű leképezés $X \times Y$ -t $X' \times Y'$ -re képezi le, így ezek is ekvivalensek. Egy $h \subset X \times Y$ reláció képe ennél a leképezésnél a $h' = g \circ h \circ f^{-1} \subset X' \times Y'$ reláció: $(x', y') \in h'$ pontosan akkor, ha $x = f^{-1}(x')$ -re $(x, y) \in h$ esetén $g(y) = y'$. A függvények összetételéről tanultak szerint a $h \mapsto h'$ leképezés függvényt függvénybe, kölcsönösen egyértelmű függvényt kölcsönösen egyértelmű függvénybe, Y -ra képező függvényt Y' -re képező függvénybe visz, speciálisan Y^X és $Y'^{X'}$ ekvivalensek.

→ **4.1.4. Feladat [0].** Mutassuk meg, hogy ha $(A \setminus B) \sim (B \setminus A)$, akkor $A \sim B$.

→ **4.1.5. Feladat [1].** Adjunk meg kölcsönösen egyértelmű megfeleltetést a 0, 1 számokból és a 0, 1, 2, 3 számokból képezhető sorozatok között.

→ **4.1.6. Feladat [2].** Adjunk meg kölcsönösen egyértelmű megfeleltetést az alábbi halmazok között:

- (1) $\mathbb{Z}$ és $\mathbb{N}$;
- (2) $\mathbb{R}$ és $\mathbb{R}^+$;
- (3) $\{x \in \mathbb{R}: 0 < x \leq 1\}$ és $\{x \in \mathbb{R}: x \geq 1\}$.

→ **4.1.7. Feladat [6].** Tetszőleges halmazok elemszámaira is teljesülnek a kommutativitás, asszociativitás, disztributivitás és a hatványozás azonosságai. Ezt bizonyítandó, mutassuk meg, hogy ha A, B, C halmazok, akkor

- (1) $A \times B \sim B \times A$;

- (2) $(A \times B) \times C \sim A \times (B \times C)$;
- (3) $(A \cup B) \times C \sim (A \times C) \cup (B \times C)$, ha $A \cap B = \emptyset$;
- (4) $A^{B \cup C} \sim A^B \times A^C$, ha $B \cap C = \emptyset$;
- (5) $(A^B)^C \sim A^{B \times C}$;
- (6) $(A \times B)^C \sim A^C \times B^C$.

4.1.8. Tétel. Bármely n természetes számra $\{1, 2, \dots, n\}$ bármely valódi részhalmaza ekvivalens $\{1, 2, \dots, m\}$ -mel valamely $m < n$ természetes számra.

Bizonyítás. Indukcióval: 0-ra nyilván igaz, mert az üres halmaznak nincs valódi részhalmaza. Ha n -re teljesül az állítás, és $A \subsetneq \{1, 2, \dots, n+1\}$, akkor az $A \subset \{1, 2, \dots, n\}$ esetben az állítás nyilván teljesül. Ha $n+1 \in A$, akkor van olyan $0 < k < n+1$ természetes szám, amelyre $k \notin A$. Defináljuk az f függvényt úgy, hogy $f(i)$ legyen i , ha $i \in A$, $i \neq n+1$, és legyen $f(n+1) = k$. Az f függvény kölcsönösen egyértelmű leképezése A -nak $\{1, 2, \dots, n\}$ valamely részhalmazára. Ha f értékkészlete $\{1, 2, \dots, n\}$, akkor $m = n$ választható. Ha f értékkészlete valódi részhalmaza $\{1, 2, \dots, n\}$ -nek, akkor az indukciós feltevés használható. $\square$

4.1.9. Tétel. Ha n természetes szám, akkor nem létezik ekvivalencia $\{1, 2, \dots, n\}$ és egy valódi részhalmaza között.

Megjegyezzük, hogy $\mathbb{N}$ -re ez nem igaz: $n \mapsto n^+$ ekvivalencia $\mathbb{N}$ és $\mathbb{N}^+$ között.

Bizonyítás. Indukcióval bizonyítunk: 0-ra az állítás világos, mert az üres halmaznak nincs valódi részhalmaza. Tegyük fel, hogy n -re teljesül, de létezik egy f kölcsönösen egyértelmű leképezése $\{1, 2, \dots, n+1\}$ -nek egy A valódi részhalmazára. Ha $n+1 \notin A$, akkor f megszorítása $\{1, 2, \dots, n\}$ -re is kölcsönösen egyértelmű leképezés, mégpedig $\{1, 2, \dots, n\}$ -nek egy valódi részhalmazára, mivel $f(n+1)$ nem lesz az értékkészletben, ami ellentmond az indukciós feltevésnek. Ha $f(k) = n+1 \in A$, akkor viszont úgy kapjuk $\{1, 2, \dots, n\}$ és $A \setminus \{n+1\}$ egy ekvivalenciáját, hogy – hacsak nem $k = n+1$ – a $(k, n+1)$ és az $(n+1, l)$ párokat kihagyjuk a leképezésből, és helyettük a (k, l) párt vesszük be. Ez megint ellentmond az indukciós feltevésnek. $\square$

4.1.10. Véges és végtelen halmazok. Egy X halmazt *végesnek* nevezzünk, ha valamely n természetes számra ekvivalens a $\{1, 2, \dots, n\}$ halmazzal, egyébként *végtelennek* nevezzük.

Egy véges halmaz legfeljebb egy n -re ekvivalens a $\{1, 2, \dots, n\}$ halmazzal, mert ha ekvivalens lenne $\{1, 2, \dots, m\}$ -mel is, akkor $m < n$ vagy $n < m$ miatt $\mathbb{N}^+$ egy kezdőszelete ekvivalens lenne egy valódi részhalmazával, ami az előző tétel szerint lehetetlen.

Azt az egyértelműen meghatározott természetes számot, amelyre egy adott X véges halmaz ekvivalens $\{1, 2, \dots, n\}$ -nel, az X halmaz *elemei számának* vagy *számosságának* nevezzük, és $\natural(A)$ -val vagy (a „cardinal number” rövidítéseként) $\text{card}(A)$ -val jelöljük. Az $|A|$ és $\overline{A}$ jelölés is szokásos.

Például $\natural(\emptyset) = 0$, bármely a -ra $\natural(\{a\}) = 1$, bármely a, b -re, ha $a \neq b$, akkor $\natural(\{a, b\}) = 2$. Azt, hogy a természetes számokat nullával kezdtük, az indokolja, hogy így a természetes számok a véges halmazok számosságai.

Az előző tételből az is következik, hogy véges halmaz sohasem ekvivalens egy valódi részhalmazával. Mivel ez $\mathbb{N}$ -re nem teljesül, $\mathbb{N}$ végtelen halmaz.

4.1.11. Tétel. Legyenek X és Y halmazok. Ekkor

- (1) ha X véges és $Y \subset X$, akkor Y is véges, és $\mathfrak{h}(Y) \leq \mathfrak{h}(X)$;
- (2) ha X véges és $Y \subsetneq X$, akkor $\mathfrak{h}(Y) < \mathfrak{h}(X)$;
- (3) ha X és Y végesek és diszjunktak, akkor $X \cup Y$ is véges, és $\mathfrak{h}(X \cup Y) = \mathfrak{h}(X) + \mathfrak{h}(Y)$;
- (4) ha X és Y végesek, akkor $\mathfrak{h}(X \cup Y) + \mathfrak{h}(X \cap Y) = \mathfrak{h}(X) + \mathfrak{h}(Y)$;
- (5) ha X és Y végesek, akkor $X \times Y$ is véges, és $\mathfrak{h}(X \times Y) = \mathfrak{h}(X) \cdot \mathfrak{h}(Y)$;
- (6) ha X és Y végesek, akkor X^Y is véges, és $\mathfrak{h}(X^Y) = \mathfrak{h}(X)^{\mathfrak{h}(Y)}$;
- (7) ha X véges halmaz, akkor $\wp(X)$ is véges, és $\mathfrak{h}(\wp(X)) = 2^{\mathfrak{h}(X)}$;
- (8) ha X véges, és az f függvény X -et Y -ra képezi, akkor Y is véges, $\mathfrak{h}(Y) \leq \mathfrak{h}(X)$, és ha f nem kölcsönösen egyértelmű, akkor $\mathfrak{h}(Y) < \mathfrak{h}(X)$.

Bizonyítás. (1) nyilvánvaló, ha $Y = X$, ha viszont $Y \subsetneq X$, akkor ekvivalens $\{1, 2, \dots, \mathfrak{h}(X)\}$ egy valódi részhalmazával, amiről tudjuk, hogy ekvivalens $\{1, 2, \dots, m\}$ -mel valamely $m < n$ -re. Ezzel (2)-t is beláttuk. (3) azon múlik, hogy $\{1, \dots, n\}$ ekvivalens $\{m+1, m+2, \dots, m+n\}$ -nel. (3) szerint $\mathfrak{h}(X \cup Y) = \mathfrak{h}(X \setminus Y) + \mathfrak{h}(X \cap Y) + \mathfrak{h}(Y \setminus X)$; mindkét oldalhoz hozzáadva $\mathfrak{h}(X \cap Y)$ -t, és újra felhasználva (3)-at, kapjuk (4)-et. (5) és (6) az Y elemeinek száma szerinti indukcióval következnek, felhasználva a szorzás és a hatványozás definícióját. (7) következik (6)-ból és $\wp(X)$ -nek a karakterisztikus függvények halmazával való ekvivalenciájából. (8) bizonyításához feltehetjük, hogy $X = \{1, 2, \dots, \mathfrak{h}(X)\}$. Minden $y \in Y$ -ra legyen $g(y)$ az $f^{-1}(y)$ halmaz legkisebb eleme. Ekkor g az Y -t kölcsönösen egyértelműen képezi le X egy részhalmazára, és ha f nem volt kölcsönösen egyértelmű, akkor ez a részhalmaz valódi. $\square$

4.1.12. Skatulya elv. Ha X és Y véges halmazok, és $\mathfrak{h}(X) > \mathfrak{h}(Y)$, akkor egy $f: X \rightarrow Y$ leképezés nem lehet kölcsönösen egyértelmű.

Bizonyítás. Egyébként $\{1, 2, \dots, \mathfrak{h}(Y)\}$ egy részhalmaza, azaz $\mathfrak{h}(Y) < \mathfrak{h}(X)$ miatt $\{1, 2, \dots, \mathfrak{h}(X)\}$ egy valódi részhalmaza ekvivalens lenne $\{1, 2, \dots, \mathfrak{h}(X)\}$ -nel. $\square$

4.1.13. Tétel. Részenrendezett halmaz bármely nem üres véges részhalmazának van maximális és minimális eleme.

A tétel alapján algoritmust kaphatunk egy A véges halmaz $\leq$ részenrendezésének kiterjesztésére egy (ugyanazzal a jellel jelölt) rendezésre: rekurzióval legyen a_k az $A \setminus \{a_1, a_2, \dots, a_{k-1}\}$ egy minimális eleme, majd legyen $a_i \leq a_j$, ha $i \leq j$.

Bizonyítás. A részhalmaz elemeinek száma szerinti indukcióval: Ha $\mathfrak{h}(A) = 1$, akkor nyilvánvaló. Ha $\mathfrak{h}(A) = n + 1$, legyen $a \in A$ és $A' = A \setminus \{a\}$. Ha a nem nagyobb, mint A' (egy adott) a' maximális eleme, akkor az a' maximális elem, egyébként a maximális elem. Minimális elemre a bizonyítás hasonló. $\square$

4.1.14. Feladat [6]. Mutassuk meg, hogy egy X halmaz pontosan akkor végtelen, ha minden $f: X \rightarrow X$ leképezéshez van olyan Y valódi részhalmaza X -nek, hogy $f(Y) \subset Y$.

4.1.15. Feladat [6]. Mutassuk meg, hogy $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ és $\mathbb{C}$ végtelen halmazok.

$\rightarrow^\circ$ **4.1.16. Feladat [7].** Mutassuk meg, hogy a $\pi, 2\pi, 3\pi, \dots, 100\pi$ számok között van olyan, amelyik nincs messzebb a legközelebbi egésztől, mint $1/101$. Általánosítsuk az állítást.

→ **4.1.17. Feladat [8].** Bizonyítsuk be, hogy bármely $m \in \mathbb{N}^+$ -hoz van olyan $n \in \mathbb{N}^+$, hogy tízes számrendszerben mn minden jegye 1 vagy 0.

→° **4.1.18. Feladat [6].** Bizonyítsuk be, hogy minden páratlan n -hez van olyan m egész, amelyre n osztója $2^m - 1$ -nek.

→° **4.1.19. Feladat [6].** Legyen $a_1, a_2, \dots, a_{100}$ egész számok egy sorozata. Bizonyítsuk be, hogy egy alkalmas részsorozatra $a_{j_1} + a_{j_2} + \dots + a_{j_n}$ osztható 100-zal. Általánosítsuk az állítást.

→° **4.1.20. Feladat [3].** Legyenek $a_1, a_2, \dots, a_{51}$ egész számok az $[1, 100]$ intervallumból. Bizonyítsuk be, hogy van kettő közöttük, amely relatív prím. Általánosítsuk az állítást.

→° **4.1.21. Feladat [8].** Legyenek $a_1, a_2, \dots, a_{51}$ egész számok az $[1, 100]$ intervallumból. Bizonyítsuk be, hogy alkalmas $i \neq j$ -re a_i osztója a_j -nek. Általánosítsuk az állítást.

4.1.22. Feladat [10]. Pozitív természetes számok egy szigorúan monoton növekedő $k_1, k_2, \dots, k_m$ sorozatát *Sidon-sorozatnak* nevezzük n -ig, ha a $k_i + k_j$, $1 \leq i \leq j \leq m$ számok mind különbözőek, és $k_m \leq n$. Melyik a leghosszabb Sidon-sorozat 100-ig? Megkaphatjuk-e ezt a mohó algoritmussal, azaz úgy, hogy egytől kezdve mindig az első olyan számot, amely érvényben hagyja a Sidon-tulajdonságot, hozzávesszük a sorozathoz? Adjunk felső korlátot a Sidon-sorozatok hosszára n -ig.

* **4.1.23. Feladat: közelítés racionális számmal [10].** Mutassuk meg, hogy egy α irracionális számhoz végtelen sok olyan m/n racionális szám van, amelyre $|\alpha - m/n| < 1/n^2$.

* **4.1.24. Feladat: szimultán közelítés racionális számmal [11].** Mutassuk meg, hogy ha $\alpha_1, \alpha_2, \dots, \alpha_n$ irracionális számok, akkor végtelen sok olyan racionális számokból álló $(p_1/q, p_2/q, \dots, p_n/q)$ sorozat létezik, amelyre $|\alpha_i - p_i/q| < 1/q^{1+1/n}$, ha $1 \leq i \leq n$.

° **4.1.25. Feladat [12].** Bizonyítsuk be, hogy valamely $n > 0$ -ra az F_n Fibonacci-szám osztható 1000-rel.

4.1.26. További feladatok. [36]: 4.7, 4.21, 5.7, 5.8, 5.12.

4.2 Kombinatorika

4.2.1. Permutációk. Emlékeztetünk rá, hogy egy halmaz permutációján a halmaznak önmagára való kölcsönösen egyértelmű leképezését értjük. Az X halmaz összes permutációi csoportot alkotnak a $\circ$ műveletre, azaz az összetett függvény képzésre, amelyben $\mathbb{I}_X$ az egységelem, és egy elem csoportbeli inverze a relációként vett inverze.

Meg akarjuk határozni véges halmazok permutációinak számát. Ha egy A halmaz ekvivalens $\{1, 2, \dots, n\}$ -nel, akkor tudjuk, hogy permutációinak halmaza ekvivalens $\{1, 2, \dots, n\}$ permutációinak halmazával. Ha $A = \{a_1, a_2, \dots, a_n\}$ és $p_1, p_2, \dots, p_n$ az $\{1, 2, \dots, n\}$ egy permutációja, akkor az A megfelelő permutációja az $a_i \mapsto a_{p_i}$ leképezés (az $a_i \mapsto i$, $i \mapsto p_i$, $j \mapsto a_j$ leképezések összetétele). Így A permutációinak száma csak $n = \sharp(A)$ -től függ. Jelölje ezt a számot P_n .

Az üres halmaznak egy permutációja van, így $P_0 = 1$. A $\{1\}$ egyelemű halmaznak is egy permutációja van, így $P_1 = 1$. Indukcióval megmutatjuk, hogy $P_n = \prod_{k=1}^n k$. Feltéve,

hogy n -re igaz az állítás, tekintsük ekvivalensnek $\{1, 2, \dots, n+1\}$ két permutációját, ha mindkettőnél az 1 képe ugyanaz. Világos, hogy $n+1$ ekvivalenciaosztály van, és egy ekvivalenciaosztály elemei megfeleltethetők egy n elemű halmaz permutációinak. Így minden ekvivalenciaosztálynak P_n eleme van, ahonnan

$$P_{n+1} = \left(\prod_{k=1}^n k \right) \cdot (n+1) = \prod_{k=1}^{n+1} k.$$

A $P_n = \prod_{k=1}^n k$ szorzatot $n!$ -sal is jelöljük (n faktoriálisnak olvassuk). A továbbiakban P_n helyett ezt a jelölést fogjuk használni. Értéke néhány n -re:

n	0	1	2	3	4	5	6	7	8	9	10	11
$n!$	1	1	2	6	24	120	720	5040	40320	362880	3628800	39916800

4.2.2. Variációk. Az A halmaz elemeiből készíthető, különböző tagokból álló

$$a_1, a_2, \dots, a_k$$

sorozatokat, azaz $\{1, 2, \dots, k\}$ -t A -ba képező kölcsönösen egyértelmű leképezéseket az A halmaz k -ad osztályú *variációinak* nevezzük. Ha A véges halmaz, $\sharp(A) = n$, akkor ezek V_n^k száma megegyezik az $\{1, 2, \dots, k\}$ -t $\{1, 2, \dots, n\}$ -be képező kölcsönösen egyértelmű leképezések számával. Megmutatjuk, hogy

$$V_n^k = \frac{n!}{(n-k)!} = n(n-1) \cdots (n-k+1),$$

ha $k \leq n$ (és nulla egyébként). Soroljuk $\{1, 2, \dots, n\}$ két permutációját egy osztályba, ha $\{1, 2, \dots, k\}$ -n megegyeznek. Minden osztálynak $(n-k)!$ eleme van, az osztályok száma pedig V_n^k , ahonnan kapjuk az állítást.

4.2.3. Ismétléses variációk. Az A halmaz elemeiből készíthető $a_1, a_2, \dots, a_k$ sorozatokat, azaz $\{1, 2, \dots, k\}$ -t A -ba képező leképezéseket az A halmaz k -ad osztályú *ismétléses variációinak* nevezzük. Ha A véges halmaz, $\sharp(A) = n$, akkor ezek ${}^iV_n^k$ számáról (a $V_n^{k,i}$ jelölés is szokásos) már tudjuk, hogy n^k .

4.2.4. Kombinációk. Ha $k \in \mathbb{N}$, akkor az A halmaz k elemű részhalmazait az A halmaz k -ad osztályú *kombinációinak* nevezzük. Ha A véges halmaz, $\sharp(A) = n$, akkor ezek C_n^k száma megegyezik a $\{1, 2, \dots, n\}$ halmaz k elemű részhalmazainak számával. Megmutatjuk, hogy

$$C_n^k = \frac{n!}{k!(n-k)!} = \frac{n(n-1) \cdots (n-k+1)}{1 \cdot 2 \cdots k},$$

ha $k \leq n$ (és nulla egyébként). Soroljuk $\{1, 2, \dots, n\}$ két variációját egy osztályba, ha értékkészlete ugyanaz. Minden osztálynak $k!$ eleme van, az osztályok száma pedig C_n^k , ahonnan kapjuk az állítást. Egyébként minden osztályban egy és csak egy szigorúan monoton növekedő leképezés van, így ezek száma is C_n^k . Szokásosabb C_n^k helyett az

$$\binom{n}{k} = \frac{n(n-1) \cdots (n-k+1)}{1 \cdot 2 \cdots k}$$

jelölés (úgy olvassuk, hogy n alatt a k), amelyet a jobb oldallal tetszőleges $k \in \mathbb{N}$, $n \in \mathbb{C}$ esetén is értelmezhetünk.

4.2.5. Ismétléses kombinációk. Legyen A véges halmaz. Ha $k \in \mathbb{N}$, akkor az A halmazból k elemet kiválasztva, ismétléseket is megengedve, de tekintet nélkül a sorrendre, az A halmaz k -ad osztályú ismétléses kombinációit kapjuk. Pontosabban, tekintsük mindazokat az $f: A \rightarrow \mathbb{N}$ függvényeket, amelyekre $\sum_{a \in A} f(a) = k$; ezek az A halmaz k -ad osztályú *ismétléses kombinációi*. Ezek száma nyilván csak A elemeinek számától függ, így feltehetjük, hogy $A = \{1, 2, \dots, n\}$. Minden $g: \{1, 2, \dots, k\} \rightarrow \{1, 2, \dots, n\}$ monoton növekedő függvényhez hozzárendelve az $f(j) = \sharp(g^{-1}(j))$ függvényt, kölcsönösen egyértelmű megfeleltetést kapunk A ismétléses kombinációi és az $\{1, 2, \dots, k\}$ -t $\{1, 2, \dots, n\}$ -be képező monoton növekedő függvények között, így ezek száma az A ismétléses kombinációinak ${}^iC_n^k$ száma (a $C_n^{k,i}$ jelölés is szokásos). Megmutatjuk, hogy

$${}^iC_n^k = \binom{n+k-1}{k}.$$

Egy $g: \{1, 2, \dots, k\} \rightarrow \{1, 2, \dots, n\}$ monoton növekedő függvényhez definiáljuk a h függvényt a $h(j) = g(j) + j - 1$ összefüggéssel. Ezzel kölcsönösen egyértelmű megfeleltetést létesítettünk az $\{1, 2, \dots, k\}$ -t $\{1, 2, \dots, n\}$ -be képező monoton növekedő függvények és az $\{1, 2, \dots, k\}$ -t $\{1, 2, \dots, n+k-1\}$ -be képező szigorúan monoton növekedő (tehát kölcsönösen egyértelmű) függvények között, mely utóbbiak megfelelnek k elem kiválasztásának. A megfeleltetés létezéséből következik az állítás, amely az $n = k = 0$ esetben is igaz marad.

4.2.6. Ismétléses permutációk. Ha $r, i_1, i_2, \dots, i_r \in \mathbb{N}$, akkor az $a_1, a_2, \dots, a_r$ (különböző) elemek $i_1, i_2, \dots, i_r$ ismétlődésű *ismétléses permutációi* az olyan $n = i_1 + i_2 + \dots + i_r$ -tagú sorozatok, amelyekben az a_j elem i_j -szer fordul elő. Az $A = \{a_1, a_2, \dots, a_r\}$ jelöléssel ezek olyan $\{1, 2, \dots, n\}$ -et A -ba képező leképezések, amelyeknél a_j teljes inverz képe i_j elemű. Megmutatjuk, hogy ezek száma

$$P_n^{i_1, i_2, \dots, i_r} = \frac{n!}{i_1! i_2! \dots i_r!}.$$

Ha $r = 0$ és ha $r = 1$, akkor triviális az állítás. Egyébként soroljuk az $a_1, a_2, \dots, a_r$ elemek két $i_1, i_2, \dots, i_r$ ismétlődésű ismétléses permutációját egy osztályba, ha az a_1 elem összes előfordulását kihagyva a sorozatból, ugyanazt a $b_1, b_2, \dots, b_{n-i_1}$ ismétléses permutációt kapjuk. Nyilván $P_{n-i_1}^{i_2, i_3, \dots, i_r}$ osztályunk lesz. A $b_1, b_2, \dots, b_{n-i_1}$ ismétléses permutációból úgy kaphatjuk vissza az osztály elemeit, hogy b_1 elé valahányszor beírjuk az a_1 -et, majd b_1 és b_2 közé valahányszor beírjuk az a_1 -et, stb., végül b_{n-i_1} után valahányszor beírjuk az a_1 -et, összesen i_1 darab a_1 -et írva be. Így tulajdonképpen az $n - i_1 + 1$ lehetséges hely közül i_1 -et választunk ki, megengedve egy hely többszöri kiválasztását is, ami

$${}^iC_{n-i_1+1}^{i_1} = \binom{n-i_1+1+i_1-1}{i_1} = \binom{n}{i_1} = \frac{n!}{(n-i_1)!i_1!}$$

számú módon tehető meg. Innen adódik az indukciós lépés.

→ **4.2.7. Feladat [0].** Hány szótárra van szükségünk az EU-ban, hogy bármely hivatalos nyelvről bármely hivatalos nyelvre közvetlenül fordíthassunk?

- **4.2.8. Feladat [0].** Hány rendezése van egy n elemű halmaznak?
- **4.2.9. Feladat [0].** Hány $f: \{\uparrow, \downarrow\}^n \rightarrow \{\uparrow, \downarrow\}^m$ logikai függvény van?
- **4.2.10. Feladat [1].** Hányféleképpen ültethetünk le n embert egy kerek asztal mellé? Két ültetést megegyezőnek tekintünk, ha forgatással átvihetők egymásba.
- **4.2.11. Feladat [1].** Egy postahivatalban 10 különböző képeslapot árulnak. Hányféleképpen vásárolhatunk 12 képeslapot?
- **4.2.12. Feladat [1].** Hányféleképpen helyezkedhet el 12 ember három szobában, ha az elsőben 2, a másodikban 6, a harmadikban pedig 4 fér el?
- **4.2.13. Feladat [5].** Tizenhatszáz forintot osztunk szét öt gyerek között. Hányféleképpen lehetséges ez? Mi a helyzet, ha mindenki legalább száz forintot kap? Mi a helyzet, ha mindenki legalább kétszáz forintot kap? Általánosítsuk az állítást.
- **4.2.14. Feladat [0].** Egy esemény *esélyén* a bekövetkezését eredményező esetek számának és az összes esetek számának hányadosát fogjuk érteni. Lottóban mennyi az 5, 4, 3, 2, 1, illetve 0 találat esélye?
- **4.2.15. Feladat [0].** Egy n elemű halmazon hány binér reláció van? Ezekből hány reflexív, hány szimmetrikus és hány reflexív és szimmetrikus?
- **4.2.16. Feladat [0].** Hányféleképpen választhatunk ki három különböző számot az $\{1, 2, \dots, 100\}$ halmazból úgy, hogy az összegük páros legyen?
- **4.2.17. Feladat [0].** Hány k hosszú infixe van egy n hosszú szónak? Azonos, de különböző helyen lévő infixeket különbözőnek tekintünk.
- **4.2.18. Feladat [5].** Bridzsben hány leosztás van? Mennyi az esélye, hogy mindenkinél van ász? Hány lehetséges „kéz” van? Mennyi az esélye, hogy egy adott kézben van minden ász? Mennyi az esélye, hogy egy adott kézben egy színből nyolc lap van? Mennyi az esélye, hogy egy adott kéz 4-4-4-1 „elosztású”?
- **4.2.19. Feladat: születésnap-paradoxon [3].** Egy tanár fogadást ajánl fel egy 30 fős osztálynak, hogy van két diák, akinek ugyanakkor van a születésnapja. Becsüljük meg annak esélyét, hogy veszít.
- **4.2.20. Feladat [10].** Az előző feladat folytatásaként határozzuk meg V_n^k/n^k határértékét, ha $n, k \rightarrow \infty$ úgy, hogy $k^2/n \rightarrow c$.
- **4.2.21. Feladat [5].** Mennyi az esélye, hogy öt lapos pókerben osztás után a kezünkben royalflös, színsor, póker, full, flös, sor, drill, két pár, egy pár, illetve magas lap van? Mi a helyzet, ha magyar kártyával játszunk?
- **4.2.22. Feladat [3].** Bizonyítsuk be, hogy ha $m, n \in \mathbb{N}$, $m \leq n$, akkor

$$\binom{n}{m} = \binom{n}{n-m}$$

értéke akkor maximális, ha $m = \lfloor n/2 \rfloor$ vagy $m = \lceil n/2 \rceil$. Készítsünk grafikont $n \leq 8$ -ra.

→ **4.2.23. Feladat** [8]. Bizonyítsuk be, hogy ha $z, w, v \in \mathbb{C}$ és $k, m, n \in \mathbb{N}$, akkor

$$(1) \quad (z+1) \binom{z}{k} = (k+1) \binom{z+1}{k+1};$$

$$(2) \quad z \binom{z-1}{k} = (z-k) \binom{z}{k};$$

$$(3) \quad \binom{-z}{k} = (-1)^k \binom{z+k-1}{k};$$

$$(4) \quad \binom{z}{m+k} \binom{m+k}{k} = \binom{z}{k} \binom{z-k}{m};$$

$$(5) \quad \binom{z}{k} + \binom{z}{k+1} = \binom{z+1}{k+1};$$

$$(6) \quad \sum_{k=0}^n \binom{z-k}{m} = \binom{z+1}{m+1} + \binom{z-n}{m+1};$$

$$(7) \quad \sum_{k=0}^n \binom{z+k}{k} = \binom{z+n+1}{n};$$

$$(8) \quad \sum_{k=0}^n (-1)^k \binom{z}{k} = (-1)^n \binom{z-1}{n};$$

$$(9) \quad \sum_{k=0}^n \binom{z}{k} \binom{w}{n-k} = \binom{z+w}{n} \quad (\text{összegzési tétel});$$

$$(10) \quad \sum_{k=0}^n \binom{z+n-k-1}{k} \binom{w+k-1}{n-k} = \binom{z+w+n-1}{n};$$

$$(11) \quad \sum_{0 \leq k+m \leq n} \binom{z}{k} \binom{w}{m} \binom{v}{n-k-m} = \binom{z+w+v}{n}.$$

→° **4.2.24. Feladat** [3]. Az analízisben bebizonyítják a *Stirling-formulát*: ha $n \in \mathbb{N}^+$, akkor $n! \approx \sqrt{2\pi n} n^n / e^n$, pontosabban

$$n! = \sqrt{2\pi} \frac{n^{n+1/2}}{e^n} e^{\frac{1}{12n} - c_n}, \quad \text{ahol} \quad 0 \leq c_n \leq \frac{1}{180n^3}.$$

Itt

$$e = 2,71828\,18284\,59045\,23536\,02874\,71352\,66249\,77572\ldots$$

és

$$\pi = 3,14159\,26535\,89793\,23846\,26433\,83279\,50288\,41971\ldots$$

Használjuk fel a formulát $n!$ becslésére $c_n = 0$ választással, ha $n = 1, 2, \dots, 10$, és minden esetben számoljuk ki (közelítőleg) a *relatív hibát*, azaz a közelítés és a pontos érték eltérésének és a pontos értéknek a hányadosát. Vegyük észre, hogy n növelésével a relatív hiba csökken. Megjegyezzük, hogy nagy n esetén a túlsordulás elkerülésére $n!$ helyett célszerűbb lehet annak e alapú logaritmusát számolni, amelyet *természetes logaritmusnak* (*logarithmus naturalis*) neveznek, és $\ln$ -nel jelölnek. (A következő feladat szerint ha $n > 8$, akkor a relatív hiba kisebb, mint 0,0008%.)

°* **4.2.25. Feladat** [7]. Mutassuk meg, hogy az előző feladatban szereplő Stirling-formulát használva $n!$ becslésére $c_n = 0$ választással, ha $n > 8$, akkor a relatív hiba kisebb, mint 0,0008%.)

°* **4.2.26. Feladat** [7]. Meg tudjuk-e a Stirling-formula segítségével pontosan határozni, hogy 1000! hány jegyű? Mi az első néhány jegy? Mi az utolsó jegy?

4.2.27. Feladat [3]. Mutassuk meg indukcióval, hogy

$$\binom{2n}{n} < 4^{n-1}, \quad \text{ha } n \in \mathbb{N}, \quad n > 4.$$

°* **4.2.28. Feladat** [4]. Adjunk pontosabb becslést $\binom{2n}{n}$ értékére a Stirling-formulával.

4.2.29. Feladat [5]. Hány olyan részhalmaza van a $H = \{1, 2, \dots, n\}$ halmaznak, amelyre teljesül, hogy ha $j \in H$, akkor $j + 1 \notin H$?

4.2.30. Feladat [6]. Hány olyan részhalmaza van a $H = \{1, 2, \dots, n\}$ halmaznak, amelyre teljesül, hogy ha $j, j + 1 \in H$, akkor $j + 2 \in H$?

4.2.31. Feladat [11]. Tervezzünk programot, amely valamilyen sorrendben megadja az $\{1, 2, \dots, n\}$ halmaz összes permutációját, k -ad osztályú varációját, k -ad osztályú kombinációját, k -ad osztályú ismétléses variációját, k -ad osztályú ismétléses kombinációját, illetve $i_1, i_2, \dots, i_n$ ismétlődésű ismétléses permutációját.

4.2.32. Feladat [6]. Ha $m, n \in \mathbb{N}$ és $m \leq n$, akkor az *elsőfajú Stirling-számokat* a

$$\left[\begin{matrix} n \\ m \end{matrix} \right] = \sum_{0 < k_1 < k_2 < \dots < k_{n-m} < n} k_1 k_2 \cdots k_{n-m}$$

formulával, a *másodfajú Stirling-számokat* pedig a

$$\left\{ \begin{matrix} n \\ m \end{matrix} \right\} = \sum_{1 \leq k_1 \leq k_2 \leq \dots \leq k_{n-m} \leq m} k_1 k_2 \cdots k_{n-m}$$

formulával definiáljuk. Mutassuk meg, hogy ha $m > 0$, akkor

$$\left[\begin{matrix} n+1 \\ m \end{matrix} \right] = n \left[\begin{matrix} n \\ m \end{matrix} \right] + \left[\begin{matrix} n \\ m-1 \end{matrix} \right] \quad \text{és} \quad \left\{ \begin{matrix} n+1 \\ m \end{matrix} \right\} = m \left\{ \begin{matrix} n \\ m \end{matrix} \right\} + \left\{ \begin{matrix} n \\ m-1 \end{matrix} \right\}.$$

Ezen összefüggések alapján foglaljuk táblázatba $\left[\begin{matrix} n \\ m \end{matrix} \right]$, illetve $\left\{ \begin{matrix} n \\ m \end{matrix} \right\}$ értékeit, ha $0 \leq m \leq n \leq 8$.

4.2.33. Feladat [3]. Mutassuk meg, hogy bármely $z \in \mathbb{C}$ -re és $n \in \mathbb{N}$ -re

$$n! \binom{z}{n} = \sum_{m=0}^n (-1)^{n-m} \begin{bmatrix} n \\ m \end{bmatrix} z^m.$$

4.2.34. Feladat [7]. Mutassuk meg, hogy bármely $z \in \mathbb{C}$ -re és $n \in \mathbb{N}$ -re

$$z^n = \sum_{m=0}^n m! \left\{ \begin{matrix} n \\ m \end{matrix} \right\} \binom{z}{m}.$$

4.2.35. Feladat [3]. Mutassuk meg, hogy egy n elemű halmaz m elemű osztályozásainak száma $\left\{ \begin{matrix} n \\ m \end{matrix} \right\}$.

4.2.36. Feladat [7]. Ha f az X egy permutációja, egy $x \in X$ elem pályáját az $x, f(x), f(f(x)), \dots$ elemek alkotják. Mutassuk meg, hogy a pályák X egy osztályozását adják. Mutassuk meg, ha X -nek n eleme van, akkor olyan permutációja X -nek, amelyre a pályák m elemű osztályozást adnak, $\left[\begin{matrix} n \\ m \end{matrix} \right]$ van.

4.2.37. További feladatok megoldásokkal. [56]: 1.3-4–1.3-16, 1.3-18–1.4-25, 1.4-27–1.5-36.

4.2.38. További feladatok. [25]: VIII.1.2–VIII.1.7, VIII.1.9–VIII.1.12, VIII.1.14–VIII.1.18, VIII.1.20–VIII.1.23, VIII.1.25; [46]: 1.2.6.1–1.2.6.2, 1.2.6.4, 1.2.6.6–1.2.6.7, 1.2.6.8–1.2.6.9, 1.2.6.12, 1.2.6.18, 1.2.6.19–1.2.6.24, 1.2.6.31–1.2.6.32, 1.2.6.38–1.2.6.39, 1.2.6.47–1.2.6.48, 1.2.6.50–1.2.6.56, 1.2.6.59, 1.2.6.61–1.2.6.63, 1.2.6.66, 1.2.6.67, 1.2.6.68; [59]: I.3.25, I.3.45; [63]: 1.§1–1.§8, 1.§16–1.§18, 1.§26–1.§27, 1.§30–1.§33, 1.§35–1.§38, 1.§42–1.§43; [64]: 1.3.1–1.3.4, 1.4.1, 1.4.2, 1.5.1–1.5.6, 1.6.1, 1.6.2, 1.7.1–1.7.4, 1.8.1–1.8.34, 3.2.1–3.2.3, 3.3.1–3.3.4, 3.4.1–3.4.3, 3.6.1–3.6.4, 5.1.1–5.1.5, 5.2.1–5.2.4, 5.4.1–5.4.5; [82]: IV.5.2–IV.5.4, IV.5.7, IV.5.9–IV.5.11, IV.5.13, IV.5.14, IV.5.15, IV.5.17, IV.5.22, IV.5.24–IV.5.30, IV.5.32; [84]: 1.24–1.26.

4.3 Binomiális és polinomiális tétel, szita formula

4.3.1. Binomiális tétel. Legyenek x, y egy R kommutatív egységelemes gyűrű elemei, $n \in \mathbb{N}$. Ekkor

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}.$$

Ha a gyűrű nem egységelemes, akkor is igaz az állítás $n \in \mathbb{N}^+$ esetén, ha a formailag szereplő, de nem létező nulladik hatványokat egyszerűen kihagyjuk.

Az $\binom{n}{k}$ együtthatókat *binomiális együttható*knak is nevezik. Szokásos elrendezésük a *Pascal-háromszög*: az n indexű sorban az $(x+y)^n$ -ben fellépő együtthatók vannak.

[illegible]

Bizonyítás. Indukcióval: $n = 0, 1$ -re az állítás nyilvánvaló. Ha n -re teljesül, akkor a disztributivitást felhasználva,

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

így csak azt kell belátnunk, hogy

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1},$$

ha $0 \leq k < n$, ami a bal oldalt közös nevezőre hozva adódik. $\square$

4.3.2. Következmény.

$$\sum_{k=0}^n \binom{n}{k} = 2^n \quad \text{és} \quad \sum_{k=0}^n \binom{n}{k} (-1)^k = 0.$$

Bizonyítás. A binomiális tételből $x = 1$, $y = 1$, illetve $x = 1$, $y = -1$ helyettesítéssel adódik. $\square$

4.3.3. Polinomiális tétel. Legyen $r \in \mathbb{N}$, $x_1, x_2, \dots, x_r$ egy R kommutatív egységelemes gyűrű elemei, $n \in \mathbb{N}$. Ekkor

$$(x_1 + x_2 + \cdots + x_r)^n = \sum_{\substack{i_1 + i_2 + \cdots + i_r = n \\ i_1, i_2, \dots, i_r \in \mathbb{N}}} P_n^{i_1, i_2, \dots, i_r} x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r}.$$

Ha a gyűrű nem egységelemes, akkor is igaz az állítás $r, n \in \mathbb{N}^+, i_1, \dots, i_r \in \mathbb{N}$ esetén, ha a formailag szereplő, de nem létező nulladik hatványokat egyszerűen kihagyjuk.

A tételben játszott szerepük miatt szokás a $P_n^{i_1, i_2, \dots, i_r}$ számokat *polinomiális együtt-hatóknak* is nevezni.

Bizonyítás. Indukcióval: $r = 0$, 1-re az állítás nyilvánvaló, az $r = 2$ esetet már láttuk. Ha $r - 1$ -re teljesül, akkor $y = x_2 + \dots + x_r$ jelöléssel, a binomiális tételt és az indukciós feltevést felhasználva,

$$\begin{aligned}
 (x_1 + x_2 + \dots + x_r)^n &= (x_1 + y)^n = \sum_{i_1=0}^n \binom{n}{i_1} x_1^{i_1} y^{n-i_1} \\
 &= \sum_{i_1=0}^n \binom{n}{i_1} x_1^{i_1} \sum_{i_2+\dots+i_r=n-i_1} P_{n-i_1}^{i_2, \dots, i_r} x_2^{i_2} \dots x_r^{i_r} \\
 &= \sum_{i_1=0}^n \frac{n!}{i_1!(n-i_1)!} x_1^{i_1} \sum_{i_2+\dots+i_r=n-i_1} \frac{(n-i_1)!}{i_2! \dots i_r!} x_2^{i_2} \dots x_r^{i_r} \\
 &= \sum_{i_1+i_2+\dots+i_r=n} P_n^{i_1, i_2, \dots, i_r} x_1^{i_1} x_2^{i_2} \dots x_r^{i_r}. \quad \square
 \end{aligned}$$

4.3.4. Logikai szita formula. Legyenek $X_1, X_2, \dots, X_k$ az X véges halmaz részhalmazai, f az X -en értelmezett, egy Abel-csoportba képező függvény. Legyen

$$S = \sum_{x \in X} f(x),$$

$$S_r = \sum_{1 \leq i_1 < i_2 < \dots < i_r \leq k} \sum_{x \in X_{i_1} \cap X_{i_2} \cap \dots \cap X_{i_r}} f(x),$$

és legyen

$$S_0 = \sum_{x \in X \setminus \bigcup_{i=1}^k X_i} f(x).$$

Ekkor

$$S_0 = S - S_1 + S_2 - S_3 + \dots + (-1)^k S_k,$$

vagy másként

$$S - S_0 = S_1 - S_2 + \dots + (-1)^{k+1} S_k.$$

A formulát leggyakrabban az $f \equiv 1$ függvénnyel alkalmazzuk, ekkor S_0 a „jó” száma, az X_i -k pedig a „rosszak” halmazai.

Bizonyítás. Ha $x \in X \setminus \bigcup_{i=1}^k X_i$, akkor $f(x)$ mindkét oldalon egyszer szerepel, a jobb oldalon csak S -ben. Egyébként legyenek $X_{j_1}, X_{j_2}, \dots, X_{j_t}$ azok a részhalmazok, amelyek tartalmazzák x -et. A bal oldalon $f(x)$ nem szerepel. A jobb oldalon valamely

$$\sum_{x \in X_{i_1} \cap X_{i_2} \cap \dots \cap X_{i_r}} f(x)$$

összegben $f(x)$ pontosan akkor lép fel, ha $\{i_1, i_2, \dots, i_r\} \subset \{j_1, j_2, \dots, j_t\}$. Ha $r > t$, akkor nincs ilyen $\{i_1, i_2, \dots, i_r\}$. Ha $r \leq t$, akkor pontosan

$$\binom{t}{r}$$

ilyen $\{i_1, i_2, \dots, i_r\}$ van, így a jobb oldalon $f(x)$ együtthatója

$$\sum_{r=0}^t \binom{t}{r} (-1)^r = 0. \quad \square$$

◦ **4.3.5. Példa.** Határozzuk meg a 120-nál nem nagyobb prímek számát. Az $1, 2, \dots, n$ számok között k többszöröseinek száma $\lfloor n/k \rfloor$. Innen 120-ig

$$\begin{aligned} & 120 - \lfloor 120/2 \rfloor - \lfloor 120/3 \rfloor - \lfloor 120/5 \rfloor - \lfloor 120/7 \rfloor \\ & + \lfloor 120/6 \rfloor + \lfloor 120/10 \rfloor + \lfloor 120/14 \rfloor + \lfloor 120/15 \rfloor + \lfloor 120/21 \rfloor + \lfloor 120/35 \rfloor \\ & - \lfloor 120/30 \rfloor - \lfloor 120/42 \rfloor - \lfloor 120/70 \rfloor - \lfloor 120/105 \rfloor \\ & + \lfloor 120/210 \rfloor \\ & = 120 - 60 - 40 - 24 - 17 + 20 + 12 + 8 + 8 + 5 + 3 - 4 - 2 - 1 - 1 + 0 = 27 \end{aligned}$$

olyan szám van, amely nem többszöröse sem 2-nek, sem 3-nak, sem 5-nek, sem 7-nek. Az 1 nem prímszám, így $26 + 4 = 30$ prímszám van 120-ig.

→ **4.3.6. Feladat [0].** Mi köze a Pascal-háromszögnek ahhoz, hogy $11^4 = 14641$?

→ **4.3.7. Feladat [3].** Hány nullára végződik a $11^{100} - 1$ szám?

→ **4.3.8. Feladat [3].** Bizonyítsuk be, hogy ha $k, n \in \mathbb{N}$, akkor

$$\sum_{k=0}^n \binom{n}{k} \binom{n}{n-k} = \sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}.$$

→ **4.3.9. Feladat [3].** Bizonyítsuk be, hogy ha $k, m, n \in \mathbb{N}$ és $m \leq n$, akkor

$$\sum_{k=m}^n \binom{k}{m} = \binom{n+1}{m+1}.$$

→◦ **4.3.10. Feladat [6].** Bizonyítsuk be a *Moivre-tételt*: ha $n \in \mathbb{N}$, $\varphi \in \mathbb{R}$, akkor

$$\cos(n\varphi) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \cos^{n-2k}(\varphi) \sin^{2k}(\varphi)$$

és

$$\sin(n\varphi) = \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} (-1)^k \cos^{n-2k-1}(\varphi) \sin^{2k+1}(\varphi),$$

azaz hogy $\cos(n\varphi)$ és $\sin(n\varphi)$ is $\cos \varphi$ és $\sin \varphi$ polinomja.

→ **4.3.11. Feladat [3].** Bizonyítsuk be, hogy

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} = \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n}{2k+1} = 2^{n-1}, \quad \text{ha } n \in \mathbb{N}^+.$$

→ **4.3.12. Feladat [5].** Hányféleképpen választhatunk ki n tárgy közül páratlan számú tárgyat?

4.3.13. Feladat [6]. Legyen $k, n \in \mathbb{N}$. Bizonyítsuk be, hogy

(1)

$$\sum_{k=1}^n k \binom{n}{k} = n2^{n-1};$$

(2)

$$\sum_{k=2}^n k(k-1) \binom{n}{k} = n(n-1)2^{n-2};$$

(3)

$$\sum_{k=0}^n (2k+1) \binom{n}{k} = (n+1)2^n;$$

(4)

$$\sum_{k=0}^n \frac{1}{k+1} \binom{n}{k} = \frac{1}{n+1} (2^{n+1} - 1);$$

(5)

$$\sum_{k=0}^n \frac{(-1)^k}{k+1} \binom{n}{k} = \frac{1}{n+1};$$

(6)

$$\sum_{k=0}^n \frac{(2n)!}{(k!)^2((n-k)!)^2} = \binom{2n}{n}^2.$$

4.3.14. Feladat [7]. Figyelembe véve, hogy

$$k^4 = 24 \binom{k}{4} + 36 \binom{k}{3} + 14 \binom{k}{2} + \binom{k}{1},$$

számoljuk ki a $\sum_{k=0}^n k^4$ összeget.

→ **4.3.15. Feladat [3].** Az **a** és **b** betűkből hány olyan n tagú sorozat készíthető, amelyben legfeljebb m számú **a** szerepel? (Nincs jó zárt formula az összegre: lásd [46], 1.2.6.)

4.3.16. Feladat [3]. Egy m elemű véges ábécé betűiből hány olyan n hosszúságú szó készíthető, amelyben

- (1) egy rögzített betű legalább kétszer előfordul;
- (2) egy rögzített betű legalább háromszor előfordul;
- (3) két rögzített betű legalább egyszer előfordul.

→ **4.3.17. Feladat [2].** Egy társasutazás résztvevői mindannyian beszélnek angolul, németül vagy franciául. Hatan tudnak németül, ugyanennyien angolul, heten franciául. Négyen beszélnek angolul és németül, hárman németül és franciául, ketten franciául és angolul. Egyvalaki mindhárom nyelven beszél. Hány résztvevője van a társasutazásnak? Hányan beszélnek csak angolul, illetve csak franciául?

→ **4.3.18. Feladat [3].** A logikai szita formulánál használt jelölésekkel mutassuk meg, hogy ha $X = \cup_{i=1}^k X_i$, akkor $S = S_1 - S_2 + \dots + (-1)^{k-1} S_k$.

4.3.19. Feladat [7]. Egy n házaspárból álló társaság táncol. Hány olyan eset van, amikor senki sem táncol a saját feleségével?

4.3.20. Feladat [7]. A szita-formulával határozzuk meg, hogy hány szürjektív leképezése van egy n elemű halmaznak egy k elemű halmazra. Mi köze ennek a Stirling-számokhoz?

4.3.21. Feladat [7]. Hányféleképpen ültethető le n házaspár egy kerek asztal köré úgy, hogy nők ne kerüljenek egymás mellé, hogy házaspárok ne kerüljenek egymás mellé, illetve hogy mindkét feltétel teljesüljön?

4.3.22. Feladat [9]. Legyen $X_i, i = 1, 2, \dots, n$ egy indexelt halmazcsalád. Ha

$$H \subset \{1, 2, \dots, n\},$$

legyen $P_H = \cup_{i \in H} X_i$ és $Q_H = \cap_{i \in H} X_i$. Jelölje $\mathcal{F}_k$ az $\{1, 2, \dots, n\}$ halmaz összes k elemű részhalmazainak rendszerét. Mutassuk meg, hogy

$$\cup_{H \in \mathcal{F}_k} Q_H \supset \cap_{H \in \mathcal{F}_k} P_H, \quad \text{ha} \quad 2k \leq n+1$$

és

$$\cup_{H \in \mathcal{F}_k} Q_H \subset \cap_{H \in \mathcal{F}_k} P_H, \quad \text{ha} \quad 2k \geq n+1.$$

4.3.23. További feladatok megoldásokkal. [56]: 4.6-37–4.6-39, 4.6-42, 4.8-44–4.8-47; [57], 1.6-37–1.6-39, 1.6-42, 1.8-44–1.8-47.

4.3.24. További feladatok. [63]: 2.§1–2.§4; [64]: 2.3.1, 2.4.1, 2.5.5–2.5.8, 3.1.1–3.1.3, 3.5.1, 3.5.2, 3.7.1, 3.7.2, 3.8.1–3.8.15; [25]: VIII.2.1–VIII.2.7; [3]: I.13–I.16; [82]: IV.5.8, IV.5.18–IV.5.21; [84]: 1.21, 1.23.

Végtelen halmazok

Ebben a fejezetben a végtelen halmazok tulajdonságait tárgyaljuk. A halmazok összehasonlítására vonatkozó tételek után elsősorban a megszámlálható halmazokra koncentrálunk, de a kontinuum számosságú halmazokról is lesz szó.

5.1 Kiválasztási axióma

*** 5.1.1. Kiválasztási axióma.** *Nem üres halmazok bármely indexelt családjához létezik kiválasztási függvény.*

Az axióma úgy is fogalmazható, hogy nem üres halmazok bármely indexelt családjának a Descartes-szorzata nem üres. (Nyilván, ha a halmazcsalád tagjai között van üres is, akkor a szorzat üres.)

Ez az ártatlan kinézetű axióma sok, végtelen halmazokra vonatkozó tétel bizonyításában alapvető szerepet játszik. Leggyakrabban a Zorn-lemma, illetve a jólrendezési tétel alakjában használjuk fel. Ezek bizonyításához szükségünk lesz egy fogalomra és egy lemmára.

*** 5.1.2. Feladat [5].** Mutassuk meg, hogy a kiválasztási axióma ekvivalens azzal a látszólag gyengébb feltétellel, hogy nem üres páronként diszjunkt halmazok bármely indexelt családjához létezik kiválasztási függvény.

*** 5.1.3. Feladat [5].** Mutassuk meg, hogy a kiválasztási axióma ekvivalens a *Zermelo-axiómával* is, amelyben indexelt halmazcsalád helyett halmazrendszer szerepel: nem üres páronként diszjunkt halmazok bármely rendszeréhez van olyan halmaz, amely a halmazrendszer minden halmazával pontosan egy közös elemet tartalmaz.

*** 5.1.4. Feladat [5].** Mutassuk meg, hogy a kiválasztási axióma ekvivalens azzal is, hogy minden $f: X \rightarrow Y$ szürjektív leképezésnek van olyan megszorítása, amely bijektív.

*** 5.1.5. Véges jellegű halmazrendszer.** Halmazok egy $\mathcal{F}$ osztályát *véges jellegűnek* (vagy *véges tulajdonságúnak*) nevezzük, ha egy F halmaz pontosan akkor eleme $\mathcal{F}$ -nek, ha F minden véges részhalmaza eleme $\mathcal{F}$ -nek. Nyilván $\emptyset \in \mathcal{F}$, ha $\mathcal{F} \neq \emptyset$. Véges tulajdonság például részbenrendezett halmaz részhalmazaira a láncság.

*** 5.1.6. Lemma.** *Ha $\mathcal{F}$ véges jellegű, $\mathcal{C} \subset \mathcal{F}$, és $\mathcal{C}$ lánc (a tartalmazásra nézve), akkor $\cup \mathcal{C} \in \mathcal{F}$.*

Bizonyítás. Csak azt kell belátnunk, hogy $\cup \mathcal{C}$ bármely $F = \{x_1, x_2, \dots, x_n\}$ véges részhalmaza eleme $\mathcal{F}$ -nek. Léteznek olyan $C_1, C_2, \dots, C_n$ halmazok $\mathcal{C}$ -ben, amelyekre $x_i \in C_i$ ($i = 1, 2, \dots, n$). Mivel $\mathcal{C}$ lánc, van olyan $i_0 \in \{1, 2, \dots, n\}$, amelyre $C_i \subset C_{i_0}$, ha $i = 1, 2, \dots, n$. Innen $F \subset C_{i_0} \in \mathcal{F}$, és mivel $\mathcal{F}$ véges jellegű, $F \in \mathcal{F}$. $\square$

* **5.1.7. Tétel.** Az alábbi állítások páronként ekvivalensek:

- (1) kiválasztási axióma;
- (2) minden nem üres véges jellegű halmazosztálynak van (a tartalmazásra nézve) maximális eleme (Teichmüller–Tukey-lemma);
- (3) minden részbenrendezett halmaznak van a tartalmazásra nézve maximális lánc (Hausdorff-féle maximumelv);
- (4) ha egy részbenrendezett halmaz minden lánc felülről korlátos, akkor a halmaznak van maximális eleme (Zorn-lemma);
- (5) minden halmaz jólrendezhető (jólrendezési tétel).

Bizonyítás. Először azt mutatjuk meg, hogy a Zorn-lemma következik a Hausdorff-féle maximumelvből. Valóban, ha az X részbenrendezett halmaznak $A \subset X$ egy maximális lánc, és a ennek egy felső korlátja, akkor a maximális kell legyen, mivel $b > a$ esetén $B = A \cup \{b\}$ az A -nál bővebb lánc lenne X -nek.

Mivel egy X részben rendezett halmaz láncai nem üres véges jellegű osztályt alkotnak, a Hausdorff-féle maximumelv következik a Teichmüller–Tukey-lemmából.

Tegyük fel indirekt, hogy a kiválasztási axióma teljesül, de a Teichmüller–Tukey-lemma állítása nem teljesül. Ekkor van olyan véges jellegű $\mathcal{F}$ halmazosztály, amelynek nincs a tartalmazásra nézve maximális eleme. Minden $F \in \mathcal{F}$ -re legyen $\mathcal{A}_F = \{E \in \mathcal{F} : F \subsetneq E\}$. Így az indirekt feltevés szerint nem üres halmazok nem üres rendszerét kapjuk. Legyen f egy ehhez tartozó – a kiválasztási axióma szerint létező – kiválasztási függvény, azaz f az $\mathcal{F}$ -en definiált függvény, amelyre $f(F) \in \mathcal{A}_F$ minden $F \in \mathcal{F}$ -re, azaz $F \subsetneq f(F) \in \mathcal{F}$ minden $F \in \mathcal{F}$ -re. Nevezzük az $\mathcal{F}$ egy $\mathcal{I}$ részosztályát f -induktívnak, ha az alábbi három tulajdonsággal rendelkezik:

- (6) $\emptyset \in \mathcal{I}$;
- (7) $A \in \mathcal{I}$ esetén $f(A) \in \mathcal{I}$;
- (8) ha $\mathcal{B} \subset \mathcal{I}$ egy lánc a tartalmazásra nézve, akkor $\cup \mathcal{B} \in \mathcal{I}$.

Mivel $\mathcal{F}$ nem üres, $\emptyset \in \mathcal{F}$, így az előző lemma szerint maga az $\mathcal{F}$ egy f -induktív halmazosztály. Jelölje $\mathcal{I}_0$ az összes f -induktív halmazosztályok metszetét. Nyilván ez is f -induktív, így ez a legszűkebb f -induktív halmazosztály.

Ennek leírására legyen

$$\mathcal{H} = \{A \in \mathcal{I}_0 : B \in \mathcal{I}_0 \text{ és } B \subsetneq A \text{ esetén } f(B) \subset A\}.$$

Azt állítjuk, hogy ha $A \in \mathcal{H}$ és $C \in \mathcal{I}_0$, akkor $C \subset A$ vagy $f(A) \subset C$. A bizonyításhoz legyen $A \in \mathcal{H}$ és legyen

$$\mathcal{G}_A = \{C \in \mathcal{I}_0 : C \subset A \text{ vagy } f(A) \subset C\}.$$

Állítjuk, hogy minden $A \in \mathcal{H}$ -ra $\mathcal{G}_A = \mathcal{I}_0$. Elég megmutatni, hogy $\mathcal{G}_A$ is f -induktív, mert ekkor $\mathcal{G}_A \supset \mathcal{I}_0$, tehát $\mathcal{G}_A = \mathcal{I}_0$. (6) nyilván teljesül. Legyen $C \in \mathcal{G}_A$. Ekkor $C \subsetneq A$, $C = A$ vagy $f(A) \subset C$. Ha $C \subsetneq A$, akkor $f(C) \subset A$, mivel $A \in \mathcal{H}$. Ha $C = A$, akkor $f(A) \subset f(C)$. Ha $f(A) \subset C$, akkor $f(A) \subset f(C)$, mivel $C \subset f(C)$. Így minden esetben $f(C) \in \mathcal{G}_A$, tehát (7) fennáll. Végül legyen $\mathcal{C}$ egy $\mathcal{G}_A$ -beli lánc. Vagy $C \subset A$ minden

$C \in \mathcal{C}$ -re, amikor is $\cup \mathcal{C} \subset A$, vagy van olyan $C \in \mathcal{C}$, amelyre $f(A) \subset C \subset \cup \mathcal{C}$. Így $\cup \mathcal{C} \in \mathcal{G}_A$ és (8) is teljesül.

Végül azt állítjuk, hogy $\mathcal{H} = \mathcal{J}_0$. Megint elég megmutatni, hogy $\mathcal{H}$ is f -induktív. (6) nyilván fennáll. Legyen $A \in \mathcal{H}$ és $B \in \mathcal{J}_0$ olyan halmaz, amelyre $B \subsetneq f(A)$. Mivel $B \in \mathcal{J}_0 = \mathcal{G}_A$, azt kapjuk, hogy $B \subset A$. Ha $B \subsetneq A$, akkor $\mathcal{H}$ definíciója szerint $f(B) \subset A \subset f(A)$. Ha $B = A$, akkor $f(B) \subset f(A)$. Tehát mindkét esetben $f(B) \subset f(A)$, így $f(A) \in \mathcal{H}$, amivel (7) fennállását beláttuk. Végül legyen $\mathcal{C}$ egy lánc $\mathcal{H}$ -nak, és tegyük fel, hogy $B \in \mathcal{J}_0$ -ra $B \subsetneq \cup \mathcal{C}$. Mivel $B \in \mathcal{J}_0 = \mathcal{G}_A$ minden $A \in \mathcal{C}$ -re, azt kapjuk, hogy $B \subset A$ valamely $A \in \mathcal{C}$ -re, vagy pedig $f(A) \subset B$ minden $A \in \mathcal{C}$ -re. Ha az utóbbi eset állna fenn, azt kapnánk, hogy

$$B \subsetneq \cup \mathcal{C} \subset \cup \{f(A) : A \in \mathcal{C}\} \subset B,$$

ami lehetetlen. Így van olyan $A \in \mathcal{C}$, amelyre $B \subset A$. Ha $B \subsetneq A$, akkor, mivel $A \in \mathcal{H}$, kapjuk, hogy $f(B) \subset A \subset \cup \mathcal{C}$. Ha $B = A$, akkor $B \in \mathcal{H}$ és $\cup \mathcal{C} \in \mathcal{J}_0 = \mathcal{G}_B$. Ebből az következik, hogy $f(B) \subset \cup \mathcal{C}$ (mivel $\cup \mathcal{C} \subset B$ nem lehetséges, hiszen $B \subsetneq \cup \mathcal{C}$). Tehát mindkét esetben $f(B) \subset \cup \mathcal{C}$, és így $\cup \mathcal{C} \in \mathcal{H}$. Ez mutatja, hogy $\mathcal{H}$ -ra teljesül (8) is.

A fenti érvelésekből azt kapjuk, hogy ha $A \in \mathcal{J}_0 = \mathcal{H}$ és $B \in \mathcal{J}_0 = \mathcal{G}_A$, akkor $B \subset A$ vagy $A \subset f(A) \subset B$. Tehát $\mathcal{J}_0$ egy lánc. Legyen $M = \cup \mathcal{J}_0$. Mivel $\mathcal{J}_0$ egy f -induktív osztály, (8) szerint $M \in \mathcal{J}_0$. De (7) szerint $\cup \mathcal{J}_0 = M \subsetneq f(M) \in \mathcal{J}_0$. Ez az ellentmondás bizonyítja, hogy a Teichmüller–Tukey-lemma teljesül.

Következő lépésként a Zorn-lemmából bebizonyítjuk a jólrendezési tételt. Legyen X egy halmaz, és tekintsük $X \times X$ azon részhalmazainak $\mathcal{F}$ osztályát, amelyek az X valamely részhalmazának jólrendezései. Az $\mathcal{F}$ osztályon legyen $A < B$, ha A a B jólrendezésnek $\text{dmn}(B)$ valamely kezdőselejtére való megszorítása, azaz ha A -nak B „folytatása”. A $<$ reláció $\mathcal{F}$ -en szigorú részenrendezés. A megfelelő gyenge relációval ($A \leq B$, ha $A < B$ vagy $A = B$) a $\mathcal{F}$ osztály részenrendezett. Nem nehéz ellenőrizni, hogy ha $\mathcal{G} \subset \mathcal{F}$ egy lánc, akkor $\mathcal{G}$ felülről korlátos, mert $G = \cup \mathcal{G}$ is az X egy részhalmazának a jólrendezése, amely $\mathcal{G}$ felső korlátja. A Zorn-lemma szerint $\mathcal{F}$ -nek van maximális eleme. Legyen F az $\mathcal{F}$ egy maximális eleme. Ha $\text{dmn}(F) \neq X$ lenne, akkor választva egy $x \in X \setminus \text{dmn}(F)$ elemet, $G = F \cup \{(y, x) : y \in \text{dmn}(F) \cup \{x\}\}$ is az X egy részhalmazának, a bővebb $\text{dmn}(F) \cup \{x\}$ -nek a jólrendezése lenne, ami ellentmond F maximális voltának. Így $\text{dmn}(F) = X$, amivel a tételt beláttuk.

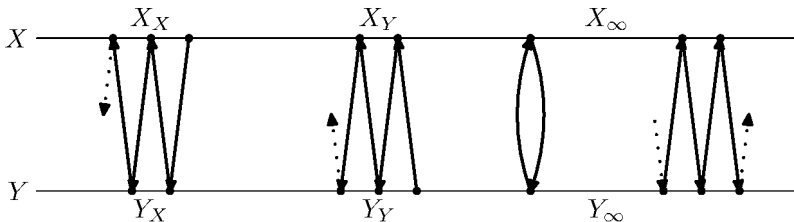
A jólrendezési tételből könnyen megkaphatjuk a kiválasztási axiómát: ha A_i , $i \in I$ nem üres halmazok egy nem üres rendszere, akkor az $A = \cup_{i \in I} A_i$ halmazt tetszőlegesen jólrendezve az $a_i = \min A_i$, ha $i \in I$ definícióval $a : i \mapsto a_i$ egy kiválasztási függvény. $\square$

5.1.8. Halmazok összehasonlítása. Ha X és Y halmazok, és X ekvivalens Y valamely részhalmazával, akkor azt írjuk, hogy $X \preceq Y$ vagy $Y \succeq X$, és azt mondjuk, hogy Y *majorálja* X -et. Véges halmazokra tudjuk, hogy $X \preceq Y$ azzal ekvivalens, hogy $\mathfrak{h}(X) \leq \mathfrak{h}(Y)$. Világos, hogy minden halmazra $X \preceq X$ (*reflexivitás*), és az is, hogy ha $X \preceq Y$ és $Y \preceq Z$, akkor $X \preceq Z$ (*transzitivitás*). Nem világos azonban, hogy ha $X \preceq Y$ és $Y \preceq X$, akkor ebből következik-e, hogy $X \sim Y$. Az sem világos, hogy bármely két halmaz összehasonlítható-e, azaz bármely X, Y halmazokra $X \preceq Y$ és $Y \preceq X$ közül valamelyik fennáll (*dichotómia*). Az is kérdéses, hogy van-e minden X halmazhoz olyan Y , amelyre $X \prec Y$, ahol $X \prec Y$ (vagy $Y \succ X$) azt jelenti, hogy $X \preceq Y$, de $X \not\sim Y$, és úgy nevezzük, hogy Y *szigorúan majorálja* X -et. A következő három tétel erre a három kérdésre ad választ.

5.1.9. Schröder–Bernstein-tétel. Ha $X \lesssim Y$ és $Y \lesssim X$, akkor $X \sim Y$.

Bizonyítás. Feltehetjük, hogy X és Y diszjunktak, mert egyébként az egyik elemeit 0-val, a másikat 1-el állítva párba (azaz mesterségesen „megcímkézve” az elemeiket), ezt elérhetjük. Legyenek $f: X \rightarrow Y$ és $g: Y \rightarrow X$ a feltétel szerint létező kölcsönösen egyértelmű függvények. Egy X -beli x elemet az $f(x)$ „szülőjének” egy Y -beli y elemet pedig a $g(y)$ „szülőjének” fogunk nevezni. Minden X -beli x elemhez létezik x „utódainak” egy $f(x)$, $g(f(x))$, $f(g(f(x)))$, ... végtelen sorozata, és hasonlóan az Y -beli y elem „utódainak” egy $g(y)$, $f(g(y))$, $g(f(g(y)))$, ... végtelen sorozata. A sorozat minden tagja „utódja” az összes megelőzőnek. Azt mondjuk, hogy a sorozat minden tagja „őse” az utána következő tagnak.

Minden elemre vagy a végtelenségig nyomon követhetjük az őseinek sorozatát, vagy végül is egy olyan X -beli x elemhez érünk, amelynek nincs „szülője” (ezek az „árvák” $X \setminus g(Y)$ elemei), vagy egy olyan Y -beli y elemhez érünk, amelynek nincs „szülője” (ezek az „árvák” meg $Y \setminus f(X)$ elemei). Legyen X_X azon X -beli elemek halmaza, amelyek X -ból „származnak” (azaz az X_X halmaz $X \setminus g(Y)$ -ből és ezen halmaz elemeinek X -beli „utódaiból” áll), az X_Y legyen azon X -beli elemek halmaza, amelyek Y -ból „származnak” (azaz az X_Y halmaz $Y \setminus f(X)$ elemeinek X -beli „utódaiból” áll), végül pedig X_∞ legyen azoknak az X -beli elemeknek a halmaza, amelyeknek nincs „árva ősök”. Hasonlóképpen osszuk fel Y -t is az Y_X , Y_Y és Y_∞ halmazra. (Lásd az 5.1.1 ábrát.)



5.1.1 ábra: a bizonyításhoz.

Ha $x \in X_X$, akkor $f(x) \in Y_X$, és az f függvény X_X -re való leszűkítése kölcsönösen egyértelmű megfeleltetés X_X és Y_X között. Ha $x \in X_Y$, akkor x a g^{-1} függvény értelmezési tartományához tartozik, és $g^{-1}(x) \in Y_Y$; a g^{-1} függvény X_Y -ra való leszűkítése kölcsönösen egyértelmű megfeleltetés X_Y és Y_Y között. Végül, ha $x \in X_\infty$, akkor $f(x) \in Y_\infty$, és az f függvény X_∞ -re való leszűkítése kölcsönösen egyértelmű megfeleltetés X_∞ és Y_∞ között, de x a g^{-1} függvény értelmezési tartományához is hozzátartozik, és $g^{-1}(x) \in Y_\infty$, így a g^{-1} függvény X_∞ -re való leszűkítése is kölcsönösen egyértelmű megfeleltetés X_∞ és Y_∞ között. E két utóbbiból akármelyiket választva, és egyesítve a három diszjunkt, kölcsönösen egyértelmű megfeleltetést, egy X és Y közötti kölcsönösen egyértelmű megfeleltetést kapunk.

Ha valaki a fenti bizonyítást nem találja elég meggyőzőnek, akkor itt egy másik bizonyítás: Legyen

$$(1) \quad \varphi(A) = X \setminus g(Y \setminus f(A)), \quad \text{ha } A \subset X.$$

Az alapgondolat, hogy megkeressük a részhalmazok közötti φ leképezés egy „fixpontját”, egy olyan D halmazt, amelyre $\varphi(D) = D$.

Könnyű látni, hogy

$$A \subset B \subset X \text{ esetén } \varphi(A) \subset \varphi(B).$$

Legyen D az összes olyan $A \subset X$ halmazok egyesítése, amelyekre $A \subset \varphi(A)$. Minden ilyen A halmazra $A \subset \varphi(A) \subset \varphi(D)$, így $D \subset \varphi(D)$. Mivel ebből $\varphi(D) \subset \varphi(\varphi(D))$, maga $\varphi(D)$ is egy olyan halmaz, amely része a képének, így $D \supset \varphi(D)$. Innen $D = \varphi(D)$, így (1) szerint

$$D = X \setminus g(Y \setminus f(D)).$$

Tehát $X \setminus D = g(Y \setminus f(D))$. Legyen $h(x) = f(x)$, ha $x \in D$, és $h(x) = g^{-1}(x)$, ha $x \in X \setminus D$. Ekkor h kölcsönösen egyértelmű leképezése X -nek Y -ra, hiszen f kölcsönösen egyértelműen képezi le D -t $f(D)$ -re, g pedig kölcsönösen egyértelműen képezi le $f(D)$ komplementerét D komplementére. $\square$

5.1.10. Következmény. Ha $X \prec Y$ és $Y \preceq Z$, vagy ha $X \preceq Y$ és $Y \prec Z$, akkor $X \prec Z$.

Bizonyítás. Nyilván $X \preceq Z$. Indirekt, ha $X \sim Z$ állna fenn, akkor $Z \preceq X$ is teljesülne, és ebből a tranzitivitás miatt $Y \preceq X$, illetve $Z \preceq Y$ következne, amiből $X \sim Y$, illetve $Y \sim Z$ adódna. $\square$

5.1.11. Tétel. Ha X és Y halmazok, akkor $X \preceq Y$ vagy $Y \preceq X$.

* **Bizonyítás.** Jelölje $\mathcal{F}$ az összes kölcsönösen egyértelmű $X \rightarrow Y$ -beli függvények halmazát. A $\mathcal{F}$ osztály nyilván részbenrendezett a tartalmazásra, azaz a függvények kiterjesztésére vonatkozóan. Megmutatjuk, hogy a Zorn-lemma alkalmazható. Azt kell észrevenni, hogy ha $\mathcal{G} \subset \mathcal{F}$ egy lánc, akkor $g = \bigcup \mathcal{G}$ egy kölcsönösen egyértelmű $X \rightarrow Y$ -beli függvény. Ez nyilván felső korlátja $\mathcal{G}$ -nek.

A Zorn-lemma szerint $\mathcal{F}$ -nek van maximális eleme. Legyen f az $\mathcal{F}$ egy maximális eleme. Azt kell belátnunk, hogy $\text{dmn}(f) = X$ vagy $\text{rng}(f) = Y$. Ha nem ez lenne a helyzet, akkor $x \in X \setminus \text{dmn}(f)$ és $y \in Y \setminus \text{rng}(f)$ választással $f \cup \{(x, y)\}$ is egy $X \rightarrow Y$ -beli kölcsönösen egyértelmű függvény lenne, ami ellentmond f maximális voltának. $\square$

5.1.12. Cantor tétele. Bármely X halmazra $X \prec \wp(X)$.

Bizonyítás. Nyilván $x \mapsto \{x\}$ kölcsönösen egyértelmű leképezése X -nek $\wp(X)$ -be, így $X \preceq \wp(X)$. Legyen f egy X -et $\wp(X)$ -be leképező kölcsönösen egyértelmű függvény, és legyen $Y = \{x \in X : x \notin f(x)\}$. Ha $f(y) = Y$ valamely $y \in X$ -re, akkor $y \in Y$ nem lehetséges Y definíciója szerint. De $y \notin Y$ sem lehetséges, mert $f(y) = Y$ miatt ebből $y \in Y$ következne. Azaz f értékkészlete nem lehet az egész $\wp(X)$.

A bizonyítás alapötlete legjobban az $X = \mathbb{N}$ esetben érthető meg. Az $\mathbb{N}$ részhalmazai a karakterisztikus függvényeikkel, azaz végtelen 0–1 sorozatokkal azonosíthatók. Ha adott végtelen 0–1 sorozatok egy f_n , $n \in \mathbb{N}$ végtelen sorozata, akkor mindig kaphatunk egy olyan g végtelen 0–1 sorozatot, amely ebben a felsorolásban nem szerepel: legyen $g(n) = 1 - f_n(n)$, mert ekkor g az f_n -től biztosan különbözik az n helyen (Cantor-féle átlós eljárás). $\square$

→ **5.1.13. Feladat [1].** Mutassuk meg, hogy ha $C \subset A$ és $B \subset D$, de $C \cup D \sim C$, akkor $A \cup B \sim A$.

* **5.1.14. Feladat [5].** Mutassuk meg, hogy tetszőleges A_i ($i \in I$) indexelt halmazcsalád diszjunktta tehető, azaz létezik hozzá olyan, páronként diszjunkt halmazokból álló B_i ($i \in I$) indexelt halmazcsalád, amelyre $\cup_{i \in I} A_i = \cup_{i \in I} B_i$.

* **5.1.15. Feladat [6].** Mutassuk meg, hogy ha létezik A -t B -re képező függvény, akkor $B \preceq A$.

* **5.1.16. Feladat [6].** Mutassuk meg, hogy ha létezik A -t B -re képező függvény és létezik B -t A -ra képező függvény, akkor $A \sim B$.

5.1.17. Feladat [6]. Mutassuk meg, hogy tetszőleges A, B, C halmazokra

- (1) ha $A \preceq B$, akkor $A \times C \preceq B \times C$;
- (2) ha $A \preceq B$, akkor $A^C \preceq B^C$;
- (3) ha $A \preceq B$, akkor $C^A \preceq C^B$.

5.1.18. Feladat [8]. Legyen A egy négyzet, B pedig egy körlap. Mutassuk meg, hogy léteznek olyan $A = A_1 \cup A_2$ és $B = B_1 \cup B_2$ diszjunkt felbontások, hogy A_1 hasonló B_1 -hez és A_2 hasonló B_2 -höz.

* **5.1.19. Feladat [8].** Mutassuk meg, hogy $\mathbb{R}$ egy korlátos részhalmaza nem lehet egybevágó egy valódi részhalmazával. (Nem korlátos halmazokra ez nyilván nem igaz.)

* **5.1.20. Feladat [8].** Mutassuk meg, hogy egy $H \subset \mathbb{R}$ halmazhoz legfeljebb egy olyan $x \in H$ létezik, amelyre H egybevágó $H \setminus \{x\}$ -szel.

* **5.1.21. Feladat [12].** Adjunk meg $\mathbb{C}$ -ben olyan korlátos halmazt, amely egybevágó egy valódi részhalmazával.

* **5.1.22. Feladat [12].** Mutassuk meg, hogy ha $\mathbb{C}$ egy korlátos részhalmaza egybevágó egy valódi részhalmazával, akkor az egybevágóság forgatás.

* **5.1.23. Feladat [10].** Mutassuk meg, hogy minden részben rendezés kiterjeszthető rendezéssé.

* **5.1.24. Feladat [10].** Mutassuk meg, hogy ha A az F test feletti X vektortér egy lineárisan független részhalmaza, S pedig a vektortér egy olyan részhalmaza, hogy X minden eleme előáll S -beli elemek véges lineáris kombinációjaként (generátorrendszer), és $A \subset S$, akkor a vektortérnek létezik olyan B maximális lineárisan független részhalmaza (Hamel-bázisa), amelyre $A \subset B \subset S$; speciálisan minden vektortérnek létezik Hamel-bázisa. Mutassuk meg, hogy egy adott bázis esetén a vektortér minden eleme egyértelműen állítható elő a báziselemek (véges) lineáris kombinációjaként.

* **5.1.25. Feladat [10].** Az előző feladat folytatásaként mutassuk meg, hogy az X vektortér bármely két bázisa, mint halmaz, ekvivalens. (A bázisok közös elemszáma a tér *algebrai dimenziója*.)

* **5.1.26. Feladat [10].** Mutassuk meg, hogy minden X rendezett halmaznak van olyan jólrendezett W részhalmaza, amelyre minden $x \in X$ -hez van olyan $y \in W$, hogy $x \leq y$.

5.1.27. További feladatok. [36]: 10.1–10.7; [84]: 1.18, 2.2, 2.5–2.9, 2.11–2.14, 16, 8.1–8.20.

5.2 Megszámlálható halmazok

5.2.1. Megszámlálható halmazok. Egy halmazt *megszámlálhatóan végtelennek* nevezünk, ha ekvivalens $\mathbb{N}$ -nel. Ha egy halmaz véges vagy megszámlálhatóan végtelen, akkor *megszámlálhatónak* nevezzük. (Vannak, akik megszámlálható alatt megszámlálhatóan végtelent értenek.)

5.2.2. Tétel. *Egy halmaz akkor és csak akkor végtelen, ha van megszámlálhatóan végtelen részhalmaza.*

Bizonyítás. Ha egy halmaznak van végtelen részhalmaza, akkor nem lehet véges, mert véges halmaz minden részhalmaza is véges. A másik irány bizonyításának ötlete, hogy az X végtelen halmazból kiválasztunk egy különböző elemekből álló $x_0, x_1, \dots$ sorozatot.

A bizonyítás felhasználja a kiválasztási axiómát és az általános rekurziótételt. Legyen F egy, az X véges részhalmazaihoz a komplementerük egy elemét rendelő (kiválasztási) függvény. Ha $h:]\leftarrow, n[\rightarrow X$ egy függvény, legyen $f(h) = F(\text{rng}(h))$, és alkalmazzuk az általános rekurziótételt. Egy $x: \mathbb{N} \rightarrow X$ kölcsönösen egyértelmű leképezést kapunk, ennek értékkészlete X -nek megszámlálható végtelen részhalmaza. $\square$

5.2.3. Tétel. *Egy X halmaz akkor és csak akkor véges, ha $X \prec \mathbb{N}$, akkor és csak akkor megszámlálható, ha $X \preceq \mathbb{N}$, és akkor és csak akkor végtelen, ha $\mathbb{N} \preceq X$.*

Bizonyítás. Ha X véges, akkor $X \preceq \mathbb{N}$, de $X \approx \mathbb{N}$ az előző tétel szerint, így $X \prec \mathbb{N}$. Megfordítva, ha $X \prec \mathbb{N}$, akkor X nem lehet végtelen, mert az előző tétel szerint $\mathbb{N} \preceq X$ következne, ebből pedig $X \prec X$, ami ellentmondás. A második állítás most már nyilvánvaló. A harmadik állítás következik az előző tételből. $\square$

5.2.4. Következmény. *Megszámlálható halmaz bármely részhalmaza is megszámlálható.* $\square$

5.2.5. Tétel. *Egy X nem üres halmazra $X \preceq Y$ pontosan akkor teljesül, ha létezik Y -t X -re képező g leképezés.*

Bizonyítás. Válasszunk ki minden $g^{-1}(x)$, $x \in X$ halmazból egy $f(x)$ elemet. Az f kölcsönösen egyértelműen képezi le X -et Y -ba, így $X \preceq Y$. Megfordítva, ha f az X -et kölcsönösen egyértelműen képezi le Y -ba, akkor legyen az értékkészletén $g = f^{-1}$, az Y többi eleméhez pedig rendeljük hozzá X egy tetszőleges elemét. $\square$

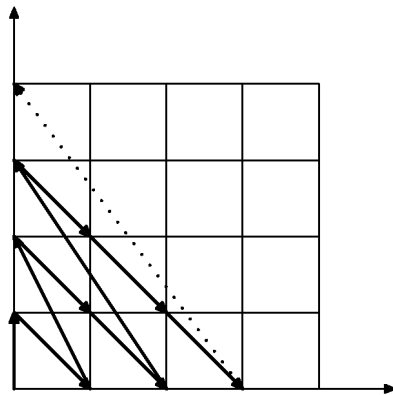
5.2.6. Következmény. *Egy X nem üres halmaz akkor és csak akkor megszámlálható, ha létezik $\mathbb{N}$ -et X -re képező leképezés.*

Bizonyítás. Az előző tételt is felhasználva következik. $\square$

5.2.7. Tétel. *Az $\mathbb{N} \times \mathbb{N}$ halmaz megszámlálhatóan végtelen.*

Bizonyítás. Ha $(m, n) \in \mathbb{N} \times \mathbb{N}$ és $k = m + n$, akkor legyen

$$f(m, n) = \frac{k(k+1)}{2} + m.$$



5.2.1 ábra: átlós bejárás.

Az f kölcsönösen egyértelmű és $\mathbb{N}$ -re képez, mert a $(0, k), (1, k-1), \dots, (k, 0)$ párokat rendre a

$$\frac{k(k+1)}{2}, \frac{k(k+1)}{2} + 1, \dots, \frac{k(k+1)}{2} + k = \frac{k^+(k^+ + 1)}{2} - 1$$

számokba viszi át. $\square$

Az f függvény „működése” az 5.2.1 ábrán tanulmányozható.

5.2.8. Tétel. *Megszámlálható halmazok megszámlálható indexelt családjának az egyesítése megszámlálható.*

Bizonyítás. Legyen I megszámlálható, és X_i megszámlálható minden $i \in I$ -re. Nyilván feltehetjük, hogy I és minden X_i nem üres. Válasszunk olyan $f_i, i \in I$ és g függvényeket, amelyek $\mathbb{N}$ -et X_i -re, illetve I -re képezik le. Legyen $h(m, n) = f_{g(m)}(n)$. Ekkor h az $\mathbb{N} \times \mathbb{N}$ -et $X = \bigcup_{i \in I} X_i$ -re képezi le, így az előző tételből következik az állítás. $\square$

5.2.9. Következmény. $\mathbb{Z}, \mathbb{Q}, \mathbb{N}^n$ ($n \in \mathbb{N}$), $\bigcup_{n=0}^{\infty} \mathbb{N}^n$ halmazok megszámlálhatóak.

Bizonyítás. Mivel $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$, $\mathbb{Q} = \bigcup_{n=1}^{\infty} \{m/n : m \in \mathbb{Z}\}$, az előző tételből kapjuk az első két állítást. A harmadik állítás is az előző tételből következik indukcióval. A negyedik állítás a harmadik következménye, szintén az előző tétel miatt. $\square$

5.2.10. Tétel. *Ha X megszámlálható halmaz, Y végtelen halmaz, akkor $X \cup Y \sim Y$.*

Bizonyítás. Az X -et helyettesítve $X \setminus Y$ -nal feltehetjük, hogy X és Y diszjunktak. Legyen Z megszámlálhatóan végtelen részhalmaza Y -nak. Legyen f a megszámlálhatóan végtelen Z -t a megszámlálhatóan végtelen $X \cup Z$ -re képező kölcsönösen egyértelmű leképezés, és legyen $g(x) = f(x)$, ha $x \in Z$ és $g(x) = x$, ha $x \in Y \setminus Z$. Ekkor g az Y -t $X \cup Y$ -ra képező kölcsönösen egyértelmű leképezés. $\square$

5.2.11. Következmény. *Egy halmaz akkor és csak akkor végtelen, ha ekvivalens egy valódi részhalmazával.*

Bizonyítás. Már láttuk, hogy véges halmaz nem lehet ekvivalens valódi részhalmazával. Ha X végtelen, és $x \in X$, akkor $Y = X \setminus \{x\}$ sem lehet véges, és az előző tétel szerint ekvivalens X -szel. $\square$

→ **5.2.12. Feladat [3].** Bizonyítsuk be, hogy az egész számokból képezhető véges sorozatok halmaza megszámlálható.

→ **5.2.13. Feladat [3].** Bizonyítsuk be, hogy a véges hosszúságú magyar nyelvű szövegek halmaza megszámlálható.

→ **5.2.14. Feladat [3].** Bizonyítsuk be, hogy a matematikai tételek halmaza megszámlálható.

5.2.15. Feladat [6]. Bizonyítsuk be, hogy $\mathbb{R}$ nem üres nyílt intervallumainak bármely páronként diszjunkt rendszere megszámlálható.

5.2.16. Feladat [7]. Bizonyítsuk be, hogy a síkbeli nem üres nyílt körlapok bármely páronként diszjunkt rendszere megszámlálható.

° **5.2.17. Feladat [5].** Bizonyítsuk be, hogy az *algebrai számok* halmaza, azaz azon $z \in \mathbb{C}$ komplex számok halmaza, amelyekhez van olyan egész együtthatós nem azonosan nulla polinom, amelynek z gyöke, megszámlálható.

5.2.18. Feladat [6]. Bizonyítsuk be, hogy egy halmaz pontosan akkor véges, ha részhalmazai bármely nem üres rendszerében van maximális elem.

* **5.2.19. Feladat [8].** Legyen X megszámlálható rendezett halmaz a következő tulajdonsággal: ha $x, y \in X$, $x < y$, akkor léteznek olyan $u, v, w \in X$, hogy $u < x < v < y < w$. Bizonyítsuk be, hogy X és $\mathbb{Q}$ rendezése hasonló.

°* **5.2.20. Feladat [11].** A síkon mászik egy hangya, minden egész másodpercben egy rácspontban van, a következő másodpercben pedig egy szomszédos rácspontban; irányt nem változtat. A síkon ugrál egy vak bolha, minden egész másodpercben egy rácspontból átugrik egy tetszőleges másik rácspontba. Nem tudja, hogy a hangya honnan indult és merre tart. Adjunk számára stratégiát, amellyel előbb-utóbb letapossa a hangyát. Mi a helyzet, ha a hangyát egy véges automata vezérli, és minden másodpercben az algoritmus által megadott szomszédos rácspontba mászik tovább, a bolhát pedig egy Turing-gép?

°* **5.2.21. Feladat [13].** Bizonyítsuk be, hogy a síkon elhelyezett, páronként diszjunkt T betűk tetszőleges halmaza megszámlálható.

5.2.22. További feladatok. [59]: I.4.1–I.4.23; [84]: 3.14, 3.16–3.18, 3.24–3.29, 3.32, 3.46.

5.3 Nem megszámlálható halmazok

5.3.1. Kontinuum számosságú halmazok. Az X halmazt *kontinuum számosságúnak* nevezzük, ha ekvivalens $\mathbb{R}$ -rel. Természetesen a kontinuum számosságú halmazok végtelenek.

5.3.2. Tétel. Az $\mathbb{R}$ és a $]0, 1[$, $[0, 1]$, $[0, 1[$ és $[0, 1]$ részintervallumai ekvivalensek.

° **Bizonyítás.** Az $f(x) = (1-2x)/(x-x^2)$ kölcsönösen egyértelmű leképezése $]0, 1[$ -nek $\mathbb{R}$ -re. A többi állítás következik az 5.2.10 tételből. $\square$

5.3.3. Tétel. A $\wp(\mathbb{N})$ halmaz és $\mathbb{R}$ ekvivalensek, Cantor tétele szerint tehát a kontinuum számosságú halmazok nem megszámlálhatóak.

° **Bizonyítás.** Mivel $\bigcup_{n=0}^{\infty} \mathbb{N}^n$ megszámlálható, $\mathbb{N}$ összes véges részhalmazainak $\mathcal{F}$ halmaza megszámlálható. Ha $A \subset \mathbb{N}$, jelölje χ_A az A halmaz $\mathbb{N}$ -en értelmezett karakterisztikus függvényét. Az

$$A \mapsto \sum_{k=0}^{\infty} \frac{\chi_A(k)}{2^{k+1}}$$

leképezés kölcsönösen egyértelműen képezi le a $\wp(\mathbb{N}) \setminus \mathcal{F}$ halmazt, azaz $\mathbb{N}$ összes végtelen részhalmazait $[0, 1]$ -re; a $\mathcal{F}$ elemeinek megfelelő véges 0 – 1 sorozatokat azért zártuk ki, mert ha $[0, 1]$ egy elemének van kettes alapú számrendszerben véges előállítása, akkor van egy végtelen is. Így $[0, 1] \sim \wp(\mathbb{N}) \setminus \mathcal{F} \sim \wp(\mathbb{N})$. $\square$

5.3.4. Tétel. Az $\mathbb{R} \times \mathbb{R} = \mathbb{C}$ halmaz kontinuum számosságú.

Bizonyítás. Mivel $\mathbb{R} \sim \wp(\mathbb{N})$, kapjuk, hogy $\mathbb{R} \times \mathbb{R} \sim \wp(\mathbb{N}) \times \wp(\mathbb{N})$. De az $\mathbb{N}$ részhalmazából alkotott párok azonosíthatók $\mathbb{N} \times \{0, 1\}$ részhalmazával, azaz egy megszámlálható végtelen halmaz részhalmazával. $\square$

5.3.5. Következmény. Minden $n \in \mathbb{N}^+$ -ra $\mathbb{R}^n$ kontinuum számosságú.

Bizonyítás. Indukcióval adódik. $\square$

* **5.3.6. A pótlás axiómája.** Ha az

$$\mathcal{F}(x, y, u_1, \dots, u_n)$$

formulára rögzített $u_1, \dots, u_n$ esetén minden x -hez pontosan egy y létezik, amelyre $\mathcal{F}(x, y, u_1, \dots, u_n)$ teljesül, akkor bármely X halmazhoz létezik olyan X -en értelmezett f függvény, amelyre $f(x) = y$ minden $x \in X$ -re.

Az axióma jelentősége, hogy a formulák segítségével megadott „hozzárendelésekből” függvényeket tudunk csinálni.

* **5.3.7. ZFC.** Az előző axiómával teljes a halmazelmélet axiómarendszere. Az általunk tanult változat Zermelo német matematikustól származik, aki azonban a pótlás axiómáját nem vette be az axiómarendszerbe. Az axiómarendszert Fraenkel izraeli matematikus egészítette ki a pótlás axiómájával, kihagyta a kiválasztási axiómát, és kizárt mindent az elméletből, ami nem halmaz (így nem kell a „halmaz” predikátum). Az így kapott axiómarendszert szokás *Zermelo–Fraenkel-axiómarendszernek*, rövidítve *ZF*-nek nevezni. Ha a kiválasztási axiómát (angolul: axiom of choice) is hozzávesszük az axiómarendszerhez, akkor *ZFC*-vel jelöljük. Mivel az eredeti Zermelo-féle axiómarendszer jobban illik a gyakorlati alkalmazásokhoz, például komputeralgebra rendszerekhez, ezt tanultuk.

* **5.3.8. Számosságok.** Számosságon az ekvivalens halmazok „közös tulajdonságát” kívánjuk érteni. Megpróbálhatjuk a számosságot mint az ekvivalens halmazok „osztályát” definiálni, de már az egyelemű halmazok „osztálya” sem halmaz, hiszen ha az lenne, uniója is halmaz lenne, annak pedig minden dolog eleme, ez tehát az általunk tanult axiómákkal nem megy. Ha nem kívánjuk a fenti, *absztrakcióval való definíciót* (bármit is jelentsen ez) elfogadni, egy lehetőségünk marad: az ekvivalens halmazok közül valamilyen szempontok szerint kiemelünk egyet, és azt nevezzük számosságnak. A véges halmazoknál is ezt tettük a $\aleph$ definíciójánál. A megszámlálható végtelen halmazok számosságát $\aleph_0$ -val fogjuk jelölni (ejtsd: alef zéró), és az $\aleph_0 := \omega$ definíciót fogadjuk el. Hasonlóan járhatunk

el nagyobb halmazok számosságának definíciójánál. Például a kontinuum számosságot $\mathfrak{c}$ -vel jelöljük, és elfogadhatnánk a $\mathfrak{c} := \mathbb{R}$ vagy $\mathfrak{c} := \wp(\omega)$ definíciót. Egyik sem szokásos, a nem megszámlálható halmazok számosságát egységes szempontok alapján szokás definiálni, a definíció azonban sok további fogalom bevezetését igényli, így túl bonyolult ahhoz, hogy itt megadjuk. (Számosságokkal kifejezve, $X \sim Y$ azt jelenti, hogy X és Y számossága megegyezik, $X \lesssim Y$ pedig azt, hogy X számossága kisebb vagy egyenlő, mint Y számossága.)

A számosságokkal kapcsolatos legalapvetőbb ismeretek megtalálhatók Szendrei [83] könyvében. A „naív” halmazelmélet szintjén a számosságokat Hewitt–Stromberg [38] könyve tárgyalja. Pontosabb tárgyalás található a Halmos és Sigler [37] könyvben. Axiomatikus tárgyalást ad Hajnal–Hamburger [32], illetve Kelley [43] könyve.

*** 5.3.9. Kontinuumhipotézis.** Még Cantor német matematikus, a halmazelmélet megalapítója vetette fel azt a problémát, hogy van-e olyan halmaz, amely nem megszámlálható, de kontinuumnál kisebb számosságú, azaz van-e olyan X halmaz, amelyre $\mathbb{N} \prec X \prec \wp(\mathbb{N})$. Az az állítás, hogy ilyen halmaz nincs, a *kontinuumhipotézis*. Általánosabban, mivel bármely Y halmazra $Y \prec \wp(Y)$, megkérdezhetjük, hogy van-e olyan Y végtelen halmaz és olyan X halmaz, hogy $Y \prec X \prec \wp(Y)$. Az az állítás, hogy ilyen X, Y halmazok nincsenek, az *általánosított kontinuumhipotézis*. Gödel osztrák matematikus és elméleti fizikus 1939-ben bebizonyította, hogy ha ZFC ellentmondástalan (ezt reméljük), akkor még az általánosított kontinuumhipotézist sem lehet benne megcáfolni. Másrészt jóval később, 1963-ban Cohen amerikai matematikus bebizonyította, hogy ha ZFC ellentmondástalan, akkor a kontinuumhipotézist nem lehet benne bebizonyítani. Ez a két állítás együtt azt jelenti, hogy a kontinuumhipotézis eldönthetetlen.

→ **5.3.10. Feladat [3].** Bizonyítsuk be, hogy minden félegyenes kontinuum számosságú.

→ **5.3.11. Feladat [3].** Bizonyítsuk be, hogy egy kör kerülete kontinuum számosságú.

→ **5.3.12. Feladat [3].** Bizonyítsuk be, hogy ha A és B kontinuum számosságú halmazok, akkor $A \cup B$ is kontinuum számosságú.

→ **5.3.13. Feladat [3].** Bizonyítsuk be, hogy ha $\mathbb{C}$ egy részhalmaza tartalmaz egy pozitív hosszúságú szakaszt, akkor kontinuum számosságú.

5.3.14. Feladat [6]. Bizonyítsuk be, hogy $\mathbb{N} \times \mathbb{R}$, $\mathbb{N}^{\mathbb{N}}$, $\mathbb{R}^{\mathbb{N}}$ és $\mathbb{N}$ összes permutációinak halmaza kontinuum számosságú.

5.3.15. Feladat [6]. Bizonyítsuk be, hogy megszámlálható végtelen sok legalább kételemű megszámlálható halmaz Descartes-szorzata kontinuum számosságú.

5.3.16. Feladat [7]. Bizonyítsuk be, hogy $\wp(\mathbb{R}) \sim \mathbb{N}^{\mathbb{R}} \sim \mathbb{R}^{\mathbb{R}}$.

5.3.17. Feladat [10]. Adjunk meg olyan függvényt, amely $]0, 1[$ -et kölcsönösen egyértelműen ráképezi a pozitív természetes számokból álló sorozatok halmazára.

→ **5.3.18. Feladat [5].** Bizonyítsuk be, hogy az irracionális valós számok halmaza kontinuum számosságú.

→^o **5.3.19. Feladat [5].** Bizonyítsuk be, hogy a nem algebrai valós számok halmaza kontinuum számosságú.

◦ **5.3.20. Feladat [5].** Bizonyítsuk be, hogy $\mathbb{R}$ véges részhalmazainak halmaza kontinuum számosságú.

◦ **5.3.21. Feladat [5].** Bizonyítsuk be, hogy $\mathbb{R}$ felbontható kontinuum sok kontinuum számosságú halmazra.

◦ **5.3.22. Feladat [8].** Bizonyítsuk be, hogy $\mathbb{R}^{\mathbb{R}}$ folytonos függvényeinek halmaza kontinuum számosságú.

◦ **5.3.23. Feladat [10].** Mutassuk meg, hogy van olyan $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ függvény, hogy minden egyváltozós $p: \mathbb{R} \rightarrow \mathbb{R}$ polinomfüggvényhez van olyan $y \in \mathbb{R}$, hogy $p(x) = f(x, y)$ minden $x \in \mathbb{R}$ -re. Választható-e f polinomfüggvénynek?

◦ **5.3.24. Feladat [10].** Mutassuk meg, hogy van olyan $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ függvény, hogy minden egyváltozós $g: \mathbb{R} \rightarrow \mathbb{R}$ folytonos függvényhez van olyan $y \in \mathbb{R}$, hogy $g(x) = f(x, y)$ minden $x \in \mathbb{R}$ -re. Választható-e f folytonos függvénynek?

◦ **5.3.25. Feladat [8].** Bizonyítsuk be, hogy $\mathbb{R}^{\mathbb{R}}$ monoton függvényeinek halmaza kontinuum számosságú.

◦* **5.3.26. Feladat [13].** Állítsuk elő $\mathbb{R}^3$ -at páronként diszjunkt, pozitív sugarú körvonalak egyesítéseként. Lehetnek-e a körvonalak egyenlő sugarúak?

5.3.27. Feladat [11]. Mutassuk meg, hogy ha A végtelen halmaz, akkor $A \sim A \times \{0, 1\}$.

5.3.28. Feladat [5]. Az előző feladatot felhasználva mutassuk meg, hogy ha A végtelen halmaz és $B \precsim A$, akkor $A \cup B \sim A$.

5.3.29. Feladat [11]. Mutassuk meg, hogy ha A végtelen halmaz, akkor $A \times A \sim A$.

5.3.30. Feladat [5]. Az előző feladatot felhasználva mutassuk meg, hogy ha A végtelen halmaz és $\emptyset \neq B \precsim A$, akkor $A \times B \sim A$.

5.3.31. Feladat [7]. Legyen $A \subset \mathbb{R}$ legalább kételemű. Mutassuk meg, hogy $A^{\mathbb{N}} \sim \mathbb{R}$ és $A^{\mathbb{R}} \sim \wp(\mathbb{R})$.

5.3.32. Feladat [7]. Mutassuk meg, hogy bármely A végtelen halmaz véges részhalmazainak rendszere hasonló A -hoz.

5.3.33. Feladat [7]. Mutassuk meg, hogy bármely $A \subset \mathbb{R}$ végtelen halmaz megszámlálható részhalmazainak rendszere kontinuum számosságú.

5.3.34. Feladat [7]. Mutassuk meg, hogy ha egy halmaz az R és az R^{-1} relációval is jólrendezett, akkor véges.

5.3.35. Feladat [12]. Bizonyítsuk be a *König-egyenlőtlenséget*: Ha I nem üres indexhalmaz, és $A_i \prec B_i$ minden $i \in I$ -re, akkor $\cup_{i \in I} A_i \prec \prod_{i \in I} B_i$.

5.3.36. Feladat [7]. Legyen A olyan végtelen rendezett halmaz, amely egyetlen végtelen részhalmazának sincs legnagyobb eleme. Mutassuk meg, hogy A hasonlóan rendezett $\mathbb{N}$ -hez.

5.3.37. Feladat [7]. Legyen A végtelen halmaz. Mutassuk meg, hogy A -nak van olyan jólrendezése, amelyre nincs legnagyobb elem, és olyan is, amelyre van legnagyobb elem.

5.3.38. Feladat [9]. Legyen X legalább kételemű.

- (1) Mutassuk meg, hogy X -nek van olyan p permutációja, amelyre $p(x) \neq x$ minden $x \in X$ -re.
- (2) Mikor van olyan p permutációja X -nek, amelyre $p \circ p = \mathbb{I}_X$?
- (3) Mutassuk meg, hogy X -nek van olyan p permutációja, amelyre $p \circ p \circ p \circ p \circ p \circ p = \mathbb{I}_X$.

5.3.39. Feladat [7]. Mutassuk meg, hogy ha X végtelen halmaz, akkor X permutációinak halmaza ekvivalens $\wp(X)$ -szel.

◦ **5.3.40. Feladat [13].** Mutassuk meg, hogy egy vektortér bármely két Hamel-bázisa ekvivalens mint halmaz.

◦ **5.3.41. Feladat [7].** Legyen X vektortér az F test felett, B pedig egy Hamel-bázisa X -nek. Mutassuk meg, hogy ha B végtelen, akkor X ekvivalens F és B közül a nagyobbikkal.

◦ **5.3.42. Feladat [5].** Legyen B Hamel-bázisa $\mathbb{R}$ -nek mint $\mathbb{Q}$ feletti vektortérnek. Mutassuk meg, hogy B kontinuum számosságú. Lehet-e $B \subset [0, 1]$?

* **5.3.43. Feladat [4].** A ZF axiómarendszerhez hozzá szokás venni a *regularitási axiómát*: minden nem üres halmaznak van tőle diszjunkt eleme. Ennek az axiómának a segítségével bizonyítsuk be:

- (1) nincs olyan x halmaz, amelyre $x \in x$;
- (2) bármely x, y halmazokra $x \notin y$ vagy $y \notin x$;
- (3) nem létezik $x_0 \ni x_1 \ni x_2 \ni \dots$ végtelen halmazsorozat.

5.3.44. További feladatok. [36]: 8.26–8.28, 14.31; [59]: I.4.24–I.4.46; [84]: 3.37, 3.38, 3.43, 3.47, 3.48, 3.52, 3.53.

Számelmélet

Ebben a fejezetben a számelmélet alapjaival foglalkozunk, ideértve néhány rejtjelezési alkalmazást is.

6.1 Oszthatóság

6.1.1. Oszthatóság a természetes számok körében. Az m természetes számot az n természetes szám *osztójának*, az n -et pedig az m *többszörösének* nevezzük, illetve azt mondjuk, hogy n *osztható* m -mel, ha van olyan k természetes szám, hogy $n = mk$; jelölése $m|n$. Az $m = 0$ esetet kivéve, az egyszerűsítési szabály miatt, legfeljebb egy $k \in \mathbb{N}$ (sőt, $k \in \mathbb{R}$) létezik, amelyre $n = mk$, mert ha $n = mk'$ is fennáll, akkor $mk = mk'$, ahonnan $k = k'$. Ha $m \neq 0$, akkor $m|n$ azzal ekvivalens, hogy $n/m \in \mathbb{N}$. A $|$ az *oszthatóság*.

→ **6.1.2. Feladat [0].** Játsszunk osztójátékot! Egy megadott $n > 1$ természetes számnak két játékos felváltva nevezi meg az osztóit. Már megnevezett osztót vagy annak többszörösét nem lehet megnevezni. Az veszít, aki az 1-et mondja.

* **6.1.3. Feladat [10].** Bizonyítsuk be, hogy az osztó játékban minden lépésben valamelyik játékosnak van nyerő stratégiája. Mutassuk meg, hogy a kezdő lépésben az első játékosnak van nyerő stratégiája.

* **6.1.4. Feladat [13].** Adjunk nyerő stratégiát a Nim játékra.

6.1.5. Az oszthatóság tulajdonságai $\mathbb{N}$ -ben. A természetes számok körében

- (1) ha $m|n$ és $m'|n'$, akkor $mm'|nn'$;
- (2) a nullának minden természetes szám osztója;
- (3) a nulla csak saját magának osztója;
- (4) az 1 minden természetes számnak osztója;
- (5) ha $m|n$, akkor $mk|nk$ minden $k \in \mathbb{N}$ -re;
- (6) ha $k \in \mathbb{N}^+$ és $mk|nk$, akkor $m|n$;
- (7) ha $m|n_i$ és $k_i \in \mathbb{N}$, ($i = 1, 2, \dots, j$), akkor $m|\sum_{i=1}^j k_i n_i$;
- (8) bármely nem nulla természetes szám bármely osztója kisebb vagy egyenlő, mint a szám;
- (9) az $|$ reláció reflexív, tranzitív és antiszimmetrikus, azaz részbenrendezés.

Megjegyezzük, hogy bár az $|$ reláció $\mathbb{N}^+$ -on az $\mathbb{N}^+$ -beli $\leq$ leszűkítése, de $\mathbb{N}$ -ben a 0 a legnagyobb elem az $|$ relációra nézve, így ott már $|$ nem leszűkítése $\leq$ -nek, például $0 \nmid 1$, míg $0 \leq 1$ (de $0|0$).

Bizonyítás. A bizonyítások a definíció alapján triviálisak. $\square$

6.1.6. Törzsszámok és prímszámok. Ha egy $n > 1$ természetes szám csak $1 \cdot n = n \cdot 1$ alakban (azaz csak triviális módon) írható fel természetes számok szorzataként, akkor *törzsszámnak* (vagy *felbonthatatlannak*, illetve *irreducibilisnek*) nevezzük. Ekkor n -nek nincs más osztója, mint 1 és saját maga. Például 2, 3, 5, 7, 11, 13, 17, 19, 23 felbonthatatlan számok. A $p > 1$ természetes számot *prímszámnak* nevezzük, ha $p|km$ ($k, m \in \mathbb{N}$) esetén $p|k$ vagy $p|m$. Például $6|2 \cdot 3$, de $6 \nmid 2$ és $6 \nmid 3$, így 6 nem prímszám. Minden prímszám törzsszám, mert ha $p = xy$, akkor $p|x$ esetén $x = pz = x(yz)$ miatt $yz = 1$, ahonnan $y = 1$ és $z = 1$, azaz $x = p$, és hasonlóan $p|y$ esetén $y = p$.

Meg fogjuk mutatni, hogy fordítva, ha egy természetes szám törzsszám, akkor prímszám is, továbbá $\mathbb{N}^+$ minden eleme sorrendtől eltekintve egyértelműen írható fel prímek szorzataként. Célszerűbb azonban $\mathbb{Z}$ -ben dolgozni, mert $\mathbb{Z}$ egységelemes integritási tartomány. Általánosabban is definiálhatunk oszthatóságot, tetszőleges egységelemes integritási tartományban.

→ **6.1.7. Feladat [2].** Mutassuk meg, hogy bármely 3-nál nagyobb páratlan prím két szomszédjának a szorzata osztható 24-gyel.

6.1.8. Feladat [2]. Bizonyítsuk be, hogy öt egymás melletti természetes szám szorzata mindig osztható 120-szal.

6.1.9. Feladat [2]. Mutassuk meg, hogy ha öt egymás melletti természetes számból a középső páros szám, de négyel nem osztható, akkor a szorzatuk osztható 960-nal.

→ **6.1.10. Feladat [2].** Bizonyítsuk be, hogy ha a tízes számrendszerben felírt bármelyik háromjegyű természetes számot kétszer egymás mellé írjuk, akkor a kapott hatjegyű szám osztható 7-tel, 11-gyel és 13-mal.

6.1.11. Feladat [7]. Indukcióval igazoljuk, hogy $n \in \mathbb{N}^+$ -ra

- (1) $6|n(2n+1)(7n+1)$;
- (2) $64|3^{2n+1} - 24n + 61$;
- (3) $8|5^n + 2 \cdot 3^{n-1} + 1$;
- (4) $18|2^{2n} + 24n - 10$;
- (5) $133|11^{n+1} + 12^{2n-1}$;
- (6) $7|5^{2n} + 3 \cdot 2^{5n-2}$;
- (7) $13|3^{n+2} + 4^{2n+1}$;
- (8) $27|2^{5n-4} + 5^{n+1}$;
- (9) $43|6n + 1 + 7^{2n-1}$.

6.1.12. Oszthatóság egységelemes integritási tartományban. Legyen R egységelemes integritási tartomány. Ha $a, b \in R$, azt mondjuk, hogy b az a *osztója*, vagy a a b *többszöröse*, illetve hogy a *osztható* b -vel, ha van olyan $c \in R$, hogy $a = bc$; jelölése $b|a$. A $b = 0$ esetet kivéve legfeljebb egy c létezik, amelyre $a = bc$, mert ha $a = bc'$ is teljesül, akkor $bc = bc'$, ahonnan egyszerűsítéssel $c = c'$.

6.1.13. Az oszthatóság tulajdonságai egységelemes integritási tartományban. Egy egységelemes integritási tartomány elemei körében

- (1) ha $b|a$ és $b'|a'$, akkor $bb'|aa'$;

- (2) a nullának minden elem osztója;
- (3) a nulla csak saját magának osztója;
- (4) az 1 egységelem minden elemnek osztója;
- (5) ha $b|a$, akkor $bc|ac$ minden $c \in R$ -re;
- (6) ha $bc|ac$ és $c \neq 0$, akkor $b|a$;
- (7) ha $b|a_i$ és $c_i \in R$, ($i = 1, 2, \dots, j$), akkor $b|\sum_{i=1}^j c_i a_i$;
- (8) az $|$ reláció reflexív és tranzitív. $\square$

6.1.14. Asszociáltak és egységek. Legyen R egységelemes integritási tartomány. Az „osztója” reláció általában nem antiszimmetrikus (például az egész számok körében). Ha $a|b$ és $b|a$, akkor azt mondjuk, hogy a és b *asszociáltak*. Ez a reláció nyilván reflexív, szimmetrikus és tranzitív, azaz ekvivalenciareláció, továbbá kompatibilis a szorzással. A nullának nincs más asszociáltja, csak saját maga. Az $|$ reláció kompatibilis ezzel az ekvivalenciarelációval, és az ekvivalenciaosztályokon tekintve részbenrendezést kapunk.

Egy elem asszociáltjait leírhatjuk az 1 asszociáltjai segítségével, amelyek nem mások, mint 1 osztói, hiszen 1 bárminek osztója; ezeket *egységeknek* nevezzük. Az egységek R azon elemei, amelyeknek van a szorzásra nézve inverzük. (Így egy egységelemes integritási tartomány pontosan akkor test, ha minden nem nulla eleme egység.) Az egységek a szorzásra nézve Abel-csoportot alkotnak, a gyűrű *egységscsoportját*. Az egységek bármely $a \in R$ -nek osztói, mert $a = 1a$ -nak osztói. Megfordítva nyilvánvaló: ha egy elem minden $a \in R$ -nek osztója, akkor egység. Az egységeket ezzel a tulajdonsággal tetszőleges $R \neq \{0\}$ integritási tartományban is lehet definiálni, de könnyen adódik, hogy ha van egység, akkor R egységelemes: ha ε egy egység, akkor $\varepsilon|\varepsilon$, így valamely $0 \neq e \in R$ -re $\varepsilon = e\varepsilon$. Innen $a\varepsilon = ae\varepsilon$ minden $a \in R$ -re. Mivel $\varepsilon \neq 0$, lehet vele egyszerűsíteni. Az $a \in R$ asszociáltjai az εa alakú elemek, ahol ε egység.

Egy elemnek az asszociáltjaitól különböző osztóit az elem *valódi osztóinak* nevezzük. Egy nem nulla elemnek az asszociáltjai és az egységek a *triviális osztói*.

6.1.15. Felbonthatatlan elem és prímelem. Legyen R egységelemes integritási tartomány. Egy $0 \neq a \in R$ elemet *felbonthatatlannak* (vagy *irreducibilisnek*) nevezünk, ha nem egység, és csak triviális módon írható fel szorzatként, tehát $a = bc$, $b, c \in R$ esetén b vagy c egység. Ez azzal ekvivalens, hogy a -nak nincs más osztója, mint az egységek és az asszociáltjai. A $0 \neq p \in R$ elemet *prímelemnek* nevezzük, ha nem egység és $p|ab$ ($a, b \in R$) esetén $p|a$ vagy $p|b$. (Vannak, akik nem kötik ki, hogy p nem nulla és nem egység.) Minden prímelem felbonthatatlan, mert ha $p = xy$, akkor $p|x$ esetén $x = pz = x(yz)$ miatt $yz = 1$, ahonnan y és z egységek, x és p pedig asszociáltak, és hasonlóan $p|y$ esetén x egység, y és p pedig asszociáltak. (A megfordítás nem minden egységelemes integritási tartományban teljesül! Lásd a 8.2.68 pontot.)

6.1.16. Oszthatóság az egész számok körében. Mivel ha $k, m \in \mathbb{Z}$, akkor $|km| = |k| \cdot |m|$, az egész számok körében $m|n$ pontosan akkor teljesül, ha $|m||n|$ az $\mathbb{N}$ -ben. Az egészek körében az egységek ± 1 , az m egész szám asszociáltjai $\pm m$, továbbá $n \in \mathbb{Z}$ pontosan akkor felbonthatatlan az egész számok körében, ha $|n|$ törzsszám $\mathbb{N}$ -ben, és $p \in \mathbb{Z}$ pontosan akkor prímelem, ha $|p|$ prímszám $\mathbb{N}$ -ben. Ennek alapján az oszthatóságra vonatkozó $\mathbb{N}$ -beli állításokat átfogalmazhatjuk $\mathbb{Z}$ -beli állításokká és viszont. Az egész számok körében vett oszthatóság $\mathbb{N}$ -en visszaadja az ottani oszthatóságot. A 2-vel osztható egészeket *párosnak*, a többi *páratlannak* hívjuk.

6.1.17. Példa: Gauss-egészek. A $G = \{n + im : n, m \in \mathbb{Z}\} \subset \mathbb{C}$ úgynevezett Gauss-egészek egységelemes integritási tartományt alkotnak. Nyilván ± 1 és $\pm i$ egységek. Mivel $|bc|^2 = |b|^2|c|^2$, azt kapjuk, hogy $b|a$ esetén $|b|^2|a|^2$, de $|a|^2$ és $|b|^2$ természetes számok, így $a = 1$ választással kapjuk, hogy nincs is más egység. Emiatt a nulla kivételével minden elemnek négy asszociáltja van.

6.1.18. Legnagyobb közös osztó, legkisebb közös többszörös, relatív prímek. Ezeket a fogalmakat $\mathbb{N}^+$ -ban általában a rendezést felhasználva definiálják. Gyűrűben nincs rendezés, így más utat kell választanunk. Azt mondjuk, hogy az R egységelemes integritási tartományban a $b \in R$ elem az $a_1, a_2, \dots, a_n \in R$ elemeknek egy *legnagyobb közös osztója*, ha $i = 1, 2, \dots, n$ esetén $b|a_i$, és ha $i = 1, 2, \dots, n$ esetén $b'|a_i$, akkor $b'|b$. Ha létezik az $a_1, a_2, \dots, a_n$ elemeknek b legnagyobb közös osztója, akkor minden asszociáltja is az, és más legnagyobb közös osztó nincs. A legnagyobb közös osztó definíciója éppen azt jelenti, hogy a b asszociáltjai által alkotott osztály maximális az oszthatóságra nézve az $a_1, a_2, \dots, a_n$ elemek közös osztóinak osztályai között. Ha az $a_1, a_2, \dots, a_n$ elemek legnagyobb közös osztói egységek, akkor azt mondjuk, hogy $a_1, a_2, \dots, a_n$ *relatív prímek*.

Azt mondjuk, hogy $b \in R$ az $a_1, a_2, \dots, a_n \in R$ elemek *legkisebb közös többszöröse*, ha $i = 1, 2, \dots, n$ esetén $a_i|b$, és ha $i = 1, 2, \dots, n$ esetén $a_i|b'$, akkor $b|b'$. Ha létezik az $a_1, a_2, \dots, a_n$ elemeknek b legkisebb közös többszöröse, akkor minden asszociáltja is az, és más legkisebb közös többszörös nincs. A legkisebb közös többszörös definíciója éppen azt jelenti, hogy b asszociáltjai által alkotott osztály minimális az oszthatóságra nézve az $a_1, a_2, \dots, a_n$ elemek közös többszöröseinek osztályai között.

→ **6.1.19. Feladat [3].** Mutassuk meg, hogy egységelemes integritási tartományban $a|b$ pontosan akkor teljesül, ha a -nak és b -nek létezik d legnagyobb közös osztója, és d az a asszociáltja.

→ **6.1.20. Feladat [3].** Mutassuk meg, hogy ha egy integritási tartományban az a és b elemeknek létezik d legnagyobb közös osztója és $a = da'$, $b = db'$, akkor a' és b' relatív prímek.

→ **6.1.21. Feladat [6].** Határozzuk meg $R = \{a/b : a, b \in \mathbb{Z}, 2 \nmid b\}$ -ben az egységeket és az irreducibilis elemeket.

→ **6.1.22. Feladat [6].** Adjunk meg $R = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$ -ben 1-től és -1 -től különböző egységeket.

6.1.23. Feladat [6]. Bizonyítsuk be, hogy ha egy integritási tartomány bármely két elemének van legnagyobb közös osztója, akkor benne minden irreducibilis elem prímelem.

6.1.24. Legnagyobb közös osztó, legkisebb közös többszörös az egész számok körében. Ha létezik az $a_1, a_2, \dots, a_n \in \mathbb{Z}$ számoknak legnagyobb közös osztója, akkor ezek közül az egyik nemnegatív, ezt $\text{lko}(a_1, a_2, \dots, a_n)$ -nel jelöljük. (A $\text{gcd}(a_1, a_2, \dots, a_n)$ és az $(a_1, a_2, \dots, a_n)$ jelölés is használatos.) Nyilván $\text{lko}(0, \dots, 0) = 0$, egyébként pedig az a_i -k közül a nullákat elhagyva, a közös osztók nem változnak. Az, hogy $a_1, a_2, \dots, a_n$ relatív prímek, azzal ekvivalens, hogy $\text{lko}(a_1, a_2, \dots, a_n) = 1$. Ha létezik az $a_1, a_2, \dots, a_n \in \mathbb{Z}$ számoknak legkisebb közös többszöröse, akkor ezek közül az egyik nemnegatív, jelölje ezt $\text{lkkt}(a_1, a_2, \dots, a_n)$. (Az $\text{lcm}(a_1, a_2, \dots, a_n)$ és az $[a_1, a_2, \dots, a_n]$ jelölés is használatos.) Nyilván, ha valamelyik a_i nulla, akkor az egyetlen közös többszörös a nulla. Például

$$\text{lko}(12, 18) = \text{lko}(-12, 18) = 6$$

és

$$\text{lkt}(12, 18) = \text{lkt}(12, -18) = 36.$$

Az $a, b \in \mathbb{Z}$ számok legnagyobb közös osztója meghatározásának alapgondolata, hogy $\text{lko}(a, b) = \text{lko}(b, a \bmod b)$, és $a \bmod b$ abszolút értéke kisebb, mint b abszolút értéke.

6.1.25. Bővített euklideszi algoritmus. A következő eljárás meghatározza az $a, b \in \mathbb{Z}$ egészek egy d legnagyobb közös osztóját, valamint $x, y \in \mathbb{Z}$ egész számokat úgy, hogy $d = ax + by$ teljesüljön. (Az eljárás során végig $ax_n + by_n = r_n$, $n = 0, 1, \dots$)

(1) [Inicializálás.] Legyen $x_0 \leftarrow 1$, $y_0 \leftarrow 0$, $r_0 \leftarrow a$, $x_1 \leftarrow 0$, $y_1 \leftarrow 1$, $r_1 \leftarrow b$, $n \leftarrow 0$.

(2) [Vége?] Ha $r_{n+1} = 0$, akkor $x \leftarrow x_n$, $y \leftarrow y_n$, $d \leftarrow r_n$, és az eljárás véget ért.

(3) [Ciklus.] Legyen

$$q_{n+1} \leftarrow \lfloor r_n / r_{n+1} \rfloor, \quad r_{n+2} \leftarrow r_n \bmod r_{n+1} = r_n - r_{n+1}q_{n+1},$$

$$x_{n+2} \leftarrow x_n - x_{n+1}q_{n+1}, \quad y_{n+2} \leftarrow y_n - y_{n+1}q_{n+1},$$

$n \leftarrow n + 1$ és menjünk (2)-re.

Bizonyítás. Az $|r_1|, |r_2|, \dots$ természetes számok – mivel r_{n+2} az r_{n+1} -gyel való osztás maradéka – szigorúan monoton csökkenő sorozatot alkotnak, így az eljárás véges sok lépésben véget ér, mert egyébként $\mathbb{N}$ nem lenne jólrendezett. Indukcióval, ha $ax_n + by_n = r_n$ és $ax_{n+1} + by_{n+1} = r_{n+1}$, akkor a második összefüggést szorozva q_{n+1} -gyel és kivonva az elsőből, $ax_{n+2} + by_{n+2} = r_{n+2}$, így végül $d = ax + by$. Innen a és b közös osztói mind osztói d -nek. Kilépéskor $r_{n+1} = 0$, és két eset van: Ha $n = 0$, akkor $d = a$ és $b = 0$. Ha $n > 0$, akkor $r_0, r_1, \dots, r_{n-1}$ mind többszörösei $r_n = d$ -nek, mert $r_{n-1} = q_n r_n$, $r_{n-2} = q_{n-1} r_{n-1} + r_n$, és így tovább, speciálisan $a = r_0$ és $b = r_1$ is többszörösei d -nek. Így d egy legnagyobb közös osztó. $\square$

6.1.26. Megjegyzés. Elég a mindenkor $r_n, x_n, y_n, r_{n+1}, x_{n+1}$ és y_{n+1} értékét tárolni. Ha az x, y számokra nincs szükségünk, az x_n, y_n számok kiszámítását teljesen elhagyhatjuk, és az euklideszi algoritmust kapjuk. Ha csak x -re, illetve csak y -ra van szükség, akkor az y_n -ek, illetve az x_n -ek számítását hagyjuk el. Vegyük észre egyébként, hogy y , illetve x még ekkor is kiszámítható a, b, d és x , illetve a, b, d és y felhasználásával.

6.1.27. Példa: bővített euklideszi algoritmus. Számítsuk ki $\text{lko}(172, 62)$ értékét.

n	q_{n+1}	r_{n+2}	x_{n+2}	y_{n+2}	$r_{n+2} = ax_{n+2} + by_{n+2}$
-2		172	1	0	$172 = 172 \cdot 1 + 62 \cdot 0$
-1		62	0	1	$62 = 172 \cdot 0 + 62 \cdot 1$
0	$2 = \lfloor 172/62 \rfloor$	$48 = 172 \bmod 62$	1	-2	$48 = 172 \cdot 1 + 62 \cdot (-2)$
1	$1 = \lfloor 62/48 \rfloor$	$14 = 62 \bmod 48$	-1	3	$14 = 172 \cdot (-1) + 62 \cdot 3$
2	$3 = \lfloor 48/14 \rfloor$	$6 = 48 \bmod 14$	4	-11	$6 = 172 \cdot 4 + 62 \cdot (-11)$
3	$2 = \lfloor 14/6 \rfloor$	$2 = 14 \bmod 6$	-9	25	$2 = 172 \cdot (-9) + 62 \cdot 25$
4	$3 = \lfloor 6/2 \rfloor$	$0 = 6 \bmod 2$	31	-86	$0 = 172 \cdot 31 + 62 \cdot (-86)$

Tehát az eredmény $2 = 172 \cdot (-9) + 62 \cdot 25$. Érdekes egy számolás elvégezni abban az esetben is, amikor az egyik szám negatív.

6.1.28. Következmény. Bármely $a_1, a_2, \dots, a_n \in \mathbb{Z}$ számoknak létezik legnagyobb közös osztója, és kiszámítása visszavezethető két szám legnagyobb közös osztójának kiszámítására:

$$\text{lko}(a_1, a_2, \dots, a_n) = \text{lko}(\text{lko}(a_1, a_2), a_3, a_4, \dots, a_n).$$

Bizonyítás. Az a_1, a_2 számoknak létezik egy $d_{1,2}$ legnagyobb közös osztója. Az a_1, a_2 közös osztói pontosan $d_{1,2}$ osztói. Így $a_1, a_2, \dots, a_n$ közös osztói $d_{1,2}, a_3, a_4, \dots, a_n$ közös osztói. $\square$

6.1.29. Tétel. A $\mathbb{Z}$ egy eleme pontosan akkor felbonthatatlan, ha prímelem.

A természetes számokra fogalmazva az állítást, egy természetes szám pontosan akkor prímszám, ha törzsszám.

Bizonyítás. Azt már beláttuk, hogy prímelem felbonthatatlan. Tegyük fel, hogy p felbonthatatlan, és legyen $p|mn$. Tegyük fel, hogy $p \nmid m$. Ekkor p és m relatív prímek. A bővített euklideszi algoritmussal kaphatunk olyan x, y egészeket, hogy $px + my = \pm 1$. Innen $pnx + mny = \pm n$. Mivel p osztója a bal oldalnak, a jobb oldalnak is. $\square$

6.1.30. Megjegyzés. Ugyanúgy, mint az előző tétel bizonyításában, kapjuk, hogy ha a és b relatív prímek és $a|bc$, akkor $a|c$.

6.1.31. A számelmélet alaptétele. Minden pozitív természetes szám a sorrendtől eltekintve egyértelműen felírható prímszámok szorzataként.

A természetes és az egész számok körében tekintett oszthatóság kapcsolatát felhasználva, egész számokra átfogalmazva az állítást, minden nem nulla és nem egység egész szám előáll prímelemek szorzataként, és az előállítás sorrendtől és asszociáltaktól eltekintve egyértelmű.

Bizonyítás. Ha $n = 1$, a felbontás az üres szorzat. Egyébként ha n nem irreducibilis, akkor felírható két, nála kisebb, de 1-nél nagyobb szám szorzataként. Indukcióval folytatjuk ezt az eljárást: ha a kapott szorzatnak van nem törzsszám tényezője, akkor a legnagyobb ilyen tényező minden előfordulását helyettesítsük két nála kisebb, de 1-nél nagyobb természetes szám szorzatával. Az eljárás a természetes számok jólrendezettsége miatt véges sok lépésben csupa törzsszám tényezőből álló felbontáshoz vezet.

A felbontás egyértelműségének bizonyításához tegyük fel indirekt, hogy van olyan természetes szám, amely két lényegesen különböző módon bontható fel, és legyen n a legkisebb ilyen:

$$n = p_1 p_2 \cdots p_j = q_1 q_2 \cdots q_k.$$

Mivel $p_1|n$, azaz $p_1|q_1 q_2 \cdots q_k$, a p_1 prímtulajdonsága miatt van olyan i , hogy $p_1|q_i$. Ekkor viszont $p_1 = q_i$, mert q_i törzsszám. Egyszerűsítve a kapott közös tényezővel egy kisebb n' számot kapunk, amelynek felbontása nem egyértelmű. Ez ellentmondás. $\square$

6.1.32. Feladat [0]. Néha szükségünk van arra, hogy egy tízes számrendszerben felírt hosszabb számról megállapítsuk, hogy osztható-e valamely kis számmal, amely relatív prím 10-hez, például 31-gyel. A számból levonva (vagy hozzáadva) 31 valamely többszörösét, olyan számot kaphatunk, amelynek utolsó jegye 0. Ezt elhagyhatjuk, így a szám rövidebb lesz. Állapítsuk meg ezzel a módszerrel, hogy igaz-e, hogy

- (1) $31|23754$;
- (2) $19|20513$;
- (3) $7|8638$.

6.1.33. Feladat [5]. Igazoljuk, hogy az $n > 1$ páratlan szám akkor és csak akkor prím, ha nem állítható elő három vagy háromnál több egymást követő pozitív egész összegeként.

6.1.34. Feladat [5]. Igazoljuk, hogy az $n > 1$ természetes szám akkor és csak akkor prím, ha az

$$\binom{n}{k}$$

binomiális együtthatók az első és az utolsó kivételével mind oszthatók n -nel.

6.1.35. Feladat [5]. Adjuk meg mindazokat az n természetes számokat, amelyekre $n^2 + 1$ osztható $n + 1$ -gyel.

6.1.36. Feladat [5]. Adjuk meg mindazokat az n egész számokat, amelyekre $n^3 - 3$ osztható $n - 3$ -mal.

6.1.37. Feladat [5]. Bizonyítsuk be, hogy az 5^n , $n \in \mathbb{N}^+$ számok utolsó négy számjegyből képzett sorozat tagjai szakaszosan ismétlődnek, adjuk meg a szakaszt, és állapítsuk meg, hogy honnan kezdődik az ismétlődés.

6.1.38. Feladat [3]. Bizonyítsuk be, hogy bármely $s \in \mathbb{N}^+$ -hoz és előre megadott s jegyű tízes számrendszerbeli számhoz van olyan négyzetszám, amelynek első s jegye az előre megadott szám.

6.1.39. Feladat [4]. Adjuk meg mindazokat az n természetes számokat, amelyekre $(n - 1)! + 1 = n^2$.

6.1.40. Feladat [7]. Bizonyítsuk be, hogy $13|2^{70} + 3^{70}$.

→ **6.1.41. Feladat [4].** Alkalmazzuk a bővített euklidészi algoritmust az alábbi szám-párookra:

- (1) 368, 161;
- (2) 12661, 1279;
- (3) 367651, 36802.

6.1.42. Feladat: Lamé tétele [9]. Bizonyítsuk be, hogy ha $a > b \geq 0$ bemenettel az euklidészi algoritmus n osztást végez, akkor $a \geq F_{n+1}$ és $b \geq F_n$, ahol az F_n számok a Fibonacci-számok.

6.1.43. Feladat [5]. Mutassuk meg, hogy $a = F_{n+1}$ és $b = F_n$ bemenettel, ahol az F_n számok a Fibonacci-számok, az euklidészi algoritmus n osztást végez.

6.1.44. Feladat [4]. Adjuk meg tetszőleges $a > b \geq 0$ bemenetre az euklidészi algoritmusban szükséges osztások számát.

6.1.45. Feladat: bináris lko [8]. Az $\text{lko}(a, b) = \text{lko}(|a|, |b|)$, $\text{lko}(2a, 2b) = 2 \text{lko}(a, b)$, $\text{lko}(a, b) = \text{lko}(a - b, b)$ ($a, b \in \mathbb{Z}$), továbbá az $\text{lko}(2a, b) = \text{lko}(a, b)$ ($a, b \in \mathbb{Z}$ és b páratlan) észrevételeket felhasználva adjunk bináris számítógépen hatékony algoritmust a legnagyobb közös osztó kiszámítására.

6.1.46. Eukleidész tétele. Végtelen sok prímszám van.

Bizonyítás. Tegyük fel indirekt, hogy csak véges sok prímszám van, $p_1, p_2, \dots, p_k$, és legyen $n = \prod_{j=1}^k p_j$. Ekkor $n+1$ minden p_j -vel osztva 1-et ad maradékként, tehát nem osztható egyetlen p_j -vel sem. Így prímtényezős felbontásában kell hogy legyen a p_j -ktől különböző prímszám, ami ellentmondás. $\square$

6.1.47. Megjegyzés. Ha, hasonlóan mint az előző bizonyításban, n az összes, a p_k prímnél nem nagyobb prímek szorzata, akkor $n+2, n+3, n+4, \dots, n+p_k$ mind összetettek, azaz a természetes számok sorozatában találtunk $p_k - 1$ egymás utáni összetett számot. Mivel tetszőlegesen nagy prímszám létezik, van akármilyen hosszú csupa összetett számot tartalmazó intervallum.

6.1.48. Megjegyzés. Megmutatható, hogy „elég sok” prímszám van, például a prímszámok reciprokainak összege végtelen. A *prímszámtétel* azt állítja, hogy

$$\lim_{x \rightarrow \infty} \frac{\#\{p: p \leq x, p \text{ prímszám}\}}{\frac{x}{\ln x}} = 1.$$

Illusztrációként lásd a 6.1.1 ábrát: a páratlan számok közül a prímekeket fekete képpont jelzi; soronként 300 páratlan szám.

Az is megmutatható, hogy rögzített $d \in \mathbb{N}^+$ differenciára a prímek „egyenlően oszlanak el” az $a + dn$ ($n \in \mathbb{N}$) számtani sorozatok között, ahol $0 < a \leq d$, $\text{luko}(a, d) = 1$. (Nyilván $\text{luko}(a, d)$ osztja a számtani sorozat minden tagját, így ha nem egy, akkor legfeljebb $n = 0$ -ra kaphatunk prímet.)

6.1.49. Kanonikus alak. A számelmélet alaptételében szereplő prímtényezős felbontást gyakran

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

összevont alakban írjuk, ahol $p_1, p_2, \dots, p_k$ különböző prímek, a kitevők pedig $\mathbb{N}^+$ elemei. Ezt nevezzük a szám *kanonikus alakjának*. A kanonikus alak a tényezők sorrendjétől eltekintve egyértelmű. (Például 9180 kanonikus alakja $2^2 \cdot 3^3 \cdot 5 \cdot 17$.) A kanonikus alakból leolvashatók n pozitív osztói, ezek a

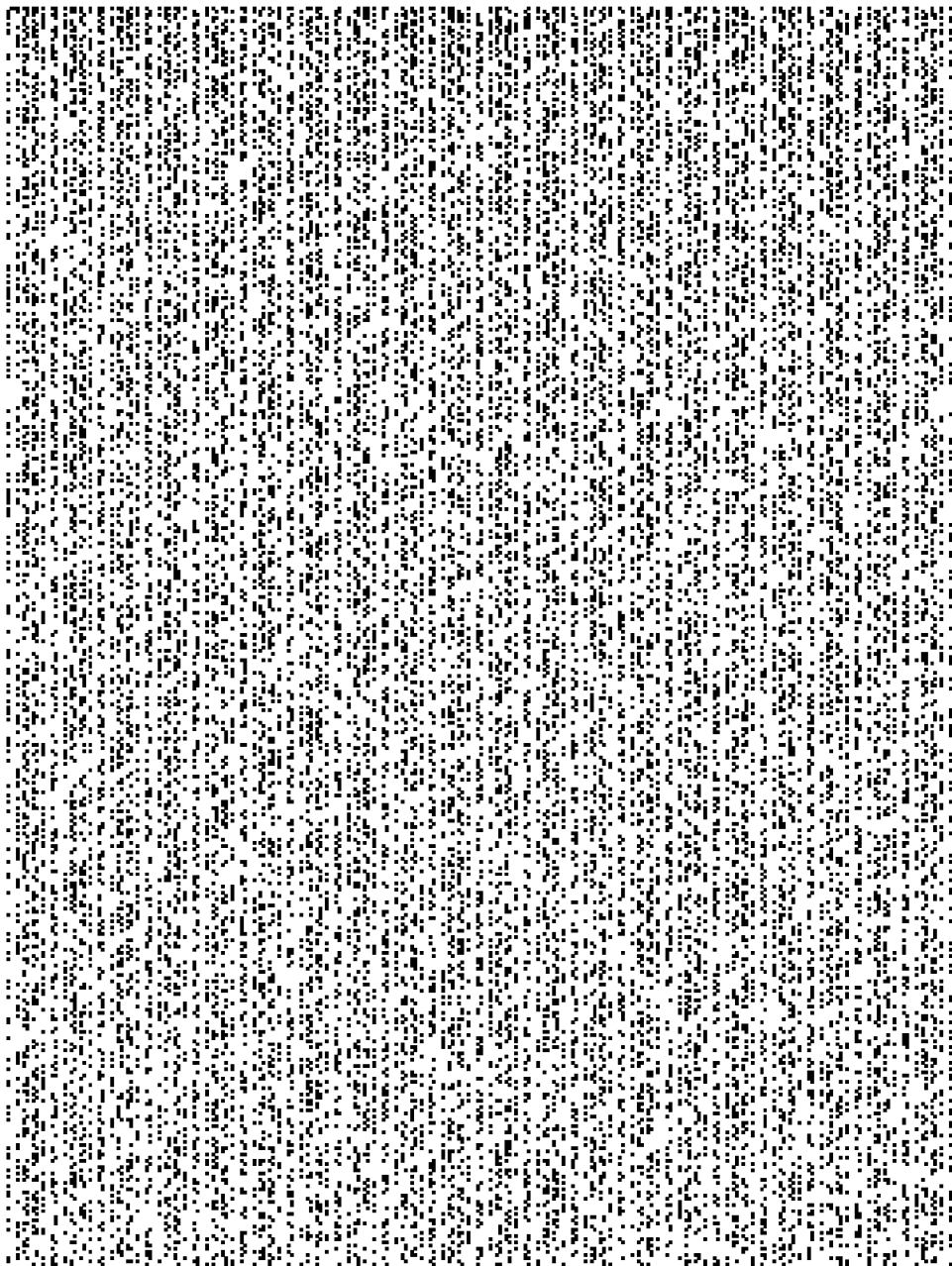
$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

alakú számok, ahol $\beta_j \in \mathbb{N}$, $\beta_j \leq \alpha_j$, ha $j = 1, 2, \dots, k$, hiszen ha $n = cd$, akkor c és d prímtényezős felbontásának szorzata n prímtényezős felbontása kell hogy legyen. Ha több számunk van, és mindnek adott a prímtényezős felbontása, akkor ezekből közös osztóik, valamint hasonlóan közös többszöröseik is leolvashatók. Ez azonban nem hatékony eljárás a legnagyobb közös osztó, illetve a legkisebb közös többszörös meghatározására, mert a prímtényezős felbontás meghatározása nagy számoknál általában időigényes eljárás.

6.1.50. Következmény. Ha $a, b, c \in \mathbb{Z}$ és a is, b is relatív prím c -hez, akkor ab is. $\square$

6.1.51. Következmény. Tetszőleges $a, b \in \mathbb{Z}$ számoknak létezik legkisebb közös többszöröse, és $\text{luko}(a, b) \cdot \text{lkkt}(a, b) = |ab|$.

Bizonyítás. Vagy mindkét oldal nulla, vagy mindkét oldal kanonikus alakjában ugyanazok a prímtényezők szerepelnek ugyanazon a hatványon. $\square$



6.1.1 ábra: A 240 000-nél kisebb páratlan prímek, sorfolytonosan, 400 sor.

6.1.52. Következmény. Ha $a, b \in \mathbb{Z}$ és $c \in \mathbb{N}$, akkor

$$\text{lkt}(ac, bc) = c \cdot \text{lkt}(a, b).$$

Bizonyítás. Vagy mindkét oldal nulla, vagy mindkét oldal kanonikus alakjában ugyanazok a prímtényezők szerepelnek ugyanazon a hatványon. $\square$

6.1.53. Következmény. Tetszőleges $a_1, a_2, \dots, a_n \in \mathbb{Z}$ számoknak létezik legkisebb közös többszöröse, és

$$\text{lkt}(a_1, a_2, \dots, a_n) = \text{lkt}(\text{lkt}(a_1, a_2), a_3, a_4, \dots, a_n). \quad \square$$

6.1.54. Megjegyzés. Számos további észrevétel kiolvasható a számelmélet alaptételéből. Például, ha $n > 1$ összetett szám, és p a legkisebb prímtényezője, akkor $p^2 \leq n$. Ezért, ha egy n számot megpróbáltunk minden p prímmel (vagy minden olyan $p > 1$ természetes számmal) osztani, amelyre $p^2 \leq n$, és egyik sem osztja, akkor n prím. Ez a *próbaosztás* nevű eljárás alkalmas tehát prímtényezőkre bontásra is, meg prímtesztelésre is, de futásideje nagyon gyorsan nő a szám hosszával. 2002-ben talált Agrawal, Kayal és Saxena egy olyan algoritmust, amely bármely n természetes számra képes eldönteni, hogy prím-e, és futásideje nem hosszabb, mint egy konstansszor az n hosszának a 13-adik hatványa. (A konstans attól függ, hogy milyen egységben mérjük az időt, milyen gyors a gép, a program, és milyen alapú számrendszerben felírt alak hosszát tekintjük.) A gyakorlatban sokkal jobban használható a Miller–Rabin-féle valószínűségi prímszámteszt, amely ugyan nem ad bizonyítást arra, hogy a szám prím, de a tévedés valószínűségét bármilyen kicsire, mondjuk 10^{-100} -ra leszoríthatjuk, és a futásidő legfeljebb konstansszor a szám hosszának köbe: lásd 6.2.43.

6.1.55. Eratoszthenész szitája. Ha egy adott n -ig az összes prímet meg akarjuk találni, a következő egyszerű eljárás hatékony módszert ad: írjuk fel a számokat 2-től n -ig. Az első szám, a 2 prím, összes (valódi) többszöröse összetett, ezeket húzzuk ki. A megmaradó számok közül az első a 3, ez prím, ennek minden (valódi) többszöröse összetett, ezeket húzzuk ki, és így tovább. Az eljárás végén az n -nél nem nagyobb prímek maradnak meg.

→ **6.1.56. Feladat [6].** Írjunk szita-programot, amivel határozzuk meg az x -nél nem nagyobb prímek számát, ha $x = 10^n$, $n = 1, 2, \dots$ ameddig a gép bírja, és vessük össze $x/\ln(x)$ értékével.

6.1.57. Feladat [12]. Írjunk olyan programot próbaosztásra, amely minden 2^{64} -nél kisebb pozitív természetes számra működik. A 2-vel és 3-mal való próbaosztás után válasszuk a próbaosztók sorozatát a $d_0 = 5$, $d_k = d_{k-1} + 3 + (-1)^k$ ($k > 0$) sorozatnak. Mérjük a futásidőt; mivel arányos?

→ **6.1.58. Feladat [5].** Mutassuk meg, hogy egy p prímszámmal a legnagyobb k kitevő, amelyre p^k osztja az $n!$ ($n \in \mathbb{N}^+$) számot,

$$k = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \dots$$

(az összeg véges).

→ **6.1.59. Feladat [5].** Osztható-e 1599-cel $\binom{3400}{1700}$?

→ **6.1.60. Feladat [2].** Mutassuk meg, hogy minden $4k - 1$ ($k \in \mathbb{N}^+$) alakú számnak van ugyanilyen alakú osztója.

→ **6.1.61. Feladat** [4]. Mutassuk meg, hogy végtelen sok $4k - 1$ ($k \in \mathbb{N}^+$) alakú prímszám van.

6.1.62. Feladat [4]. Mutassuk meg, hogy végtelen sok $6k - 1$ ($k \in \mathbb{N}^+$) alakú prímszám van.

6.1.63. Feladat [5]. Bizonyítsuk be, hogy az $M_n = 2^n - 1$ ($n \in \mathbb{N}^+$) úgynevezett *Mersenne-számokra* $\text{luko}(M_m, M_n) = M_{\text{luko}(m, n)}$. Keressünk közöttük prímekeket és össze-tetteket.

6.1.64. Feladat [5]. Bizonyítsuk be, hogy az $F_n = 2^{2^n} + 1$, $n \in \mathbb{N}$ úgynevezett *Fermat-számok* páronként relatív prímekek. Keressük meg az első olyat, amely nem prím.

6.1.65. Feladat [4]. Mutassuk meg, hogy ha $n > 1$, akkor az $F_n = 2^{2^n} + 1$ Fermat-szám nem állítható elő két prímszám összegeként.

6.1.66. Feladat [4]. Mutassuk meg, hogy ha $n > 1$, akkor az $F_n = 2^{2^n} + 1$ Fermat-szám utolsó jegye tízes számrendszerben 7.

6.1.67. Feladat [7]. Mutassuk meg, hogy ha egy Fermat-szám prímhatvány, akkor a kitevő 1.

6.1.68. Feladat [10]. Mutassuk meg, hogy a $2^{2^n} + 3$ ($n \in \mathbb{N}$) számok között végtelen sok összetett van.

6.1.69. Feladat [7]. Határozzuk meg azokat a 10^{12} -nél kisebb prímekeket, amelyek $n^n + 1$ alakúak, ahol $n \in \mathbb{N}$.

6.1.70. Feladat [8]. Mutassuk meg, hogy $2^j + 1$ összetett, ha $j > 1$ és j nem kettő-hatvány.

6.1.71. Feladat [8]. Mutassuk meg, hogy a

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

úgynevezett *harmonikus számok* $n > 1$ esetén nem egészek.

6.1.72. Feladat [8]. Bizonyítsuk be, hogy ha $n, k \in \mathbb{N}^+$, akkor a $\sum_{j=n}^{n+k} (1/j)$ összeg sohasem egész.

6.1.73. Feladat [7]. Bizonyítsuk be, hogy az $\binom{n}{k}$, $0 < k < n$ binomiális együtthatók legnagyobb közös osztója p , ha n a p prímszám hatványa, minden más $n > 1$ -re pedig 1.

6.1.74. Feladat [7]. Bizonyítsuk be, hogy ha $n, k \in \mathbb{N}^+$ és n, k relatív prímekek, akkor n osztója az $\binom{n}{k}$ binomiális együtthatónak.

6.1.75. Feladat [7]. Bizonyítsuk be, hogy bármely tíz egymás utáni pozitív természetes szám között van olyan, amelyik relatív prím a többi kilenc szorzatához. Keressük meg a legkisebb olyan n -et, amelyre ez nem igaz tíz helyett n számra.

6.1.76. További feladatok megoldásokkal. [56]: 5.1-4-5.1-9, 5.3-4-5.3-5, 4-1-5.4-6; [54]: 3.1-1-3.1-2, 3.1-4, 3.1-6-3.1-27, 5.3.3-1-3.3-8, 3.4-1-3.4-14.

6.1.77. További feladatok. [25]: VIII.1.8; [46]: 1.2.5.11–12, 1.2.5.14, 1.2.6.11; [64]: 6.1.1–6.1.6, 6.3.1–6.3.7, 6.4.1, 6.6.1–6.6.12; [69]: 1.2.1–1.2.36, 1.3.1–1.3.48, 2.6.1–2.6.3, 4.1.1, 4.1.2, 4.1.5, 4.1.9, 4.1.11–4.1.14, 4.1.17, 4.1.19, 4.1.21, 4.1.25–4.1.27; [80]: 3–5, 7–116, 159–168, 173–175, 199–200.

6.2 Kongruenciák

6.2.1. Kongruenciák. Ha $a, b, m \in \mathbb{Z}$ és m osztója $a - b$ -nek, akkor azt mondjuk, hogy a és b *kongruensek modulo m* ; ezt úgy jelöljük, hogy $a \equiv b \pmod{m}$. Ha a és b nem kongruensek modulo m , akkor azt mondjuk, hogy *inkongruensek modulo m* , és azt írjuk, hogy $a \not\equiv b \pmod{m}$. (Szokásos a tömörebb $a \equiv b \pmod{m}$, illetve $a \not\equiv b \pmod{m}$ jelölés is.) Például $7 \equiv 22 \pmod{15}$, $9 \equiv -7 \pmod{8}$, de $1 \not\equiv -1 \pmod{4}$. Nyilván, ha $a \equiv b \pmod{m}$ és $d|m$, akkor $a \equiv b \pmod{d}$ is teljesül. Ha $0 \neq d \in \mathbb{Z}$, akkor $a \equiv b \pmod{m}$ ekvivalens azzal, hogy $ad \equiv bd \pmod{md}$.

Az oszthatóság tulajdonságaiból azonnal következik, hogy bármely adott $m \in \mathbb{Z}$ -re a kongruencia ekvivalenciareláció $\mathbb{Z}$ -ben. Az m és a $-m$ szerinti kongruencia ugyanazt jelenti, így legtöbbször feltesszük, hogy $m \in \mathbb{N}$. Ha $a \in \mathbb{Z}$, akkor az ekvivalenciaosztályának elemei az $a + km$, $k \in \mathbb{Z}$ alakú egészek; valóban, ezek nyilván kongruensek a -val, és ha $a' \equiv a \pmod{m}$, akkor $a' - a = km$ valamely $k \in \mathbb{Z}$ -re. Az, hogy $a' \equiv a \pmod{m}$, pontosan akkor teljesül, ha $a' \bmod m = a \bmod m$; valóban az $m = 0$ eset triviális, $m \neq 0$ esetén pedig ha $a' = a + km$, akkor $\lfloor a'/m \rfloor = \lfloor a/m \rfloor + k$, ahonnan $a' \bmod m = a \bmod m$ következik, és megfordítva, ha $a' \bmod m = a \bmod m$, akkor $a' - \lfloor a'/m \rfloor m = a - \lfloor a/m \rfloor m$, ahonnan $k = \lfloor a'/m \rfloor - \lfloor a/m \rfloor$ -szel $a' = a + km$.

Megjegyezzük, hogy ha $a' \equiv a \pmod{m}$, akkor

$$\text{lko}(a, m) = \text{lko}(a', m),$$

mert $a' = a + km$, illetve $a = a' - km$ miatt a' és m közös osztói osztói a -nak is, és megfordítva, a és m közös osztói osztói a' -nek is.

→ **6.2.2. Feladat [1].** Állapítsuk meg, milyen maradékot adnak a természetes számok négyzetei 3-mal, 5-tel, illetve 7-tel osztva.

6.2.3. Maradékosztályok. Egy $m \in \mathbb{Z}$ modulus szerinti kongruencia ekvivalenciaosztályait *maradékosztályoknak* nevezzük. A maradékosztályokat rendszerint elemeikkel reprezentáljuk. Az a elem által reprezentált maradékosztályt $\tilde{a} \bmod m$ vagy rövidebben $\tilde{a}$ jelöli. Természetesen a maradékosztály bármely eleme választható reprezentánsnak. Leggyakrabban az osztályok legkisebb nemnegatív elemét választjuk reprezentánsnak, vagy az osztályok legkisebb abszolút értékű elemét. (Ha $m \neq 0$ páros szám, akkor $-m/2$ és $m/2$ kongruensek modulo m , és abszolút értékük megegyezik; akármelyiket választhatjuk.) Ha egy maradékosztály valamelyik eleme relatív prím a modulushoz, akkor mindegyik, és ekkor a maradékosztályt *redukált maradékosztálynak* nevezzük. Páronként inkongruens egészek egy rendszerét *maradékrendszernek* nevezzük. Ha egy maradékrendszer minden maradékosztályból tartalmaz elemet, akkor *teljes maradékrendszernek* nevezzük. Ha egy maradékrendszer pontosan a redukált maradékosztályokból tartalmaz elemet, akkor *redukált maradékrendszernek* nevezzük. Például 2, 10 nem maradékrendszer, 2, 8 maradékrendszer, 8, 1, 10, 19, 4, 29, -10 , 7 teljes maradékrendszer, míg 1, 19, 29, 7 redukált maradékrendszer modulo 8. Teljes maradékrendszert alkotnak modulo m a $0, 1, \dots, |m| - 1$

számok, továbbá páratlan modulus esetén a $0, \pm 1, \dots, \pm(|m| - 1)/2$ számok, páros modulus esetén pedig a $0, \pm 1, \dots, \pm(|m|/2 - 1), |m|/2$ számok; az utóbbi esetben $|m|/2$ helyett $-|m|/2$ is választható.

A kongruencia kompatibilis az összeadással és a szorzással, mert ha $a \equiv a' \pmod m$, akkor $a' - a = km$ valamely $k \in \mathbb{Z}$ -re, ahonnan $a' + b - (a + b) = km$ és $a'b - ab = (bk)m$, azaz $a' + b \equiv a + b \pmod m$ és $a'b \equiv ab \pmod m$; innen az összeadás és a szorzás kommutativitását is felhasználva, már következik a kompatibilitás. Az ekvivalenciaosztályok nyilván kommutatív egységelemes gyűrűt alkotnak az összeadással és a szorzással; a nullelem a 0 osztálya, az egységelem pedig az 1 osztálya. Ezt a gyűrűt $\mathbb{Z}_m$ -mel fogjuk jelölni. (Vannak, akik a $\mathbb{Z}_m$ jelölést másra tartják fenn.) Ha $m = 0$, akkor az ekvivalenciaosztályok egyeleműek, így az $n \mapsto \{n\}$ leképezés kölcsönösen egyértelmű művelettartó leképezése $\mathbb{Z}$ -nek $\mathbb{Z}_0$ -ra, tehát $\mathbb{Z}$ és $\mathbb{Z}_0$ azonosítható, ez az eset érdektelen. Ha $m = \pm 1$, akkor $\mathbb{Z}_m$ egyelemű, a nullgyűrű, így ez az eset is érdektelen.

6.2.4. Komplement számábrázolás. Negatív számok számítógépes ábrázolására elterjedt a *komplement ábrázolás*. Csak a bináris gépek esetével foglalkozunk. Egy n -bites gépen az egyik, régebben használt lehetőség $0 \leq k < 2^{n-1}$ esetén $-k$ ábrázolására, hogy $-k \pmod{(2^n - 1)}$ kettes számrendszerbeli alakját tároljuk. Ezt úgy kapjuk, hogy k kettes számrendszerbeli alakját levonjuk $2^n - 1$ kettes számrendszerbeli alakjából. Mivel ez utóbbi csupa egyesből áll, a kivonás során nincs átvitel, k kettes számrendszerbeli alakját csak bitenként komplementáljuk. Innen ered az ábrázolás neve: *egyesekre komplement* ábrázolás. A negatív számok legfelső bitje 1, de a nullának két ábrázolása van: 000...000 és 111...111. Az ellentett képzése gyors, az ábrázolható számok intervalluma szimmetrikus a nullára, de az előjeles számok összeadását modulo $(2^n - 1)$ kell végezni. Mára kiszorította a *kettes komplement* ábrázolás: $0 < k \leq 2^{n-1}$ esetén $-k$ ábrázolására $-k \pmod{2^n}$ kettes számrendszerbeli alakját tároljuk. Ezt úgy kapjuk, hogy k kettes számrendszerbeli alakjának vesszük a bitenkénti komplementerét, majd hozzáadunk 1-et. Ennél pontosan a negatív számok legfelső bitje 1, és a nullának csak egy ábrázolása van. Az ellentett képzése lassabb, és az ábrázolható számok intervalluma nem szimmetrikus a nullára, de az előjeles számok összeadását is modulo 2^n kell végezni, ugyanúgy, mint az előjel nélküliekét. Természetesen mindkét ábrázolásnál előfordulhat túlcsoordulás, ha az eredmény nincs az ábrázolható intervallumban.

6.2.5. Tétel. Legyen $m > 1$ egész, $a \in \mathbb{Z}$. Ha

$$1 < \text{luko}(a, m) < m,$$

akkor a maradékosztálya nullosztó $\mathbb{Z}_m$ -ben. Ha

$$\text{luko}(a, m) = 1,$$

akkor a maradékosztályának van multiplikatív inverze $\mathbb{Z}_m$ -ben. Speciálisan, ha m prím-szám, akkor $\mathbb{Z}_m$ test.

Bizonyítás. Legyen $d = \text{luko}(a, m)$. Ha $1 < d < m$, akkor $a \cdot (m/d) = (a/d) \cdot m \equiv 0 \pmod m$, ahonnan $x = m/d$ jelöléssel $\tilde{a} \cdot \tilde{x} = \tilde{0}$, azaz $\tilde{a}$ nullosztó $\mathbb{Z}_m$ -ben. Ha $d = 1$, akkor a bővített euklideszi algoritmussal olyan $x, y \in \mathbb{Z}$ egészeket kaphatunk, amelyekre $ax + my = 1$. Innen $ax \equiv 1 \pmod m$ azaz $\tilde{a} \cdot \tilde{x} = \tilde{1}$ miatt $\tilde{x}$ az $\tilde{a}$ inverze $\mathbb{Z}_m$ -ben. $\square$

6.2.6. Következmény. Ha m prímszám, akkor $\mathbb{Z}_m$ test.

Bizonyítás. Ha m prím, és $a \not\equiv 0 \pmod{m}$, akkor a -nak van multiplikatív inverze.

□

→ **6.2.7. Feladat [2].** Számoljuk ki $\mathbb{Z}_{17}$ -ben: 5^{-1} , $9 \cdot 11$, $(15 + 10)(3 + 5)^{-1}$, $1 \cdot 2 \cdot 3 \cdots 16$.

6.2.8. Feladat [5]. Legyen $n \in \mathbb{N}^+$. Legalább hány elemet tartalmaz egy olyan maradékrendszer modulo n , amely nem üres részhalmazainak összegeként minden maradékosztályt megkapunk.

6.2.9. Diszkrét logaritmus probléma. A következő pont mutatja, hogy $\mathbb{Z}_m$ -ben nem nehéz hatványozni. Azonban a tapasztalat szerint még ha m prím is, $\mathbb{Z}_m$ invertálható elemeinek multiplikatív csoportjában egy a alap és egy a^k hatvány ismeretében nehéz meghatározni a k kitevőt, legalábbis ha $m-1$ -nek vannak nagy prímtényezői: ez a *diszkrét logaritmus probléma*. A probléma számos más csoport esetén is nehéznek tűnik.

* **6.2.10. Gyors hatványozás.** Az alábbi algoritmus akármilyen G (multiplikatív-
van írt) félcsoportban hatékonyan kiszámolja egy $g \in G$ elem n -edik hatványát, ahol $n \in \mathbb{N}^+$. Leggyakrabban moduláris hatványozásnál használjuk. (Célszerű n -et kettes számrendszerben felírni, mert akkor a mellékszámítások triviálisak.) Válasszunk olyan $k \in \mathbb{N}$ -et, amelyre $2^k \leq n < 2^{k+1}$. Minden $0 \leq j \leq k$ -ra sorban kiszámítjuk $x_j = g^{n_j}$ -t, ahol $n_j = \lfloor n/2^{k-j} \rfloor$, azaz n_j az n bináris felírásának első $j+1$ jegye által megadott természetes szám. Nyilván $n_0 = 1$, így $x_0 = g$. Ha n_j páros, akkor $n_j = 2n_{j-1}$, így $x_j = x_{j-1}^2$, ha pedig n_j páratlan, akkor $n_j = 2n_{j-1} + 1$, így $x_j = gx_{j-1}^2$, azaz minden részeredményt az előzőből egy négyzetreemeléssel és még esetleg egy szorzással kapunk. A végeredmény $x_k = g^n$. Például ha $n = 23$, akkor n kettes számrendszerben 10111, így $j = 0, 1, 2, 3, 4$ -re n_j kettes számrendszerben 1, 10, 101, 1011, 10111, tehát $x_0 = g^{n_0} = g^1 = g$, $x_1 = g^{n_1} = g^2 = x_0^2$, $x_2 = g^{n_2} = g^5 = gx_1^2$, $x_3 = g^{n_3} = g^{11} = gx_2^2$ és $x_4 = g^n = g^{23} = gx_3^2$.

6.2.11. Diffie–Hellmann–Merkle-kulcscsere. Az alapgondolat, hogy egy „csapóajtó függvényt” használunk, egy olyan függvényt, amelyet könnyű kiszámolni, de az inverze nagyon nehezen számolható: ez itt a moduláris hatványozás lesz. Az összes felhasználó megállapodik egy nagy (több száz jegyű) *Sophie Germain* prímbe, azaz olyan p prímbe, amelyre $q = 2p + 1$ is prím, valamint egy $1 < g < p - 1$ alapon. (Bár nem tudjuk, hogy van-e végtelen sok Sophie Germain prím, a tapasztalat szerint elég sűrűn vannak: az n jegyűek közötti távolság nagyságrendben n^2 .) Ha két felhasználó, Aliz és Bob valamely szokásos rejtjelzési rendszer, például az AES (lásd 8.3.57) felhasználásával titkosított üzenetet akar váltani, akkor szükségük van egy véletlenszerű közös kulcsra. (Rejtjelkulcs csak akkor lehet biztonságos, ha véletlenszerű: lásd például az Enigma rendszer feltörésének történetét.) Választanak egy $1 < a < p$, illetve $1 < b < p$ véletlen kitevőt, kiszámolják és felteszik a honlapjukra a $g^a \bmod q$, illetve $g^b \bmod q$ értékeket. Mindketten gyorsan ki tudják számolni $g^{ab} \bmod q$ értékét, ez lesz kettejük közös titkos kulcsa. Az eljárás biztonsága azon múlik, hogy g , $g^a \bmod q$ és $g^b \bmod q$ ismeretében sem látszik jobb megoldás $g^{ab} \bmod q$ meghatározására, mint a vagy b megkeresése, ez viszont a nehéz diszkrét logaritmus probléma. Ezt a kulcscserélő módszert használja az *SSH* (secure shell) és az *SSL* (Secure Socket Layer), illetve annak a továbbfejlesztése, a *TLS* (Transport Layer Security) protokoll is. Nem biztonságos hálózaton inkább egy módosított formában használják: digitálisan aláírva (lásd 6.2.41, 6.2.44) cserélik ki a $g^a \bmod q$, illetve $g^b \bmod q$

értékeket. Ez azért szükséges, mert az eredeti változat az üzenetek manipulálására képes „közbeékelődő” támadó úgynevezett „nagymester sakk támadásával” szemben védtelen: A támadás alapgondolata, hogy ha két nagymesterrel egyszerre sakkozunk a hálózaton, akkor legalább egy pontot érhetünk el, ha az egyik fehérrel, a másik feketével játszik. Megvárjuk, hogy mi az egyik nagymester kezdő lépése, és azzal kezdünk a másik ellen, megvárjuk a választ, és ezt lépjük az első ellen, stb.

Hasonlóan használható kulccserére bármely más csoport is, amelyben könnyű a hatványozás, de nehéz a diszkrét logaritmus probléma megoldása. A Diffie–Hellmann–Merkle kulccserét 1976-ban vezették be, és a szerzők felvetették a nyilvános kulcsú rejtjelzés lehetőségét is; az első ilyen rendszert, az RSA-t két évvel később fedezték fel (lásd 6.2.41).

6.2.12. Feladat [5]. Készítsünk 3 alapú logaritmustáblát $\mathbb{Z}_{17}$ -ben.

6.2.13. Az Euler-féle φ függvény. Legyen $m > 0$ egész szám, és jelölje $\varphi(m)$ a modulo m redukált maradékosztályok számát; φ az Euler-féle φ függvény. Nyilván $\varphi(m)$ az m -hez relatív prím számok száma a $0, 1, 2, \dots, m-1$ számok között. Például $\varphi(1) = 1$ (sic!), $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$.

6.2.14. Lemma. Legyen $m > 1$ egész szám, a relatív prím m -hez. Ha $a_1, a_2, \dots, a_m$ teljes maradékrendszer modulo m és $b \in \mathbb{Z}$, akkor $aa_1 + b, aa_2 + b, \dots, aa_m + b$ is teljes maradékrendszer modulo m . Ha $a_1, a_2, \dots, a_{\varphi(m)}$ redukált maradékrendszer modulo m , akkor $aa_1, aa_2, \dots, aa_{\varphi(m)}$ is redukált maradékrendszer modulo m .

Bizonyítás. Ha $i \neq j$ esetén $aa_i + b \equiv aa_j + b \pmod{m}$ teljesülne, akkor ebből $aa_i \equiv aa_j \pmod{m}$, és innen a multiplikatív inverzével szorozva $a_i \equiv a_j \pmod{m}$ következne. Tehát az $aa_i + b$, $i = 1, 2, \dots, m$ számok páronként inkongruensek, és – mivel számuk m – teljes maradékrendszert alkotnak modulo m . A másik állítás bizonyításához vegyük észre, hogy ha $\text{lko}(aa_i, m) > 1$, akkor $\text{lko}(a_i, m) > 1$. Így az aa_i , $i = 1, 2, \dots, \varphi(m)$ számok páronként relatív prímekek, a modulushoz is relatív prímekek és számuk $\varphi(m)$, tehát redukált maradékrendszert alkotnak. $\square$

6.2.15. Euler–Fermat-tétel. Legyen $m > 1$ egész szám, a relatív prím m -hez. Ekkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Bizonyítás. Legyen $a_1, a_2, \dots, a_{\varphi(m)}$ egy redukált maradékrendszer modulo m . Ekkor $aa_1, aa_2, \dots, aa_{\varphi(m)}$ is redukált maradékrendszer modulo m . Innen

$$a^{\varphi(m)} \prod_{j=1}^{\varphi(m)} a_j = \prod_{j=1}^{\varphi(m)} (aa_j) \equiv \prod_{j=1}^{\varphi(m)} a_j \pmod{m}.$$

Mivel $\prod_{j=1}^{\varphi(m)} a_j$ relatív prím m -hez, van inverze modulo m . Ezzel megszorozva mindkét oldalt, kapjuk az állítást. $\square$

6.2.16. Következmény: Fermat-tétel. Legyen p prímszám. Ha $a \in \mathbb{Z}$ és $p \nmid a$, akkor $a^{p-1} \equiv 1 \pmod{p}$. Ha $a \in \mathbb{Z}$ tetszőleges, akkor $a^p \equiv a \pmod{p}$.

Bizonyítás. Nyilván $\varphi(p) = p - 1$, így az első alak következik az előző tételből. A második alak a $p \nmid a$ esetben az első alakból következik, ha pedig $p \mid a$, akkor mindkét oldal osztható p -vel. $\square$

6.2.17. Lineáris kongruencia megoldása. Legyen $m > 1$ egész szám, $a, b \in \mathbb{Z}$ adottak. Keressük az $ax \equiv b \pmod{m}$ kongruencia megoldásait. A probléma nyilván azzal ekvivalens, hogy találjunk olyan x egész számot, amelyre valamely y egész számmal $ax + my = b$ teljesül. (Ha x -et megtaláltuk, y már adódik.) Legyen $d = \text{lko}(a, m)$. Mivel d osztója $ax + my$ -nak, osztója kell legyen b -nek, egyébként nincs megoldás. Tegyük fel, hogy $a = a'd$, $b = b'd$, $m = m'd$ valamely $a', b', m' \in \mathbb{Z}$ -re. Azt kapjuk, hogy az egyenletünk az $a'x + m'y = b'$, illetve az $a'x \equiv b' \pmod{m'}$ egyenlettel ekvivalens, ahol a' és m' relatív prímek. A legnagyobb közös osztó kiszámítását a bővített euklideszi algoritmussal végezve, olyan x_0, y_0 egészeket is kapunk, amelyekre $ax_0 + my_0 = d$, azaz $a'x_0 + m'y_0 = 1$. Szorozva b' -vel, $a'x_1 + m'y_1 = b'$, ahol $x_1 = x_0b'$ és $y_1 = y_0b'$. Az általános megoldáshoz vonjuk ki ezt az egyenletet az $a'x + m'y = b'$ egyenletből: $a'(x - x_1) = m'(y_1 - y)$, ahonnan $m' | x - x_1$, azaz $x = x_1 + km'$ valamely $k \in \mathbb{Z}$ -re. Minden ilyen x ténylegesen megoldás, mert $y = y_1 - ka'$ -vel $a'x + m'y = b'$.

Összefoglalva, ha van megoldás, akkor az összes megoldás $x \equiv x_1 \pmod{m'}$ alakban adható meg. Ez a halmaz az $x_1, x_1 + m', \dots, x_1 + (d-1)m'$ számok modulo m vett maradékosztályainak egyesítése.

6.2.18. Példa. Oldjuk meg a $172x \equiv 6 \pmod{62}$ kongruenciát, vagy ami ezzel ekvivalens, határozzuk meg a $172x + 62y = 6$ egyenlet egész megoldásait. Mivel $\text{lko}(172, 62) = 2$ osztója 6-nak, van megoldás. Az egyenlet a $86x + 31y = 3$ egyenlettel ekvivalens. A bővített euklideszi algoritmussal $172 \cdot (-9) + 62 \cdot 25 = 2$, ahonnan $x_1 = (-9) \cdot 3$, $y_1 = 25 \cdot 3$, így az egyenlet összes megoldása $x = -27 + 31k$, $y = 75 - 86k$, $k \in \mathbb{Z}$. A kongruencia az $x \equiv 4 \pmod{31}$ kongruenciával ekvivalens; ez a mod 31 ekvivalenciaosztály két mod 62 ekvivalenciaosztály egyesítése, így $x \equiv 4 \pmod{62}$ vagy $x \equiv 35 \pmod{62}$.

→ **6.2.19. Feladat [2].** Adjunk meg mod 10 egy teljes maradékrendszert és egy redukált maradékrendszert.

→ **6.2.20. Feladat [5].** Oldjuk meg az alábbi kongruenciákat:

- (1) $3x \equiv 5 \pmod{7}$;
- (2) $14x \equiv 84 \pmod{21}$;
- (3) $104x \equiv 74 \pmod{60}$;
- (4) $26x \equiv 16 \pmod{34}$;
- (5) $30x \equiv 48 \pmod{58}$;
- (6) $40x \equiv 28 \pmod{62}$;
- (7) $202x \equiv 157 \pmod{203}$;
- (8) $309x \equiv 451 \pmod{617}$.

→ **6.2.21. Feladat [5].** Oldjuk meg az alábbi egyenleteket az egész számok körében:

- (1) $47x + 72y = 4$;
- (2) $21x + 56y = 72$;
- (3) $117x - 63y = 36$;
- (4) $182524x + 4567y = 1092$;
- (5) $18x + 28y = 10$;
- (6) $17x + 11y = 22$.

6.2.22. Feladat [5]. Egy n egész számra $n^{100} \bmod 73 = 57$ és $n^{101} \bmod 73 = 11$. Mennyi $n \bmod 73$?

6.2.23. Feladat [5]. Bizonyítsuk be, hogy minden természetes számokból álló m, n számpárhoz van olyan $ax + by = c$ lineáris egyenlet (ahol $a, b, c \in \mathbb{Z}$), amelynek csak $x = m$, $y = n$ a természetes számok körében az egyetlen megoldása.

6.2.24. Feladat [5]. Bizonyítsuk be, hogy minden n természetes számhoz van olyan $ax + by = c$ lineáris egyenlet (ahol $a, b, c \in \mathbb{Z}$), amelynek pontosan n megoldása van a természetes számokból álló párok körében.

6.2.25. Lineáris kongruenciarendszer megoldása. Az előző pont alapján, ha két lineáris kongruencia adott, akkor azokat (ha megoldhatóak) $x \equiv a \pmod{m}$, illetve $x \equiv b \pmod{n}$ alakra hozhatjuk (a, b, m, n egészek, $m, n > 1$). Mivel a közös megoldásokra $x = a + my = b + nz$ valamely $y, z \in \mathbb{Z}$ -re, az $my - nz = b - a$ egyenlet egész megoldásait megkeresve, minden x megoldás megtalálható. Akkor és csak akkor van megoldás, ha $d = \text{lko}(m, n)$ osztója $b - a$ -nak, és ekkor a megoldás $x \equiv x_1 \pmod{\text{lkk}(m, n)}$ alakba írható valamely x_1 egészszel. Ha több kongruencia van, az eljárás folytatható.

→ **6.2.26. Feladat [7].** Oldjuk meg az alábbi kongruencia-rendszereket:

- (1) $3x \equiv 2 \pmod{4}$, $2x \equiv 3 \pmod{5}$;
- (2) $5x \equiv 3 \pmod{7}$, $4x \equiv 5 \pmod{10}$;
- (3) $5x \equiv 1 \pmod{6}$, $7x \equiv 9 \pmod{10}$;
- (4) $3x \equiv 1 \pmod{4}$, $5x \equiv 2 \pmod{7}$, $7x \equiv 8 \pmod{9}$;
- (5) $3x \equiv 1 \pmod{4}$, $2x \equiv 3 \pmod{5}$, $5x \equiv 2 \pmod{7}$, $7x \equiv 8 \pmod{9}$;
- (6) $5x \equiv 6 \pmod{7}$, $7x \equiv 8 \pmod{9}$, $9x \equiv 10 \pmod{11}$, $11x \equiv 12 \pmod{13}$;
- (7) $3x \equiv 12 \pmod{5}$, $10x \equiv -2 \pmod{14}$, $5x \equiv 5 \pmod{15}$, $6x \equiv 6 \pmod{22}$.

6.2.27. Diofantikus problémák. Az előző két pontban tárgyalt problémák egy $mx + ny = c$ alakú egyenlet egész megoldásainak meghatározásával voltak ekvivalensek. Ha egy egyenlet vagy egyenletrendszer egész megoldásait keressük, akkor *diofantikus problémáról* beszélünk. Némely diofantikus problémáról könnyen belátható, hogy nincs megoldása: például az $x^2 + y^2 = -4$ problémának még valós megoldása sincs, az $x^4 - 4y^4 = 3$ egyenlet egyik oldala pedig modulo 4 kongruens 0-val vagy 1-el, a másik oldala pedig 3-mal, emiatt az egyenletnek nincs egész megoldása. Más esetekben a megoldás nem ilyen egyszerű, esetleg nagyon nehéz. Például az $x^2 + y^2 = z^2$ egyenlet megoldásai a pitagoraszai számhármasok, ezeket nem túl nehéz meghatározni, míg ha $n > 2$ egész, akkor a Fermat-sejtés szerint, amelyet csak 1994-ben, több mint 300 év után sikerült Andrew Wiles-nak bebizonyítania, az $x^n + y^n = z^n$ egyenletnek nincsenek nem triviális (azaz az $xyz \neq 0$ feltételt is kielégítő) egész megoldásai. Azonban a lineáris egész együtthatós egyenletekből álló egyenletrendszerek egész megoldásai egyszerű algoritmussal meghatározhatók: lásd a következő feladatot.

6.2.28. Feladat [7]. Egész együtthatós lineáris egyenletekből álló diofantikus egyenletrendszer megoldására, azaz az egyenletrendszer egész megoldásainak megkeresésére használható az alábbi algoritmus:

- (1) Ha valamelyik egyenletben nincs ismeretlen, azaz az egyik oldal nulla, akkor ha a másik oldal is nulla, az egyenletet törölhetjük, egyébként nincs megoldás.

- (2) Ha valamelyik egyenletben egy ismeretlen van, azt megoldhatjuk. Ha a megoldás egész, visszahelyettesítjük a többibe, egyébként nincs megoldás.
- (3) Ha valamelyik egyenletben valamelyik ismeretlen együtthatója ± 1 , fejezzük ki az egyenletből, és helyettesítsük be a többibe. Minden ilyen lépéssel az egyenletek és az ismeretlenek száma legalább eggyel csökken. Ha elfogytak az egyenletek (egy sem maradt), a maradék változók „szabad változók”: ezeknek tetszőleges egész értéket adva, megkapjuk a megoldásokat.
- (4) Ha az előző lépésekkel nem tudunk már változókat illetve egyenleteket kiküszöböl-
ni, akkor válasszuk ki azt az egyenletet és azt a változót, amely együtthatójának legkisebb az abszolút értéke az összes egyenletben. Ha ez mondjuk x , és az egyenlet

$$cx + c_1x_1 + c_2x_2 + \cdots + c_kx_k = d$$

alakú, ahol tehát c abszolút értéke a legkisebb, akkor vezessünk be egy új t változót a

$$t = x + \lfloor c_1/c \rfloor x_1 + \lfloor c_2/c \rfloor x_2 + \cdots + \lfloor c_k/c \rfloor x_k$$

új egyenlettel. Levonva az új egyenlet c -szeresét az eredeti egyenletből, az x -et nem tartalmazó

$$ct + (c_1 \bmod c)x_1 + (c_2 \bmod c)x_2 + \cdots + (c_k \bmod c)x_k = d$$

egyenletet kapjuk, amelyben – egyet kivéve – minden együttható kisebb abszolút értékű, mint c . A többi egyenletből is küszöböljük ki t -vel x -et, majd ismételjük a fenti lépéseket (1)-től.

Ennek a módszernek a segítségével oldjuk meg az alábbi egyenletrendszert:

$$3x + 3y + 8z + 10w = 1, \quad -7x - 5z + 6w = 2.$$

*** 6.2.29. Feladat [9].** Bizonyítsuk be, hogy az előző feladatban leírt algoritmus helyes, azaz mindig megadja az összes megoldást.

6.2.30. Kínai maradéktétel. Legyenek $m_1, m_2, \dots, m_n$ egymánál nagyobb, páronként relatív prím természetes számok, $c_1, c_2, \dots, c_n \in \mathbb{Z}$. Az $x \equiv c_j \pmod{m_j}$, $j = 1, 2, \dots, n$ kongruenciarendszer megoldható, és bármely két megoldása kongruens modulo $m_1 m_2 \cdots m_n$.

A bizonyítás algoritmust is ad a megoldások meghatározására.

Bizonyítás. Legyen $m = m_1 m_2$. A bővített euklideszi algoritmussal olyan x_1, x_2 egész számokat kaphatunk, amelyekre $m_1 x_1 + m_2 x_2 = 1$. Legyen $c_{1,2} = m_1 x_1 c_2 + m_2 x_2 c_1$. Nyilván $c_{1,2} \equiv c_j \pmod{m_j}$, ha $j = 1, 2$. Ha $x \equiv c_{1,2} \pmod{m}$, akkor x az első két kongruencia egy megoldása, és megfordítva, ha x az első két kongruencia egy megoldása, akkor $x - c_{1,2}$ osztható m_1 -el és m_2 -vel, tehát a szorzatukkal is. Az eredeti kongruenciarendszer tehát ekvivalens az $x \equiv c_{1,2} \pmod{m}$, $x \equiv c_j \pmod{m_j}$, $j = 3, 4, \dots, n$ kongruenciarendszerrel. Így n szerinti indukcióval adódik a bizonyítás. Megjegyezzük, hogy a gyakorlatban érdemesebb $c_{1,2}$ helyett $c_{1,2} \bmod m$ -et használni, és mindig azt a két kongruenciát összevonni, amelyek modulusa a legkisebb. $\square$

6.2.31. Megjegyzés. A kínai maradéktétel felhasználható arra, hogy bonyolultabb relatív prím modulusú kongruenciák közös megoldásait megkeressük, vagy arra, hogy egy összetett m modulusú kongruencia megoldását több, egymáshoz relatív prím modulusú (ezek lehetnek például m prímtényezői) kongruenciából álló kongruenciarendszer megoldására vezessük vissza.

6.2.32. Példa. Oldjuk meg a

$$4x \equiv 2 \pmod{6}, \quad 3x \equiv 3 \pmod{12}, \quad 15x \equiv -5 \pmod{25}$$

kongruenciarendszert. A kongruenciák rendre a

$$2x \equiv 1 \pmod{3}, \quad x \equiv 1 \pmod{4}, \quad 3x \equiv -1 \pmod{5}$$

kongruenciákkal ekvivalensek. A bővített euklideszi algoritmust is használhatjuk, vagy az első és utolsó kongruenciát 2-vel szorozva azt kapjuk, hogy

$$x \equiv 2 \pmod{3}, \quad x \equiv 1 \pmod{4}, \quad x \equiv 3 \pmod{5}.$$

A lineáris kongruenciarendszerekre megadott eljárással haladhatunk tovább, vagy a kínai maradéktétel bizonyítása szerint (felhasználva, hogy a modulusok relatív prímekek), mivel $3 \cdot 3 + 4(-2) = 1$, azt kapjuk, hogy

$$x \equiv 3 \cdot 3 \cdot 1 + 4 \cdot (-2) \cdot 2 \equiv 5 \pmod{12}, \quad x \equiv 3 \pmod{5},$$

illetve mivel $12 \cdot 3 + 5 \cdot (-7) = 1$,

$$x \equiv 12 \cdot 3 \cdot 3 + 5 \cdot (-7) \cdot 5 \equiv 53 \pmod{60}.$$

6.2.33. Feladat [2]. Határozzuk meg azt a legkisebb természetes számot, amelyet a 2,3,4,5,6 számokkal osztva a maradék rendre 1,2,3,4,5.

→ **6.2.34. Feladat [5].** Mennyi $42^{600} \pmod{13}$?

→ **6.2.35. Feladat [3].** Melyek azok az n pozitív természetes számok, amelyekre $\varphi(n) = 1$, illetve $\varphi(n)$ páratlan?

→ **6.2.36. Feladat [5].** Igazoljuk, hogy ha $n \in \mathbb{N}^+$ páratlan, akkor $2^{\varphi(n)-1} \pmod{n} = (n+1)/2$.

→ **6.2.37. Feladat [5].** Hogyan számolhatjuk ki hatékonyan $n^{p-2} \pmod{p}$ értékét, ha $n \in \mathbb{Z}$ és p prímszám?

6.2.38. Feladat [5]. Bizonyítsuk be, hogy ha p prímszám és $x_1, x_2, \dots, x_n \in \mathbb{Z}$, akkor

$$(x_1 + x_2 + \dots + x_n)^p \equiv x_1^p + x_2^p + \dots + x_n^p \pmod{p}.$$

6.2.39. Feladat [6]. Mutassuk meg, hogy az $n^2 + 1$ ($n \in \mathbb{N}^+$) alakú számok minden prímosztója $4k + 1$ ($k \in \mathbb{N}$) alakú.

6.2.40. Feladat [6]. Mutassuk meg, hogy végtelen sok $4k + 1$ ($k \in \mathbb{N}$) alakú prím van.

6.2.41. Az RSA-eljárás. Az alábbi rejtjelezési sémát Rivest, Shamir és Adleman találták ki 1978-ban. Keressünk két „nagy” (például 150–160 jegyű) $p \neq q$ prímet, és legyen $n = pq$. Válasszunk egy $1 < e < (p-1)(q-1)$ kitevőt, és a bővített euklideszi algoritmussal oldjuk meg az

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

kongruenciát. (Ha a kongruencia nem oldható meg, azaz ha

$$\lnko(e, (p-1)(q-1)) > 1,$$

kezdjük előlről az eljárást.) Ha $1 < m < n$ egy üzenet, akkor $c = m^e \bmod n$ használható, mint az üzenet rejtjelezett formája, mert ebből az üzenet újabb hatványozással visszakapható: valamely k -ra $ed = k(p-1)(q-1) + 1$, és így

$$c^d = (m^e)^d = m^{k(p-1)(q-1)+1} = (m^{(p-1)})^{k(q-1)} \cdot m \equiv m \pmod{p},$$

ugyanis ha $p|m$, akkor mindkét oldal nullával kongruens, ha viszont $p \nmid m$, akkor a Fermat-tétel szerint $m^{p-1} \equiv 1 \pmod{p}$. Hasonlóan $(m^e)^d \equiv m \pmod{q}$. Innen a kínai maradéktétel szerint, mivel $p \neq q$ prímek, $m = c^d \bmod n$. Az n és e értékek nyilvánosságra hozhatók, ekkor bárki tud nekünk rejtjelezett üzenetet küldeni: az eljárás úgynevezett *nyilvános kulcsú kódolás*. Biztonsága azon múlik, hogy d , p és q értékét más nem ismeri: az n prímtényezőinek meghatározása a mai módszerekkel nagyon sokáig tartana, mert nagy prímtényezőök meghatározására nincs hatékony módszerünk.

Az RSA-eljárás felhasználható *digitális aláírás*ra is, mert e és d szerepe szimmetrikus: Aliz nemcsak az m üzenetet, hanem

$$m^{d_A} \bmod n_A$$

értékét is elküldi Bobnak (Bob kulcsával rejtjelezve), ahol (n_A, d_A) Aliz titkos kulcsa: ez az aláírás, mert csak Aliz volt képes kiszámítani. Ha az m üzenet hosszú, célszerű egy $h(m)$ véletlenszerűnek látszó „lenyomatát” használni az aláírásnál m helyett. Rejtjelezési célra kifejlesztett, jelenleg gyakran használt lenyomatképző „hash”-függvények a 160 bites lenyomatot adó *SHA-1* (Secure Hash Algorithm) illetve a szabadalommal nem védett *RIPEMD-160* (RACE Integrity Primitives Evaluation Message Digest). Újabb változataik hosszabb, nagyobb biztonságot adó lenyomatot adnak: lásd a Wikipedia-t.

Az eljárás *bizonyítványok kiállítására*, például nyilvános kulcs hitelesítésére is felhasználható. Egy hitelesítő szervezettől – aminek nyilvános kulcsát mindenki ismeri – digitálisan aláírt levélben kaphatjuk meg Aliz nyilvános kulcsát, így ha Aliztól digitálisan aláírt levelet kapunk, biztosak lehetünk benne, hogy nem csalótól kaptunk üzenetet, aki Aliznak adja ki magát.

Az RSA-eljárás egy alkalmazása nála gyorsabb, nem nyilvános, hanem úgynevezett „szimmetrikus” kulcsú (rejtjelezésre és fejtésre is ugyanazt a kulcsot használó) „klasszikus” rejtjelező eljárások (például AES, lásd 8.3.57) kulcsainak cseréje. Így működik például az e-mailek védelmére szolgáló *PGP* (Pretty Good Privacy) rendszer, amely először egy véletlen kulcsot generál, azt átküldi RSA-rejtjelezéssel, majd az aláírt üzenetet küldi el a véletlen kulccsal rejtjelezve. Ezt a módszert „*digitális boríték*nak” nevezik.

Az RSA-kódolás használatánál néhány biztonsági szabályt be kell tartani. Más-más n -et használjunk rejtjelezésre és digitális aláírásra. Az n bitjeinek száma legfeljebb néggyel legyen rövidebb, mint a névleges (maximális) bitszám, ami ma szokásosan 1024. A prímetek úgy nyerjük, hogy véletlenszerűen választott számoktól kezdve keressük meg az első prímet, ezzel biztosítható a magas (minimum 128 bit) entrópia (lásd 9.1.1). A nagyobb és a kisebb prím hányadosa legalább $\sqrt{2}$, de legfeljebb 2^{30} legyen. Véletlen hexadecimális jegyeket nyerhetünk például egy álvéletlen karaktersorozat emberi visszagépelésénél mérve az időket modulo 16 ms. Az e exponenst nem ajánlatos túl kicsinek választani, szokásos legkisebb értéke 65537. Az üzenet egy nulla bájtal kezdődik, majd ezután egy legalább 8 nem nulla bájtot tartalmazó (véletlen, minden üzenetnél más) „sózás” következik, amelyet egy újabb nulla bájt határol, és ezután következnek a tényleges szöveg bájtjai; a teljes blokkhossz 128 bájt (hosszabb üzenetet részekre bontunk). A kezdő nulla bájt biztosítja, hogy $m < n$. A „sózás” szerepe az, hogy ne lehessen kitalálni egy rövid üzenetet, és rejtjelezve ellenőrizni, hogy tényleg az-e. A dekódolás gyorsítható, ha $c^d \bmod n$ helyett $c^d \bmod p$ és $c^d \bmod q$, vagy ami ugyanaz, mivel p és q prímek, a

$$c^{d \bmod (p-1)} \bmod p \quad \text{és} \quad c^{d \bmod (q-1)} \bmod q$$

értékeket számítjuk ki, és ezekből a kínai maradéktétel alapján állítjuk vissza m -et. Az RSA általánosítható arra az esetre, amikor n kettőnél több „nagy” prím szorzata. A 2048 névleges bitszám valószínűleg legalább 10-15 évre biztosítja a titkosságot, 3072 bit jóval tovább. További részletek: *RFC 3447*.

Az eljáráshoz szükséges „nagy” prímeket például a Miller–Rabin-féle valószínűségi teszttel találhatjuk meg.

6.2.42. Feladat [8]. Mutassuk meg, hogy ha ugyanazt az m üzenetet elküldik az RSA eljárással három különböző n_i -vel, de mindegyik esetben $e = 3$ -mal rejtjelezve, akkor n_1 , n_2 , n_3 és c_1 , c_2 , c_3 ismeretében m könnyen meghatározható.

*** 6.2.43. Miller–Rabin-féle valószínűségi teszt.** Egy adott $n \geq 9$ páratlan egészre az algoritmus megpróbálja eldönteni, hogy n prím-e. Legyen $n - 1 = 2^k q$, ahol q páratlan, és legyen a egy egész, amelyre $1 < a < n$.

Az ötlet az, hogy ha $n = 1 + 2^k q$ prím, és $a^q \bmod n \neq 1$, akkor az

$$a^q \bmod n, \quad a^{2q} \bmod n, \quad a^{4q} \bmod n, \quad \dots, \quad a^{2^k q} \bmod n$$

sorozatnak – mivel $2^k q = n - 1$ – a Fermat-tétel szerint 1-re kell végződnie, és ha egyáltalán van 1-től különböző tagja, az utolsó ilyennek $n - 1$ -nek kell lenni: ha $b^2 \equiv 1 \pmod{n}$, akkor $n \mid (b-1)(b+1)$, amiből $n \mid (b-1)$ vagy $n \mid (b+1)$, mert n prím, azaz $b \equiv \pm 1 \pmod{n}$. Ha tehát ez a feltétel nem teljesül, akkor biztos, hogy n összetett.

A legfontosabb tény ezzel az algoritmussal kapcsolatban, hogy ha véletlen $1 < a < n$ alapot választunk, és $n \geq 9$ összetett, akkor $1/4$ -nél kisebb a valószínűsége, hogy ezt az algoritmus nem fedezi fel. (A bizonyítást lásd például KnuthDonaldEKnuth, Donald E.Knuth, 4.5.4, 22. feladat.) Ismételt alkalmazásával tetszőlegesen kis hibavalószínűséget elérhetünk. Például kriptográfiai célra 2^{-60} -nál kisebb hibavalószínűséget szokás előírni, amit 30 véletlen alappal elérhetünk.

A valószínűségi teszt nagyon ritkán hibázik. Az első összetett szám, amely (hibásan) a 2 alappal átmegy a teszten 2047; amely még a 3 alappal is 1 373 653; amely

még az 5 alappal is 25 326 001; amely még a 7 alappal is 3 215 031 75 amely még a 11 alappal is 2 152 302 898 747; amely még a 13 alappal is 3 474 789 660 383; és amely még a 17 alappal is 341 550 071 728 321. Ez a szám a 19 alappal is átmegy a teszten, de a legkisebb, amely még a 23 alappal is, 3 825 123 056 546 413 051. Ha a szám kisebb, mint 3 186 658 578 340 31 151 167 461, akkor elég még a 29, 31 és 37 alapokkal tesztelni, ha pedig kisebb, mint 3 317 044 046 679 887 385 961 981, akkor még a 41 alappal.

* **6.2.44. Digital Signature Standard.** A *DSS* szabvány az alábbi DSA (Digital Signature Algorithm) eljárást használja digitális aláírásra: Válasszunk egy h kriptográfiai „hash”-függvényt, amely a tetszőlegesen hosszú m üzenetből 160 bites $h(m)$ „lenyomatot” készít (lásd a 6.2.41 pontot). Keressünk egy 160 bites q prímet, majd egy olyan 1024 bites p prímet, amelyre $p - 1$ többszöröse q -nak, és válasszunk egy olyan a alapot, amelyre $g = a^{(p-1)/q} \bmod p > 1$. Minden felhasználó választ magának egy véletlen titkos $1 < x < q$ értéket, kiszámolja $y = g^x \bmod p$ értékét, és azt nyilvánosságra hozza. Egy-egy üzenet aláírásának menete a következő: Választunk egy $1 < k < q$ véletlen értéket. Kiszámoljuk az

$$r = (g^k \bmod p) \bmod q$$

és

$$s = k^{-1}(h(m) + xr) \bmod q$$

értékét. Abban a ritka esetben, amikor $r = 0$ vagy $s = 0$, új k értéket választunk, egyébként az aláírás az (r, s) pár. Az aláírás ellenőrzésére a címzett sorban kiszámolja az $w = s^{-1} \bmod q$, $u_1 = h(m)w \bmod q$, $u_2 = rw \bmod q$ és $v = (g^{u_1}y^{u_2} \bmod p) \bmod q$ értékeket (ehhez k -t nem kell ismerni). Ha $v = r$, akkor az aláírást helyesnek fogadja el, egyébként nem. Valóban, mivel a Fermat-tétel szerint $g^q \equiv a^{p-1} \equiv 1 \pmod{p}$, továbbá $k \equiv h(m)s^{-1} + xrs^{-1} \pmod{q}$, azt kapjuk, hogy

$$g^k \equiv g^{h(m)w} g^{xrw} \equiv g^{h(m)w} y^{rw} \equiv g^{u_1} y^{u_2} \pmod{p},$$

ahonnan $r = v$. (A v és r egybeesésének valószínűsége hibás aláírás esetén nagyon kicsi.)

Az eljárás hosszabb, például 224 vagy 256 bites lenyomatot adó hash-függvénnyel és ugyanennyi bites q -val, valamint 2048, illetve 3072 bites p -vel is használható.

6.2.45. Feladat: álprímek [8]. Azokat az $n \in \mathbb{N}$ összetett számokat, amelyekre $a^{n-1} \equiv 1 \pmod{n}$ egy adott $a \in \mathbb{Z}$ alapra, a alapú álprímeknek nevezzük (ekkor persze a és n relatív prímek). Keressünk számítógéppel 2 alapú álprímeket.

6.2.46. Feladat: Carmichael-számok [9]. Azokat az $n \in \mathbb{N}$ összetett számokat, amelyek álprímek minden olyan a alapra, amely relatív prím n -hez, *Carmichael-számoknak* nevezzük. Keressünk számítógéppel Carmichael-számokat. (Ismeretes, hogy végtelen sok van; a legkisebb 561.)

→ **6.2.47. Feladat [8].** Tegyük fel, hogy van egy algoritmusunk, aminek segítségével az RSA eljárásnál az (m, e) nyilvános kulcshoz hatékonyan meg tudjuk határozni a d titkos kulcsot. Mutassuk meg, hogy ekkor hatékonyan ki tudjuk számítani a $(p-1)(q-1)$ szorzatot és a p, q prímeket is.

6.2.48. Feladat: pitagoraszai számhármak [10]. Az $x^2 + y^2 = z^2$ egyenlet egész megoldásait keressük:

- (1) mutassuk meg, hogy a megoldásokat megkaphatjuk, ha ismerjük a pozitív egészekből álló megoldásokat;
- (2) mutassuk meg, hogy ha $r, s \in \mathbb{N}^+$ és $r > s$, akkor $x = r^2 - s^2$, $y = 2rs$ és $z = r^2 + s^2$ pozitív egészekből álló megoldás;
- (3) mutassuk meg, hogy nem minden pozitív egészekből álló megoldás áll elő ilyen alakban, még azok se mind, amelyekre y páros;
- (4) mutassuk meg, hogy minden pozitív egészekből álló megoldás megkapható az úgynevezett *primitív megoldásokból*: ezek olyan pozitív egészekből álló megoldások, amelyekre $\text{lnko}(x, y, z) = 1$;
- (5) mutassuk meg, hogy egy primitív megoldásra x , y és z páronként relatív prímek, és x , y közül az egyik páros, a másik páratlan;
- (6) mutassuk meg, hogy egy primitív megoldásra, ha x páratlan, y pedig páros, akkor $(z - x)/2$ és $(z + x)/2$ relatív prímek, szorzatuk $(y/2)^2$, így mindegyik négyzetszám;
- (7) mutassuk meg, hogy minden primitív megoldás, amelyre x páratlan, y pedig páros, előáll $x = r^2 - s^2$, $y = 2rs$, $z = r^2 + s^2$ alakban, ahol $r, s \in \mathbb{N}^+$, $r > s$, és az egyik páros, a másik páratlan.

6.2.49. Feladat [5]. Bizonyítsuk be, hogy ha $n \in \mathbb{N}$, akkor az

$$x^2 + y^2 + 2xy - nx - ny + x + y - n + 1 = 0$$

egyenletnek pontosan n megoldása van a természetes számokból álló párok körében.

6.2.50. Feladat [4]. Adjuk meg $2x^3 + xy - 7 = 0$ egyenlet összes egész megoldását, és mutassuk meg, hogy végtelen sok racionális megoldása van.

6.2.51. Feladat [9]. Bizonyítsuk be, hogy ha az n pozitív egész szám felírható $m = x^2 - 2y^2$ alakban, ahol $x, y \in \mathbb{N}^+$, akkor ebben az alakban végtelen sokféleképpen írható fel.

6.2.52. Feladat [4]. Bizonyítsuk be, hogy egyetlen $8k + 3$ vagy $8k + 5$ alakú n egész szám sem írható fel $n = x^2 - 2y^2$ alakban, ahol $x, y \in \mathbb{Z}$.

6.2.53. További feladatok megoldásokkal. [56]: 5.5-1-5.5-4, 5.7-8, 5.7-13-5.7-14, 5.7-16, 8-1-5.8-13, 5.9-1-5.9-8; [54]: 3.5-1-3.5-6, 3.7-3-3.7-9, 3.7-12-3.7-15, 3.8-1-3.8-15, 3.9-1-3.9-9.

6.2.54. További feladatok. [46]: 1.2.6.10; [64]: 6.5.1-6.5.4, 6.7.1-6.7.5, 6.8.1-6.8.6, 9.1-6.9.5, 6.10.1-6.10.23, 15.2.1-15.2.3, 15.3.1, 15.3.2, 15.6.1; [69]: 2.1.1-2.1.50, 2.3.1-2.3.16, 2.4.23, 5.2.1-5.2.10, 5.3.1-5.3.10, 5.4.1; [80]: 117-121, 123-154, 158, 178-189, 191; [83]: VIII.3.4, VIII.3.12.

6.3 Számelméleti függvények

6.3.1. Számelméleti függvények. Egy $f: \mathbb{N}^+ \rightarrow \mathbb{C}$ függvényt *számelméleti függvénynek* fogunk nevezni. Ha relatív prím $m, n \in \mathbb{N}^+$ számok esetén $f(mn) = f(m) + f(n)$, akkor f -et *additív*nak nevezzük, ha pedig ez bármely $m, n \in \mathbb{N}^+$ esetén fennáll, akkor f -et *teljesen additív*nak (vagy *totálisan additív*nak) nevezzük. Ha relatív prím $m, n \in \mathbb{N}^+$ számok esetén $f(mn) = f(m)f(n)$, akkor f -et *multiplikatív*nak nevezzük, ha pedig ez bármely $m, n \in \mathbb{N}^+$ esetén fennáll, akkor f -et *teljesen multiplikatív*nak (vagy *totálisan multiplikatív*nak) nevezzük. Az $m = 1$ helyettesítéssel kapjuk, hogy egy additív számelméleti függvény 1 helyen felvett értéke mindig nulla, és hogy egy nem azonosan nulla multiplikatív számelméleti függvény 1 helyen felvett értéke 1.

6.3.2. Tétel. Legyen $n \in \mathbb{N}^+$ kanonikus alakja $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Ekkor

(1) ha f additív számelméleti függvény, akkor

$$f(n) = f(p_1^{\alpha_1}) + \cdots + f(p_k^{\alpha_k});$$

(2) ha f multiplikatív számelméleti függvény, akkor

$$f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k});$$

(3) ha f teljesen additív számelméleti függvény, akkor

$$f(n) = \alpha_1 f(p_1) + \cdots + \alpha_k f(p_k);$$

(4) ha f teljesen multiplikatív számelméleti függvény, akkor

$$f(n) = f(p_1)^{\alpha_1} \cdots f(p_k)^{\alpha_k}.$$

Megfordítva, tetszőleges, a prímszámokra megadott f függvényre az (1)-ben, illetve (2)-ben szereplő összefüggés egy additív, illetve multiplikatív számelméleti függvényt definiál, és tetszőleges, a prímszámokra megadott f függvényre a (3)-ban, illetve (4)-ben szereplő összefüggés egy teljesen additív, illetve teljesen multiplikatív számelméleti függvényt definiál.

Bizonyítás. A k szerinti indukcióval adódik az első két állítás, ezekből pedig az α szerinti indukcióval adódik $f(p^\alpha) = \alpha f(p)$, illetve $f(p^\alpha) = f(p)^\alpha$ állítások felhasználásával adódik (3), illetve (4). A megfordítás azonnal adódik a definíció alapján. $\square$

6.3.3. Példák. Az azonosan nulla függvény nyilván teljesen additív és teljesen multiplikatív is. Az azonosan 1 függvény teljesen multiplikatív. Az $E(1) = 1$, $E(n) = 0$, ha $n > 1$ összefüggéssel definiált függvény teljesen multiplikatív. Bármely r valós számra $n \mapsto n^r$, azaz az $\mathbb{N}_+^r$ függvény teljesen multiplikatív. Ha $r > 0$, $r \neq 1$ valós szám, akkor $n \mapsto \log_r n$ teljesen additív.

Definiáljuk a μ Möbius-függvényt a következőképpen: $\mu(n) = 0$, ha n osztható egy prímszám négyzetével, és $\mu(n) = (-1)^k$, ha n pontosan k darab különböző prímszám szorzata. Például $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$. Mint a definíció alapján könnyen ellenőrizhető, μ multiplikatív, de nyilván nem teljesen multiplikatív, például $0 = \mu(4) \neq \mu(2)^2 = 1$.

Legyen $\kappa(n)$ az n szám prímtenyezőinek, $\nu(n)$ pedig az n különböző prímosztóinak száma. Például $\kappa(1) = 0$, $\kappa(2) = 1$, $\kappa(3) = 1$, $\kappa(4) = 2$, $\kappa(5) = 1$, $\kappa(6) = 2$ és $\nu(1) = 0$,

$\nu(2) = 1, \nu(3) = 1, \nu(4) = 1, \nu(5) = 1, \nu(6) = 2$. Könnyen végiggondolható, hogy κ teljesen additív számelméleti függvény, míg ν additív, de nyilván nem teljesen additív, például $1 = \nu(4) \neq 2\nu(2) = 2$.

Ha r tetszőleges valós szám, legyen $\sigma_r(n) = \sum_{0 < d|n} d^r$, és legyen $\tau = \sigma_0, \sigma = \sigma_1$, azaz τ az osztók száma, σ pedig az osztók összege. Például $\tau(1) = 1, \tau(2) = 2, \tau(3) = 2, \tau(4) = 3, \tau(5) = 2, \tau(6) = 4$ és $\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 7, \sigma(5) = 6, \sigma(6) = 12$. Mivel ha m és n relatív prímekek, akkor mn minden pozitív osztója egyértelműen írható fel cd alakban, ahol c az m, d pedig az n pozitív osztója,

$$\begin{aligned}\sigma_r(mn) &= \sum_{0 < cd|mn} (cd)^r = \sum_{0 < c|m} \sum_{0 < d|n} c^r d^r = \sum_{0 < c|m} c^r \sum_{0 < d|n} d^r \\ &= \sum_{0 < c|m} c^r \sigma_r(n) = \sigma_r(m) \sigma_r(n),\end{aligned}$$

azaz σ_r multiplikatív minden r -re. Mivel a p^α prímhatalvány osztói $1, p, p^2, \dots, p^\alpha$, kapjuk, hogy $\tau(p^\alpha) = \alpha + 1$ és $\sigma_r(p^\alpha) = (p^{r(\alpha+1)} - 1)/(p^r - 1)$, ha $r \neq 0$. Innen, ha $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ az n kanonikus alakja, akkor

$$\tau(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1)$$

és

$$\sigma_r(n) = \prod_{j=1}^k \frac{p_j^{r(\alpha_j+1)} - 1}{p_j^r - 1}, \quad \text{ha } r \neq 0.$$

A számelméleti függvények értékének számítása általában nem egyszerű, ismernünk kell hozzá a szám kanonikus alakját.

6.3.4. Tétel. Az Euler-féle φ függvény multiplikatív, és ha $n \in \mathbb{N}^+$ kanonikus alakja $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, akkor

$$\varphi(n) = \prod_{j=1}^k \left(p_j^{\alpha_j} - p_j^{\alpha_j-1} \right) = n \prod_{j=1}^k \left(1 - \frac{1}{p_j} \right).$$

Bizonyítás. Az, hogy φ multiplikatív, következik a kínai maradéktételből, mert ha n és m relatív prímekek, akkor a kínai maradéktétel szerint kölcsönösen egyértelmű megfeleltetés áll fenn a $0 \leq x < m$ és $0 \leq y < n$ egészek párpai és a $0 \leq z < nm$ egészek között, és triviálisan z pontosan akkor lesz ennél a megfeleltetésnél relatív prím mn -hez, ha x relatív prím m -hez, y pedig relatív prím n -hez. Mivel emiatt

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}),$$

elég azt belátnunk, hogy $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - 1/p)$, ha p prím és $\alpha > 0$. Ez viszont következik abból, hogy egy $0 \leq x < p^\alpha$ egész pontosan akkor nem relatív prím p^α -hoz, ha többszöröse p -nek. $\square$

6.3.5. Példa. Az $5500 = 2^2 \cdot 5^3 \cdot 11$ számra $\varphi(5500) = (4 - 2)(125 - 25)10 = 2000$.

→ **6.3.6. Feladat [2].** Keressük meg azt a legkisebb n -et, amelyre

- (1) $\varphi(n) = 6$;
- (2) $\tau(n) = 6$;
- (3) $\kappa(n) = 6$;
- (4) $\nu(n) = 6$.

→ **6.3.7. Feladat [4].** Keressük meg azt a legkisebb m egészet, amelyre a $\sigma(n) = m$ egyenletnek pontosan 0, 1, 2, illetve 3 megoldása van.

→ **6.3.8. Feladat [2].** Keressük meg a legkisebb olyan m egészet, amelyhez van olyan $n \neq m$, hogy $\sigma(n) = \sigma(m)$.

→ **6.3.9. Feladat [2].** Adjuk meg az összes, harmincnál nem nagyobb n pozitív természetes számot, amelyre $\varphi(n) = \tau(n)$. Keressünk számítógéppel nagyobb ilyen n -et.

6.3.10. Feladat [5]. Bizonyítsuk be, hogy $\tau(n)$ pontosan akkor páratlan, ha n négyzetszám.

6.3.11. Feladat [5]. Bizonyítsuk be, hogy tetszőleges $m > 1$ egészhez végtelen sok olyan n van, amelyre $\tau(n) = m$.

6.3.12. Feladat [5]. Bizonyítsuk be, hogy tetszőleges $m \in \mathbb{N}$ egészhez csak véges sok olyan n van, amelyre $\sigma(n) = m$.

→ **6.3.13. Feladat [6].** Mennyi

- (1) $109^{355} \bmod 14$;
- (2) $439^{291} \bmod 60$;
- (3) $1993^{1993^{192}} \bmod 1456$?

→ **6.3.14. Feladat [6].** Határozzuk meg az alábbi számok utolsó két számjegyét tízes számrendszerben:

- (1) $39^{39^{390}}$;
- (2) $63^{493^{640}}$;
- (3) $19^{93^{92}}$;
- (4) $39^{39^{39}}$.

→ **6.3.15. Feladat [6].** Mennyi

- (1) $18^{39} \bmod 91$;
- (2) $26^{143} \bmod 73$;
- (3) $5^{193} \bmod 84$;
- (4) $14285^{203} \bmod 84$?

6.3.16. Feladat [3]. Igazoljuk, hogy minden $n \in \mathbb{N}^+$ -ra $\varphi(n) + \sigma(n) \geq n$.

6.3.17. Feladat [6]. Bizonyítsuk be a $\tau(n) < 2\sqrt{n}$ egyenlőtlenséget.

6.3.18. Feladat [7]. Adjuk meg az összes olyan $n \in \mathbb{N}^+$ számot, amelyre $\varphi(n) | n$.

6.3.19. Feladat [10]. Azt mondjuk, hogy n *tökéletes szám*, ha valódi osztóinak összege n , azaz ha $\sigma(n) = 2n$. (Nem tudjuk, hogy van-e páratlan tökéletes szám). Bizonyítsuk be, hogy

- (1) ha $p = 2^k - 1$ prím, akkor $2^{k-1}p$ tökéletes szám (keressünk ilyen számokat);
- (2) n pontosan akkor prím, ha $\sigma(n) = n + 1$;
- (3) ha $\sigma(n) = n + m$, ahol $m|n$ és $m < n$, akkor $m = 1$;
- (4) minden páros tökéletes szám az (1)-ben megadott alakú.

* **6.3.20. Konvolúció.** Az f és g számelméleti függvények *konvolúcióját* (vagy *Dirichlet-szorzatát*) az

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} f(d_1)g(d_2), \quad \text{ha } n \in \mathbb{N}^+$$

összefüggéssel definiáljuk; a második alakból látjuk, hogy a konvolúció kommutatív művelet. Ugyancsak a második alakból

$$\begin{aligned} ((f * g) * h)(n) &= \sum_{d_3=n} (f * g)(d)h(d_3) = \sum_{d d_3=n} \sum_{d_1 d_2=d} f(d_1)g(d_2)h(d_3) \\ &= \sum_{d_1 d_2 d_3=n} f(d_1)g(d_2)h(d_3) = \sum_{d_1 d=n} \sum_{d_2 d_3=d} f(d_1)g(d_2)h(d_3) \\ &= \sum_{d_1 d=n} f(d_1)(g * h)(d) = (f * (g * h))(n), \end{aligned}$$

azaz a konvolúció asszociatív is. Nyilván az $E(1) = 1$, $E(n) = 0$, ha $n > 1$ összefüggéssel definiált függvény egységelem a konvolúcióra nézve, így a számelméleti függvények a konvolúcióval mint szorzással kommutatív egységelemes félcsoportot alkotnak. A következő tétel azt mutatja, hogy ezen belül a multiplikatív számelméleti függvények részhalmaza is egységelemes félcsoport.

* **6.3.21. Tétel.** *Multiplikatív számelméleti függvények konvolúciója is multiplikatív.*

Bizonyítás. Legyen $h = f * g$, és tegyük fel, hogy $m, n \in \mathbb{N}^+$ relatív prímelek. Ekkor

$$\begin{aligned} h(mn) &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) = \sum_{d_1|m, d_2|n} f(d_1 d_2)g\left(\frac{mn}{d_1 d_2}\right) \\ &= \sum_{d_1|m, d_2|n} f(d_1)f(d_2)g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right) \\ &= \sum_{d_1|m} f(d_1)g\left(\frac{m}{d_1}\right) \sum_{d_2|n} f(d_2)g\left(\frac{n}{d_2}\right) = h(m)h(n). \quad \square \end{aligned}$$

* **6.3.22. Összegzési függvény.** Egy f számelméleti függvény *összegzési függvényét* az $F(n) = \sum_{d|n} f(d)$ összefüggéssel definiáljuk. Az összegzési függvényt megkaphatjuk konvolúcióként: ha I az azonosan 1 multiplikatív függvény, akkor nyilván $F = I * f$, és így multiplikatív függvény összegzési függvénye is multiplikatív. Egy számelméleti függvénynek a μ Möbius-függvénnyel való konvolúcióját a függvény *Möbius-transzformált* Möbius-transzformáltjának nevezzük. A Möbius-transzformáció jelentősége az, hogy az összegzési függvényből visszaadja az eredeti függvényt:

* **6.3.23. Möbius-féle inverziós formula.** Ha F a f számelméleti függvény összegzési függvénye, akkor F Möbius-transzformáltja f .

Bizonyítás. A μ Möbius-függvény összegzési függvénye az $E(1) = 1$, $E(n) = 0$, ha $n > 1$ függvény; valóban, ha I az azonosan 1 függvény, akkor μ összegzési függvénye, $\mu * I$ multiplikatív, így $(\mu * I)(1) = 1$ és $(\mu * I)(p^\alpha) = \sum_{j=0}^{\alpha} \mu(p^j) = 1 - 1 + 0 + \dots + 0 = 0$, ha $\alpha > 0$, tehát $\mu * I = E$, a konvolúció egységeleme. Innen akármilyen f függvényre $f = f * (I * \mu) = (f * I) * \mu = F * \mu$. $\square$

°* **6.3.24. Példa.** Tetszőleges r valós számra a σ_r számelméleti függvény multiplikatívítása következik abból, hogy az $n \mapsto n^r$ (teljesen) multiplikatív számelméleti függvény összegzési függvénye.

* **6.3.25. Tétel.** Az $E(1) = 1$, $E(n) = 0$, ha $n > 1$ függvényre, az I azonosan 1 függvényre, valamint a μ , τ , φ és σ számelméleti függvényekre

- (1) $\mu * I = E$;
- (2) $I * I = \tau$;
- (3) $\mu * \mathbb{I}_{\mathbb{N}^+} = \varphi$;
- (4) $I * \mathbb{I}_{\mathbb{N}^+} = \sigma$;
- (5) $\varphi * \tau = \sigma$;
- (6) $\sigma * \varphi = \mathbb{I}_{\mathbb{N}^+} * \mathbb{I}_{\mathbb{N}^+} = \tau \cdot \mathbb{I}_{\mathbb{N}^+}$.

Bizonyítás. (1)-et már láttuk a Möbius-féle inverziós formula bizonyításában. Mivel minden szereplő függvény multiplikatív, elég prímhatványokra belátni, hogy (2), (3) és (4) teljesülnek:

$$\begin{aligned} (I * I)(p^\alpha) &= \sum_{d|p^\alpha} 1 = \tau(p^\alpha); \\ (\mu * \mathbb{I}_{\mathbb{N}^+})(p^\alpha) &= \sum_{d|p^\alpha} \mu(d) \frac{p^\alpha}{d} = p^\alpha - p^{\alpha-1} = \varphi(p^\alpha); \\ (I * \mathbb{I}_{\mathbb{N}^+})(p^\alpha) &= \sum_{d|p^\alpha} d = \sigma(p^\alpha). \end{aligned}$$

Végül

$$\varphi * \tau = (\mu * \mathbb{I}_{\mathbb{N}^+}) * (I * I) = I * \mathbb{I}_{\mathbb{N}^+} = \sigma$$

és

$$\sigma * \varphi = (I * \mathbb{I}_{\mathbb{N}^+}) * (\mu * \mathbb{I}_{\mathbb{N}^+}) = \mathbb{I}_{\mathbb{N}^+} * \mathbb{I}_{\mathbb{N}^+} = \tau \cdot \mathbb{I}_{\mathbb{N}^+}. \quad \square$$

* **6.3.26. Tétel.** Azok a számelméleti függvények, amelyek az 1 helyen nem nulla értéket vesznek fel, a konvolúcióval Abel-csoportot alkotnak. A nem azonosan nulla multiplikatív számelméleti függvények is Abel-csoportot alkotnak a konvolúcióval.

Bizonyítás. Tudjuk, hogy a konvolúció kommutatív és asszociatív, valamint az $E(1) = 1$, $E(n) = 0$ ($n > 1$) függvény az egységeleme. Ha $f(1) \neq 0$ és $g(1) \neq 0$, akkor nyilván $(f * g)(1) \neq 0$, így a nem azonosan nulla multiplikatív függvények köréből nem vezet ki a konvolúció. Ha $f(1) \neq 0$, akkor az $(f * g)(n) = E(n)$ egyenletrendszer a $g(n)$, $n = 1, 2, \dots$ ismeretlenekre (ebben a sorrendben) egyértelműen megoldható, és

megadja f inverzét. Ha f nem azonosan nulla és még multiplikatív függvény is, akkor definiáljuk a h függvényt a $h(p^\alpha) = g(p^\alpha)$ összefüggéssel a prímszámok helyeken, és legyen $h(n) = h(p_1^{\alpha_1}) \cdots h(p_k^{\alpha_k})$, ha $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Ekkor h multiplikatív, így $f * h$ is, továbbá

$$(f * h)(p^\alpha) = \sum_{d_1 d_2 = p^\alpha} f(d_1) h(d_2) = \sum_{d_1 d_2 = p^\alpha} f(d_1) g(d_2) = E(p^\alpha).$$

Így $f * h$ megegyezik E -vel a prímszámokon, és mivel mindketten multiplikatívak, mindenütt, tehát h az f inverze. $\square$

6.3.27. Feladat [3]. Legyen $k, n \in \mathbb{N}^+$, legyen $\tau_k(n)$ az $n = x_1 x_2 \cdots x_k$, $x_1, \dots, x_k \in \mathbb{N}^+$ egyenlet megoldásainak száma (sorrend is számít). Mutassuk meg, hogy $\tau_1(n) = 1$ minden n -re és $\tau_2 = \tau$. Mutassuk meg, hogy a τ_k függvények multiplikatívak, és τ_{k+1} a τ_k összegzési függvénye, ha $k \in \mathbb{N}^+$.

* **6.3.28. Feladat [8].** Mutassuk meg, hogy $\tau^2 * \mu = \tau * \mu^2$, ahol a négyzetreemelés a sorozatok tagonkénti négyzetreemelése, nem a sorozat önmagával vett konvolúciójának az eredménye.

6.3.29. További feladatok megoldásokkal. [56]: 5.2-1–5.2-5, 5.6-1, 5.6-4–5.6-6, 5.7-10, 5.7-12; [54]: 3.2-1–3.2-6, 3.7-10–3.7-11, 3.6-1–3.6-18;

6.3.30. További feladatok. [69]: 2.4.1–2.4.22, 4.2.1–4.2.23, 4.3.1–4.3.15, 4.4.1–4.4.10; [80]: 196; [83]: VIII.3.9–VIII.3.11, VIII.3.13–VIII.3.15.

6.4 Lánctörtek

* **6.4.1. Lánctörtek.** Valós számok $q_1, q_1 + 1/q_2, q_1 + 1/(q_2 + 1/q_3), \dots$ alakú közelítéseivel kívánunk foglalkozni, amelyeket *lánctörtek*nek nevezünk ($q_1 \in \mathbb{Z}$, $q_n \in \mathbb{N}^+$, ha $n > 1$). Általánosabban, ha $x_1, x_2, x_3, \dots \in \mathbb{R}$ és $x_i > 0$, ha $i > 1$, vezessük be az $//x_1// = x_1, //x_1, x_2// = x_1 + 1/x_2, //x_1, x_2, x_3// = x_1 + 1/(x_2 + 1/x_3), \dots$ jelöléseket, azaz pontosabban fogalmazva, rekurzióval, legyen $//x_1// = x_1$ és

$$//x_1, x_2, x_3, \dots, x_n// = x_1 + \frac{1}{//x_2, x_3, \dots, x_n//},$$

ha $n > 1$; indukcióval nyilván $//x_2, x_3, \dots, x_n// > 0$. (Az $//x_1, x_2, x_3, \dots, x_n//$ jelölés helyett $\langle x_1, x_2, x_3, \dots, x_n \rangle$, illetve $[x_1, x_2, x_3, \dots, x_n]$ is használatos.)

Egy $\alpha \in \mathbb{R}$ valós szám lánctörtközelítéseit rekurzióval definiáljuk: legyen $\alpha_1 = \alpha$, és ha $n \geq 1$ és $\alpha_1, \alpha_2, \dots, \alpha_n$ definiálva vannak, akkor legyen $q_n = \lfloor \alpha_n \rfloor$, és ha α_n nem egész, akkor legyen $\alpha_{n+1} = 1/(\alpha_n - q_n) = 1/(\alpha_n \bmod 1)$, ha α_n egész, akkor pedig megállunk. Ha $q_1, q_2, \dots, q_n$ definiálva vannak, akkor $\delta_n = //q_1, q_2, \dots, q_n//$ az α szám n -edik lánctörtközelítése. Vegyük észre, hogy a lánctörtközelítések mind racionális számok, továbbá, hogy (indukcióval) $\alpha = //q_1, q_2, \dots, q_{n-1}, \alpha_n//$. Speciálisan, ha α megegyezik egy lánctörtközelítésével, akkor racionális.

A megfordítás is teljesül. Ennek bizonyításához figyeljük meg, hogy szoros kapcsolat van a lánctörtközelítések és az euklideszi algoritmus között: ha $\alpha = a/b$, ahol $a, b \in \mathbb{R}$, $b > 0$, és az a, b számokra formálisan alkalmazzuk az euklideszi algoritmust, azaz ha

$r_0 = a$, $r_1 = b$, és ha $n \in \mathbb{N}$ és $r_{n+1} \neq 0$ esetén $q_{n+1} \leftarrow \lfloor r_n/r_{n+1} \rfloor$ és $r_{n+2} \leftarrow r_n - q_{n+1}r_{n+1}$, akkor $\alpha_{n+1} = r_n/r_{n+1}$, $\alpha_{n+1} - q_{n+1} = r_{n+2}/r_{n+1}$, a két eljárás ugyanakkor ér véget, és ugyanazt a $q_1, \dots, q_n$ sorozatot szolgáltatja. Mivel $a, b \in \mathbb{Z}$ esetén az euklideszi algoritmus mindig véget ér, a racionális számok lántörtközelítéseinek sorozata véges.

◦* **6.4.2. Példák.** (1) Határozzuk meg $172/62$ lántörtközelítéseit. A számítás:

n	$q_n = \lfloor \alpha_n \rfloor$	$\alpha_{n+1} = 1/(\alpha_n - q_n)$
0		$172/62$
1	$2 = \lfloor 172/62 \rfloor$	$62/48 = 1/(172/62 - 2)$
2	$1 = \lfloor 62/48 \rfloor$	$48/14 = 1/(62/48 - 1)$
3	$3 = \lfloor 48/14 \rfloor$	$14/6 = 1/(48/14 - 3)$
4	$2 = \lfloor 14/6 \rfloor$	$6/2 = 1/(14/6 - 2)$
5	$3 = \lfloor 6/2 \rfloor$	

Ennek alapján a lántörtközelítések

$$2, \quad 2 + \frac{1}{1}, \quad 2 + \frac{1}{1 + \frac{1}{3}}, \quad 2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{2}}}, \quad 2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{2 + \frac{1}{3}}}},$$

az utolsó éppen $172/62$ lántört alakban megadva: $172/62 = //2, 1, 3, 2, 3//$.

(2) Határozzuk meg az $\alpha = (\sqrt{5} + 1)/2$ szám lántörtközelítéseit. Mivel $2 < \sqrt{5} < 3$, azt kapjuk, hogy $q_1 = 1$, $\alpha_1 - q_1 = (\sqrt{5} - 1)/2$, így $\alpha_2 = 2/(\sqrt{5} - 1) = (\sqrt{5} + 1)/2$. Innen indukcióval $q_n = 1$ minden n -re; formálisan $(\sqrt{5} + 1)/2 = //1, 1, \dots //$.

(3) Hasonlóan határozhatjuk meg bármely olyan valós szám lántörtközelítéseit, amely valamely racionális együtthatós másodfokú egyenlet gyöke.

* **6.4.3. Feladat [1].** Határozzuk meg $139/102$, $17/3$, $3/17$ és $8/1$ összes lántört közelítését.

* **6.4.4. Feladat [3].** Alakítsuk át a $//2, 1, 4//$, $// - 3, 2, 12//$ és $//0, 1, 1, 100//$ lántörteket törtkékké.

* **6.4.5. Feladat [2].** Határozzuk meg $\sqrt{2}$, $\sqrt{2} - 1$, $\sqrt{2}/2$, $\sqrt{3}$ és $1/\sqrt{3}$ összes lántört közelítését.

* **6.4.6. Feladat [3].** Mutassuk meg, hogy az $//1, 1, \dots, 1, \sqrt{2}//$ számok mind irracionálisak.

* **6.4.7. Lántörtközelítések zárt alakja.** Az előző definíció jelöléseivel, ha

$$q_1, q_2, \dots, q_n$$

definiálva vannak, akkor legyen $P_0 = 1$, $Q_0 = 0$, $P_1 = q_1$, $Q_1 = 1$ és $1 < k \leq n$ esetén legyen

$$P_k = q_k P_{k-1} + P_{k-2}, \quad Q_k = q_k Q_{k-1} + Q_{k-2}.$$

Ekkor ha $n \geq 1$, akkor $\delta_n = P_n/Q_n$, a P_n és Q_n egészek relatív prímek, továbbá ha $n > 1$, akkor

$$\delta_n - \delta_{n-1} = \frac{(-1)^n}{Q_n Q_{n-1}},$$

és

$$|\alpha - \delta_{n-1}| \leq \frac{1}{Q_n Q_{n-1}},$$

valamint egyenlőség csak $\delta_n = \alpha$ esetén áll.

Bizonyítás. A $\delta_n = P_n/Q_n$ állítás igaz $n = 1, 2$ esetén. Tegyük fel, hogy $n - 1$ -ig igaz. Vegyük észre, hogy δ_n -et úgy kapjuk $\delta_{n-1} = //q_1, q_2, \dots, q_{n-1} //$ -ből, hogy q_{n-1} helyébe $q_{n-1} + 1/q_n$ -t írunk. Így

$$\delta_{n-1} = \frac{P_{n-1}}{Q_{n-1}} = \frac{q_{n-1}P_{n-2} + P_{n-3}}{q_{n-1}Q_{n-2} + Q_{n-3}}$$

felhasználásával, mivel az indukciós feltételből az is adódik, hogy $P_{n-2}, P_{n-3}, Q_{n-2}, Q_{n-3}$ csak a $q_1, \dots, q_{n-2}$ függvényei, azaz q_{n-1} -től nem függenek,

$$\begin{aligned} \delta_n &= \frac{(q_{n-1} + 1/q_n)P_{n-2} + P_{n-3}}{(q_{n-1} + 1/q_n)Q_{n-2} + Q_{n-3}} = \frac{q_n(q_{n-1}P_{n-2} + P_{n-3}) + P_{n-2}}{q_n(q_{n-1}Q_{n-2} + Q_{n-3}) + Q_{n-2}} \\ &= \frac{q_nP_{n-1} + P_{n-2}}{q_nQ_{n-1} + Q_{n-2}} = \frac{P_n}{Q_n}. \end{aligned}$$

Indukcióval megmutatjuk, hogy $P_n Q_{n-1} - Q_n P_{n-1} = (-1)^n$. Ebből egyrészt következik $\delta_n - \delta_{n-1}$ megadott előállítás, másrészt, hogy P_n és Q_n legnagyobb közös osztója osztója $(-1)^n$ -nek is, azaz hogy P_n és Q_n relatív prímek. Nyilván teljesül az állítás, ha $n = 1$. Ha $n - 1$ -re teljesül, akkor

$$\begin{aligned} P_n Q_{n-1} - Q_n P_{n-1} &= (q_n P_{n-1} + P_{n-2})Q_{n-1} - (q_n Q_{n-1} + Q_{n-2})P_{n-1} \\ &= Q_{n-1}P_{n-2} - P_{n-1}Q_{n-2} = (-1)^n. \end{aligned}$$

Végül vizsgáljuk $\delta_n - \alpha$ előjelét. A δ_n -et úgy kapjuk, hogy az

$$\alpha = //q_1, q_2, \dots, q_{n-1}, \alpha_n //$$

összefüggésben α_n helyére q_n -et írunk. Ettől a cserétől $//\alpha_n //$ csökken, $//q_{n-1}, \alpha_n //$ nő stb., $//q_1, q_2, \dots, q_{n-1}, \alpha_n //$ csökken, ha n páratlan, és nő, ha n páros. Így $\delta_n - \alpha$ előjele megegyezik $(-1)^n$ előjelével. Az utolsó állítás ebből már következik. $\square$

* **6.4.8. Példa.** Számítsuk ki $172/62 = //2, 1, 3, 2, 3 //$ láncörtközelítéseit zárt alakban.

n	q_n	$P_n = q_n P_{n-1} + P_{n-2}$	$Q_n = q_n Q_{n-1} + Q_{n-2}$	$\delta_n = P_n/Q_n$
0		1	0	
1	2	2	1	2
2	1	$3 = 1 \cdot 2 + 1$	$1 = 1 \cdot 1 + 0$	3
3	3	$11 = 3 \cdot 2 + 5$	$4 = 3 \cdot 1 + 1$	$11/4$
4	2	$25 = 2 \cdot 11 + 3$	$9 = 2 \cdot 4 + 1$	$25/9$
5	3	$86 = 3 \cdot 25 + 11$	$31 = 3 \cdot 9 + 4$	$86/31$

Az utolsó közelítő érték $86/31$, a $172/62$ szám redukált alakja.

◦* **6.4.9. Megjegyzés.** Egy valós szám láncörtökölítései meglehetősen gyorsan konvergálnak a számhoz. Valóban, indukcióval $Q_n \geq F_n$, ha $n \in \mathbb{N}$, ahol F_n az n -edik Fibonacci-szám, és mint indukcióval könnyen látható,

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

Innen azt kapjuk, hogy

$$|\alpha - \delta_n| \leq \frac{1}{F_n F_{n+1}} \leq \frac{5}{\left(\frac{1+\sqrt{5}}{2} \right)^{2n+1} - \sqrt{5} - 1}.$$

* **6.4.10. Megjegyzés.** Történeti érdekesség, hogy a görögök a láncörtöket használták irracionális számok definiálására, míg Eudoxosz javaslatára át nem tértek a szeletekkel való definícióra. Megmutatható, hogy egy irracionális szám láncörtökölítése pontosan akkor periodikus valahonnan kezdve, ha a szám gyöke valamely racionális együtthatós másodfokú egyenletnek. Az előző tétel szerint, ha α irracionális szám, akkor végtelen sok olyan $p, q \in \mathbb{Z}$, $q \neq 0$ pár létezik, amelyre $|\alpha - p/q| < 1/q^2$, tudniillik bármely P_n, Q_n pár ilyen. Az is megmutatható, hogy még ha a jobb oldalon az 1 helyére $1/2$ -et teszünk, akkor is bármely két egymás utáni láncörtökölítés közül az egyik eleget tesz az egyenlőtlenségnek. Sőt, ha 1 helyére $1/\sqrt{5}$ -öt teszünk, még akkor is bármely három egymás utáni láncörtökölítés közül az egyik eleget tesz az egyenlőtlenségnek. Megmutatható viszont, hogy például $\alpha = (1 + \sqrt{5})/2$ esetén a konstans tovább már nem csökkenthető úgy, hogy még mindig végtelen sok p, q párra álljon fenn az egyenlőtlenség. Mindezen tények bizonyítása megtalálható Niven és Zuckerman [69] könyvében, 143–154. oldal.

Még fontosabb tény, hogy adott korlátnál nem nagyobb nevezőjű törtek közül a láncörtökölítések adják a legjobb közelítéseket:

* **6.4.11. Tétel.** Legyen α egy irracionális szám. Az előző tétel jelöléseivel, ha $p \in \mathbb{Z}$, $q \in \mathbb{N}^+$ és

$$|\alpha - p/q| < |\alpha - P_n/Q_n|$$

valamely $n > 1$ -re, akkor $q > Q_n$. Sőt, ha csak a gyengébb

$$|\alpha q - p| < |\alpha Q_n - P_n|$$

feltétel teljesül valamely $n > 0$ -ra, akkor is $q \geq Q_{n+1}$.

* **Bizonyítás.** Lásd Niven és Zuckerman [69] könyvét, 140. oldal. $\square$

◦* **6.4.12. Példa.** Közelítsük a π számot láncörtökölés segítségével. Mivel

$$314159265/10^8 \leq \pi \leq 314159266/10^8,$$

azt kapjuk, hogy $q_1 = \lfloor \pi \rfloor = 3$ és $314159265/10^8 \leq 1/\alpha_2 \leq 14159266/10^8$, ahonnan $50000000/7079633 \leq \alpha_2 \leq 20000000/2831853$. Innen $q_2 = 7$ és $2831853/177029 \leq \alpha_3 \leq 7079633/442569$, ahonnan $q_3 = 15$ és $442569/441098 \leq \alpha_4 \leq 177029/176418$, továbbá $q_4 = 1$ és $176418/611 \leq \alpha_5 \leq 441098/1471$. Innen már csak azt kapjuk, hogy $288 \leq$

$q_5 \leq 299$, amiből q_5 értékét nem tudjuk meghatározni, annak ellenére, hogy tudjuk, hogy egész. Így a π láncörtközelítései 3, $22/7$, $331/106$, $355/113$, ... Az egyiptomiak a 3-at, Arkhimédész pedig a $3 + 1/7 = 22/7$ közelítést használta, ami 3 értékes jegyre pontos. A könnyen megjegyezhető $//3, 7, 15, 1// = 355/113$ közelítés hét értékes jegyre pontos.

Megjegyezzük, hogy törtek helyett lebegőpontos számokkal is számolhattunk volna, csak arra kell ügyelni, hogy minden lépésben olyan intervallumot határozzunk meg, amely tartalmazza az α_n értéket. Ez adja az intervallumaritmetika ötletét.

6.4.13. Intervallumaritmetika. Ha $x \in [a_x, f_x]$ és $y \in [a_y, f_y]$, akkor nyilván $z = x + y \in [a_x + a_y, f_x + f_y]$, és így ha a_z az $a_x + a_y$ lefelé ($-\infty$ felé) kerekítésével kapott érték, f_z pedig az $f_x + f_y$ felfelé ($+\infty$ felé) való kerekítésével kapott érték, akkor $z \in [a_z, f_z]$. Hasonló a helyzet más műveleteknél is. Így ahelyett, hogy x és y közelítő értékével számolunk, számolhatunk a pontos értékeket tartalmazó, pontosan ábrázolható alsó és felső végpontú intervallumokkal is, és eredményként egy, a pontos eredményt tartalmazó intervallumot kapunk. Az IEEE 754 lebegőpontos aritmetikai szabványnak eleget tévő modern mikroprocesszorok támogatják az ilyen, úgynevezett *intervallum-aritmetikai* számításokat azzal, hogy különböző kerekítési irányok állíthatók be, a legközelebbi ábrázolható számra való kerekítés mellett a felfele, illetve lefele kerekítés is, de a kerekítés ki is kapcsolható.

°* **6.4.14. Feladat [6].** Határozzuk meg az alábbi végtelen láncörtök értékét:

- (1) $//1, 1, 1, \dots //$;
- (2) $//2, 1, 1, 1, \dots //$;
- (3) $//2, 3, 1, 1, 1, \dots //$;
- (4) $//2, 2, 2, \dots //$;
- (5) $//1, 2, 1, 2, 1, 2, \dots //$;
- (6) $//2, 1, 2, 1, 2, 1, \dots //$;
- (7) $//1, 3, 1, 2, 1, 2, 1, 2, \dots //$.

* **6.4.15. Feladat [3].** Legyenek $a_0, a_1, \dots, a_n$ és c pozitív valós számok. Mutassuk meg, hogy $//a_0, a_1, \dots, a_n// > //a_0, a_1, \dots, a_n + c//$ teljesül, ha n páratlan, de nem teljesül, ha n páros.

* **6.4.16. Feladat [6].** Legyenek $a_0, a_1, \dots, a_n$ és $b_0, b_1, \dots, b_{n+1}$ pozitív egész számok. Mi a feltétele annak, hogy $//a_0, a_1, \dots, a_n// > //b_0, b_1, \dots, b_{n+1}//$ fennálljon?

* **6.4.17. Feladat [6].** Keressünk két olyan p/q racionális számot, amely kielégíti a $|\sqrt{2} - p/q| < 1/(\sqrt{5}q^2)$ egyenlőtlenséget.

* **6.4.18. Feladat [6].** Keressünk két olyan p/q racionális számot, amely kielégíti a $|\pi - p/q| < 1/(\sqrt{5}q^2)$ egyenlőtlenséget.

* **6.4.19. Feladat [7].** Bizonyítsuk be, hogy a következő állítás tetszőleges $c > 2$ konstansra hamis: bármely ξ irracionális számhoz végtelen sok olyan p/q racionális szám létezik, amelyre $|\xi - p/q| < 1/q^c$.

°* **6.4.20. Feladat [7].** Legyen c tetszőleges konstans. Bizonyítsuk be, hogy az előző feladat állításából annyi igaz, hogy létezik olyan ξ irracionális szám, amelyre végtelen sok p/q racionális számra $|\xi - p/q| < 1/q^c$.

* **6.4.21. Feladat [10].** Bizonyítsuk be, hogy bármely ξ irracionális szám két egymás utáni P_n/Q_n lánctört közelítése közül legalább az egyik kielégíti a $|\xi - P_n/Q_n| < 1/(2Q_n^2)$ egyenlőtlenséget.

* **6.4.22. Feladat [11].** Adjuk meg a $\sqrt{D}$ szám lánctörtbe fejtését, ha

$$D = ((4m^2 + 1)n + m)^2 + 4mn + 1,$$

ahol $m, n \in \mathbb{N}^+$.

◦ **6.4.23. Feladat [6].** Adjunk módszert numerikusan (alsó és felső korláttal) adott alapra és számra a szám logaritmusának bináris alakja alsó és felső közelítésének meghatározására csak négyzetreemeléssel és osztással. Határozzuk meg így $\ln(2)$ alsó és felső közelítését intervallumaritmetikával.

6.4.24. Feladat [4]. Bizonyítsuk be, hogy a $((3!)!)!$ szám tízes számrendszerben több, mint 1000 jegyű, és állapítsuk meg, hogy hány nullára végződik.

◦ **6.4.25. Feladat [4].** Bizonyítsuk be, hogy az $F_{1945} = 2^{2^{1945}} + 1$ Fermat-szám több, mint 10^{582} számjegyből áll tízes számrendszerben, és határozzuk meg, hány jegyű az $5 \cdot 2^{1947} + 1$ szám (amely az F_{1945} szám legkisebb prímosztója).

◦ **6.4.26. Feladat [4].** Határozzuk meg, hogy a jelenleg ismert legnagyobb prímszám, $2^{43112609} - 1$ tízes számrendszerben hány jegyű.

◦ **6.4.27. Feladat [4].** Határozzuk meg, hogy a jelenleg ismert legnagyobb tökéletes szám (azaz olyan n természetes szám, amelyre $d(n) = 2n$), a $2^{43112609}(2^{43112609} - 1)$ szám tízes számrendszerben hány jegyű.

* **6.4.28. További feladatok megoldásokkal.** [56]: 5.10-4; [54]: 3.10-1–3.10-12.

* **6.4.29. További feladatok.** [69]: 7.1.2, 7.1.4, 7.4.2–7.4.6, 7.5.1–7.5.6, 7.1, 7.8.1–7.8.4.

Gráfelmélet

Ebben a fejezetben a gráfelmélet alapjaival foglalkozunk. Számos problémában csak bizonyos dolgok közötti kapcsolatok létezése vagy nem létezése fontos, ilyenkor rendszerint gráfelméleti problémához jutunk. Például bejárható-e a sakktábla huszárral úgy, hogy ugyanoda érjünk vissza, ahonnan elindultunk? Kiszínezhető-e egy térkép mindig négy színnel? Írhatunk-e 0-kat és 1-eket egy kör mellé úgy, hogy adott irányban körbemenve minden lehetséges módon leolvassa a négy egymás utáni számjegyet, minden négy hosszú 0–1-sorozatot pontosan egyszer kapjunk meg? Legfeljebb hány összeköttetés (vagy hány gép) eshet ki egy adott számítógépes hálózathoz úgy, hogy még legyen bármely két gép között összeköttetés? Mennyi egy számítógépes hálózat „átviteli kapacitása”? Hogyan térképezhetők fel az emberek közötti ismeretségek? Legalább hány rétegű nyomtatott áramkört kell egy adott áramkör legyártásához? Melyik a legrövidebb vilamos hálózat? Hányféleképpen kapcsolódhatnak össze adott atomok? Milyen lehetséges „reakciútak” vannak egy részecskefizikai folyamatnál? A problémák különböző területekről jönnek, szerteágazóak és változó nehézségűek, de talán a legfontosabb alkalmazásokat az informatika adja.

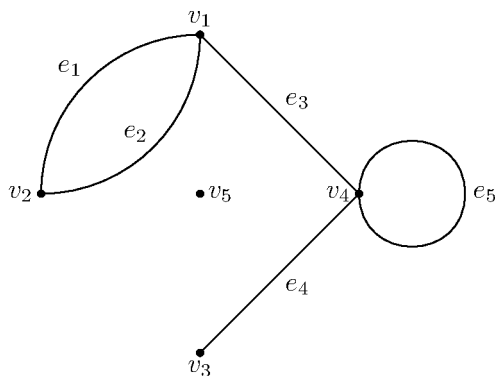
7.1 Irányítatlan gráfok

7.1.1. Irányítatlan gráfok. Egy irányítatlan gráfon szemléletesen pontoknak egy halmazát értjük, amelyek közül bizonyosakat éleknek nevezett ívekkel összekötünk. Előfordulhat, hogy két pontot több különböző él is összeköt, sőt az is, hogy egy vagy több él egy pontot saját magával köt össze. Csak az érdekel bennünket, hogy melyik él mely pontokat köt össze. A pontos definíció megértéséhez gondoljunk arra, hogy hogyan ábrázolnánk egy gráfot számítógépben: egy *irányítatlan gráf* vagy röviden *gráf* alatt egy $G = (\varphi, E, V)$ hármast értünk, ahol V a *csúcsok* vagy *szögpontok* halmaza, E az *élek* halmaza, a φ *illeszkedési leképezés* pedig egy E -t a V -beli elemekből álló rendezetlen párok halmazába képező leképezés. Ha valamely $e \in E$ -re és $v \in V$ -re $v \in \varphi(e)$, akkor azt mondjuk, hogy e *illeszkedik* v -re, vagy v *végpontja* e -nek. Megjegyezzük, hogy a jelölésből E elhagyható lenne, hiszen az $\text{dmn}(\varphi)$, azonban V nem, mert nem biztos, hogy minden csúcsra illeszkedik él: azokat a csúcsokat, amelyekre nem illeszkedik él, *izolált csúcsoknak* nevezzük. Még az is előfordulhat, hogy az E halmaz üres; ilyen esetben *üres gráfról* beszélünk.

Gyakran szokás némileg pontatlanul az illeszkedési leképezést elhagyni a jelölésből, és egy $G = (E, V)$ gráfról beszélni. Egyébként az élek és csúcsok közötti illeszkedés egy reláció E és V között, amelyet *illeszkedési relációnak* nevezzük.

Két különböző élt *szomszédosnak* nevezzük, ha van olyan csúcs, amelyre mindkettő illeszkedik. Két különböző csúcsot *szomszédosnak* nevezzük, ha van olyan él, amely mindkettőre illeszkedik.

Ha egy él csak egy csúcsra illeszkedik, akkor *hurokélnek* nevezzük. Ha az $e_1 \neq e_2$ élek ugyanazokra a csúcsokra illeszkednek, akkor *párhuzamos élekről* vagy *többszörös*



7.1.1 ábra: Példa gráfra.

élekről beszélünk. Ha egy gráf nem tartalmaz sem hurokért, sem párhuzamos éleket, akkor *egyszerű gráfnak* nevezzük. Az 7.1.1 ábrán például e_1, e_2 párhuzamos élek, e_5 huroké.

Ha E és V véges halmazok, akkor a gráfot *végesnek*, egyébként *végtelennek* nevezzük. Mivel számunkra a gráfok informatikai alkalmazásai miatt fontosak, az informatikában pedig csaknem kizárólag a véges gráfok játszanak szerepet, a továbbiakban elsősorban a véges gráfok vizsgálatával foglalkozunk.

Ha $G = (\varphi, E, V)$ egy gráf, és $S \subset V$, akkor jelölje $E(S)$ azon élek halmazát, amelyek egyik végpontja S -ben, a másik pedig pedig $V \setminus S$ -ben van. (Ezt a jelölést különböző könyvek más-más értelemben használják.) Nyilván $E(S) = E(V \setminus S)$.

Ha egy csúcsra csak véges sok él illeszkedik, akkor a csúcs *fokszámán* a rá illeszkedő élek számát értjük, a csúcsra illeszkedő hurokéleket kétszer számolva. Egy $v \in V$ csúcs fokát rendszerint $\deg(v)$ -vel vagy $d(v)$ -vel jelöljük. Ha egy gráfban minden csúcs foka n , akkor *n -regulárisnak* nevezzük; *reguláris gráf* alatt olyan gráfot értünk, amely valamely $n \in \mathbb{N}$ -re n -reguláris. Példa n -reguláris gráfra a H_n n -dimenziós *hiperkocka*: ennek csúcsai az n hosszú 0–1-sorozatok (amelyek a csúcs koordinátái sorozatának tekinthetők), és két csúcs akkor van összekötve, ha szomszédos, azaz ha a két sorozat pontosan egy helyen különbözik. További példák a *Petersen-gráf* és az öt szabályos test élei és csúcsai által alkotott gráfok: lásd a 7.1.2 ábrát.

Ha $G = (\varphi, E, V)$ egy véges gráf, akkor nyilván

$$\sum_{v \in V} d(v) = 2\sharp(E),$$

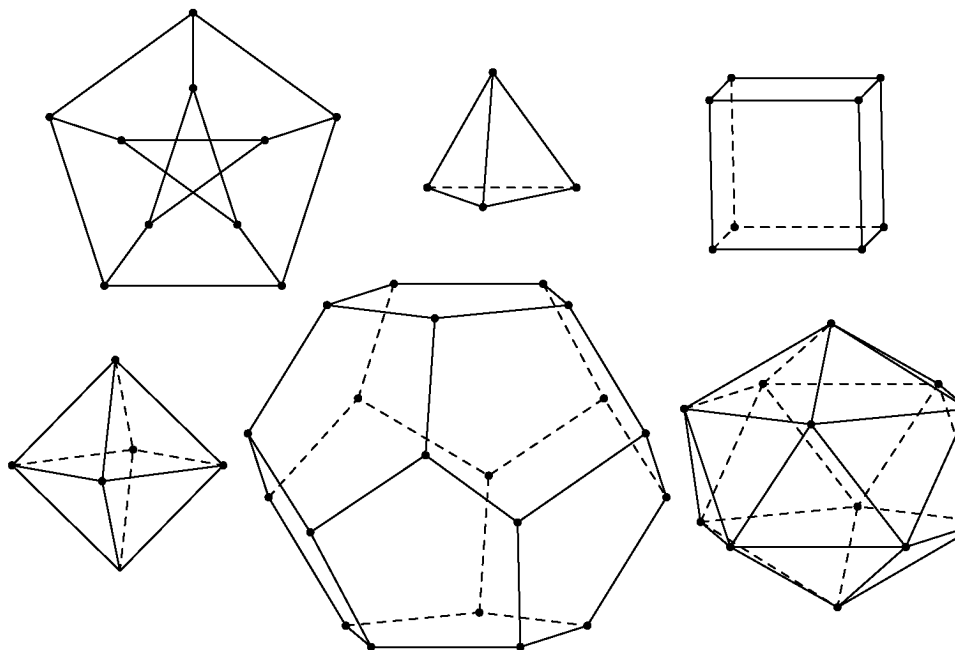
hiszen minden újabb él a bal oldali összeget kettővel növeli. Ebből azonnal következik, hogy egy véges gráfban a páratlan fokszámú csúcsok száma páros.

→ **7.1.2. Feladat [3].** Mutassuk meg, hogy tetszőleges, legalább két csúcsot tartalmazó gráfban van két egyenlő fokú csúcs.

7.1.3. Feladat [5]. Adott E és V véges halmazokra hány (φ, E, V) egyszerű gráf van?

7.1.4. Feladat [5]. Adott E és V véges halmazokra hány (φ, E, V) gráf van?

7.1.5. Feladat [5]. Mutassuk meg, hogy ha a $d_1, d_2, \dots, d_n$ természetes számok összege $2m$, $m \in \mathbb{N}$, akkor van olyan m élű gráf, amelyben a fokszámok sorozata $d_1, d_2, \dots, d_n$.



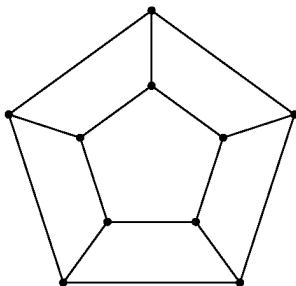
7.1.2 ábra: Néhány reguláris gráf.

* **7.1.6. Feladat [15].** Mutassuk meg, hogy pontosan akkor létezik egyszerű gráf a $d_1 \leq d_2 \leq \dots \leq d_n$ fokszámsorozattal, ha létezik egyszerű gráf a

$$d'_k = \begin{cases} d_k, & \text{ha } k = 1, 2, \dots, n - d_n - 1, \\ d_k - 1, & \text{ha } k = n - d_n, \dots, n - 1 \end{cases}$$

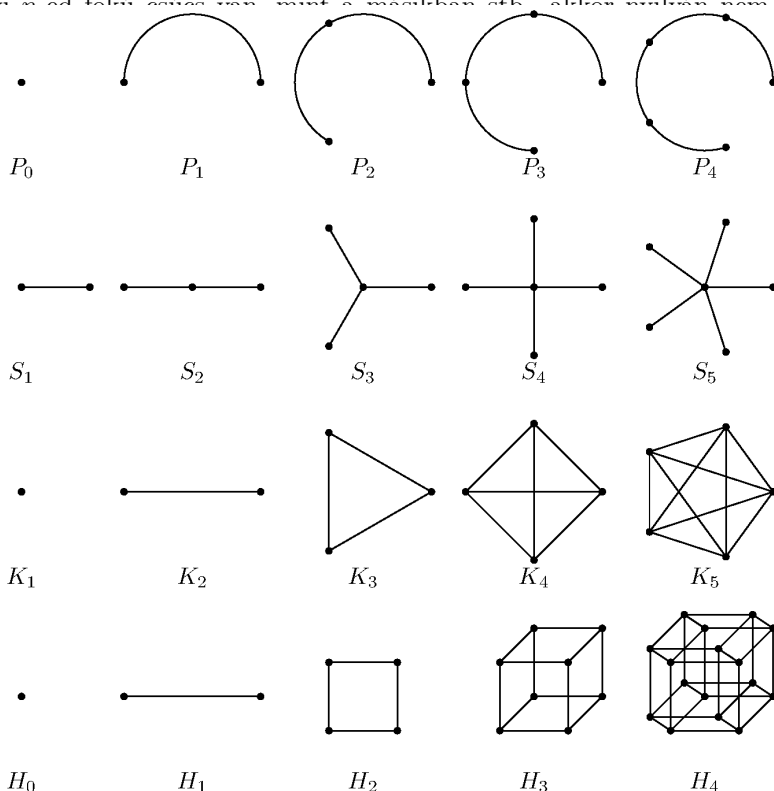
fokszámsorozattal.

7.1.7. Gráfok izomorfája. A $G = (\varphi, E, V)$ és $G' = (\varphi', E', V')$ gráfok *izomorfak*, ha van olyan az E -t E' -re képező kölcsönösen egyértelmű f és a V -t V' -re képező kölcsönösen egyértelmű g leképezés, hogy minden $e \in E$ -re és $v \in V$ -re e pontosan akkor illeszkedik v -re, ha $f(e)$ illeszkedik $g(v)$ -re, azaz az (f, g) pár tartja az illeszkedési relációt.



7.1.3 ábra: A Petersen gráffal nem izomorf gráf.

7.1.8. I
akkor a g
halmazai
két teljes
élek elnev
esetén az
éle van, é
test élgráf
példa: A
séggyökök
él törlésév
(például a



7.1.4 ábra: Nevezetes gráfok.

7.1.9. Gráfok Descartes-szorzata. Ha $G_i = (\varphi_i, E_i, V_i)$, $i \in I$ egyszerű gráfok indexelt családja, akkor a $\times_{i \in I} G_i$ Descartes-szorzatuk az a $G = (\varphi, E, V)$ gráf, amelyben a csúcsok halmaza $\times_{i \in I} V_i$, és két csúcs pontosan akkor van összekötve, ha egy kivételével minden koordinátájuk megegyezik, és ha a j -edik koordináták különböznek, akkor a megfelelő csúcsok össze vannak kötve a G_j gráfban. (Gráfok más szorzatait is szokták definiálni.) Például ha H_1 -ből n példány Descartes-szorzatát vesszük, H_n -et kapjuk. Ilyen Descartes-szorzatot használnak összeköttetési gráfnak masszív paralel számítógépekben: H_n mellett P_m két vagy három példányának Descartes-szorzata (síkrács illetve térrács), valamint C_m két vagy három példányának Descartes-szorzata (két- illetve háromdimenziós tórusz) fordul elő gyakran; rendszerint m kettőhatvány.

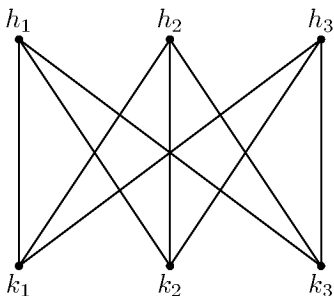
→ **7.1.10. Feladat** [5]. Határozzuk meg öt csúcsig az összes páronként nem izomorf egyszerű gráfot. Hány összefüggő, illetve reguláris van köztük?

→ **7.1.11. Feladat [4].** Hány olyan, páronként nem izomorf gráf van, amelyben

- (1) két-két másod-, harmad- és negyedfokú csúcs van, más foksám nem fordul elő;
- (2) három-három másod-, harmad- és negyedfokú csúcs van, más foksám nem fordul elő.

→ **7.1.12. Feladat [6].** Határozzuk meg a $H_n, P_n, P_n \times P_n, P_n \times P_n \times P_n, C_n, C_n \times C_n$ és $C_n \times C_n \times C_n$ ($n \in \mathbb{N}^+$) csúcsainak számát, a csúcsok fokát, és a gráfok átmérőjét.

7.1.13. Páros gráfok. Egy *páros gráf* (vagy *kétrészes gráf*) egy olyan gráf, amelynél adott a csúcsok V halmazának egy V', V'' diszjunkt halmazokra való felbontása úgy, hogy minden él egyik végpontja az egyik, másik végpontja a másik halmazba esik. Egy páros gráfot tehát egy (φ, E, V', V'') négyesként adhatunk meg. A legismertebb példa a „három ház, három kút” gráf, amelynél V' három házból, V'' három kútból áll, és bármely ház és bármely kút között van egy él, de több él nincs. Azt az egyszerű páros gráfot, amelyben $\mathfrak{h}(V') = m, \mathfrak{h}(V'') = n$, és minden V' -beli csúcs minden V'' -beli csúccsal össze van kötve, $K_{m,n}$ -nel jelöljük. A $K_{3,3}$ („három ház, három kút”) páros gráf a 7.1.5 ábrán látható.

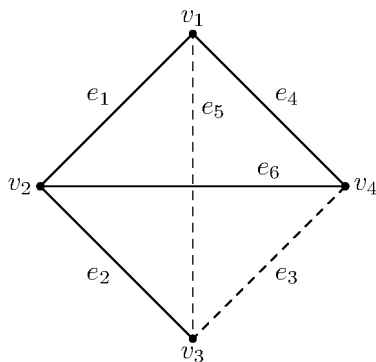


7.1.5 ábra: Három ház, három kút.

→ **7.1.14. Feladat [0].** Mutassuk meg, hogy egy véges (φ, E, V', V'') páros gráfra $\sum_{v \in V'} d(v) = \sum_{v \in V''} d(v) = \mathfrak{h}(E)$.

7.1.15. Részgráf. A $G' = (\varphi', E', V')$ gráfot a $G = (\varphi, E, V)$ gráf *részgráfjának* nevezzük, ha $E' \subset E, V' \subset V$ és $\varphi' \subset \varphi$. Néha azt mondjuk, hogy G a G' *szupergráfja*. Ha a G' részgráf mindazokat az éleket tartalmazza, amelyek végpontjai V' -ben vannak, azaz ha G' a legbővebb részgráf V' -beli csúcsokkal, akkor G' -t a V' által meghatározott *feszített részgráfnak* vagy *telített részgráfnak* nevezzük. Ha $G' = (\varphi', E', V')$ részgráfja a $G = (\varphi, E, V)$ gráfnak, akkor a G' -nek G -re vonatkozó *komplementerén* a $(\varphi|_{E \setminus E'}, E \setminus E', V)$ gráfot értjük. Ha G' egyszerű gráf, és külön nem mondjuk meg, hogy mely gráfra vonatkozó komplementeréről van szó, akkor a V' -beli csúcspontokkal rendelkező olyan egyszerű gráfra gondolunk, amelyben pontosan azok a csúcsok szomszédosak, amelyek G' -ben nem; ez lényegében a V' -beli csúcspontokkal rendelkező teljes gráfra vonatkozó komplementer. (Az ilyen gráfok az élek elnevezésétől eltekintve azonosak, azaz izomorfak.) A 7.1.6 ábrán szaggatott vonal mutatja a komplementer gráfot, $(\{e_1, e_4, e_6\}, \{v_1, v_2, v_4\})$ feszített, $(\{e_1, e_6\}, \{v_1, v_2, v_4\})$ nem feszített részgráf.

Ha $G = (\varphi, E, V)$ egy gráf és $E' \subset E$, akkor a G -ből az E' *elhalmaz törlésével kapott gráfon* a $G' = (\varphi|_{E \setminus E'}, E \setminus E', V)$ részgráfot értjük. Ha $G = (\varphi, E, V)$ egy gráf és $V' \subset V$,



7.1.6 ábra: Komplementer gráf.

akkor legyen E' az összes olyan élk halmaza, amelyek illeszkednek valamely V' -beli csúcsra. A G -ből a V' csúcs-halmaz törlésével kapott gráfon a $G' = (\varphi|_{E \setminus E'}, E \setminus E', V \setminus V')$ részgráfot értjük.

→ **7.1.16. Feladat [3].** Mutassuk meg, hogy minden 6 szögpon-tú egyszerű gráf vagy a komplementere tartalmaz 3 szögpon-tú teljes részgráfot.

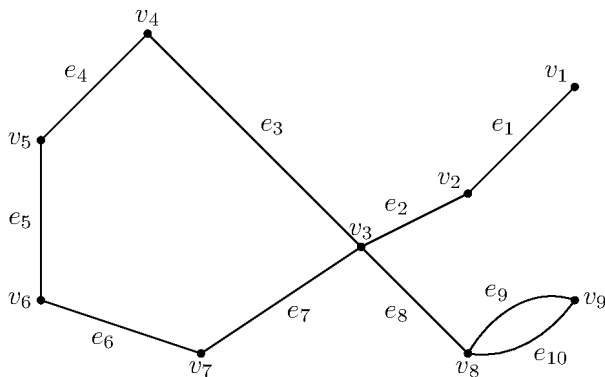
→ **7.1.17. Feladat [4].** Mely C_n gráfok részgráfjai a Petersen-gráfnak?

→ **7.1.18. Feladat [6].** Hány olyan 3, 4, illetve 5 szögpon-tú egyszerű gráf van, amely izomorf a komplementerével?

7.1.19. Séták, vonalak, utak és körök. Legyen $G = (\varphi, E, V)$ egy gráf. Egy G -beli n hosszú séta v -ből v' -be egy olyan

$$v_0, e_1, v_1, e_2, v_2, \dots, v_{n-1}, e_n, v_n,$$

véges sorozat, amelyre e_i a v_{i-1} és v_i csúcsokra illeszkedő él, ha $1 \leq i \leq n$ és $v_0 = v$, $v_n = v'$. (Egy séta nem részgráf, például egy él akárhányszor előfordulhat benne, van kezdőpontja és végpontja stb.) Ha $v = v'$, a sétát *zárt sétának* nevezzük, egyébként *nyílt sétának*. (Az út és az élsorozat elnevezés is elterjedt a séta helyett.) Ha a sétában szereplő élk mind különbözőek, akkor *vonálnak* nevezzük. Ha egy vonal zárt séta, akkor *zárt vonálnak* nevezzük, egyébként *nyílt vonálnak*. Egy sétát *útnak* fogunk nevezni, ha a $v_0, v_1, \dots, v_n$ csúcsok mind különbözők. (Aki a sétát útnak nevezik, ilyenkor az *egyszerű út* kifejezést használják.) A nulla hosszú séták mind utak és egyetlen csúcsból állnak. Az egy hosszú séták utak, ha a bennük szereplő egyetlen él nem hurokél. Egy út nem tartalmazhat sem hurokél-t, sem párhuzamos élket, sem ugyanazt az élt kétszer. Speciálisan, egy út mindig vonal. Egy legalább egy hosszú zárt vonalat *körnek* nevezünk, ha a kezdő- és a végpont megegyeznek, de egyébként a vonal pontjai különbözők. Az egy hosszú körök egyetlen hurokél-t tartalmaznak. A kettő hosszú körök két különböző, de párhuzamos élt tartalmaznak. Ha egy kör 3, 4, ... hosszú, akkor néha *háromszögnek*, *négyszögnek*, ... nevezzük. A gráf két csúcsának a *távolságán* az elsőt a másodikkal összekötő séták hosszának minimumát értjük (ha nincs ilyen, akkor a távolság $+\infty$). A gráf *átmérője* a csúcspon-tok távolságainak szuprémuma.



7.1.7 ábra: Vegyes példa.

A 7.1.7 ábrán $v_3, e_8, v_8, e_9, v_9, e_{10}, v_8, e_8, v_3$ zárt séta, de nem út és nem vonal;

$$v_1, e_1, v_2, e_2, v_3, e_3, v_4, e_4, v_5, e_5, v_6, e_6, v_7, e_7, v_3, e_8, v_8$$

vonal, de nem út; v_1, e_1, v_2, e_2, v_3 út is, vonal is; $v_3, e_3, v_4, e_4, v_5, e_5, v_6, e_6, v_7, e_7, v_3$ kör.

7.1.20. Állítás. Az előző pont jelöléseivel, bármely G gráfban a különböző v és v' csúcsokat összekötő sétából alkalmasan törölve e_i, v_i párokat, a v -t v' vel összekötő utat kaphatunk.

Bizonyítás. Ha $v_i = v_j$, $i < j$, töröljük az

$$e_{i+1}, v_{i+1}, e_{i+2}, v_{i+2}, \dots, e_j, v_j$$

részt, és ismételjük ezt, amíg minden csúcs különböző lesz. Mivel a séta hossza minden lépésben csökken, az eljárás véges sok lépésben véget ér. $\square$

7.1.21. Állítás. Bármely G gráfban egy legalább egy hosszúságú zárt vonal véges sok páronként éldiszjunkt kör egyesítése.

Bizonyítás. Ha nincs ismétlődő csúcs, kivéve, hogy az első és utolsó megegyezik, a vonal már kör, és készen vagyunk. Egyébként egy ismétlődő csúcs első előfordulásától a másodikig haladva egy rövidebb zárt vonalat kapunk, és ezt kihagyva az eredeti vonalból is egy rövidebb zárt vonal marad. Ezek közül azokkal, amelyek nem körök, megismételjük az eljárást. Minden lépésben, ha van még olyan zárt vonal, amely nem kör, abból két rövidebb vonalat kapunk. Végül csupa kör marad. $\square$

→ **7.1.22. Feladat [3].** Mutassuk meg, hogy tetszőleges páratlan hosszúságú zárt séta tartalmaz kört. Igaz-e ez páros hosszúságúra?

→ **7.1.23. Feladat [3].** Mutassuk meg, hogy ha egy véges gráfban minden csúcs legalább másodfokú, akkor tartalmaz kört. Igaz-e ez végtelen gráfra?

7.1.24. Összefüggőség. Egy gráfot *összefüggőnek* nevezünk, ha bármely két csúcsa összeköthető sétával. Ez nyilván azzal ekvivalens, hogy bármely két csúcsa összeköthető úttal. Nyilván egy adott gráf csúcsaira az a reláció, hogy két csúcs összeköthető úttal,

ekvivalenciareláció a csúcsok halmazán, így meghatároz egy osztályozást. A csúcsok egy adott ilyen osztálya által meghatározott telített részgráf a gráf egy *komponense*. Vegyük észre, hogy két különböző osztályba tartozó csúcs nem lehet szomszédos, így a gráf minden éle hozzátartozik egy komponenshez. Nyilván egy gráf akkor és csak akkor összefüggő, ha minden csúcs ugyanabba az osztályba tartozik, azaz ha csak egyetlen komponense van.

→ **7.1.25. Feladat [0].** Ha egy összefüggő gráfból elhagyunk egy d fokú csúcsot, legfeljebb hány komponensre esik szét?

→ **7.1.26. Feladat [4].** Mutassuk meg, hogy ha egy egyszerű gráf nem összefüggő, akkor a komplementere összefüggő.

7.1.27. Feladat [5]. Igazoljuk, hogy ha az n csúcsú egyszerű gráfban a minimális foksám nem kisebb, mint $(n - 1)/2$, akkor összefüggő. Írhatjuk-e $(n - 1)/2$ helyett az alsó egész részét?

7.1.28. Fák. Egy gráfot *fának* nevezünk, ha összefüggő és nincs köre.

7.1.29. Tétel. Egy G egyszerű gráfra a következő feltételek ekvivalensek:

- (1) G fa;
- (2) G összefüggő, de bármely él törlésével a kapott részgráf már nem összefüggő;
- (3) ha v és v' a G különböző csúcsai, akkor pontosan egy út van v -ből v' -be;
- (4) G -nek nincs köre, de bármilyen új él hozzávételével kapott gráf már tartalmaz kört.

Bizonyítás. Ha egy, mondjuk v, v' végpontú élt törölve a gráf összefüggő maradna, akkor létezne út v -ből v' -be, amit kiegészítve a törölt éllel, egy kört kapnánk, így (1)-ből következik (2). Ha most két különböző út lenne v -ből v' -be, akkor az egyiken szereplő csúcsokat $v, v_1, v_2, \dots$ -vel, a másikban szereplőket $v, v'_1, v'_2, \dots$ -vel jelölve, legyen k a legkisebb olyan index, amelyre $v_k \neq v'_k$. Törölve a v_{k-1}, v_k végpontú élt, a gráf összefüggő maradna, mivel bármely sétában, amelyben ez az él szerepel, helyettesíthetjük a $v_{k-1}, v'_k, v'_{k+1}, \dots, v', \dots, v_{k+1}, v_k$ csúcsokon át haladó sétával. Ezzel beláttuk, hogy (2)-ből következik (3). Ha a gráfban van egy $v, v', \dots, v$ kör, akkor nyilván két út vezet v -ből v' -be, így (3)-ból következik (1).

Végül, ha a gráf fa, akkor körmentes. Ha egy új hurokért veszünk hozzá, akkor már tartalmaz kört, ha pedig az új él végpontjai $v \neq v'$, akkor a v -ből v' -be vezető utat ezzel kiegészítve, kört kapunk. Megfordítva, ha (4) teljesül, akkor azt kell megmutatni, hogy bármely $v \neq v'$ -re vezet séta v -ből v' -be. Vegyünk hozzá egy új élt a gráfhoz, amelynek végpontjai v és v' . Az új gráfban van kör. Ebben az új él kell hogy szerepeljen. Törölve a körből az új élt, egy utat kapunk v -ből v' -be. $\square$

7.1.30. Tétel. Ha egy G véges gráfban nincs kör, de van él, akkor van legalább két elsőfokú csúcs.

Bizonyítás. A G -beli utak között van maximális hosszúságú. Válasszunk egy ilyet, ennek hossza legalább 1; vezessen v -ből v' -be. Megmutatjuk, hogy v és v' is elsőfokúak. Ha valamelyik nem lenne elsőfokú, akkor belőle még vezetne valahova él. Ha egy olyan csúcsba, amely nincs az adott úton, akkor az út hossza nem lenne maximális. Ha egy olyan csúcsba, amely az úton van, akkor a gráfban lenne kör. $\square$

7.1.31. Tétel. Egy G egyszerű véges, $n > 0$ csúcsú gráfra a következő feltételek ekvivalensek:

- (1) G fa;
- (2) G -ben nincs kör és $n - 1$ éle van;
- (3) G összefüggő és $n - 1$ éle van.

Bizonyítás. Ha $n = 1$, az állítás triviális. Tegyük fel, hogy G fa, $n > 1$, és legyen v_n egy olyan csúcsa G -nek, amelynek csak egy szomszédja van, v_{n-1} . Töröljük a v_n csúcsot: a maradék G' gráf is fa, mivel G -ben bármely útnak v_n csak a kezdőpontja vagy a végpontja lehet. Így n szerinti indukcióval kapjuk (1)-ből (2)-t. Hasonlóan kapjuk (2)-ből (3)-at: a fenti jelölésekkel G összefüggő, mivel v_n -ből vezet út v_{n-1} -be és (indukcióval) v_{n-1} -ből vezet út G' -ben minden más csúcsba. Végül tegyük fel, hogy (3) teljesül. Ha G -nek lenne köre, akkor a kör bármely élét törölve, egy olyan gráfot kapnánk, amely még mindig összefüggő. Folytassuk az élek törlését addig, amíg végül már nem marad kör a gráfban, azaz fát kapunk. Ha k lépést tettünk, akkor egy n csúcsú fát kapunk $n - k - 1$ éllel. De mivel (1)-ből következik (2), csak $k = 0$ lehetséges. $\square$

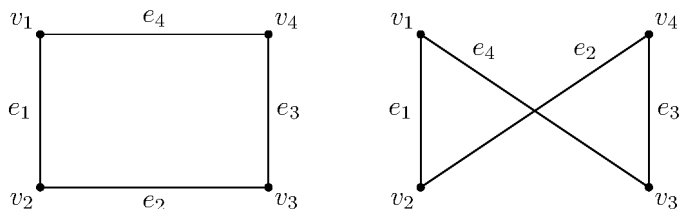
→ **7.1.32. Feladat [0].** Adott n pont. Ketten felváltva húznak be éleket. Az veszít, aki olyan élt rajzol be, amely után lesz kör. Kinek van nyerő stratégiája?

→ **7.1.33. Feladat [2].** Igazoljuk, hogy bármely legalább három csúcsú fában van elvágó csúcs.

7.1.34. Feladat [7]. Hány paraffin van 8 szénatommal?

* **7.1.35. Feladat: Cayley tétele [15].** Igazoljuk, hogy $n > 1$ csúccsal n^{n-2} fa van, ha az élek elnevezésétől eltekintünk.

7.1.36. Feszítőfa. Egy G gráf egy *feszítőfája* egy olyan F részgráfja G -nek, amely fa és a csúcsainak halmaza megegyezik G csúcsainak halmazával. (Persze, csak összefüggő gráfnak létezhet feszítőfája.) Az 7.1.8 ábrán két izomorf, de nem azonos gráf látható. Az e_4 törlésével kapott részgráf feszítőfa a bal oldali gráfban.



7.1.8 ábra: Izomorf gráfok.

7.1.37. Állítás. Minden összefüggő véges gráfnak létezik feszítőfája.

A bizonyítás konstruktív.

Bizonyítás. Amíg van a gráfban kör, hagyjuk el annak egyik élét. A maradék gráf összefüggő marad. Véges sok lépésben az eljárás megakad: ekkor a kapott gráf összefüggő és körmentes. $\square$

7.1.38. Állítás. Egy $G = (\varphi, E, V)$ összefüggő véges gráfban létezik legalább $\mathfrak{h}(E) - \mathfrak{h}(V) + 1$ kör, amelyek élhalmaza különböző.

Bizonyítás. Legyen F egy feszítőfája G -nek. Ennek $\mathfrak{h}(V) - 1$ éle van. Legyen E' a G azon éleinek halmaza, amelyek nem szerepelnek F -ben. Ha $e \in E'$, akkor ezt az élt hozzáadva F -hez, a kapott gráf tartalmaz legalább egy K_e kört. Természetesen az eredeti gráf is tartalmazza K_e -t. A kapott K_e kör tartalmazza e -t, de ha $e \neq e' \in E'$, akkor $K_{e'}$ nem tartalmazza e -t, így a $K_e, e \in E'$ körök élhalmazai mind különbözőek. $\square$

7.1.39. Megjegyzés. Az előző bizonyításban szereplő K_e kör élhalmazát az $e \in E'$ él egyértelműen meghatározza. Ha ugyanis az F feszítőfához hozzáadva az e élt, a kapott gráfban két különböző élhalmazú kör lenne, mivel mindkettő tartalmazza e -t, az e egyik végpontjától a másikig két különböző úton is el lehetne jutni F -ben, így F nem lenne fa. Ezt a körrendszert az F feszítőfához tartozó *alapkörrendszer*nek nevezzük. Lehet, hogy a gráfban más élhalmazú körök is vannak, de megmutatható, hogy egy alapkörrendszer segítségével algoritmikusan megadható G valamennyi köre. A tételben szereplő szám csak alsó korlát, hiszen például a tetraéder élgrájában több kör van, mint $\mathfrak{h}(E) - \mathfrak{h}(V) + 1$.

7.1.40. Vágás. Legyen $G = (\varphi, E, V)$ egy gráf. Ha v', v'' csúcsok, $V' \subset V$, és minden v' -ből v'' -be vivő útban szerepel valamely $v \in V'$ csúcs, akkor azt mondjuk, hogy V' *elvágyja* a v' és v'' csúcsokat. Ha $E' \subset E$, és minden v' -ből v'' -be vivő útban szerepel valamely $e \in E'$ él, akkor azt mondjuk, hogy E' *elvágyja* a v', v'' csúcsokat. Ha vannak olyan csúcsok, amelyeket az E' élhalmaz elvág, akkor E' -t *elvágó halmaznak* nevezzük. Ha egy elvágó halmaznak nincs olyan valódi részhalmaza, amely ugyancsak elvágó halmaz, akkor *vágásnak* nevezzük. Az 7.1.1 ábrán szereplő gráfban csak az üres halmaz vágás, mert a gráf nem összefüggő, de ha elhagyjuk a v_5 csúcsot, akkor a visszamaradó gráfban $\{e_3\}$, $\{e_4\}$ illetve $\{e_1, e_2\}$ a vágások.

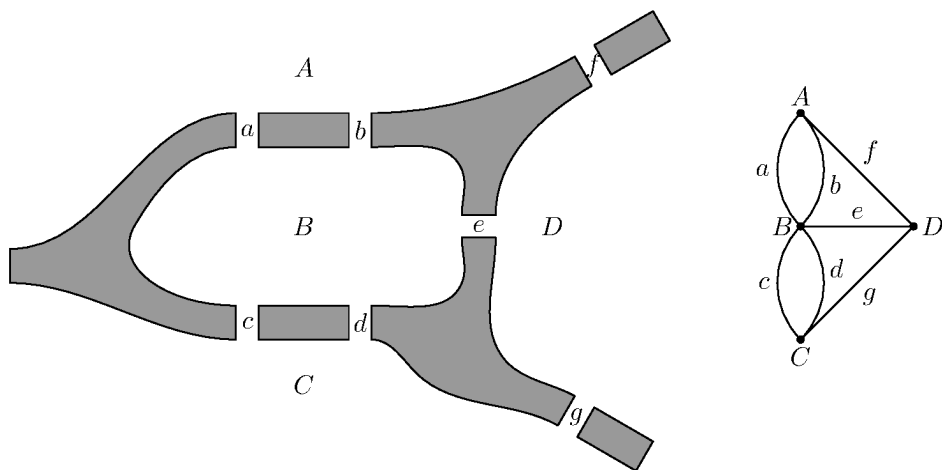
7.1.41. Állítás. Egy $G = (\varphi, E, V)$ összefüggő véges gráfban létezik legalább $\mathfrak{h}(V) - 1$ különböző vágás.

Bizonyítás. Legyen F egy feszítőfája G -nek, az F éleinek halmaza legyen E' . Konstruálunk E_e ($e \in E'$) vágásokat úgy, hogy E_e tartalmazza az $e \in E'$ élt, de semmilyen más $e' \in E'$ élt nem tartalmaz. Az $E \setminus E'$ élhalmaz nem elvágó halmaz, hiszen F összefüggő. Az $(E \setminus E') \cup \{e\}$, $e \in E'$ halmazok viszont elvágó halmazok. Tehát minden ilyen halmaz tartalmaz legalább egy vágást, legyen ez E_e . Ez nyilván tartalmazza az e élt, de más $e' \in E'$ élt nem tartalmaz. Egyébként az $(E \setminus E') \cup \{e\}$ élhalmaz pontosan egy vágást tartalmaz, mivel e törlése E' -ből két komponensre vágja a fát. A vágásban pontosan azok az élek vannak, amelyeknek végpontjai különböző komponensekben vannak. $\square$

7.1.42. Erdő. Körmentes gráfot *erdőnek* nevezzük. Egy erdő komponensei nyilván fák, a fák pedig összefüggő erdők. Egy gráf olyan részgráját, amely a gráf minden komponenséből egy feszítőfát tartalmaz, a gráf *feszítőerdőjének* nevezzük. Egy véges erdő éleinek száma nyilván a csúcsok számának és a komponensek számának különbsége. A nem összefüggő gráfoknál az erdők, illetve feszítőerdők ugyanazt a szerepet töltik be, mint az összefüggő gráfoknál a fák, illetve feszítőfák.

→ **7.1.43. Feladat [2].** Igazoljuk, hogy egy véges gráfban a komponensek számának és az élek számának összege nem kisebb, mint a csúcsok száma.

7.1.44. Euler-vonal. A legelső gráfelméleti problémával Eulernél találkozunk: egy folyón két sziget van, amelyeket híd köt össze. Az egyik szigetet két-két, a másikat egy-egy híd köti össze mindkét parttal. Be lehet-e járni egy pontból indulva a hét hidat úgy, hogy mindegyiken pontosan egyszer haladunk át, és ugyanoda érkezünk vissza? (Lásd a 7.1.9 ábrát.)



7.1.9 ábra: Königsbergi hidak.

Általánosabban kérdezhetjük, hogy egy véges gráfban létezik-e olyan zárt vonal, amelyben minden él szerepel, illetve adott v, v' csúcsokhoz a v -ből v' -be vezető olyan vonal, úgynevezett *Euler-vonal*, amelyben minden él szerepel. Ha $v \neq v'$, akkor v minden előfordulásánál az Euler-vonalban két él szerepel, amely illeszkedik v -re, kivéve az elsőt, így v páratlan fokú. Hasonlóan adódik, hogy v' is páratlan fokú, minden más csúcs pedig páros fokú, és ha $v = v'$, akkor minden csúcs páros fokú. Ez az egyszerű szükséges feltétel mutatja, hogy Euler problémájára a válasz negatív. Másrészt ez a szükséges feltétel elégséges is, ha a (véges) gráf összefüggő. A következő állítás egy általánosabb kérdést is megválaszol.

7.1.45. Állítás. Egy összefüggő véges gráfban pontosan akkor létezik zárt Euler-vonal, ha minden csúcs páros fokú. Ha véges összefüggő gráf $2s$ páratlan fokú csúcsot tartalmaz, ahol $s \in \mathbb{N}^+$, akkor a gráf s darab páronként éldiszjunkt nyílt vonal egyesítése.

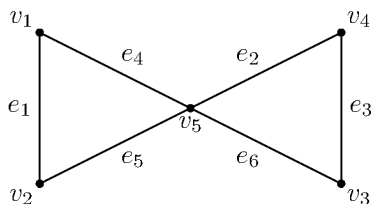
Bizonyítás. A bizonyítás konstruktív. Először tegyük fel, hogy $s = 0$. Induljunk ki egy tetszőlegesen kiválasztott v csúcsból álló, élt nem tartalmazó zárt vonalból. Ha az eddig kapott zárt vonalban nem minden él szerepel, akkor az összefüggőség miatt van a vonalon olyan v' csúcs, amelyre illeszkedő élek közül eddig nincs minden él felhasználva. Induljunk el ebből a csúcsból egy fel nem használt élen, és haladjunk mindig fel nem használt éleken. Mivel minden csúcsra páros sok fel nem használt él illeszkedik, a továbbhaladás csak akkor nem lehetséges, ha visszaérünk v' -be. Ha most az eredeti vonalon elme gyünk v -ből v' -be, az új vonalon körbemegyünk, majd az eredeti vonalon haladunk tovább, akkor az eredeti vonalnál hosszabb zárt vonalat kapunk.

Az általános (s tetszőleges) eset bizonyításához kössük össze páronként a páratlan fokú csúcsokat egy-egy új éllel. A kapott gráfban van zárt Euler-vonal. Ebből törölve az s új élt, s nyílt vonalra esik szét. $\square$

→ **7.1.46. Feladat [0].** Van-e olyan egyszerű gráf, amelyben van zárt Euler-vonal, páros számú pontja és páratlan számú éle van?

→ **7.1.47. Feladat [1].** Igazoljuk, hogy bármely összefüggő gráfban van olyan séta, amely a gráf minden élt pontosan kétszer tartalmazza. Igaz-e, hogy ez zárt séta?

7.1.48. Hamilton-út. Az Euler-vonal létezéséhez hasonlóan tűnő, mégis sokkal nehezebben megválaszolható kérdés, van-e egy gráfban olyan v -ből v' -be vezető út, amelyen a gráf minden pontja pontosan egyszer szerepel. Egy ilyen utat *Hamilton-útnak* nevezünk. *Hamilton-körnek* egy olyan kört nevezünk, amelyben a gráf minden csúcsa szerepel. Nyilván a Hamilton-út vagy Hamilton-kör létezéséhez a gráfnak végesnek és összefüggőnek kell lenni. Bár vannak tételek, amelyek azt mutatják, hogy ha egy összefüggő véges gráf minden pontja „élég magas” fokú, akkor létezik Hamilton-út, illetve Hamilton-kör, nem ismerünk igazán jó kritériumot Hamilton-út, illetve Hamilton-kör létezésére. Az összes lehetőség kipróbálásánál nem ismerünk lényegesen gyorsabb algoritmust Hamilton-kör keresésére, a lehetőségek száma pedig nagyon gyorsan nő a gráf növelésével: ezt szoktuk „kombinatorikus robbanásnak” nevezni. A 7.1.10 ábrán egy olyan gráfot láthatunk, amelyben van zárt Euler-vonal, de nincs Hamilton-kör.



7.1.10 ábra: Példa.

→ **7.1.49. Feladat [0].** Mutassuk meg, hogy ha egy páros gráfban van Hamilton-kör, akkor a gráf két pontosztálya egyforma elemszámú.

→ **7.1.50. Feladat [1].** Bejárható-e egy 9×9 -es sakktábla lóugrással úgy, hogy a kiindulási mezőre érjünk vissza?

7.1.51. Feladat [8]. Írjunk programot, amely megmutatja, hogy a 8×8 -as sakktábla lóugrással bejárható úgy, hogy a kiindulási mezőre érjünk vissza.

→ **7.1.52. Feladat [5].** Mutassuk meg, hogy egy dominócsomagból kirakható kör.

→ **7.1.53. Feladat [3].** Mutassuk meg, hogy a Petersen-gráfban nincs Hamilton-kör, de a belőle egyetlen csúcs elhagyásával kapott gráfban már van Hamilton-kör.

→ **7.1.54. Feladat [3].** Mutassuk meg, hogy ha egy gráfban van Hamilton-kör, akkor akárhogy hagyunk el belőle egy élt vagy egy csúcsot, a maradék gráf összefüggő.

7.1.55. Feladat [5]. Igazoljuk, hogy ha egy gráfban található $n \in \mathbb{N}^+$ csúcs úgy, hogy ezek elhagyásával a gráf $n + 1$ komponensre esik szét, akkor nincs Hamilton-köre.

7.1.56. Feladat [5]. Legyen $n \in \mathbb{N}^+$. Írhatunk-e 0-kat és 1-eket egy kör mellé úgy, hogy adott irányban körbemenve minden lehetséges módon leolvassa az n egymás utáni számjegyet, minden n hosszú 0–1-sorozatot pontosan egyszer kapjunk meg? Ezekkel a sorozatokkal kódolva a $0, 1, \dots, 2^n - 1$ számokat, a kapott kódot *Gray-kódnak* nevezzük.

7.1.57. Feladat [10]. Írjunk programot az összes n -csúcsú páronként nem izomorf gráf meghatározására. Ezek között hány lesz összefüggő, körmentes, fa, reguláris, hányban lesz Euler-vonal, zárt Euler-vonal, Hamilton-út, Hamilton-kör?

* **7.1.58. Feladat: Dirac tétele [13].** Mutassuk meg, hogy ha egy n szögpontú ($n > 2$) egyszerű gráfban minden csúcs foka legalább $n/2$, akkor van Hamilton-köre.

* **7.1.59. Feladat [13].** Egy táncmulatságon azonos számú férfi és nő van jelen. Mutassuk meg, hogy ha minden nő ismeri a férfiak több, mint felét, és minden férfi ismeri a nők több, mint felét (az ismeretség szimmetrikus), akkor az egész társaság körtáncot járhat úgy, hogy férfiak és nők felváltva vannak a körben, és mindenki ismeri mindkét szomszédját. Fogalmazzuk meg az állításnak megfelelő gráfelméleti tételt.

7.1.60. Címkezett és súlyozott gráfok. Gyakorlati alkalmazásokban gyakran további adatokat csatolunk a gráf éleihez, illetve csúcsaihoz. Ha adott egy $G = (\varphi, E, V)$ gráf, a C_e és C_v halmazok, az *élcímkek*, illetve *csúcscímkek* halmaza, valamint a $c_e: E \rightarrow C_e$ és $c_v: V \rightarrow C_v$ leképezések, az *élcímkezés*, illetve *csúcscímkezés*, akkor a $(\varphi, E, V, c_e, C_e, c_v, C_v)$ hetest *címkezett gráfnak* nevezzük. Ha csak élcímkek és élcímkezés adott, akkor *élcímkezett gráfról*, ha pedig csak csúcscímkek és csúcscímkezés adott, akkor *csúcscímkezett gráfról* beszélünk. Gyakran *színezett gráfról* beszélünk címkezett gráf helyett. A címkeket felhasználhatjuk például arra, hogy az adott csúcsra illeszkedő éleket megszámozzuk, rendezzük stb. Igen gyakori, hogy $C_e = \mathbb{R}$, illetve $C_v = \mathbb{R}$, ekkor *élsúlyozásról* és *élsúlyozott gráfról*, illetve *csúcssúlyozásról* és *csúcssúlyozott gráfról* beszélünk, és a jelölésből C_e -t, illetve C_v -t elhagyjuk. Egy (φ, E, V, w) élsúlyozott gráfban egy $E' \subset E$ véges élhalmaz *súlya* $\sum_{e \in E'} w(e)$. Hasonlóan egy (φ, E, V, w) csúcssúlyozott gráfban egy $V' \subset V$ véges csúcselhalmaz *súlya* $\sum_{v \in V'} w(v)$. Nagyon sok gráfalgoritmus súlyozott gráfokkal foglalkozik. Gráfalgoritmusokkal kapcsolatban lásd részletesebben a Rónyai–Iványos–Szabó [74] és a Cormen–Leiserson–Rivest [8] könyveket. Gráfalgoritmusok programozásával Donald E. Knuth [46] könyvének készülő negyedik kötete is foglalkozik. Ennek elkészült részeit lásd Knuth honlapján. Knuth „The Stanford Graph-Base” című [47] könyve gráfalgoritmusok C nyelvű programjainak gyakorlati példákkal bőségesen illusztrált gyűjteménye.

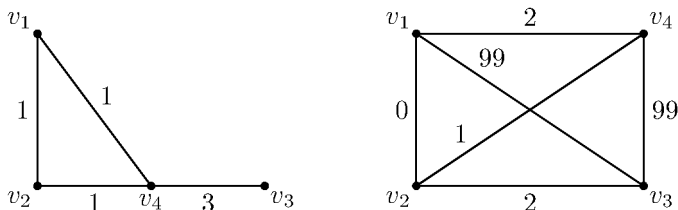
7.1.61. Mohó algoritmus minimális összsúlyú feszítőerdő konstrukciójára. Egy w élsúlyozással ellátott véges gráfban az összes csúcsot tartalmazó üres részgráfból indulva, és a már kiválasztott részgráfhoz, amíg lehet, hozzávéve valamely minimális súlyú olyan élt, amellyel a kiválasztott részgráf még nem tartalmaz kört, egy minimális súlyú feszítőerdőt kapunk.

Az algoritmus általában Kruskal algoritmusának néven ismeretes, bár Boruvka egy jóval előbb felfedezett és a moráviai villamoshálózat megtervezésére használt általánosabb, de bonyolultabb algoritmusának a speciális esete. Felhasználható rekordok csoportosítására, úgynevezett klaszterezésre is, ha a rekordokat csúcsoknak tekintjük egy teljes gráfban, a rekordok „különbözőségét” pedig az őket összekötő élt súlyának, és egy adott súlyhatár

feletti éleket nem használunk fel: a kapott feszítőerdőben a hasonló adatok kerülnek egy komponensbe.

Bizonyítás. Elég egy komponensre szorítkozni. Világos, hogy a kiválasztott élék egy F feszítőfát adnak. Tegyük fel, hogy a minimális súlyú F' feszítőfa súlya kisebb, mint F súlya; válasszunk olyan F' -t, amelynek a lehető legtöbb közös éle van F -fel. Legyen e' olyan él F' -nek, amely nem él F -nek. Ha e' -t hozzávesszük F -hez, keletkezik pontosan egy K kör. A kör minden e élére $w(e) \leq w(e')$, mert ha valamelyikre $w(e) > w(e')$ teljesülne, az algoritmus ezen e helyett e' -t választotta volna F -be. Ha F' -ből elhagyjuk e' -t, a kapott gráf nem összefüggő, hanem két komponense van. A K körön szereplő élék egyike, e' , összekötötte a két komponenst. Kell hogy legyen a körön legalább még egy (nyilván nem F' -beli) él, amely összeköti a két komponenst; jelöljük ezt e'' -vel. Az F' gráfból elhagyva e' -t, és hozzávéve e'' -t, a kapott F'' gráf is feszítőfa. Már tudjuk, hogy $w(e'') \leq w(e')$. Ha $w(e'') < w(e')$ lenne, akkor ebből az következne, hogy F'' súlya kisebb, mint F' súlya, így F' súlya nem minimális. Ha $w(e'') = w(e')$ teljesülne, akkor F'' is minimális súlyú feszítőfa lenne, de több közös éle lenne F -el, mint F' -nek. Mindkét eset ellentmondásra vezetett, így beláttuk, hogy az algoritmus jól működik. $\square$

A 7.1.11 ábra bal oldalán látható gráf mutatja, hogy nem mindig tudunk a maradék él közül minimális súlyú élt választani, különben a harmadik ilyen él behúzásakor kört kapnánk.



7.1.11 ábra: Amikor a mohó algoritmus nem működik.

7.1.62. Mohó algoritmusok. Kruskal algoritmusra példa úgynevezett *mohó algoritmus*ra: minden lépésben az adódó lehetőségek közül az adott lépésben legkedvezőbbek egyikét választjuk. A mohó algoritmusok nem mindig adják meg az optimumot. Még a Hamilton-kör keresésénél is nehezebb probléma az *utazó ügynök problémája*: véges, összefüggő, élsúlyozott gráfban a minimális összsúlyú Hamilton-kör megtalálása (egyúttal azt is eldöntve, van-e Hamilton-kör). Nem meglepő tehát, hogy az a mohó algoritmus, amely a legkisebb súlyú élből indulva, a kapott vonalat mindig valamelyik végén egy minimális súlyú éllel hosszabbítja meg, már egy 4 csúcspontú teljes gráfban sem feltétlenül találja meg a minimális súlyú Hamilton-kört, ahogy az a 7.1.11 ábrán jobb oldalon látható.

7.1.63. Feladat: minimális összsúlyú feszítőfa fanövesztéssel [10]. Mutassuk meg, hogy egy véges összefüggő élsúlyozott gráfban az egyik minimális súlyú éllel, mint egyélű fával indulva, ehhez minden lépésben a fa csúcsainak S halmazából kivezető $E(S)$ élék közül az egyik minimális súlyút hozzávéve, egy minimális súlyú feszítőfát kapunk. (Az algoritmust Prim algoritmus néven szokás emlegetni, bár Jarník már jóval korábban közölte.)

7.1.64. Feladat: piros-kék algoritmus [10]. Mutassuk meg, hogy egy véges összefüggő élsúlyozott gráfban, amelynek kezdetben minden éle szintelen, az alábbi két lépés tetszőleges sorrendben való ismétlése kékre színezi egy minimális feszítőfa éleit, a többi élt pedig pirosra:

- (1) [Kék lépés.] Egy $\emptyset \neq S \subsetneq V$ halmazra, amelyben $E(S)$ nem tartalmaz kék élt, az egyik minimális súlyú $E(S)$ -beli élt fessük be kékre.
- (2) [Piros lépés.] Egy körben, amelyben nincs piros él, az egyik maximális súlyú élt fessük be pirosra.

* **7.1.65. Feladat: a kínai postás-probléma [12].** Írjunk programot véges, összefüggő, pozitív valós súlyokkal élsúlyozott gráfban minimális összsúlyú, minden élt legalább egyszer tartalmazó zárt séta megtalálására.

* **7.1.66. Feladat: az utazó ügynök problémája [12].** Írjunk programot az utazó ügynök problémájának megoldására.

7.1.67. További feladatok. [25]: IV.1.7–IV.1.28, IV.1.33–IV.1.44, IV.4.3–IV.4.13; [34]: 1.2.6–1.2.8, 1.3.14–1.3.28, 1.5.9–1.5.18, 1.6.8–1.6.15, 1.8.6, 1.10.8, 1.10.9, 1.10.11–1.10.24, 2.1.8–2.1.11, 2.3.20–2.3.29, 8.1.1–8.1.3; [63]: 5§1, 5§2, 5§7, 5§12, 5§13; [64]: 7.1.1–7.1.7, 7.2.1–7.2.11, 7.3.1–7.3.15, 8.1.1–8.1.3, 8.2.1–8.2.3, 8.3.1, 8.3.2, 8.4.1–8.4.3, 8.5.1–8.5.13, 9.1.1, 9.1.2, 9.2.1–9.2.8; [83]: XV.7.5–XV.7.6, XV.7.9, XV.7.11–XV.7.12, XV.7.14, XV.7.18.

7.2 Irányított gráfok

7.2.1. Irányított gráfok. Egy irányított gráfon szemléletesen pontoknak egy halmazát értjük, amelyek közül bizonyosakat irányított éleknek nevezett irányított ívekkel összekötünk. A pontos definíció megértéséhez gondoljunk arra, hogy hogyan ábrázolnánk egy irányított gráfot számítógépben: egy *irányított gráf* alatt egy $G = (\psi, E, V)$ hármast értünk, ahol V a csúcsok vagy szögpontok halmaza, E az élek halmaza, a ψ *illeszkedési leképezés* pedig egy E -t $V \times V$ -be képező leképezés. Ha $\psi(e) = (v, v')$, akkor azt mondjuk, hogy v az e *kezdőpontja*, v' pedig a *végpontja*.

Bármely $G = (\psi, E, V)$ irányított gráfból kapható egy $G' = (\varphi, E, V)$ irányítatlan gráf úgy, hogy az irányítást „elfelejtjük”, azaz $\psi(e) = (v, v')$ esetén $\varphi(e)$ -t $\{v, v'\}$ -nek definiálva. Fontos, hogy mindazokat a fogalmakat, amelyeket irányítatlan gráfokra definiáltunk – ideértve a címkézést, súlyozást, stb. is – használni fogjuk irányított gráfokra is; ilyenkor mindig a megfelelő irányítatlan gráfra gondolunk. Azt is mondjuk, hogy G a G' egy *irányítása*. Természetesen egy gráfnak általában több irányítása is van. A $G = (\psi, E, V)$ irányított gráf *megfordításán* azt a $G' = (\psi', E, V)$ irányított gráfot értjük, amelyre $\psi(e) = (v, v')$ esetén $\psi'(e) = (v', v)$. (Természetesen hurokél megfordítása saját maga.)

Irányított gráfoknál is gyakran szokás némileg pontatlanul az illeszkedési leképezést elhagyni a jelölésből és egy $G = (E, V)$ irányított gráfról beszélni.

Ha az $e_1 \neq e_2$ éleknek ugyanaz a kezdőpontja és a végpontja, akkor *szigorúan párhuzamos élekről* beszélünk.

Ha $G = (\psi, E, V)$ egy irányított gráf, és $S \subset V$, akkor jelölje $E^+(S)$ azon élek halmazát, amelyek kezdőpontja S -ben, végpontja pedig $V \setminus S$ -ben van, és jelölje $E^-(S)$ azon

élek halmazát, amelyek végpontja S -ben, kezdőpontja pedig $V \setminus S$ -ben van. Nyilván $E(S)$ az $E^+(S)$ és $E^-(S)$ diszjunkt halmazok uniója és $E^+(S) = E^-(V \setminus S)$.

Ha egy csúcs csak véges sok élnek kezdőpontja, akkor ezek számát a csúcs *kifokának* nevezzük. Hasonlóan, ha egy csúcs csak véges sok élnek végpontja, akkor ezek számát a csúcs *befokának* nevezzük. Ha egy csúcs kifoka nulla, akkor *nyelőnek*, ha pedig befoka nulla, akkor *forrásnak* nevezzük. Egy $v \in V$ csúcs kifokát rendszerint $\deg^+(v)$ -vel vagy $d^+(v)$ -vel, befokát rendszerint $\deg^-(v)$ -vel vagy $d^-(v)$ -vel jelöljük.

Ha $G = (\psi, E, V)$ egy véges irányított gráf, akkor nyilván

$$\sum_{v \in V} d^+(v) = \sum_{v \in V} d^-(v) = \sharp(E),$$

hiszen minden újabb él mindhárom összeget eggyel növeli.

7.2.2. Példa. Legyen E egy V -beli binér reláció és legyen $\psi(e) = e$, ha $e \in E$, azaz egy csúcspot egy másikkal pontosan akkor kössünk össze, ha az első relációban áll a másodikkal. Ekkor (ψ, E, V) irányított gráf. Így relációk irányított gráfokkal szemléltethetők. Ezt már használtuk is a relációknál.

→ **7.2.3. Feladat [0].** Igazoljuk, hogy minden olyan gráf, amelyben van zárt Euler-vonal, irányítható úgy, hogy minden pont befoka egyenlő a kifokával.

→ **7.2.4. Feladat [4].** Jellemezzük véges halmazokon az ekvivalencia-relációk gráfjait.

→ **7.2.5. Feladat [4].** Bizonyítsuk be, hogy bármely véges, hurokélmentes gráf irányítható úgy, hogy a kapott gráf nem tartalmaz irányított kört.

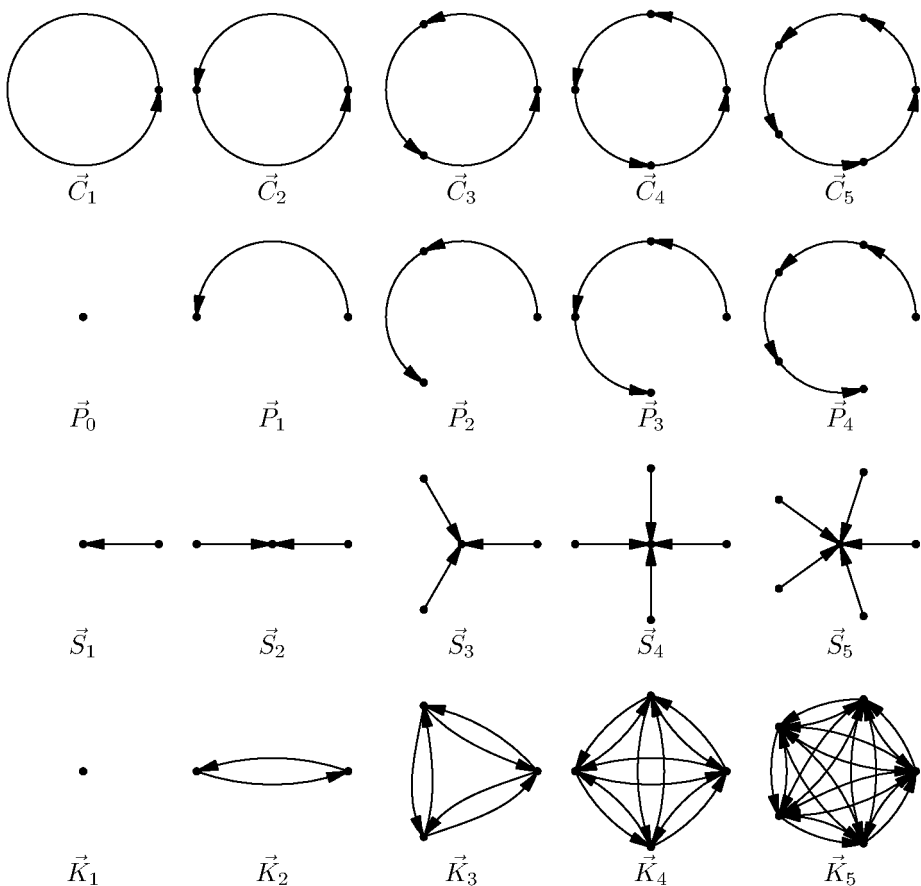
7.2.6. Feladat [5]. Adott E és V véges halmazokra hány (φ, E, V) egyszerű irányított gráf van?

7.2.7. Feladat [5]. Adott E és V véges halmazokra hány (φ, E, V) irányított gráf van?

7.2.8. Feladat [6]. Bizonyítsuk be, hogy egy teljes gráf tetszőleges irányításánál van olyan csúcs, ahonnan minden más csúcsba vezet irányított út.

7.2.9. Irányított gráfok izomorfiaja. A $G = (\psi, E, V)$ és $G' = (\psi', E', V')$ irányított gráfok *izomorfak*, ha van olyan az E -t E' -re képező kölcsönösen egyértelmű f és a V -t V' -re képező kölcsönösen egyértelmű g leképezés, hogy minden $e \in E$ -re egy $v \in V$ pontosan akkor kezdőpontja e -nek, ha $g(v)$ kezdőpontja $f(e)$ -nek, és pontosan akkor végpontja e -nek, ha $g(v)$ végpontja $f(e)$ -nek, azaz az (f, g) pár tartja a „kezdőpontja” és a „végpontja” relációkat.

7.2.10. Példák. Hasonlóan, mint az irányítatlan gráfoknál, az alábbi példák izomorfizációtól (tehát a csúcsok és élek elnevezésétől) eltekintve értendők. Egy $\vec{C}_n$ *irányított ciklus* csúcsai egy szabányos n -szög csúcsai, például az n -edik egységgyökök, és irányított él megy minden egységgyökből a következőbe (ciklikusan). A $\vec{P}_n$ *irányított ösvény* $\vec{C}_{n+1}$ -ből valamelyik él törlésével adódik. Az $\vec{S}_n$ *irányított csillagban* egy szabányos n -szög csúcsai-ból visz irányított él a középpontba, például az n -edik egységgyökökből a nullába. Adott csúcshalmaznál az *irányított teljes gráfban* minden csúcsból minden tőle különböző csúcsba visz irányított él. Az n -csúcsú irányított teljes gráfot $\vec{K}_n$ jelöli; ez nem K_n irányítása, sőt nem is egyszerű gráf, ha $n > 1$. Lásd a 7.2.1 ábrát.



7.2.1 ábra: Nevezetes irányított gráfok.

7.2.11. Véges gráfok éllistasz ábrázolása. Legyen (ψ, E, V) egy irányított gráf. A csúcsok beolvasásakor minden csúcshoz adunk egy sorszámot, és egy táblázatban (célszerűen egy hashtáblában) eltároljuk ezt a sorszámozást. Minden csúchhoz felépítjük azon élek listáját, amelyeknek ez a csúcs a kezdőpontja: a ψ leképezés olvasásakor, ha az $(e, (v, v'))$ párt olvassuk, akkor az (n, n') párt hozzáfűzzük az n sorszámú csúcs listájához, ahol n a v , az n' pedig a v' csúcs sorszáma. Egyéb járulékos információkat, például a csúcsok illetve élek nevét, címkéket, stb., is a csúchhoz, illetve az élhez fűzhetünk. Sok gráfalgoritmus kényelmesen megvalósítható az éllistasz ábrázolással. Például a gráf megfordítását úgy kaphatjuk, hogy az éllistaszt végigolvasva felépítjük a megfordítás éllistasz ábrázolását.

Irányítatlan gráfok éllistasz ábrázolásánál minden élt mindegyik végpontjának az éllistaszába beírunk. Ez annak felel meg, hogy minden nem hurokél egy oda-vissza menő irányított élpárnak tekintünk. Számos, irányított gráfokra kidolgozott algoritmus ezzel az ábrázolással irányítatlan gráfokra is működik.

7.2.12. Irányított részgráf. A $G' = (\psi', E', V')$ irányított gráfot a $G = (\psi, E, V)$ irányított gráf *irányított részgráfnak* nevezzük, ha $E' \subset E$, $V' \subset V$ és $\psi' \subset \psi$. Néha azt mondjuk, hogy G a G' *irányított szupergráfnak*. Ha a G' irányított részgráf mindazokat az éleket tartalmazza, amelyek kezdőpontjai és végpontjai is V' -ben vannak, akkor G' -t a V' által meghatározott *feszített irányított részgráfnak* vagy *telített irányított részgráfnak* nevezzük. Ha $G' = (\psi', E', V')$ irányított részgráfnak a $G = (\psi, E, V)$ irányított gráfnak, akkor a G' -nek G -re vonatkozó *komplementerén* a $(\psi|_{E \setminus E'}, E \setminus E', V)$ gráfot értjük. Ha nem mondjuk meg, hogy melyik gráfra vonatkozó komplementerről van szó, akkor az irányított teljes gráfra vonatkozó komplementerre gondolunk.

Ha $G = (\psi, E, V)$ egy irányított gráf és $E' \subset E$, akkor a G -ből az E' *élhalmaz törlésével kapott irányított gráfon* a $G' = (\psi|_{E \setminus E'}, E \setminus E', V)$ irányított részgráfot értjük. Ha $G = (\psi, E, V)$ egy irányított gráf és $V' \subset V$, akkor legyen E' az összes olyan él halmaza, amelyeknek kezdőpontja vagy végpontja valamely V' -beli csúcs. A G -ből a V' *csúcshalmaz törlésével kapott irányított gráfon* a $G' = (\psi|_{E \setminus E'}, E \setminus E', V \setminus V')$ részgráfot értjük.

7.2.13. Irányított séták, vonalak, utak és körök. Legyen $G = (\psi, E, V)$ egy irányított gráf. Egy G -beli n hosszú *irányított séta* v -ből v' -be egy olyan

$$v_0, e_1, v_1, e_2, v_2, \dots, v_{n-1}, e_n, v_n,$$

véges sorozat, amelyre e_i kezdőpontja v_{i-1} végpontja pedig v_i , ha $1 \leq i \leq n$, és $v_0 = v$, $v_n = v'$. Nyilván elegendő az él sorozatát megadni, mert azok meghatározzák a csúcsokat. Ha $v = v'$, az irányított sétát *zárt irányított sétának* nevezzük, egyébként séta *nyílt irányított sétának*. Ha az irányított sétában szereplő él mind különbözőek, akkor *irányított vonalnak* nevezzük. Ha egy irányított vonal zárt irányított séta, akkor *zárt irányított vonalnak* nevezzük, egyébként *nyílt irányított vonalnak*. Egy irányított sétát *irányított útnak* fogunk nevezni, ha a $v_0, v_1, \dots, v_n$ csúcsok mind különbözőek. Egy legalább egy hosszú zárt irányított vonalat *irányított körnek* nevezünk, ha a kezdő- és a végpont megegyeznek, de egyébként az irányított vonal pontjai különbözőek.

Az, hogy v -ből vezet irányított séta v' -be, nyilván azzal ekvivalens, hogy v -ből v' -be vezet irányított út. Ez a reláció nyilván tranzitív. Ha a megfelelő szigorú reláció szigorúan antiszimmetrikus is – ami azzal ekvivalens, hogy nincs irányított kör – akkor részbenrendezés. Az alábbi algoritmus eldönti, hogy van-e irányított kör, és ha nincs, akkor ezt a részbenrendezést kiterjeszti rendezéssé.

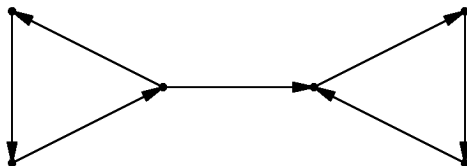
*** 7.2.14. Topologikus rendezés.** Az alábbi algoritmus egy gráf véges irányított gráfra eldönti, hogy van-e benne irányított kör, és ha nincs, akkor megadja a csúcsok egy olyan sorrendjét, hogy csak akkor megy él egy v csúcsból egy v' csúcsba, ha ebben a sorrendben v előbb van, mint v' .

- (1) [Inicializálás.] Beolvassuk a gráfot és felépítjük az éllistas ábrázolását, egyúttal minden csúcshoz meghatározva a befokát is. A nulla befokú csúcsokat betesszük az eredmény sorba. Legyen n a csúcsok száma, m az eredmény sorban lévő csúcsok száma és $i \leftarrow 1$ a következő feldolgozandó csúcs sorszáma.
- (2) [Vége?] Ha $i > n$, a sorrend az eredmény sorban. Egyébként, ha $m < i \leq n$, akkor van irányított kör a maradék $n - m$ -csúcsú gráfban. Mindkét esetben az algoritmus véget ér.

- (3) [Éltörlések.] Az eredmény sor i -edik eleméből kiinduló éleket egyenként töröljük, az él végpontjának befokát mindig eggyel csökkentve. Ha valamelyik végpont befoka nulla lesz, akkor a sor végére tesszük, eggyel növelve m -et. Végül legyen $i \leftarrow i + 1$, és menjünk (2)-re.

Bizonyítás. Ha egy csúcs bekerül az eredmény sorba, akkor már minden olyan csúcs, amelyből hozzá vezet él, a sorban van. Ha $i > m$, de nem minden csúcs került be az eredmény sorba, akkor a maradék gráf csúcsain nem lehet részben rendezés az a reláció, hogy vezet irányított út az egyikből a másikba, mert nincs legkisebb elem, hiszen az nulla befokú lenne. Így a megfelelő szigorú reláció nem irreflexív, tehát van irányított kör. $\square$

7.2.15. Erős összefüggőség. Egy irányított gráfot *erősen összefüggőnek* nevezünk, ha bármely (v, v') csúcspár esetén vezet irányított út v -ből v' -be (és így, v és v' szerepét megcserélve, v' -ből v -be is). Nyilván egy adott gráf csúcsaira az a reláció, hogy az egyikből a másikba és a másikból az egyikbe is vezet irányított út, ekvivalenciareláció a csúcsok halmazán, így meghatároz egy osztályozást. A csúcsok egy adott osztálya által meghatározott telített irányított részgráf az irányított gráf egy *erős komponense*. Vegyük észre, hogy – az irányítatlan gráfokkal ellentétben – nem feltétlenül tartozik az irányított gráf minden éle valamely erős komponenshez: lásd a 7.2.2 ábrát. Nyilván egy irányított gráf akkor és csak akkor erősen összefüggő, ha minden csúcs ugyanabba az osztályba tartozik, azaz ha csak egyetlen erős komponense van.



7.2.2 ábra: Az erős komponenshez.

7.2.16. Irányított fa. Az *irányított fa* olyan irányított gráf, amely fa, és van egy csúcsa, amelynek a befoka 0, az összes többi csúcs befoka 1. Azt a csúcspot, amelynek befoka 0, *gyökérnek* nevezzük. (Vannak, akik az irányított fát a megfordított irányítással értik: ilyenkor a gyökér kifoka 0, minden más csúcs kifoka 1.) Az úthossz szerinti indukcióval adódik, hogy a gyökérből bármely adott csúcsba vezető egyetlen út egyben irányított út is; ennek hossza az adott csúcs *szintje*. A csúcsok szintjeinek maximumát (amely véges irányított fa esetén nyilván létezik) a fa *magasságának* nevezzük. Ha van olyan él, amelynek v a kezdőpontja, v' pedig a végpontja, akkor az mondjuk, hogy v' a v *gyereke*, illetve hogy v a v' *szülője*. Ha két csúcsnak ugyanaz a szülője, akkor *testvéreknek* nevezzük őket. Bármely v csúcsra tekinthetjük azon csúcsok halmazát, amelyekhez vezet irányított út v -ből. Ezek a csúcsok meghatároznak egy feszített irányított részgráfot, amely nyilván irányított fa, és v a gyökere; ezt a v -ben gyökerező *irányított részfának* nevezzük. Irányított fának azokat a csúcsait, amelyek kifoka nulla, *levélnek* nevezzük.

Ha egy irányítatlan fában kijelölünk egy csúcspot, akkor *gyökeres fáról* beszélünk. Gyökeres fának egy és csak egy olyan irányítása van, amellyel irányított fa lesz úgy, hogy a kijelölt csúcs a gyökér: a kijelölt csúcsból egy másik adott csúcsba vezető egyetlen út

utolsó éle legyen az adott csúcshoz tartozó egyetlen bemenő él (a többi majd kimenő él lesz). Így a gyökér kijelölése ekvivalens az irányítás megadásával.

Egy q -ad rendű fa egy olyan élcímkezett irányított fa, amelyben minden él címkéje egy q -nál kisebb természetes szám, és minden csúcsra a kimenő élek címkéi különböznek. Legfontosabbak a másodrendű vagy *bináris fák*: itt 0 vagy 1 helyett *bal kimenő élről*, illetve *jobb kimenő élről*, *bal gyerekről*, illetve *jobb gyerekről*, *részfáról* stb. beszélünk. Megjegyezzük, hogy két q -ad rendű fát akkor is különbözőnek tekintünk, ha csak a címkézésben különböznek, például, ha egy bináris fában csak egyetlen él van, akkor sem mindegy, hogy az bal vagy jobb él.

Az irányított fákat úgy szoktuk lerajzolni, hogy a gyökér van felül. Ez nem felel meg a szóhasználatnak, de megfelel a gondolkodásunknak: a szülő alatt vannak a gyerekei stb.

7.2.17. Kőnig-lemma. *Ha egy végtelen irányított fában minden csúcsnak csak véges sok gyereke van, akkor van olyan, a gyökérrel induló $v_0, v_1, v_2, \dots$ végtelen csúcssorozat, amelyben v_n szülője v_{n+1} -nek ($n \in \mathbb{N}$).*

Bizonyítás. Indukcióval, v_{n+1} -et válasszuk v_n gyerekei közül olyannak, hogy a v_{n+1} -ben gyökerező irányított részfa végtelen legyen.

* **7.2.18. Kupac.** Legyen $q \in \mathbb{N}$, $q \geq 2$. Egy q -alapú kupac rendezett halmazból vett elemeknek (legtöbbször rekordoknak) egy $R_0, R_1, \dots, R_{n-1}$ sorozata, amelyre teljesül a kupac tulajdonság: ha $0 \leq i < j < n$ és $i = \lfloor (j-1)/q \rfloor$, akkor $R_i \leq R_j$. A kupac úgy is felfogható, mint egy irányított fa „szintenként sorfolytonosan ábrázolva”, amelyben az R_i csúcsnak legfeljebb q gyereke van: az R_j rekordok, ahol $j = qi + 1, qi + 2, \dots, qi + q$ és $j < n$; a kupac tulajdonság azt jelenti, hogy a szülő sohasem nagyobb, mint a gyereke. Így a kupacban az R_0 gyökérnél nincs kisebb rekord. Ezért alkalmas a kupac úgynevezett *elsőbbségi sorok* kezelésére, amelyekben mindig a legkisebb elemre van szükségünk, mint feldolgozandóra.

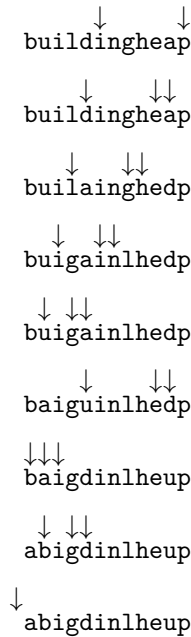
Ha $R_0, R_1, \dots, R_{n-2}$ már kupac, és új rekordot akarunk a kupachoz adni, akkor azt a sorozat végére tesszük, majd ha kisebb, mint a szülője, megcseréljük vele, és ezt folytatjuk, míg a kupac tulajdonság helyreáll. Néha elsőbbségi soroknál egy rekord megváltozik, csökken: ekkor is a fent leírt lépés ismétlésével állíthatjuk helyre a kupac tulajdonságot.

A legfontosabb kupac művelet egy rekord „süllyesztése”. Ezt alkalmazzuk például, ha egy R_i rekord megváltozik, nagyobb lesz: Tegyük fel, hogy az R_i rekord gyerekeihez tartozó részfákra teljesül a kupac tulajdonság, és azt akarjuk elérni, hogy az R_i -hez tartozó részfára is teljesüljön. Legyen R_j az R_i gyerekei közül a legkisebb. Ha ez nem kisebb, mint R_i , akkor készen vagyunk. Ha kisebb, akkor cseréljük meg R_i -t és R_j -t: az R_i „egy szinttel lesüllyedt”. Folytassuk a süllyesztést az új R_j -vel.

A süllyesztés segítségével könnyű az R_0 rekordot kicserélni egy új rekordra: R_0 helyére tesszük az új rekordot, majd süllyesztjük. Hasonlóan, ha az $R_0, R_1, \dots, R_n$ kupacból el akarjuk venni R_0 -at, akkor R_n -et a helyére tesszük, majd „süllyesztjük”. Ha tetszőleges másik rekordot akarunk elvenni, akkor úgy tekintjük, mintha lecsökkent volna minden más rekordnál kisebbre, így R_0 helyére kerül, és így már el tudjuk venni. Egy $R_0, R_1, \dots, R_{n-1}$ sorozatból úgy építhetünk kupacot, hogy az utolsóval kezdve a rekordokat sorra süllyesztjük.

Leggyakrabban a $q = 2$ esetet használjuk, ekkor *bináris kupac*ról beszélünk. A $q > 2$ esetnek csak akkor van jelentősége, ha a rekordok gyakran csökkennek, mert minél nagyobb q , annál kevesebb szint van, így csökkenésnél a kupac-tulajdonság helyreállítása

annál olcsóbb. Bináris kupacnál célszerű a sorozatot 0 helyett 1-től indexelni, mert az $i' = i + 1$, $j' = j + 1$ jelölésekkel az $i = \lfloor (j - 1)/q \rfloor$ összefüggés megfelelője az egyszerűbb szerkezetű $i' = i + 1 = 1 + \lfloor (j - 1)/q \rfloor = \lfloor j'/2 \rfloor$ összefüggés. A 7.2.3 ábra a kupacépítést mutatja bináris kupacra, egybetűs rekordokkal, a sorrend az ábácé sorrend; a nyilak a szülőt és gyerekeit jelzik, amelyekkel éppen dolgozunk.



7.2.3 ábra: Kupacépítés.

* **7.2.19. Kupacrendezés.** A kupacstruktúra felhasználható rendezett halmazból vett rekordok egy sorozatának a rendezésére. Először építsünk bináris kupacot. Ezután a legkisebb rekordot elvéve, csökkentsük eggyel a kupac méretét, és tegyük a legkisebb rekordot a felszabaduló helyre, a többi mögé. Ezt ismételve mindaddig, amíg a kupac el nem fogy, a kapott rekordsorozat monoton csökkenő. Ha monoton növekvő sorozatot akarunk, akkor megfordítjuk a rendezést.

A kupacrendezés felhasználható külső tárban tárolt rekordsorozat (fájl) rendezésére is. Az első fázisban feltöltjük a belső tárat rekordokkal, ezekből bináris kupacot építünk, majd kivisszük a legkisebb rekordot, és beolvasunk egy új rekordot. Ha az új rekord nem kisebb, mint a kivitt rekord, akkor a kupacba kerül, ha kisebb, akkor a kupac mérete eggyel csökken, és az új rekord a kupac mögé kerül. Amikor a kupac elfogyott, elkészült egy rendezett részfájl, egy „menet”. A bent lévő rekordokból kupacot építve új menetet kezdünk, egészen addig, amíg a bemenet el nem fogy. Az a trükk, hogy az éppen beolvasott új rekordot ha lehet, beépítjük az aktuális menetbe, átlagosan kétszer akkora meneteteket eredményez, mint az operatív tár.

A második fázis a menetek „összefésülésével” növeli azok méretét. Jónéhány menetet megnyitva (hogy mennyit, az az operációs rendszertől függ), mindegyikből beolvassuk

az első rekordot, és bináris kupacot építünk. A legkisebb rekord kivitele után ugyanaból a menetből, amiből ez származott, beolvasunk a helyére egy másikat, mindaddig, amíg minden megnyitott menet elfogy. A menetek számát – mindig a rövidebb menetek összefésülésével – csökkentjük: ha csak egy menet maradt, ez a rendezett kimenet.

Gyakran a rekordok nagyok, mozgatásuk időigényes (esetleg bonyolult is, mert nem egyforma hosszúak). Ekkor a kupacot csak a kulcsaiból építjük, a kulcshoz hozzátéve a rekord címét, de lehet csak a címekből építeni a kupacot.

*** 7.2.20. B-fa.** Rekordok rendezett halmazból vett kulcsainak mágneslemezen való tárolására szolgáló struktúra. Egy q -ad rendű B -favagy B_q -fa egy adattábla rekordjainak kulcsaiból épített q -adrendű irányított fa ($q \geq 3$), amelyben a gyökér és a levelek kivételével minden csúcsnak legalább $q/2$ gyereke van, és a levelek mind ugyanazon a szinten vannak. Ha egy csúcsnak $k + 1$ gyereke van, akkor k kulcsot is tartalmaz, a következő elrendezésben:

$$P_0, K_1, P_1, K_2, \dots, P_{k-1}, K_k, P_k;$$

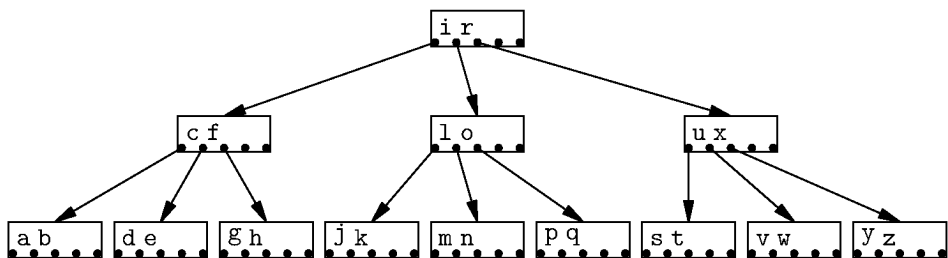
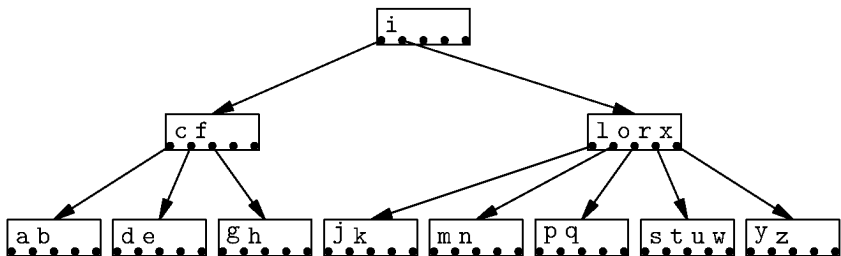
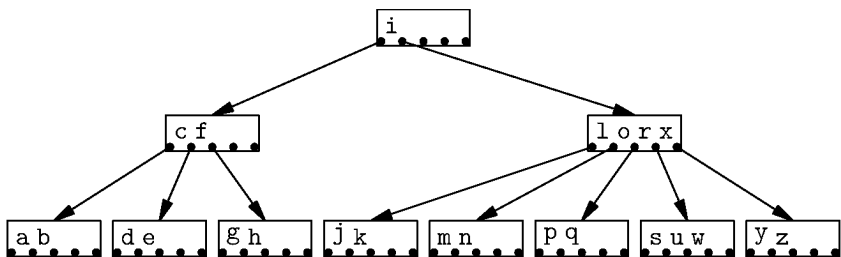
itt $K_1 < K_2 < \dots < K_k$ kulcsok, P_i pedig egy mutató (pointer), azaz egy abszolút vagy relatív cím, amely egy olyan részfára mutat, amelyben szereplő kulcsok szigorúan K_i és K_{i+1} közé esnek. A levelekben nincs információ, így azokra mindre a NULL mutató fog mutatni. Ugyancsak NULL mutató van a $P_{k+1}, \dots, P_{q-1}$ mutatók helyén is. Célszerűen minden csúcs egy szektort foglal el a lemezen, így egyben olvasható vagy írható. (A „kulcs” – ha nem az egész rekord – tartalmaz egy további mutatót is, amely a hozzá tartozó rekordra mutat.) Lásd a 7.2.4 ábrát.

A keresés nyilvánvaló. Új kulcs beszúrásához „megkeressük a helyét” a legalsó szinten, és oda szűrjük be; probléma csak akkor van, ha az adott szektorban ez lenne a q -adik kulcs. Ekkor a szektort „kettévágjuk”, a „középső” kulcsot egy szinttel feljebb szűrjük be, a maradékot pedig két szektorba tesszük, a „középső” kulcsnál kisebb kulcsokat az egyikbe, a nagyobbakat a másikba. A törlés sem sokkal bonyolultabb: csak arra kell vigyáznunk, hogy legalább $q/2$ mutató maradjon; ha ez nem teljesülne, a szomszédos testvérek valamelyikétől hozunk át, vagy ha lehet, összevonunk egy szomszédos testvérrel.

*** 7.2.21. Oszd meg és uralkodj.** Az előző két példa, a kupacrendezés és a B-fa tipikus példa az „*oszd meg és uralkodj*” elv alkalmazására: a feladatot kisebb részekre bontjuk, majd még kisebbekre, stb., amelyek úgy épülnek egymásra mint egy irányított fa szintjei.

7.2.22. Dijkstra módszere. A (ψ, E, V, w) véges élsúlyozott irányított gráfról tegyük fel, hogy az élsúlyok pozitívak, $s \in V$ és $T \subset V$. Az alábbi algoritmus a csúcsalmazon értelmez egy $d: V \rightarrow \overline{\mathbb{R}}$ függvényt, amely $t \in T$ esetén az adott s csúcsból a t csúcsba vezető irányított séták súlyának minimuma ($+\infty$, ha nincs ilyen séta):

- (1) [Inicializálás.] Legyen $S = \emptyset$, $H = \{s\}$ és $d(s) = 0$; minden más v csúcsra legyen $d(v) = +\infty$. (Az S halmaz a „már kész” csúcsok halmaza, H pedig a „már munkába vett” csúcsok halmaza.)
- (2) [Kész?] Ha $T \subset S$, vagy $H = \emptyset$, akkor az algoritmus véget ért.
- (3) [S bővítése.] Legyen $t \in H$ egy olyan csúcs, amelyre $d(t)$ minimális. Tegyük át t -t S -be, és minden e élre, amely t -ből $v \in V \setminus S$ -be vezet, ha $d(t) + w(e) < d(v)$, akkor legyen $d(v) = d(t) + w(e)$, és ha $v \notin H$, tegyük át v -t H -ba. Menjünk (2)-re.



7.2.4 ábra: A t majd v beszúrása egy B_5 -fába.

Bizonyítás. Az S elemszáma szerinti indukcióval megmutatjuk, hogy minden $t \in S$ -re $d(t)$ az s csúcsból a t csúcsba vezető irányított séták súlyának minimuma, ha pedig $v \in H$, akkor minden olyan s -ből v -be vezető irányított sétának, amelynek minden csúcsa S -ben van, kivéve v -t, a súlya legalább $d(v)$. Inicializálás után ezek nyilvánvalók. Tegyük fel, hogy (3)-ban $t \in H$ -t választottuk, és tekintsünk egy tetszőleges s -ből t -be vezető irányított sétát. Legyen ennek súlya W . Belátjuk, hogy $W \geq d(t)$. Legyen t' a séta első olyan csúcsa, amely nincs S -ben. A séta s -ből t' -ig vivő részének W' súlyára $W' \leq W$, az indukciós feltevés második része szerint $W' \geq d(t')$, és mivel t -t választottuk, $d(t) \leq d(t')$, így $W \geq d(t)$, amivel az indukciós feltevés első részét beláttuk. Miután (3)-ban a $d(v)$ értékeket megváltoztattuk, ha egy séta s -ből v -be visz, és csak az utolsó csúcsa nincs S -ben, legyen t' az utolsó előtti csúcsa, e pedig az utolsó éle. Mivel $t' \in S$, az s -től t' -ig vezető részséta súlya legalább $d(t')$, így a teljes séta súlya legalább $d(t') + w(e)$,

és amikor t' -t bevettük S -be, legfeljebb ennyire állítottuk $d(v)$ értékét, azóta pedig csak csökkenhetett. $\square$

7.2.23. Megjegyzés. Az előző algoritmus könnyen módosítható úgy, hogy megkapjunk egy, az s -ből t -be vezető minimális összsúlyú sétát is: amikor $d(v)$ értékét csökkentjük, jegyezzük fel a v csúchoz az e élt, felülírva az előző feljegyzést, ha volt olyan. A feljegyzések segítségével visszafelé követhetünk egy minimális összsúlyú irányított sétát. Ha minden ilyen sétára szükségünk van, akkor minden v csúcsnál éleknél egy listáját kell nyilvántartanunk: amíg $v \notin H$, a lista üres, egyébként, ha a (3) lépésben $d(t) + w(e) = d(v)$, akkor e -vel bővítjük a listát, ha pedig $d(t) + w(e) < d(v)$, akkor töröljük, és beletesszük e -t. Természetesen minden ilyen irányított séta irányított út is, mert az élek súlya pozitív.

7.2.24. Dinamikus programozás. Néha olyan feladattal találkozunk, amely számos hasonló, „egymást átfedő” részfeladatra vezet. Ilyenkor célszerűbb lehet az összes részfeladatot megoldani. Például ha – az előző pont jelöléseivel – csak a rögzített s -ből adott t -be vezető minimális összsúlyú séta súlya érdekel bennünket, akkor is célszerűbb – mint azt Dijkstra algoritmusában tesszük – minden csúcsra elkezdni megoldani a feladatot. Ezt a megoldási módszert nevezik *dinamikus programozásnak*.

* **7.2.25. Feladat [7].** Bináris kupac és éllista ábrázolás segítségével írjunk hatékony programot Dijkstra módszerére.

* **7.2.26. Feladat [5].** Miért nem működik Dijkstra módszere, ha valamelyik él súlya negatív?

* **7.2.27. Feladat [7].** Működik-e Dijkstra módszere, ha minden él súlya nemnegatív?

* **7.2.28. Feladat [12].** Keressünk olyan algoritmust, amely egy tetszőleges élsúlyozott irányított gráfban megkeresi az s csúcsból a t csúcsba vezető legkisebb súlyú utat.

* **7.2.29. Szélességi bejárás.** Dijkstra módszere arra is felhasználható, hogy egy vég-es irányított gráfban keressünk egy irányított fákból álló „irányított erdőt”, amelyben minden irányított fában a gyökérből az eredeti gráfban az adott csúcsba vezető legrövidebb irányított út szerepel: Minden él súlya legyen 1. Választva egy tetszőleges csúcsot, alkalmazzuk Dijkstra módszerét. Ha maradt még csúcs, a maradék csúcsokra újra alkalmazzuk a módszert stb. A módszer a gráfot úgy járja be, hogy a gyökérből először a szomszédos csúcsokat éri el, majd az azokkal szomszédos csúcsokat stb.; ezért nevezzük *szélességi bejárásnak*.

Észrevehetjük, hogy most a Dijkstra módszerénél szereplő H halmazban lévő csúcsok súlya mindig legfeljebb kétféle lehet, a csúcsok súlya soha nem csökken, és a H -ba újonnan bekerülő csúcsok súlya a nagyobbik súly. Ez azt jelenti, hogy a H halmaz elemeit tarthatjuk egy sorban, amelynek a végére tesszük az új belépőket, és az elejéről léptetünk át az S halmazba.

Azt is észrevehetjük, hogy ha irányítatlan gráf éllista ábrázolására alkalmazzuk a módszert, az eredeti gráf egy feszítőerdő[feszítőerdejét] kapjuk.

* **7.2.30. Mélységi bejárás.** A szélességi bejárást módosítsuk úgy, hogy amikor kivesszünk egy csúcsot a H sorból, a szomszédait betesszük a sorba, de az újonnan belépő csúcsokat nem a sor végére tesszük, hanem az elejére (a már a sorban lévőket átugorjuk). Itt tehát a gyökér egy szomszédjából annak egy szomszédjába megyünk stb., csak ha már

nem tudunk tovább haladni „mélységben”, akkor lépünk vissza; innen ered a *mélységi bejárás* elnevezés. A csúcsok itt nem súlyt kapnak, hanem két sorszámot. Az első a *bejárási szám*, ez azt mondja meg, hogy az adott csúcs hányadikként került be a H halmazba, a második a *befejezési szám*, ez azt mondja meg, hogy az adott csúcs hányadikként került át az S halmazba. (Induláskor minden csúcsnak mindkét számát nullára állítjuk.) A bejárési és befejezési számok egyrészt mutatják, hogy egy csúcs melyik halmazban van (attól függ, hogy a szám még nulla, vagy már nem nulla), másrészt más algoritmusok használják őket; lásd a feladatokat.

* **7.2.31. Feladat: Warshall–Floyd-algoritmus [10].** Igazoljuk, hogy egy véges élsúlyozott (ψ, E, V, w) gráfra, amelynek csúcsai $\{1, 2, \dots, n\}$, és nem tartalmaz negatív összsúlyú irányított kört (tehát gyengébb feltételek mellett, mint Dijkstra algoritmusában), a $(c_{i,j})_{i=1, j=1}^n$ mátrixszal indulva, amelyben $c_{i,j}$ értéke az i kezdőpontú, j végpontú

élek súlyának minimuma, és $+\infty$, ha nincs ilyen él, az összes $(i, j, k) \in \{1, \dots, n\}^3$ hármásra lexikografikus sorrendben végrehajtva a $c_{i,j} \leftarrow \min\{c_{i,j}, c_{i,k} + c_{k,j}\}$ értékadást, $c_{i,j}$ az i -ből j -be vezető minimális összsúlyú út súlya lesz.

* **7.2.32. Feladat [5].** Módosítsuk az előző algoritmust úgy, hogy a minimális összsúlyú utakat is feljegyezzük.

* **7.2.33. Feladat: erős komponensek meghatározása [10].** Igazoljuk, hogy egy irányított gráfot bejárva mélységi bejárással, majd a megfordítását újra bejárva mélységi bejárással, de mindig azt a csúcsot választva új gyökernek, amelyik a legnagyobb befejezési számot kapta az első bejárásnál, a kapott fák az erős komponensek.

* **7.2.34. PERT.** Egy nagy feladat (például egy nagy építkezés) részekre bontásának és a részfeladatok ütemezésének módszere a *PERT* (Program Evaluation and Review Technique). A részfeladatok egy irányított gráf éleinek felelnek meg, amelyek súlya a részfeladat elvégzésének ideje. A csúcsok állapotoknak felelnek meg: a csúcsba befutó éleknek megfelelő részmunkáknak be kell fejeződnie, mielőtt a csúcsból kifutó éleknek megfelelő részmunkák megkezdődhetnek. Az egész munkafolyamat az s start állapotból indul, és a t terminál állapotban fejeződik be. A gráf nem tartalmazhat irányított kört, s befoka és t kifoka nulla, és minden v csúcs rajta van valamely s -ből t -be vezető irányított úton. A *minimális befejezési időtartamot* a maximális összsúlyú s -ből t -be vezető irányított út összsúlya adja. Ezt az utat (vagy az ilyen utakat) *kritikus útnak* nevezzük, a kritikus utakon fekvő csúcsok illetve élek pedig a *kritikus csúcsok*, illetve *kritikus élek*: ezek késlekedése az egész munka befejezésének késlekedését jelenti, ezek gyorsítása pedig gyorsíthatja az egész munkát. Bár a hasonló feladatok általában nehezek, de most segít az, hogy a gráf nem tartalmaz irányított kört. Az egyes csúcsok elérésének legkorábbi időpontjai meghatározhatók, ha a csúcsokat megszámozzuk egy topologikus rendezésnek megfelelő sorrendben. Legyen $d(s) = d(1) = 0$ és $i = 2, 3, \dots, n$ -re legyen

$$d(i) = \min\{d(j) + w(e) : e \in E^+(j), \psi(e) = (j, i)\}.$$

A $d(n)$ maximális érték adja a legkorábbi befejezés idejét. Ugyanúgy, mint Dijkstra módszerénél, nyomonkövethetjük a kritikus utakat is.

* **7.2.35. Feladat [5].** Módosítsuk a PERT-nél tanult algoritmust úgy, hogy az az s -ből kiinduló minimális összsúlyú utakat találja meg tetszőleges irányított kört nem tartalmazó élsúlyozott gráfban.

* **7.2.36. Folyamprobléma.** Egy $G = (\psi, E, V)$ véges irányított gráfot két kijelölt pontjával, az s forrással (source) és a t céllal (terminal), $s \neq t$, valamint egy $c: E \rightarrow \mathbb{R}^+$ élsúlyozással *hálózatnak* nevezzük. A c függvény jelentése az egyes élek szállítási kapacitása (időegység alatt).

Egy hálózatot egy újabb $f: E \rightarrow \mathbb{R}$ élsúlyozással *folyamnak* nevezzük, ha minden $s \neq v \neq t$ pont esetén teljesül az $\sum_{e \in E^+(v)} f(e) = \sum_{e \in E^-(v)} f(e)$ *megmaradási feltétel* és tetszőleges e él esetén teljesül a $0 \leq f(e) \leq c(e)$ *kapacitásfeltétel*. Az f függvény jelentése az egyes éleken (időegység alatt) átszállított mennyiség. A *folyam értéke* $\|f\| = \sum_{e \in E^-(t)} f(e) - \sum_{e \in E^+(s)} f(e)$, a t -be (időegység alatt) beérkező mennyiség, az esetleg onnan kimenő mennyiséget negatív előjellel véve figyelembe. Tetszőleges hálózat esetén az azonosan nulla f egy *folyam*. Célunk maximális értékű *folyam* keresése. Ha egy *folyamban* egy élre $f(e) = c(e)$, akkor az élt *telített élnek* nevezzük. Ha egy *folyamban* minden s -ből t -be vezető irányított úton van telített él, akkor azt mondjuk, hogy a *folyam blokkoló folyam*. Az 7.2.5 ábrán balra fenn egy példát láthatunk blokkoló folyamra, amely azonban nem maximális *folyam*; az élek mellé a kapacitás és a *folyamérték* van írva. A maximális *folyam* megkereséséhez szükségünk lesz egy újabb fogalomra.

Ha (G, s, t, c, f) egy *folyam*, ahol $G = (\psi, E, V)$, definiáljuk a *folyamhoz tartozó javító hálózatot*: a csúcsok halmaza ugyancsak V , és minden $e \in E$ -hez az új G_f gráfban két él tartozhat: ha $f(e) < c(e)$, azaz ha van még kihasználatlan kapacitás, akkor a G_f -ben szerepel egy e^+ él, amelyek kezdőpontja és végpontja ugyanaz, mint e -nek, de kapacitása $c_f(e^+) = c(e) - f(e)$, ha pedig $f(e) > 0$, azaz már használtunk fel a kapacitásból, akkor szerepel egy e^- él, amelynek kezdőpontja e végpontja, végpontja e kezdőpontja, és $c_f(e^-) = f(e)$. Vegyük észre, hogy ha a javító hálózatban van egy pozitív értékű $g: E_f \rightarrow \mathbb{R}$ *folyam*, akkor $h(e) = f(e) + g(e^+) - g(e^-)$ egy olyan *folyam* a (G, s, t, c) hálózaton, amelynek értéke nyilván $\|h\| = \|f\| + \|g\| > \|f\|$. Javító *folyamot* már akkor tudunk konstruálni, ha találunk egy *javító utat*, ami egyszerűen egy irányított út G_f -ben s -ből t -be: legyen az irányított út minden e^* élére $g(e^*) = c$, ahol $c > 0$ a $c(e^*) > 0$ értékek minimuma az útban szereplő e^* élekre, minden más $e^* \in E_f$ -re pedig legyen $g(e^*) = 0$.

A következő lemma mutatja, hogy a *folyam értéke* $E(S)$ alakú elvágó élhalmazok segítségével is számolható, és ezek segítségével a *folyam értékére* könnyen kiszámolható felső becslést kaphatunk. A következő tétel pedig azt mutatja, hogy ez a felső becslés éles.

* **7.2.37. Lemma.** Az előző definíció jelöléseivel, minden *folyamra* és minden $S \subset V$ halmazra, amelyre $s \in S$ és $t \notin S$, teljesül, hogy $\|f\| = \sum_{e \in E^+(S)} f(e) - \sum_{e \in E^-(S)} f(e)$, és így $\|f\| \leq c(E^+(S))$.

Bizonyítás. Az egyenlőség a definícióból következik, ha $S = V \setminus \{t\}$, és ha teljesül $S \cup \{v\}$ -re valamely $v \neq s$ -re, akkor S -re is, mert v eltávolításakor a különbség egyik tagja $\sum_{e \in E^+(v)} f(e)$ -vel, a másik tagja pedig $\sum_{e \in E^-(v)} f(e)$ -vel csökken, de a *megmaradási feltétel* szerint a két mennyiség ugyanaz. Az egyenlőségből a felső becslés nyilvánvaló:

$$\|f\| = \sum_{e \in E^+(S)} f(e) - \sum_{e \in E^-(S)} f(e) \leq \sum_{e \in E^+(S)} f(e) \leq c(E^+(S)). \quad \square$$

* **7.2.38. Ford–Fulkerson-tétel (maximális *folyam*, minimális *vágás tétel*).** Az előző definíció jelöléseivel az alábbiak ekvivalensek:

(1) f *maximális értékű folyam*;

- (2) f -hez nem létezik javító út;
 (3) létezik olyan $S \subset V$ „minimális vágás”, amelyre $s \in S$, $t \notin S$, és $c(E^+(S)) = \|f\|$.

Bizonyítás. Az nyilvánvaló, hogy (1)-ből következik (2). Ha (2) teljesül, akkor legyen S azon pontok halmaza, amelyek s -ből irányított úton elérhetők G_f -ben. Nyilván $s \in S$, és mivel nincs javító út, $t \notin S$. Minden $e \in E^+(S)$ -re $f(e) = c(e)$ és minden $e \in E^-(S)$ -re $f(e) = 0$, hiszen egyébként $V \setminus S$ valamely pontja is elérhető lenne G_f -ben irányított úton. Ekkor viszont az előző lemmából $\|f\| \leq c(E^+(S))$. Végül az előző lemma szerint bármely folyam értéke legfeljebb $c(E^+(S))$ lehet, így ha (3) teljesül, akkor $\|f\|$ maximális. $\square$

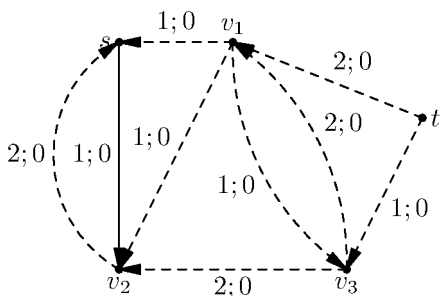
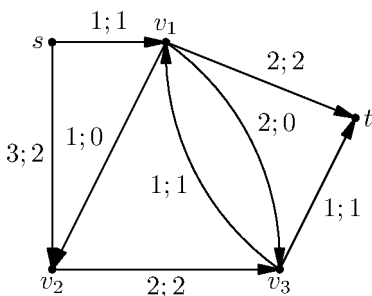
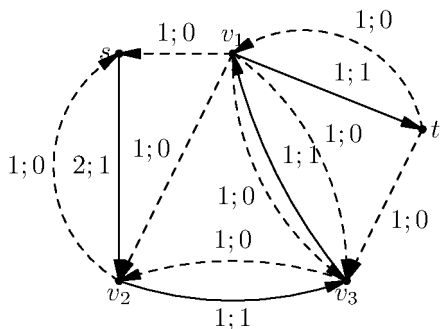
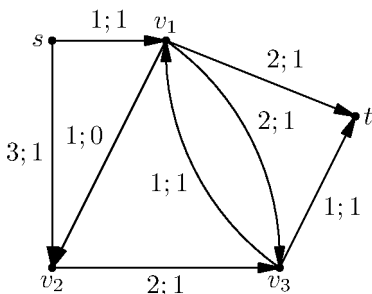
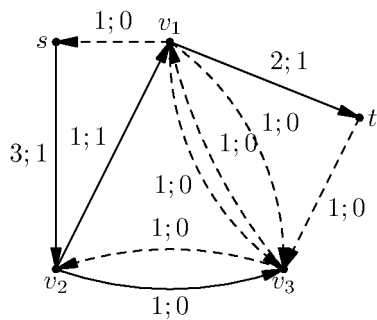
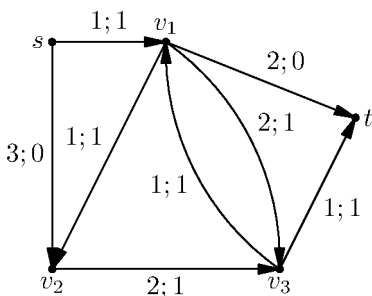
* **7.2.39. Edmonds–Karp-heurisztika.** Az előző tétel alapján még nem világos, hogyan érdemes a javító utakat választani, sőt, még azt sem láttuk be, hogy létezik maximális folyam. Az is előfordulhat, hogy „gondatlanul” választva a javító utakat, a növekvő folyamérték konvergál egy értékhez, de ez kisebb, mint a maximális folyam értéke. Az *Edmonds–Karp-heurisztika* abban áll, hogy mindig a legkevesebb élből álló javító utak közül választunk. Megmutatható, hogy ekkor a javító utak élszámai monoton növekedő sorozatot alkotnak, és egy élszám legfeljebb $\mathfrak{h}(E)$ -szer fordulhat elő. Mivel a javító út élszáma maximum $\mathfrak{h}(V) - 1$ lehet, az eljárás véges sok lépésben véget ér.

* **7.2.40. Dinic módszere.** Az előző pontban leírtnál is jobb taktika egy lépésben nem csak javító utat, hanem blokkoló folyamat keresni a javító hálózatban, pontosabban egy részében, mert ekkor $\mathfrak{h}(V) - 1$ lépésben célhoz érünk. Nevezzük egy v csúcs szintjének a javító hálózatban az s -ből a v csúcsba vezető legrövidebb út élszámát. A szintek az s -ből kiinduló szélességi bejárással könnyen meghatározhatók. Ha t -be nem vezet a javító hálózatban irányított út, akkor a Ford–Fulkerson-tétel szerint készen vagyunk, mert nincs javító út. Egyébként legyen t szintje k . Dobjunk ki a javító hálózatból minden olyan élt, amely nem „előre megy”, azaz amely nem egy magasabb (nyilván csak eggyel magasabb) szinten lévő csúcsba visz. A megmaradó H hálózat nem tartalmazhat irányított kört. Ha ebben a hálózatban sikerül egy g blokkoló folyamat találni, akkor azt – a korábbi értelemben – hozzáadva f -hez, az „ $f + g$ ”-hez tartozó javító hálózatban már k -nál magasabb szinten lesz a t , mert minden s -ből t -be vezető G -beli k hosszúságú úton legalább egy él telítetté válik, így nem fog szerepelni a javító hálózatban; keletkeznek ugyan új élek, de ezek mind visszafelé, alacsonyabb szinten lévő csúcsokba visznek. Mivel t legfeljebb a $\mathfrak{h}(V) - 1$ -edik szinten lehet, véges sok lépésben véget ér az eljárás, egyúttal azt is bizonyítva, hogy van maximális folyam. Az algoritmus működését a 7.2.5 ábrán követhetjük nyomon. Maradhatnak esetleg párhuzamos éleken való oda-vissza szállítások, de ezeket már könnyű megszüntetni.

A H hálózatban az azonosan nulla g folyamból kiindulva a következő három lépés felhasználásával keresünk blokkoló folyamat:

(1) „Nyomulás”: Célja, hogy H -ban egy s -ből t -be vezető irányított utat építsünk mélységi bejárással. Az aktuális út utolsó pontjából kimenő valamelyik élen tovább haladunk egy még be nem járt pontba, addig, amíg t -be nem érünk, vagy el nem akadunk. Ha már el sem tudunk indulni s -ből, akkor készen vagyunk.

(2) „Növelés”: Ha t -be értünk, akkor találtunk egy növelő utat. A g javító folyamat az út mentén megnöveljük a növelő út legkisebb kapacitású élének kapacitásával, az út mentén a kapacitásokat ugyanennyivel csökkentjük, és a telítetté vált éleket töröljük, majd a megmaradt útdarab végétől a „nyomulással” folytatjuk.



7.2.5 ábra: Dinic módszere: folyamatok és javító hálózatok.

(3) „Takarítás”: erre akkor kerül sor, ha a „nyomulás” egy v csúsnál elakadt. Ekkor töröljük a v -be menő éleket, eggyel visszalépünk a mélységi bejárásban, és onnan próbálkozunk a „nyomulással”.

A blokkoló folyam keresése véget ér, mert minden „növelés”, illetve „takarítás” elfogyaszt legalább egy élt, így ezek száma összesen legfeljebb H éleinek száma lehet. Ugyannyi lehet a „nyomulások” száma is, mert mindegyik után vagy „növelés” vagy „takarítás” következik. Nyilvánvaló, hogy az algoritmus egy g blokkoló folyamot talál H -ban.

* **7.2.41. Feladat** [7]. Tekintsük a folyamprobléma azon általánosítását, amelyben több forrás van és több cél, és az összes szállítást akarjuk maximalizálni. Vezessük vissza a probléma ezen általánosítását az eredeti problémára.

* **7.2.42. Feladat [8].** Tegyük fel, hogy a folyamproblémában a kapacitások egészek. Mutassuk meg, hogy létezik csak egész értékeket felvevő maximális folyam.

* **7.2.43. Feladat: általánosított folyamprobléma [9].** Általánosítsuk a folyamok elméletét arra az esetre, amelyben minden csúcson is van (pozitív valós) kapacitása.

* **7.2.44. Feladat: Menger tétele elvágó élhalmazra [7].** Bizonyítsuk be, hogy egy G véges gráfban az $s \neq t$ csúcsokat elvágó élhalmazok elemszámának minimuma megegyezik az s -ből t -be vezető éldiszjunkt utak maximális számával.

* **7.2.45. Feladat: Menger tétele elvágó csúcshalmazra [7].** Bizonyítsuk be, hogy egy G véges gráfban az $s \neq t$ csúcsokat elvágó csúcshalmazok elemszámának minimuma megegyezik az s -ből t -be vezető csúcsdiszjunkt utak maximális számával.

* **7.2.46. Feladat: König tétele [9].** Egy gráf *lefogó csúcshalmaza* egy olyan csúcshalmaz, amelyben minden élnek van végpontja. Egy gráf egy *párosítása* egy páronként nem szomszédos élekből álló élhalmaz. Bizonyítsuk be, hogy egy véges páros gráfban a párosítások élhalmazainak maximális elemszáma megegyezik a lefogó csúcshalmazok elemszámának minimumával.

°* **7.2.47. Gráfok rajzolhatósága.** Legyen $X \subset \mathbb{R}^n$. Egy X -beli *görbe* egy, a $[0, 1]$ valós intervallumot X -be képező γ folytonos függvény. Azt mondjuk, hogy $\gamma(0)$ a *görbe kezdőpontja*, $\gamma(1)$ pedig a *görbe végpontja*. Ha legfeljebb a kezdőpont és a végpont egyeznek meg, akkor azt mondjuk, hogy γ *egyszerű görbe*. Egy $G = (\psi, E, V)$ irányított gráf egy X -beli *lerajzolásán* azt értjük, hogy a gráf csúcsaihoz X különböző pontjait, éleihez pedig X -beli egyszerű görbéket rendelünk, amelyek egymást nem metszik; pontosan fogalmazva, a G gráf X -beli lerajzolásán egy (f, g) függvénpárt értünk, ahol $f: V \rightarrow X$ kölcsönösen egyértelmű, g pedig minden $e \in E$ -hez egy olyan X -beli g_e egyszerű görbét rendel, amelynek kezdőpontja e kezdőpontjának f általi képe, végpontja e végpontjának f általi képe, és a $g_e([0, 1])$, $e \in E$ halmazok egymástól és $\text{rng}(f)$ -től diszjunktak. Egy irányítatlan gráf egy X -beli *lerajzolásán* bármelyik irányításának az X -beli lerajzolását értjük. Ha a G (irányított vagy irányítatlan) gráfnak létezik egy $X \subset \mathbb{R}^n$ -beli lerajzolása, akkor azt mondjuk, hogy G az X -be *rajzolható*. (Az X -be rajzolhatóságot nyilván általánosíthatjuk arra az esetre, amikor X tetszőleges metrikus tér.)

Nyilvánvaló, hogy nem minden gráf rajzolható, mert például lehet, hogy olyan sok csúcs van, hogy eleve nem létezik $f: V \rightarrow X$ kölcsönösen egyértelmű leképezés. Ezért csak véges gráfokkal foglalkozunk. Bár a rajzolhatóságra vonatkozó állításaink könnyen átvihetők tetszőleges véges gráfokra is, csak egyszerű véges gráfokra foglazzuk meg őket. Csak a síkba, gömbfelületre és a (három dimenziós) térbe rajzolhatósággal foglalkozunk.

°* **7.2.48. Állítás. Tetszőleges véges egyszerű gráf $\mathbb{R}^3$ -ba rajzolható.**

Bizonyítás. Ha legfeljebb három csúcs van, az állítás nyilvánvaló. Egyébként a csúcsok száma szerinti indukcióval haladunk: kiválasztva egy v csúcsot, a többi csúcs által feszített részgráf $\mathbb{R}^3$ -ba rajzolható. A többi csúcs $\mathbb{R}^3$ -beli képei közül bármely három meghatároz egy síkot. Válasszuk v képét úgy, hogy ezen síkok egyikén se legyen rajta. Legyenek azon élek képei, amelyeknek végpontja v , lineáris függvények. $\square$

Gráfok rajzolhatóságának vizsgálatánál sokszor olyan, szemléletesen igaznak tűnő állításokat kell belátnunk, amelyeknek a bizonyítása nem egyszerű analízisbeli tételeket

használ. Hogy az alábbi állítás sem teljesen nyilvánvaló, azt az mutatja, hogy van olyan $\gamma: [0, 1] \rightarrow \mathbb{R}^3$ görbe (de nem egyszerű görbe), amelynek az értékkészlete egy gömbfelület.

°* **7.2.49. Segédteétel.** Legyen $X \subset \mathbb{R}^3$ egy gömbfelület és (f, g) a $G = (\psi, E, V)$ egyszerű véges gráf egy X -beli lerajzolása. Ekkor van olyan $x \in X$ pont, amely sem f , sem a g_e , $e \in E$ egyszerű görbék értékkészletében nincs benne.

Bizonyítás. Minden $\gamma: [0, 1] \rightarrow X$ egyszerű görbe, amelynek kezdőpontja és végpontja különböznek, homeomorf leképezése $[0, 1]$ -nek $\gamma([0, 1])$ -re, azaz az inverze is folytonos, és értékkészlete zárt. Megmutatjuk, hogy γ értékkészlete nem tartalmazhat egy X -beli nyílt gömböt. Ha tartalmazna egy ilyen U -t, akkor választva olyan $0 < t < 1$ -et, amelyre $\gamma(t) \in U$, a folytonosságot felhasználva választhatnánk olyan $0 < t' < t < t'' < 1$ számokat, amelyekre $\gamma(t'), \gamma(t'') \in U$. Válasszunk egy olyan $\delta: [0, 1] \rightarrow U$ egyszerű görbét, amelyre $\delta(0) = \gamma(t')$, $\delta(1) = \gamma(t'')$, és $\gamma(t) \notin \text{rng}(\delta)$. Ekkor $\gamma^{-1} \circ \delta: [0, 1] \rightarrow [0, 1]$ olyan valós változós, valós értékű folytonos függvény, amely a 0 pontban a t' , az 1 pontban a t'' értéket veszi fel, de a közbeeső t értéket nem veszi fel, ami lehetetlen.

Legyen $x_0 \in X$ olyan pont, amely nincs f értékkészletében és $r_0 > 0$ olyan valós szám, hogy az x_0 középpontú r_0 sugarú X -beli U_0 nyílt gömb diszjunkt a zárt $\text{rng}(f)$ -től. Legyen $e_1 \in E$. Mivel g_{e_1} értékkészlete nem tartalmazza U_0 -at, van olyan $x_1 \in U_0$ pont, amely nincs az értékkészletében. Mivel g_{e_1} értékkészlete zárt, van olyan $r_1 > 0$, hogy az x_1 középpontú r_1 sugarú U_1 nyílt gömb diszjunkt g_{e_1} értékkészletétől. Az r_1 csökkentésével azt is elérhetjük, hogy $U_1 \subset U_0$ teljesüljön. Egy $e_2 \neq e_1$ éllel ugyanígy folytatva, ha n él van, az U_n gömb bármely pontja eleget tesz a tétel állításának. $\square$

°* **7.2.50. Tétel.** Egy $G = (\psi, E, V)$ egyszerű véges gráf pontosan akkor rajzolható egy $X \subset \mathbb{R}^3$ gömbfelületre, ha síkba rajzolható.

Bizonyítás. Ha a gráf síkba rajzolható, válasszunk egy, a síkot érintő gömbfelületet, és a gömbnek érintési ponttal („déli sarok”) átellenes pontjából („északi sarok”) vetítsük a gráf síkba rajzolását a gömbfelületre.

A megfordítás az előző segédteételen múlik: válasszuk ki a segédteételben leírt x pontot, legyen ez az „északi sarok”, és vegyünk fel olyan síkot, amely az ezzel átellenes pontban („déli sarok”) érinti a gömbfelületet, majd az x pontból vetítsük a gráf gömbfelületre rajzolását a síkra. $\square$

→ **7.2.51. Feladat [0].** Igazoljuk, hogy ha az öt szögpontú teljes gráfból elhagyunk egy élt, a maradék gráf síkba rajzolható.

→ **7.2.52. Feladat [0].** Igazoljuk, hogy ha a „három ház, három kút” gráfból elhagyunk egy élt, a maradék gráf síkba rajzolható.

°* **7.2.53. Tartományok.** Az $\mathbb{R}^n$ egy X nyílt részhalmazát *tartománynak* nevezzük, ha bármely két különböző pontjához van olyan X -beli egyszerű görbe, amelynek az egyik pont a kezdőpontja, a másik pedig a végpontja.

°* **7.2.54. Euler tétele.** Legyen (f, g) a $G = (\psi, E, V)$ egyszerű véges összefüggő gráf egy síkba rajzolása. Ekkor a $G' = \cup_{e \in E} \text{rng}(g_e)$ halmaz komplementere $2 + \mathfrak{z}(E) - \mathfrak{z}(V)$ páronként diszjunkt tartomány egyesítése.

Bizonyítás vázlat. Ha G tartalmaz kört, a kör egyik élet törölve, két tartomány, amelyeket „ez az él választott el”, egyesül, és a tartományok száma eggyel csökken (ezt

nem bizonyítjuk), ugyanúgy, mint az élek száma. Amikor ez az eljárás megáll, akkor a visszamaradó G gráf fa, amelyre G' komplementere egyetlen tartomány (ezt sem bizonyítjuk), tehát fennáll az összefüggés. $\square$

°* **7.2.55. Megjegyzés.** Euler tételéből levezethető, hogy az öt szögpontú teljes gráf nem síkba rajzolható: 7 tartományt 10 él határolna, így mivel minden él két tartomány közös határa, tartományonként $20/7 < 3$ él jutna, ami egyszerű gráfban lehetetlen. Hasonlóan adódik, hogy a „három ház, három kút” gráf sem síkba rajzolható: 5 tartományt 9 él határolna, de a gráf páros, így a tartományoknak legalább 4 oldala van.

Az előző „bizonyítások” és az előző tétel „bizonyítása” kihagyott részeinek pontos igazolása meglehetősen nehéz és a nevezetes *Jordan-tétellel* függ össze, amelynek állítása szemléletes, de bizonyítása nem egyszerű: ha egy síkbeli egyszerű görbe kezdőpontja és végpontja megegyezik, akkor értékkészletének komplementere két diszjunkt tartomány egyesítése, amelyek közül az egyik korlátos, a másik nem.

A bizonyítások nehézségének okára rávilágít az a tény, hogy a síkban megadható három (vagy akár megszámlálhatóan végtelen sok) páronként diszjunkt tartomány úgy, hogy egyesítésük komplementere egy olyan C kompakt halmaz, amely az összes tartománynak „közös határa”, azaz minden $x \in C$ pont bármely környezetében bármely tartománynak van pontja.

* **7.2.56. Gráfok topologikus izomorfizmusa.** A G és G' véges gráfokat *topologikusan izomorf*nak nevezzük, ha az alábbi lépést, illetve a fordítottját alkalmazva, véges sok lépésben az egyikből a másikkal izomorf gráfot kaphatunk: egy másodfokú pontot elhagytunk, és a szomszédjait összekötjük egy éllel.

* **7.2.57. Kuratowski tétele.** Egy egyszerű véges gráf akkor és csak akkor síkba rajzolható, ha nincs olyan részgráfja, amely topologikusan izomorf a K_5 öt szögpontú teljes gráffal vagy a $K_{3,3}$ „három ház, három kút” gráffal.

Bizonyítás. A bizonyítás nehéz, itt nem tárgyaljuk. Lásd például Hajnal [34] könyvét, 10.5.1 tétel. $\square$

A Petersen-gráf nem síkba rajzolható, mivel tartalmaz a $K_{3,3}$ -mal topologikusan izomorf részgráfot. (Töröljük bármelyik csúcsot, majd redukáljuk a kapott gráfot a másodfokú csúcsok kiküszöbölésével.)

* **7.2.58. Feladat [5].** Legalább hány élt kell elhagyni a négydimenziós kockából, hogy a maradék gráf síkba rajzolható legyen? Legalább hány csúcsot kell elhagyni a négydimenziós kockából, hogy a maradék gráf síkba rajzolható legyen?

°* **7.2.59. Feladat [6].** Igazoljuk, hogy ha egy (E, V, φ) egyszerű véges gráf síkba rajzolható, akkor $\mathfrak{h}(E) \leq 3\mathfrak{h}(V) - 6$.

°* **7.2.60. Feladat [6].** Igazoljuk, hogy ha egy (E, V, φ) egyszerű véges gráf síkba rajzolásánál (ha van ilyen) a tartományok száma legfeljebb $2\mathfrak{h}(V) - 4$.

°* **7.2.61. Feladat [6].** Igazoljuk, hogy ha egy (E, V, φ) egyszerű véges páros gráf síkba rajzolható, akkor $\mathfrak{h}(E) \leq 2\mathfrak{h}(V) - 4$.

°* **7.2.62. Feladat [7].** Igazoljuk, hogy öt szabályos konvex test van.

7.2.63. Kromatikus szám. A gráfelmélet több mint 100 évig megoldatlan problémája volt a *négyszínsejtés*: igaz-e, hogy minden térkép kiszínezhető négy színnel? Minden „országhoz” hozzárendelve a „fővárosát”, kössük össze éllel azokat a fővárosokat, amelyek (nem csak egy pontban) szomszédos országokhoz tartoznak. A kérdés most úgy hangzik, hogy bármely síkba rajzolható egyszerű véges gráf csúcsai kiszínezhetők-e négy színnel úgy, hogy a szomszédos csúcsok különböző színűek? 1976-ban Appel és Haken amerikai matematikusok bizonyították be ezt a sejtést. Ez volt az első nevezetes matematikai sejtés, amelynek bizonyításához számítógépet is használtak. Általánosan, egy gráf egy csúcsszínezését *jólszínezésnek* nevezzük, ha a szomszédos csúcsok színe különböző. Például egy gráf csúcsainak halmaza pontosan akkor vágható két részre úgy, hogy páros gráfot kapjunk, ha a gráf két színnel jólszínezhető. A gráf *kromatikus száma* a legkisebb olyan n természetes szám, amelyre a gráf jólszínezhető n színnel; ha nincs ilyen, akkor $+\infty$. Már annak eldöntése is nehéz probléma, hogy egy gráf kromatikus száma három-e.

→ **7.2.64. Feladat [2].** Mennyi egy legalább kétcsúcsú fa kromatikus száma?

7.2.65. Feladat [4]. Mennyi a kromatikus száma

- (1) a Petersen-gráfnak;
- (2) az öt szögpontú teljes gráfnak;
- (3) a „három ház, három kút” gráfnak;
- (4) a 4-dimenziós kockának?

7.2.66. Feladat [5]. Mennyi a kromatikus száma

- (1) a K_n gráfnak;
- (2) a $K_{n,n}$ gráfnak;
- (3) az n -dimenziós kockának?

7.2.67. Feladat [9]. Mutassuk meg, hogy egy gráf pontosan akkor jólszínezhető két színnel, ha nem tartalmaz páratlan hosszú kört, és ekkor a komponensek két színnel való jólszínezése lényegében egyértelmű.

7.2.68. Feladat [13]. Igazoljuk Erdős és De Bruijn tételét: egy egyszerű gráf pontosan akkor jólszínezhető három színnel, ha minden véges részgráfja jólszínezhető három színnel.

7.2.69. Gráfok mátrixai. Ha $n, m \in \mathbb{N}$ természetes számok, egy m -szer n -es *a mátrix* egy $(i, j) \mapsto a_{i,j}$, $i, j \in \mathbb{N}$, $1 \leq i \leq m$, $1 \leq j \leq n$ leképezés. Egy mátrixot rendszerint téglalap alakban rendezett táblázatként képzelünk el, ahol az i -edik sor j -edik eleme (másként a j -edik oszlop i -edik eleme) $a_{i,j}$. Ezért az első indexet *sorindexnek*, a második indexet *oszlopindexnek* nevezzük. (Néha egy mátrix sorait és oszlopait nullától kezdve indexeljük.)

Ha egy $G = (\psi, E, V)$ véges irányított gráf élei $e_1, \dots, e_n$ csúcsai pedig $v_1, \dots, v_m$, akkor az alábbi *élmátrix* vagy *illeszkedési mátrix* egyértelműen megadja a gráfot: $1 \leq i \leq m$ és $1 \leq j \leq n$ esetén $a_{i,j} = 1$, ha e_j -nek v_i kezdőpontja és $a_{i,j} = -1$, ha e_j nem hurokél, és e_j -nek v_i végpontja. A megfelelő irányítatlan gráf élmátrixán az $|a_{i,j}|$ elemekből álló mátrixot értjük. A G irányított véges gráf *b csúcsmátrixában* legyen $b_{i,j}$ a v_i kezdőpontú, v_j végpontú élek száma, ha $1 \leq i, j \leq m$. A megfelelő irányítatlan gráf csúcsmátrixát kicsit másként értelmezzük: ha $1 \leq i, j \leq m$, akkor $i = j$ esetén legyen $b_{i,j}$ a v_i csúcsra

illeszkedő hurokélek száma, egyébként pedig legyen a v_i és v_j csúcsokra is illeszkedő élek száma.

Megjegyezzük, hogy bár több más módon is rendelhetünk gráfokhoz mátrixokat és a mátrixok felhasználhatók gráfok számítógépes ábrázolására, erre a célra más adatszerkezetek, például láncolt listák gyakran gazdaságosabban használhatók.

7.2.70. Feladat [10]. Írjunk programot az összes n -csúcsú páronként nem izomorf irányított gráf meghatározására. Ezek között hány lesz erősen összefüggő, hány lesz irányított fa, hány tartalmaz irányított kört, hányban lesz irányított Euler-vonal, irányított zárt Euler-vonal, irányított Hamilton-út, irányított Hamilton-kör?

7.2.71. További feladatok. [25]: IV.1.29–IV.1.31, IV.2.1–IV.2.3, IV.2.5–IV.2.26, IV.2.28–IV.2.51, IV.3.1–IV.3.21, IV.3.29–IV.3.31, IV.4.15–IV.4.27; [34]: 1.7.14, 1.7.15, 1.10.10, 2.1.12; [64]: 10.1.1–10.1.3, 10.3.1, 10.3.2, 10.4.1–10.4.15, 11.1.1, 11.2.1, 11.3.1–11.3.8, 12.1.1, 12.1.2, 12.2.1, 12.2.2, 12.3.1–12.3.7, 13.1.1, 13.1.2, 13.2.1, 13.3.1–13.3.4, 13.4.1–13.4.9; [83]: III.5.27, XV.7.1, XV.7.13, XV.7.22, XV.7.24–XV.7.25, XV.7.27.

Algebra

Az eddigiekben már számos algebrai fogalommal találkozhattunk: félcsoporth, csoport, gyűrű, test stb. Eddig elsősorban mint egy vagy két művelet tulajdonságait röviden leíró elnevezést használtuk ezeket. Megfigyelhetjük, hogy $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ illetve $\mathbb{H}$ elemeit elsősorban „koordinátázásra” használjuk: míg a természetes számokkal egy megszámlálható halmaz elemeit, a komplex számokkal már a sík pontjait vagy a villamosságtanban impedanciákat, a kvaterniókkal pedig a téridő pontjait vagy robotkarok háromdimenziós forgatásait – az azokon végzett műveletekkel együtt – koordinátázhatjuk. Más tárgyakban is tanulunk hasonló „koordinátázó” matematikai fogalmakat, például lineáris algebrában a lineáris egyenletrendszerek és leképezések jellemzésére alkalmas mátrixokat, analízisben függvényeket, de már középiskolában is görbéket algebrai egyenletek segítségével jellemeztünk.

Az algebra célja ilyen „koordinátázó” matematikai struktúrák – egy vagy több művelettel ellátott halmazok – általános vizsgálata. Ezek egy művelet esetén rendszerint csoportok, vagy legalábbis félcsoporthok, két művelet esetén pedig gyűrűk. Fontos szerepet játszanak a művelettartó leképezések, elsősorban a reprezentációk: ezek értékkészlete valamely függvényhalmaz, például permutációk vagy lineáris leképezések. A vizsgált struktúra képe művelettartó leképezésnél úgy tekinthető, mint az eredeti struktúra egy közelítése, és csoportoknál megfelel egy faktorcsoportnak, gyűrűknél pedig egy faktorgyűrűnek; ezek a maradékosztályok általánosításai. „Elég sok” ilyen közelítést ismerve, az eredeti struktúrát megismerhetjük vagy dolgozhatunk benne. Ez a gondolat számos algoritmus alapja is. A tárgyalás elvezet bennünket a véges testek megismeréséhez, amelyek polinomokkal koordinátázhatók, és fontos alkalmazásaik vannak a rejtjelzésben és a kódoláselméletben.

8.1 Csoportok

8.1.1. Megjegyzés. Az alábbi, már tanult fogalmakat, a velük kapcsolatos jelöléseket és a rájuk vonatkozó állításokat lépten-nyomon használni fogjuk, ezért érdemes ezeket átismételni: műveletek, műveletek elvégzése halmazok között, művelettartó leképezések, binér műveletek asszociativitása és kommutativitása, félcsoporth, bal és jobb oldali semleges elem, semleges elem, egységelem, nullelem, bal és jobb inverz, inverz, csoport, Abel-csoport, szorzatok, összegek és hatványok félcsoporthban, egységelemes félcsoporthban és csoportban, osztályozás kompatibilitása művelettel. A műveletet kommutatív esetben általában összeadással, egyébként szorzással fogjuk jelölni. A legfontosabb példáinkat a fenti fogalmakra a különböző számkörök adják. További fontos példákat adnak a függvényterek.

→ **8.1.2. Feladat [4].** Melyik csoport az alábbiak közül, és ha nem, milyen feltételek nem teljesülnek:

(1) páros számok az összeadással;

- (2) páratlan számok az összeadással;
- (3) egészek a kivonással;
- (4) páros számok a szorzással;
- (5) 7 többszöröse az összeadással;
- (6) racionális számok az összeadással;
- (7) racionális számok a szorzással;
- (8) nem nulla racionális számok a szorzással;
- (9) $\{m/n: m \in \mathbb{Z}, n \in \{1, 2\}\}$ az összeadással.

8.1.3. Homomorfizmusok. Csoportok vizsgálatánál fontos szerepet játszanak a művelettartó leképezések. Legyen adott a G és G' halmazokon egy-egy binér művelet; az egyszerűség kedvéért mindegyiket szorzással jelöljük. Egy $\varphi: G \rightarrow G'$ művelettartó leképezést *homomorfizmusnak* fogunk nevezni, és azt mondjuk, hogy $\varphi(G)$ a G *homomorf képe*. Ha a φ homomorfizmus kölcsönösen egyértelmű (injektív), akkor *monomorfizmusnak*, ha pedig G' -re képez (szürjektív), akkor egy G' -re való *epimorfizmusnak* nevezzük. Ha φ kölcsönösen egyértelmű és G' -re képez (bijektív), akkor azt mondjuk, hogy φ *izomorfizmus* G és G' között. Ha G és G' között létezik izomorfizmus, akkor azt mondjuk, hogy izomorfak; ilyenkor algebrai szempontból nem lehet különbséget tenni közöttük.

Ha $G' = G$ ugyanazzal a művelettel, akkor a homomorfizmusokat *endomorfizmusoknak*, az izomorfizmusokat pedig *automorfizmusoknak* is nevezzük.

Homomorfizmusok összetétele is homomorfizmus, mert ha $\varphi': G' \rightarrow G''$ is homomorfizmus, akkor

$$(\varphi' \circ \varphi)(xy) = \varphi'(\varphi(xy)) = \varphi'(\varphi(x)\varphi(y)) = \varphi'(\varphi(x))\varphi'(\varphi(y)) = (\varphi' \circ \varphi)(x)(\varphi' \circ \varphi)(y).$$

Izomorfizmusok összetétele nyilván izomorfizmus. Izomorfizmus inverze is izomorfizmus, mert

$$\varphi^{-1}(\varphi(x)\varphi(y)) = \varphi^{-1}(\varphi(xy)) = xy = \varphi^{-1}(\varphi(x))\varphi^{-1}(\varphi(y)).$$

Nyilván $\mathbb{I}_G$ automorfizmus.

8.1.4. Példa. A $(\mathbb{C}, \cdot)$ félcsoportot az $(\mathbb{R}, \cdot)$ félcsoportba képező homomorfizmus a komplex számhoz az abszolút értékét rendelő leképezés. Ugyanide képező homomorfizmus az $n \times n$ -es mátrixokhoz a determinánsukat rendelő leképezés. Egy komplex számhoz a szignumát rendelő leképezés $(\mathbb{C}, \cdot)$ egy endomorfizmusa. Ha $a \in \mathbb{R}^+$, $a \neq 1$, akkor az $x \mapsto a^x$ leképezés $(\mathbb{R}, +)$ -nak a pozitív valós számok szorzással tekintett csoportjára izomorfizmus; inverze a $\log_a$ izomorfizmus. A komplex konjugált képzése $(\mathbb{C}, \cdot)$ -nak és $(\mathbb{C}, +)$ -nak is automorfizmusa.

8.1.5. Feladat [5]. Az alábbi leképezések közül melyik homomorfizmus, monomorfizmus, epimorfizmus, izomorfizmus, endomorfizmus illetve automorfizmus?

- (1) $(\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$, $n \mapsto -n$;
- (2) $(\mathbb{Z}, -) \rightarrow (\mathbb{R}, +)$, $n \mapsto 3n$;
- (3) $(\mathbb{N}, \cdot) \rightarrow (\mathbb{Z}, \cdot)$, $n \mapsto n^2$;
- (4) $(\mathbb{Z}, \cdot) \rightarrow (\mathbb{Z}, \cdot)$, $n \mapsto \text{sgn}(n)$;
- (5) $(\mathbb{Q}, +) \rightarrow (\mathbb{R}, +)$, $x \mapsto 1/x$, ha $x \neq 0$, egyébként 0;
- (6) $(\mathbb{Z}, \star) \rightarrow (\mathbb{Z}, \star)$, $x \mapsto 1 - x$, ahol $x \star y = 1 - x - y + xy$.

→ **8.1.6. Feladat** [5]. Írjuk le izomorfától eltekintve az összes kételemű félcsoporthot, illetve az összes egységelemes háromelemű félcsoporthot.

8.1.7. Reprezentációk. Fontos példánk egységelemes félcsoporthra egy tetszőleges X halmaz önmagába való leképezéseinek halmaza a függvényösszetétel mint művelettel. Ha egy félcsoporthnak egy ilyen leképezés-félcsoporthba való homomorfizmusát tekintjük, akkor a félcsoporth *reprezentációjáról*, magyarul *ábrázolásáról* beszélünk. Ha a reprezentáció izomorfizmus, akkor *hű reprezentációról* beszélünk. (Ha X véges halmaz, akkor elemeit megfeleltetve egy lineáris tér bázisának, X önmagába való leképezéseinek egy lineáris tér transzformációi felelnek meg, így véges halmaz leképezéseivel történő reprezentációból könnyen kaphatunk lineáris leképezésekkel való reprezentációt.)

Bármely G egységelemes félcsoporthnak könnyen megadhatjuk egy hű reprezentációját: legyen $X = G$, és ha $g \in G$, legyen $\varphi_g(x) = gx$ minden $x \in X$ -re, azaz φ_g a g -vel való balszorítás. A $g \mapsto \varphi_g$ leképezés homomorfizmus, mert minden $x \in X$ -re

$$\varphi_{gh}(x) = ghx = \varphi_g(hx) = (\varphi_g \circ \varphi_h)(x).$$

Ha $g \neq h$, akkor $\varphi_g \neq \varphi_h$, mert ha e a G egységeleme, akkor

$$\varphi_g(e) = ge = g \neq h = he = \varphi_h(e),$$

így a reprezentáció hű. Ezt a reprezentációt G *reguláris reprezentációjának* nevezzük.

8.1.8. Tétel. A homomorfizmus definíciójánál használt jelölésekkel:

- (1) ha G félcsoporth, akkor a homomorf képe is félcsoporth;
- (2) ha G -ben e jobb oldali egységelem, bal oldali egységelem, illetve egységelem, akkor a homomorf képében e képe jobb oldali egységelem, bal oldali egységelem, illetve egységelem;
- (3) ha G -ben e egységelem, és g -nek g^* jobb oldali inverze, bal oldali inverze, illetve inverze, akkor a homomorf képében g^* képe a g képének jobb oldali inverze, bal oldali inverze, illetve inverze;
- (4) ha G -ben g és h felcserélhetőek, akkor a homomorf képben g és h képei felcserélhetőek.

Használatos kifejezés a *homomorf invariáns*. Ezt használhatjuk egy tulajdonságra vagy egy speciális elem létezésére, ha az a homomorf képben változatlan marad, például mondhatjuk egyszerűen, hogy a felcserélhetőség vagy az egységelem létezése homomorf invariáns.

Bizonyítás. Jelölje x képét x' . A homomorf kép tetszőleges három elemét felírhatjuk a', b', c' alakban, ahol $a, b, c \in G$. Ekkor, a művelettartás miatt, ha G félcsoporth, akkor $(a'b')c' = (ab)'c' = (abc)' = a'(bc)' = a'(b'c')$. Hasonlóan, ha e jobboldali egységeleme G -nek, mivel a homomorf kép egy tetszőleges eleme g' alakban írható, $g'e' = (ge)' = g'$ stb. Ha g^* a g jobb oldali inverze, akkor $g'g^{*'} = (gg^*)' = e'$ stb. Végül, ha g és h felcserélhetőek, akkor $g'h' = (gh)' = (hg)' = h'g'$. □

8.1.9. Következmény. Csoport homomorf képe is csoport. Kommutatív félcsoporth homomorf képe is kommutatív félcsoporth. Abel-csoport homomorf képe is Abel-csoport.

□

◦ **8.1.10. Példa.** $(\mathbb{R}, +)$ és $(\mathbb{R}^\times, \cdot)$ nem izomorfak, mert az $x + x = 0$ egyenletnek csak egy megoldása van, míg az $x \cdot x = 1$ egyenletnek kettő, és egy ilyen egyenlet megoldásszáma izomorfizmusnál nyilván nem változik.

→ **8.1.11. Feladat [3].** Mutassuk meg, hogy a páros egész számok additív csoportja izomorf az egész számok additív csoportjával.

→ **8.1.12. Feladat [5].** Mutassuk meg, hogy az egész számok additív csoportja nem izomorf a racionális számok additív csoportjával.

A következő állításból láthatjuk, hogy a csoport fogalmának több különböző definícióját is adhatjuk.

8.1.13. Tétel. Ha G egy félcsoport, akkor az alábbi feltételek ekvivalensek:

- (1) G csoport;
- (2) $G \neq \emptyset$ és minden $a, b \in G$ esetén egy és csak egy olyan $x \in G$, illetve $y \in G$ létezik, amelyre $ax = b$, illetve $ya = b$ (elvégezhető az osztás);
- (3) $G \neq \emptyset$ és minden $a, b \in G$ esetén létezik olyan $x \in G$, illetve $y \in G$, amelyre $ax = b$, illetve $ya = b$ (a művelet invertálható).

Bizonyítás. (1)-ből könnyen következik (2), mert az első egyenletben balról, a másodikban jobbról szorozva a^{-1} -el $x = a^{-1}b$, illetve $y = ba^{-1}$ következik, és ezek megoldások is. Nyilván (2)-ből következik (3).

Belátjuk, hogy (3)-ból következik (1). Legyen $a \in G$ rögzített. Az $ax = a$ egyenlet megoldható, valamely megoldását jelölje e . Legyen $b \in G$, és y olyan eleme G -nek, amelyre $ya = b$. Ekkor

$$be = (ya)e = y(ae) = ya = b,$$

így e jobb oldali egységelem. Hasonlóan következik bal oldali egységelem létezése is, így van egységelem. Nyilván minden $b \in G$ -hez létezik olyan b^* , amelyre $bb^* = e$, mert a $bx = e$ egyenlet megoldható. Hasonlóan következik bal oldali inverz létezése is, így minden elemnek van inverze. $\square$

8.1.14. Következmény: egyszerűsítési szabály. Egy csoportban, ha $ac = bc$ vagy $ca = cb$, akkor $a = b$.

Vannak, akik ezt a tulajdonságot *regularitás*nak nevezik. Megjegyezzük, hogy ha egy egységelemes félcsoportban teljesül az egyszerűsítési szabály, abból még nem következik, hogy csoport. Példa: $(\mathbb{N}^+, \cdot)$.

Bizonyítás. A (2)-beli egyértelműségből következik. $\square$

8.1.15. Megjegyzés. Az $\{\alpha, \beta, \gamma\}$ halmazon a

$\cdot$	α	β	γ
α	β	α	γ
β	α	γ	β
γ	γ	β	α

táblázattal megadott műveletre elvégezhető az osztás, mégsem kapunk csoportot, mert a művelet nem asszociatív: $(\alpha\beta)\gamma = \alpha\gamma = \gamma$, de $\alpha(\beta\gamma) = \alpha\beta = \alpha$.

8.1.16. Példák. (1) Ha $n \in \mathbb{N}^+$, az n -edik komplex egységgyökök $\mathbb{U}_n$ halmaza a szorzással Abel-csoport.

(2) Legyen p prímszám. Az összes p^n -edik egységgyökök halmaza, ahol $n = 1, 2, \dots$, a szorzással szintén Abel-csoport, ez a $\mathbb{Z}_{p^\infty}$ Prüfer-csoport.

(3) Az összes egységgyökök $\mathbb{U}$ halmaza a szorzással (tehát az első példában szereplő csoportok egyesítése) szintén Abel-csoport.

(4) Az egységnyi abszolút értékű komplex számok $\mathbb{T}$ halmaza a szorzással Abel-csoport.

(5) A $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ kvaterniók a kvaterniószorzással nem kommutatív csoportot alkotnak.

(6) A Klein-féle csoportot a szorzótáblájával definiáljuk:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Mivel a szorzótábla szimmetrikus, a művelet kommutatív.

° **8.1.17. Geometriai példák.** (1) Az n oldalú szabályos sokszöget önmagába vivő egybevágóságok (távolságtartó leképezések) az egymás utáni végrehajtással alkotják a D_n diédercsoportot. Triviális, hogy csúcs képe csak csúcs lehet. Ha ε jelöli a középpont körüli $2\pi/n$ szöggel (pozitív irányba) történő forgatást, akkor a forgatások az ε^k leképezések, $\varepsilon^n = e$ az egységelem, az identikus leképezés. Van még n tükrözés is a csoportban: ha n páratlan, akkor ezek a csúcsokon átmenő szimmetriatengelyekre való tükrözések, ha pedig n páros, akkor $n/2$ darab átellenes csúcspáron átmenő szimmetriatengelyre és $n/2$ darab átellenes oldalpár egybeeső oldalfelező merőlegesére való tükrözés van. Jelöljön τ egy rögzített csúcson átmenő szimmetriatengelyre való tükrözést. Erre nyilván $\tau^2 = e$, és a tükrözések $\tau, \tau\varepsilon, \dots, \tau\varepsilon^{n-1}$ alakúak, mert ha a τ tükrözés tengelye α szöget zár be egy τ' tükrözés tengelyével, akkor $\tau\tau'$ egy 2α szögű forgatás, így egyenlő ε^k -val valamely $0 \leq k < n$ -re, ahonnan $\tau' = \tau\varepsilon^k$. Tehát a diédercsoport

$$D_n = \{e, \varepsilon, \dots, \varepsilon^{n-1}, \tau, \tau\varepsilon, \dots, \tau\varepsilon^{n-1}\},$$

a számoláshoz pedig elég tudni, hogy $\varepsilon^n = \tau^2 = e$ és $\varepsilon\tau = \tau\varepsilon^{-1}$, amiből már indukcióval következik, hogy $\varepsilon^k\tau = \tau\varepsilon^{-k}$. A diédercsoport elnevezés onnan ered, hogy egy sokszöget „kétlapnak” tekinthetünk, és a csoport elemeit azokkal a térbeli forgatásokkal azonosíthatjuk, amelyek ezt a „kétlapot” önmagába viszik. A diédercsoport $n = 2$ határesetete a Klein-féle csoport.

(2) Számos további geometriai példa adható: eltolások, forgatások, egybevágóságok, hasonlóságok stb. Egy $X \subset \mathbb{R}^n$ halmaz összes egybevágóságainak csoportját $\mathbb{E}_X$ -szel fogjuk jelölni. További példák: geometriai alakzatok, kristályok, kristályrácsok, molekulák összes szimmetriáinak halmaza. A csoportelmélet számos alkalmazásában a szimmetriacsoportok igen fontos szerepet játszanak. Például molekulák szimmetriacsoportjának ismerete sokat segít az elektronszerkezet meghatározásában (azaz a Schrödinger-egyenlet megoldásában), sőt Wigner Jenő alapvető felismerése szerint a fizikai törvények jó része szimmetriaelvek segítségével származtatható.

→ **8.1.18. Feladat [3].** Igazoljuk, hogy D_3 izomorf a háromszög csúcsai összes permutációjával csoportjával. Igaz-e ez más n -re is?

→ **8.1.19. Feladat [3].** Igazoljuk, hogy kételemű csoportok izomorfak, speciálisan $(\mathbb{Z}_2, +)$ és $(\mathbb{Z}^*, \cdot)$ izomorfak.

→ **8.1.20. Feladat [3].** Igazoljuk, hogy $\mathbb{R}$ és $\mathbb{T}$ nem izomorfak.

8.1.21. Feladat [6]. Igazoljuk, hogy egy G félcsoport pontosan akkor csoport, ha van egy e jobboldali egységeleme, és minden $g \in G$ -hez van olyan $g^* \in G$, amelyre $gg^* = e$.

8.1.22. Feladat [6]. Igazoljuk, hogy ha egy nem üres véges félcsoportban teljesül az egyszerűsítési szabály, akkor csoport.

8.1.23. Részfélcsoport, részcsoporth. Egy G grupoid egy H részhalmazát *részgrupoidnak* nevezzük, ha maga is grupoid a G -beli műveletet csak H elemei között tekintve. Ha H a G -beli műveletet csak H elemei között tekintve félcsoport, csoport, stb., akkor *részfélcsoportnak*, *részcsoporthnak*, stb. nevezzük. Számunkra legfontosabb az az eset lesz, amikor H részcsoporthja a G csoportnak. (Szokás ennek kifejezésére a $H \leq G$ jelölést használni.) Nyilván ha G csoport, akkor az egész G és a csak az egységelemet tartalmazó egyelemű részhalmaz részcsoporthok, ezek a *triviális részcsoporthok*. A G -től különböző részcsoporthokat *valódi részcsoporthnak* nevezzük.

Emlékeztetünk rá, hogy a műveletet a részhalmazok között is értelmeztük, elemenként (lásd az 1.4.36 pontot). Ugyanígy értelmeztük részhalmazokra az inverzképzést is, elemenként. (Szokás a részhalmazokat *komplexusoknak* is nevezni, és *komplexusműveletekről* beszélni.)

→ **8.1.24. Feladat [2].** Mutassuk meg, hogy egy egységelemes félcsoportban azok az elemek, amelyeknek van jobbinverzük, részfélcsoportot alkotnak.

→ **8.1.25. Feladat [2].** Bizonyítsuk be, hogy bármely S nem egységelemes félcsoport beágyazható egy egyetlen elemmel bővebb monoidba, azaz részfélcsoportja egy olyan T egységelemes félcsoportnak, amelynek csak az egységeleme nem tartozik bele S -be.

→ **8.1.26. Feladat [5].** Egész számok körében definiáljuk az $m \star n = m + n - mn$ műveletet. Mutassuk meg, hogy egységelemes félcsoportot kapunk. Mely elemeknek van inverze?

8.1.27. Állítás. Legyen G csoport, és $H \subset G$. Az alábbi feltételek ekvivalensek:

- (1) H részcsoporth;
- (2) a szorzás leszűkítése $H \times H$ -ra egy $H \times H$ -t H -ba képező leképezés, H tartalmazza G egységelemét, és $H^{-1} \subset H$;
- (3) $H \neq \emptyset$, $HH \subset H$ és $H^{-1} \subset H$;
- (4) $H \neq \emptyset$ és $H^{-1}H \subset H$.

Bizonyítás. Ha (1) teljesül, akkor a szorzást H elemei között végezve, az művelet, így az eredménye H -ban van, azaz $H \times H$ -t H -ba képező leképezés. Mivel H részcsoporth, tartalmaz egy mondjuk f egységelemet. Mivel bármely $h \in H$ -ra $hf = h$ és $he = h$, a G -beli egyszerűsítési szabály miatt $f = e$. Végül, mivel minden $h \in H$ -nak van inverze H -ban, de G -ben is, az inverz egyértelműsége miatt $h^{-1} \in H$ minden $h \in H$ -ra.

Nyilván (2)-ből következik (3). Ha (3) fennáll, akkor $H^{-1} \subset H$ miatt $H^{-1}H \subset HH \subset H$, tehát (3)-ból kapjuk (4)-et.

Végül, ha (4) fennáll, akkor bármely $h \in H$ -ra $h^{-1}h = e \in H$, így G egységeleme H -ban is az. Minden $h \in H$ -ra $h^{-1}e \in H^{-1}H \subset H$, azaz minden elemnek van inverze, a G -beli, továbbá $(h_1^{-1})^{-1} = h_1$ miatt $h_1 \in H^{-1}$, és így minden $h_1, h_2 \in H$ -ra $h_1h_2 \in H^{-1}H \subset H$, tehát (1) teljesül. $\square$

8.1.28. Megjegyzés. Ha H részcsoport, akkor (3)-ban és (4)-ben a tartalmazások nem valódiak, hiszen $e \in H$ miatt $H = eH \subset HH$, $H = eH \subset H^{-1}H$, és ha $h \in H$, akkor $h = (h^{-1})^{-1} \in H^{-1}$, azaz $H \subset H^{-1}$.

8.1.29. Következmény. Ha H_γ , $\gamma \in \Gamma$, a G csoport részcsoportjainak egy rendszere, akkor $H = \bigcap_{\gamma \in \Gamma} H_\gamma$ is részcsoport.

Bizonyítás. Mivel $e \in H_\gamma$ minden $\gamma \in \Gamma$ -ra, H nem üres. Mivel $H^{-1} \subset H_\gamma^{-1}$, kapjuk, hogy $H^{-1}H \subset H_\gamma^{-1}H_\gamma \subset H_\gamma$ minden $\gamma \in \Gamma$ -ra. Innen viszont $H^{-1}H \subset \bigcap_{\gamma \in \Gamma} H_\gamma = H$, tehát H részcsoport G -ben. $\square$

8.1.30. Megjegyzés. Részcsoportok egyesítése általában nem részcsoport, például a Klein-féle csoportban $\{e, a\}$ és $\{e, b\}$ részcsoportok, de egyesítésük nem az.

Úgy elméleti, mint gyakorlati vizsgálatoknál gyakori kérdés, hogy megadható-e az alaphalmaz olyan „kis” részhalmaza, amelynek elemeiből a művelet alkalmazásával előállítható a struktúra összes eleme.

8.1.31. Generátum. Legyen G egy csoport, és $K \subset G$. A K halmaz $\langle K \rangle$ generátuma a G összes, K -t tartalmazó részcsoportjának metszete. Az előző következmény szerint $\langle K \rangle$ részcsoport, így $\langle K \rangle$ a legszűkebb, K -t tartalmazó részcsoport. Ha $G = \langle K \rangle$, akkor azt mondjuk, hogy K a G csoport *generátorrendszere*. Ha egy csoportnak létezik egyelemű generátorrendszere, akkor *ciklikusnak* nevezzük, az elemet pedig egy *generátorának*.

°* **8.1.32. Példa: lineáris transzformációk csoportjai.** Egy F testre F^n invertálható lineáris transzformációinak csoportját $\mathbb{GL}(F^n)$ fogja jelölni, ez az *általános lineáris csoport*. A lineáris algebrában bizonyítják, hogy ennek elemeit az jellemzi, hogy determinánsuk nem nulla, és hogy $\mathbb{GL}(F^n)$ izomorf az F -beli elemű $n \times n$ -es nem nulla determinánsú mátrixok multiplikatív csoportjával. Az 1 determinánsú lineáris transzformációk $\mathbb{GL}(F^n)$ egy részcsoportját alkotják, ez az $\mathbb{SL}(F^n)$ *speciális lineáris csoport*. A $\mathbb{GL}(F^n)$ csoport részcsoportja az *affin transzformációk*

$$\mathbb{GA}(F^n) := \{x \mapsto Lx + b : x \in F^n, L \in \mathbb{GL}(F^n), b \in F^n\}$$

általános affin csoportjának, az $\mathbb{SL}(F^n)$ csoport pedig részcsoportja a *speciális affin transzformációk*

$$\mathbb{SA}(F^n) := \{x \mapsto Lx + b : x \in F^n, L \in \mathbb{SL}(F^n), b \in F^n\}$$

speciális affin csoportjának.

Az $F = \mathbb{R}$ esetben tekinthetjük $\mathbb{GL}(\mathbb{R}^n)$ azon lineáris transzformációinak részcsoportját, amelyek megtartják $\mathbb{R}^n$ elemeinek szokásos hosszát, ez az $\mathbb{O}(n)$ *ortogonális csoport*. Elemeinek determinánsa 1 abszolút értékű. Mátrixukat ortonormált bázisban az

jellemzi, hogy az inverze megegyezik a transzponáltjával. További fontos részcsoport $\mathrm{SO}(n) = \mathcal{O}(n) \cap \mathrm{SL}(\mathbb{R}^n)$, a *speciális ortogonális csoport*. Elemei $\mathbb{R}^n$ origó körüli forgatásainak felelnek meg: az, hogy a determináns 1, azzal ekvivalens, hogy a transzformáció nem változtatja meg a bázisok irányítását.

Hasonlóan, az $F = \mathbb{C}$ esetben is tekinthetjük $\mathrm{GL}(\mathbb{C}^n)$ azon lineáris transzformációinak részcsoportját, amelyek megtartják $\mathbb{C}^n$ elemeinek szokásos hosszát, ez az $\mathrm{U}(n)$ *unitér csoport*. Elemeinek determinánsa 1 abszolút értékű. Mátrixukat ortonormált bázisban az jellemzi, hogy az inverze megegyezik a konjugált transzponáltjával. Az unitér csoportok fontos szerepet játszanak a fizikában. Az $\mathrm{U}(1)$ csoport lényegében $\mathbb{C}$ egységnyi abszolút értékű elemeinek multiplikatív csoportja. További fontos részcsoport $\mathrm{SU}(n) = \mathrm{U}(n) \cap \mathrm{SL}(\mathbb{C}^n)$, a *speciális unitér csoport*.

Az egységnyi abszolút értékű kvaterniók multiplikatív csoportjának egy részcsoportját alkotják. Ez akkor is igaz, ha a kvaterniószorzás helyett a $(q, q') \mapsto q'q$ „fordított szorzást” tekintjük. Egy egységnyi abszolút értékű q kvaternióra tekintsük a $\varphi_q: p \mapsto pq$ leképezését $\mathbb{H} = \mathbb{C}^2$ -nek önmagába. Ha $q = (z, w) \in \mathbb{C}^2$, akkor (az $1, j$ bázisban) φ_q mátrixa

$$\begin{pmatrix} z & -\bar{w} \\ w & \bar{z} \end{pmatrix},$$

ami könnyen láthatóan 1 determinánsú, és a konjugált transzponáltja az inverze, így φ_q egy unitér transzformáció. Az $\mathrm{SU}(2)$ csoport minden eleme előáll így: ha mátrixa (az $1, j$ bázisban)

$$\begin{pmatrix} z & u \\ w & v \end{pmatrix},$$

akkor az inverze – felhasználva, hogy determinánsa 1 –

$$\begin{pmatrix} v & -u \\ -w & z \end{pmatrix},$$

amit összehasonlítva a konjugált transzponáltjával, azt kapjuk, hogy $u = -\bar{w}$ és $v = \bar{z}$, valamint – mivel a determináns 1 –, $|z|^2 + |w|^2 = 1$. A $q \mapsto \varphi_q$ leképezés izomorfizmus a fordított szorzással tekintett egységnyi abszolút értékű kvaterniók csoportja és $\mathrm{SU}(2)$ között.

Tekintsük most egy egységnyi abszolút értékű q kvaternióra a háromdimenziós valós vektorokon értelmezett $\psi_q(v) = qvq^{-1}$ forgatást: lásd a 3.4.34 pontot. Ez homomorfizmusa a fordított szorzással tekintett egységnyi abszolút értékű kvaterniók csoportjának $\mathrm{SO}(3)$ -ra, amely a q és $-q$ kvaterniókat (de csak ezeket) ugyanabba a forgatásba viszi. Összetéve az előbbi izomorfizmus inverzével, egy $\varphi_q \mapsto \psi_q$ homomorfizmust kapunk, amely az $\mathrm{SU}(2)$ -beli φ_q és $\varphi_{-q} = -\varphi_q$ leképezéseket (de csak ezeket) ugyanabba a forgatásba viszi.

Az $F = \mathbb{R}$ esetben, ha $r + s = n$, tekinthetjük $\mathrm{GL}(\mathbb{R}^n)$ azon lineáris transzformációinak $\mathcal{O}(r, s)$ részcsoportját, amelyek megtartják az

$$(x_1, x_2, \dots, x_n) \mapsto x_1^2 + x_2^2 + \dots + x_r^2 - x_{r+1}^2 - x_{r+2}^2 - \dots - x_{r+s}^2$$

kvadratikus forma értékét; ez a csoport az $\mathcal{O}(n)$ ortogonális csoport általánosítása: az $r = n, s = 0$, illetve az $r = 0, s = n$ esetben $\mathcal{O}(n)$ -et kapjuk vissza. Ennek fontos részcsoportja az $\mathrm{SO}(r, s) = \mathcal{O}(r, s) \cap \mathrm{SL}(\mathbb{R}^n)$ csoport.

A fizikában a relativitáselmélet miatt fontos szerepet játszik az $\mathbb{O}(1,3)$ Lorentz-csoport. Mivel a kvaterniók megfelelnek az $\mathbb{R}$ felett négydimenziós téridő pontjainak, a Lorenz-csoport elemeit olyan $\mathbb{R}$ -lineáris invertálható $L: \mathbb{H} \rightarrow \mathbb{H}$ leképezéseknek is tekinthetjük, amelyekre $\Re(p^2) = \Re(L(p)^2)$ minden $p \in \mathbb{H}$ -ra. Az $\mathbb{SO}(1,3)$ speciális Lorentz-csoport részcsoportját alkotja az $\mathbb{SO}^+(1,3)$ valódi Lorentz-csoport: ebben $\mathbb{SO}(1,3)$ azon elemei vannak, amelyek minden $p \in \mathbb{H}$ -ra, amelyre $\Re(p^2) > 0$, a p időszerű részének (időkoordinátájának) előjelét is megőrzi. Például p konjugálása, azaz a tértükrözés a Lorentz-csoportban van, de nincs benne a speciális Lorentz-csoportban, a $p \mapsto -p$ téridő-tükrözés a speciális Lorentz-csoportban van, de nincs benne a valódi Lorentz-csoportban.

Legyen $p = p_0 + p_1i + p_2j + p_3k$ és $q = q_0 + q_1i + q_2j + q_3k$. Megmutatható, hogy a valódi Lorentz-csoportot generálják a

$$\begin{pmatrix} q_r \\ q_s \end{pmatrix} = \begin{pmatrix} \cos \varphi & \sin \varphi \\ -\sin \varphi & \cos \varphi \end{pmatrix} \begin{pmatrix} p_r \\ p_s \end{pmatrix}$$

alakba írható $p \mapsto q$ térbeli forgatások (itt $1 \leq r < s \leq 3$, a többi koordináta nem változik, φ valós paraméter, a forgatás szöge; a forgatás inverze a $-\varphi$ -hez tartozó forgatás), valamint a

$$\begin{pmatrix} q_0 \\ q_s \end{pmatrix} = \begin{pmatrix} \cosh \varphi & \sinh \varphi \\ \sinh \varphi & \cosh \varphi \end{pmatrix} \begin{pmatrix} p_0 \\ p_s \end{pmatrix}$$

alakba írható $p \mapsto q$ leképezések, az s -edik tengely mentén való egyenes vonalú egyenletes mozgások (itt $1 \leq s \leq 3$, a többi koordináta nem változik, φ valós paraméter; a mozgás inverze a $-\varphi$ -hez tartozó mozgás).

A $p = p_0 + p_1i + p_2j + p_3k$ kvaterniót azonosítva az $1, j$ bázisban a

$$p_0 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + p_1 \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + p_2 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + p_3 \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

mátrixú $\mathbb{C}$ -lineáris $\mathbb{C}^2$ -t önmagába képező A önadjungált transzformációval, $\Re(p^2) = \det(A)$. Egy $C \in \mathbb{SL}(\mathbb{C}^2)$ transzformációhoz hozzárendelve az $A \mapsto CAC^*$ leképezést, az $\mathbb{SL}(\mathbb{C}^2)$ csoportnak az $\mathbb{O}(1,3)$ csoportba való homomorfizmusát kapjuk. Nyilván C -hez és $-C$ -hez ugyanaz a leképezés tartozik, és könnyen megmutatható, hogy csak C -hez és $-C$ -hez tartozik ugyanaz a leképezés. Az is megmutatható, hogy ezen homomorfizmus értékkészlete a valódi Lorentz-csoport. Például az $1, j$ bázisban

$$\begin{pmatrix} e^{\varphi/2} & 0 \\ 0 & e^{-\varphi/2} \end{pmatrix}$$

mátrixú $C \in \mathbb{SL}(\mathbb{C}^2)$ lineáris leképezéshez a

$$\begin{pmatrix} q_0 \\ q_1 \end{pmatrix} = \begin{pmatrix} \cosh \varphi & \sinh \varphi \\ \sinh \varphi & \cosh \varphi \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$$

mozgás tartozik.

Az összes $p \mapsto Lp + c$ alakú leképezései $\mathbb{H}$ -nak $\mathbb{H}$ -ra alkotják a Poincaré-csoportot, ahol L a valódi Lorentz-csoport tetszőleges eleme, c pedig tetszőleges kvaternió; ez $\mathbb{SA}(\mathbb{R}^4)$ részcsoportja, tartalmazza a téridőbeli eltolásokat, a forgatásokat és az egyenes vonalú egyenletes mozgásokat.

8.1.33. Állítás. Az előző definíció jelöléseivel,

$$\langle K \rangle = \{g_1 g_2 \cdots g_n : n \in \mathbb{N}, g_i \in K \cup K^{-1}, \text{ ha } 1 \leq i \leq n\}.$$

Emlékeztetünk rá, hogy az üres szorzat az egységelem. Az állításból nyilván $\langle K \rangle = \langle K^{-1} \rangle$.

Bizonyítás. Egyrészt a jobb oldalon álló halmaz részcsoport, mert tartalmazza az egységelemet, zárt a szorzásra és az inverzképzésre, továbbá tartalmazza K elemeit, így tartalmazza K generátumát. Másrészt minden elemének benne kell lennie K generátumában. $\square$

8.1.34. Következmény. Ha $g \in G$, akkor $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. Egy ciklikus csoport homomorf képe is ciklikus, egy generátor képe generálja a homomorf képet.

Bizonyítás. Az első állítás nyilvánvaló az előző állítás alapján. Tegyük fel, hogy g a G ciklikus csoport egy generátora, φ pedig egy homomorfizmusa G -nek. Ekkor indukcióval $\varphi(g^n) = \varphi(g)^n$ minden $n \in \mathbb{N}$ -re, és így $\varphi(h^{-1}) = \varphi(h)^{-1}$ miatt minden $n \in \mathbb{Z}$ -re is, azaz $\varphi(\langle g \rangle) = \langle \varphi(g) \rangle$. $\square$

8.1.35. Rend. Egy G véges csoport *rendjén* az elemeinek számát értjük, egyébként azt mondjuk, hogy a *csoport rendje végtelen*. Egy $g \in G$ elem *rendjén* azt az n legkisebb pozitív egész kitevőt értjük, amelyre $g^n = e$, ha van ilyen, egyébként azt mondjuk, hogy az *elem rendje végtelen*.

* **8.1.36. Feladat [5].** Határozzuk meg $\mathbb{GL}(F^n)$, $\mathbb{GA}(F^n)$, $\mathbb{SL}(F^n)$ és $\mathbb{SA}(F^n)$ rendjét, ha F véges test.

* **8.1.37. Feladat [8].** Legyen $a, b, c, d \in \mathbb{C}$, és tegyük fel, hogy $ad - bc \neq 0$. Tekintsük a $c \neq 0$ esetben az

$$f(z) = \frac{az + b}{cz + d}, \quad \text{ha} \quad -\frac{d}{c} \neq z \in \mathbb{C}, \quad f\left(-\frac{d}{c}\right) = \infty, \quad f(\infty) = \frac{a}{c}$$

összefüggéssel, a $c = 0$ esetben pedig az

$$f(z) = \frac{az + b}{cz + d}, \quad \text{ha} \quad z \in \mathbb{C}, \quad f(\infty) = \infty$$

összefüggéssel definiált $f: \overline{\mathbb{C}} \rightarrow \overline{\mathbb{C}}$ törtlineáris leképezést. Mutassuk meg, hogy az összes törtlineáris leképezések a függvényösszetétellel csoportot alkotnak.

8.1.38. Tétel. Végtelen ciklikus csoport izomorf az egész számok additív csoportjával, míg n elemű ciklikus csoport a modulo n maradékosztályok $\mathbb{Z}_n$ additív csoportjával izomorf. Speciálisan a ciklikus csoportok kommutatívak.

Bizonyítás. Legyen g egy generátorelem, és tekintsük az $n \mapsto g^n$, $n \in \mathbb{Z}$ homomorfizmust. Ha ez kölcsönösen egyértelmű, akkor izomorfizmusa $\mathbb{Z}$ -nek G -re. Ha ez a leképezés nem kölcsönösen egyértelmű, akkor vannak olyan $i > j$ kitevők, hogy $g^i = g^j$. Ekkor $g^{i-j} = e$, tehát van olyan pozitív egész szám, amelyre hatványozva g -t az egységelemet kapjuk. Jelölje n a legkisebb ilyen pozitív egész kitevőt, azaz g rendjét. Nyilván,

ha $0 \leq r < n$ és $g^r = e$, akkor $r = 0$. Az $e, g, g^2, \dots, g^{n-1}$ elemek mind különbözőek, mert ha $0 \leq j < i < n$ esetén $g^i = g^j$ teljesülne, akkor abból $g^{i-j} = e$ következne, ami lehetetlen. Másrészt, ha $i > j$ és $i \equiv j \pmod{n}$, akkor $i = j + kn$ valamely $k \in \mathbb{N}$ -re, így $g^i = g^{j+kn} = g^j(g^n)^k = g^j e^k = g^j$. Így G -nek n eleme van, a $\varphi: i \mapsto g^i$ leképezés $\mathbb{Z}$ -t G -re képezi, művelettartó, és minden modulo n maradékosztályon konstans. Legyen $\tilde{\varphi}$ az a leképezés, amely $\mathbb{Z}_n$ egy maradékosztályához G -nek azt az elemét rendeli, amelyet φ rendel a maradékosztály elemeihez. Nyilván $\tilde{\varphi}$ a $\mathbb{Z}_n$ additív csoportját G -re képezi, mivel mindkettőnek n eleme van, kölcsönösen egyértelmű, és mivel φ művelettartó volt, homomorfizmus is: ha $\tilde{x}, \tilde{y} \in \mathbb{Z}_n$, akkor $\tilde{\varphi}(\tilde{x} + \tilde{y}) = \tilde{\varphi}(\widetilde{x+y}) = \varphi(x+y) = \varphi(x)\varphi(y) = \tilde{\varphi}(\tilde{x})\tilde{\varphi}(\tilde{y})$, tehát $\tilde{\varphi}$ izomorfizmus. $\square$

8.1.39. Megjegyzés. Az előző bizonyítás azt is mutatja, hogy véges rendű elem rendje megegyezik az általa generált ciklikus csoport rendjével.

8.1.40. Tétel. *Ciklikus csoport minden részcsoportja is ciklikus.*

Bizonyítás. Legyen $G = \langle g \rangle$ és H a részcsoport. Ha $H = \{e\}$, készen vagyunk. Egyébként van olyan nullától különböző $k \in \mathbb{Z}$, amelyre $g^k \in H$. Feltehető, hogy $k > 0$, mert egyébként k helyett $-k$ -t vehetünk, hiszen $g^{-k} = (g^k)^{-1}$. Legyen d az a legkisebb pozitív kitevő, amelyre $g^d \in H$. Megmutatjuk, hogy $H = \langle g^d \rangle$. Csak azt kell bizonyítani, hogy H -nak tetszőleges g^j eleme g^d hatványa. Legyen $q = \lfloor j/d \rfloor$, $r = j \bmod d$. Ekkor $g^r = g^{j-qd} = g^j(g^d)^{-q} \in H$, ahonnan d definíciója miatt $r = 0$, és így $g^j = (g^d)^q$. $\square$

8.1.41. Tétel. *Legyen G egy n rendű véges ciklikus csoport, g pedig egy generátoreleme G -nek. Ha $a \in \mathbb{Z}$ és $d = \text{lko}(a, n)$, akkor g^a az egyetlen m -rendű $H = \{g^d, g^{2d}, \dots, g^{md} = e\}$ ciklikus részcsoportot generálja, ahol $n = md$. A G minden részcsoportja előáll így valamely $d|n$ -re. A G -nek $\varphi(n)$ generátora van.*

Bizonyítás. Az előző tétel bizonyítása szerint minden H részcsoport g^d hatványai-ból áll, ahol d a legkisebb pozitív kitevő, amelyre $g^d \in H$, és $j = n$ választással azt is kapjuk, hogy $n \bmod d = 0$, azaz $d|n$, $n = md$, amiből $H = \{g^d, g^{2d}, \dots, g^{md} = e\}$, tehát H rendje egyértelműen meghatározza d -t, és így H -t. Mivel g^a a g^d hatványa, így az általa generált részcsoport része H -nak. Mivel alkalmas $x, y \in \mathbb{Z}$ -re $d = ax + ny$, azt kapjuk, hogy $g^d = g^{ax+ny} = g^{ax}g^{ny} = g^{ax}e^y = g^{ax} = (g^a)^x$, és így g^a generálja is H -t. Az utolsó állítás abból következik, hogy $\varphi(n)$ darab olyan $0 \leq a < n$ természetes szám van, amelyre a és n relatív prímek. $\square$

→ **8.1.42. Feladat [4].** A D_5 diédercsoport minden részhalmazára határozzuk meg az általa generált részcsoportot.

8.1.43. Feladat [8]. Legyen G tizedrendű nemkommutatív csoport. Bizonyítsuk be az alábbi állításokat, majd általánosítsunk arra az esetre, amikor G rendje egy páratlan prím kétszerese:

- (1) G -ben nincs tizedrendű elem;
- (2) G -ben nem lehet minden elem másodrendű;
- (3) G -ben van másodrendű elem;
- (4) ötödrendű elem nem lehet felcserélhető másodrendű elemmel;
- (5) G generálható két másodrendű elemmel;
- (6) G izomorf D_5 -tel.

→ **8.1.44. Feladat [4].** Mutassuk meg, hogy ha A és B egy csoport részcsoportjai, akkor AB pontosan akkor csoport, ha $AB = BA$.

→ **8.1.45. Feladat [1].** Mik a $\mathbb{Z}$ additív csoport generátorai?

→ **8.1.46. Feladat [1].** Bizonyítsuk be, hogy az m -edik egységgyökök multiplikatív csoportja izomorf $\mathbb{Z}_m$ additív csoportjával.

→ **8.1.47. Feladat [4].** Melyek a primitív m -edik egységgyökök?

8.1.48. Feladat [8]. Igazoljuk, hogy $\mathbb{Q}$ additív csoportjában bármely véges részhalmaz ciklikus részcsoportot generál. Adjuk meg $\mathbb{Q}$ egy nem ciklikus valódi részcsoportját.

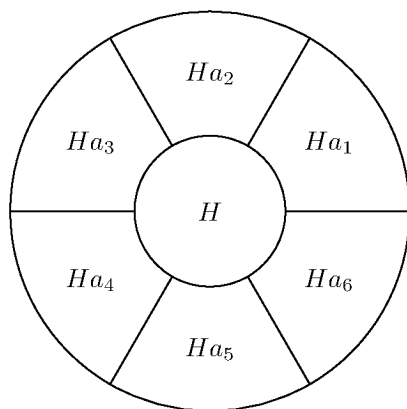
8.1.49. Feladat [10]. Mutassuk meg, hogy ha a G csoportot $\{f, g\}$ generálja, és $f^m = e = g^n$, ahol e a G egységeleme, valamint $fgf^{-1} = g^k$ valamely $k \in \mathbb{N}$ -re, akkor a csoport minden eleme felírható $f^i g^j$, illetve $g^j f^i$, $0 \leq i < m$, $0 \leq j < n$ alakban.

8.1.50. Feladat [12]. Legyen e a G csoport egységeleme, és $f, g \in G$. Igazoljuk, hogy

- (1) ha $f^2 = e = g^6$ és $fg = g^4 f$, akkor $g^3 = e$ és $fg = gf$;
- (2) ha $f^5 = e = g^4$ és $fg = g f^3$, akkor $f^2 g = g f$ és $f g^3 = f^3 g^2$;
- (3) ha $f^3 = e = g^4$ és $gf = f g^3$, akkor $fg = gf$.

Eddigi tanulmányaink során is előfordult már, hogy egy halmaz elemeit osztályokba soroltuk, és a továbbiakban ezeket az osztályokat vizsgáltuk. Például az egész számokat az n -nel való osztási maradékuk szerint n osztályba sorolhatjuk, így ha két egész szám összeadásánál az osztási maradék modulo n érdekel minket, akkor elég ebben az n elemű halmazban számolni. A következőkben egy csoport osztályokra bontását általánosabban fogjuk tárgyalni.

8.1.51. Mellékosztályok. Legyen G egy csoport, és legyen H a G egy részcsoportja. Vezessük be az $a \sim b$, ha $ab^{-1} \in H$ relációt. Ez nyilván ekvivalenciareláció. Vizsgáljuk meg az ekvivalenciaosztályokat. Azt állítjuk, hogy $a \in G$ ekvivalenciaosztálya a Ha halmaz. Ha $b \in Ha$, akkor $b = ha$ valamely $h \in H$ -ra. Innen $ba^{-1} = h$, azaz $ab^{-1} = h^{-1} \in H$. Megfordítva, ha $a \sim b$, akkor $ab^{-1} = h \in H$, ahonnan $b = h^{-1}a \in H^{-1}a \subset Ha$.



8.1.1 ábra: Mellékosztályok.

Ha most az $a \sim b$, ha $b^{-1}a \in H$ ekvivalenciarelációt vezetjük be, akkor hasonlóan számolva kapjuk, hogy az a ekvivalenciaosztálya az aH halmaz. Az előző ekvivalenciaosztályokat a G csoport H szerinti *jobb oldali mellékosztályainak*, az utóbbiakat pedig *bal oldali mellékosztályainak* nevezzük.

Megjegyezzük, hogy a $Ha \mapsto (Ha)^{-1} = a^{-1}H$ leképezés kölcsönösen egyértelműen képezi le a jobb oldali mellékosztályok halmazát a bal oldali mellékosztályok halmazára, így ezek száma egyszerre véges, és ha véges, akkor megegyezik. Ha véges sok jobb oldali mellékosztály van, akkor azok száma a H *indexe*, egyébként azt mondjuk, hogy H *indexe* végtelen. A H részcsoporthoz G -beli indexét $[G:H]$ -val jelöljük.

8.1.52. Lagrange tétele. *Ha H a G véges csoport részcsoporthja, akkor a H rendjének és indexének a szorzata G rendje.*

Bizonyítás. Dolgozhatunk jobb oldali mellékosztályokkal. Akármelyik a elem mellékosztálya és H között a $h \mapsto ha$, $h \in H$ leképezés az egyszerűsítési szabály miatt bijektív, így minden mellékosztálynak ugyanannyi eleme van, mint H -nak. Mivel páronként diszjunktak és uniójuk G , készen vagyunk. $\square$

8.1.53. Következmény. *Véges csoportban elem rendje osztja a csoport rendjét.*

Bizonyítás. Az elem rendje az általa generált részcsoporthoz rendje. $\square$

8.1.54. Következmény. *Prímszámrendű csoport ciklikus.*

Bizonyítás. Bármely, az egységelemtől különböző eleme kell, hogy generálja. $\square$

8.1.55. Tétel. *Egy nem egyelemű csoport pontosan akkor prímszámrendű, ha csak triviális részcsoporthjai vannak.*

Bizonyítás. Az, hogy prímszámrendű csoportnak csak triviális részcsoporthjai vannak, azonnal következik Lagrange tételéből. Ha csak triviális részcsoporthok vannak, akkor bármely, az egységelemtől különböző g eleme a csoportnak generálja a csoportot, így az ciklikus. A ciklikus csoportok közül pedig csak a prímszámrendűeknek nincs valódi részcsoporthjuk: ha a csoport végtelen rendű, akkor $\langle g^2 \rangle$ valódi részcsoporth, ha pedig a csoport rendje $n = n_1 n_2$, $n_1, n_2 > 1$, akkor $\langle g^{n_1} \rangle$ egy valódi részcsoporth. $\square$

→ **8.1.56. Feladat [2].** Mutassuk meg, hogy $\mathbb{Q}^+$ a szorzással a $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, illetve $\mathbb{C} \setminus \{0\}$ részcsoporthja. Mennyi a részcsoporth indexe az egyes esetekben?

→ **8.1.57. Feladat [5].** A csoportokra adott példák közül azoknál, amelyek a nem nulla komplex számok multiplikatív csoportjának részcsoporthjai, határozzuk meg, hogy melyik melyiknek részcsoporthja, és mennyi az indexe a másikon.

→ **8.1.58. Feladat [2].** Bizonyítsuk be, hogy $\mathbb{Z}_5$ nem nulla elemei a szorzásra negyedrendű ciklikus csoportot alkotnak.

→ **8.1.59. Feladat [2].** Bizonyítsuk be, hogy $\mathbb{Z}_8$ a szorzásra invertálható elemei a szorzással negyedrendű ciklikus csoportot alkotnak.

→ **8.1.60. Feladat [2].** Bizonyítsuk be, hogy $\mathbb{Z}_9$ szorzásra invertálható elemei a szorzással hatodrendű ciklikus csoportot alkotnak.

→ **8.1.61. Feladat [4].** Melyik az a legkisebb m természetes szám, amelyre $\mathbb{Z}_m$ szorzásra invertálható elemei a szorzással nem ciklikus csoportot alkotnak?

→ **8.1.62. Feladat [2].** Bizonyítsuk be, hogy két negyedrendű nem izomorf csoport van.

→ **8.1.63. Feladat [1].** Mutassuk meg, hogy ha egy csoportban minden egységelemtől különböző elem rendje 2, akkor a csoport kommutatív.

8.1.64. Feladat [2]. Mutassuk meg, hogy ha egy csoportban minden egységelemtől különböző elem rendje véges és ugyanaz, akkor az prímszám.

8.1.65. Feladat [5]. Határozzuk meg a nem izomorf hatodrendű csoportokat.

* **8.1.66. Feladat [8].** Mutassuk meg, hogy $\mathbb{R}$ -nek egy $\mathbb{Q}$ feletti vektortérbe vett összeadástartó leképezései lineárisak.

* **8.1.67. Feladat [10].** Mutassuk meg, hogy $\mathbb{R}$ és $\mathbb{C}$ additív csoportként izomorfak.

* **8.1.68. Feladat [9].** Mutassuk meg, hogy egy csoport bármely kommutatív rész-csoportjához létezik a csoportnak azt tartalmazó maximális kommutatív rész-csoportja. Igaz-e hasonló állítás félcsoportokra?

→ **8.1.69. Feladat [2].** Legyen g a G csoport m -med rendű ($m \in \mathbb{N}^+$) eleme. Bizonyítsuk be, hogy g^n pontosan akkor az egységelem, ha $m|n$.

8.1.70. Normálosztó. Egy G csoport egy N rész-csoportja szerinti mellékosztályok között a (komplexus) szorzás nem feltétlenül kompatibilis az osztályozással: $NaNb$ nem biztos hogy egyenlő Nab -vel vagy egyáltalán egy jobb oldali mellékosztállyal. Ha N rész-csoportja G -nek, és minden $a \in G$ -re $aN = Na$, akkor N -et *normálosztónak* vagy *normális rész-csoportnak* vagy *invariáns rész-csoportnak* nevezzük. (Ennek kifejezésére szokásos az $N \triangleleft G$ jelölés.) Ha N normálosztó, akkor nyilván a jobb és bal oldali mellékosztályok megegyeznek, és megfordítva, ha egy N rész-csoportra a jobb és bal oldali mellékosztályok megegyeznek, akkor – felhasználva hogy aN és Na is tartalmazza a -t – kapjuk, hogy $aN = Na$ minden $a \in G$ -re. Meg fogjuk mutatni, hogy normálosztóknál a művelet kompatibilis az osztályozással. Természetesen Abel-csoportban minden rész-csoport normálosztó. Nyilván az egész G és a csak az egységelemet tartalmazó egyelemű rész-csoport is normálosztók, ezek a *triviális normálosztók*. A G -től különböző normálosztókat *valódi normálosztónak* nevezzük. Egy kettő indexű N rész-csoport mindig normálosztó, mert csak két, bal és egyúttal jobb oldali mellékosztály van, N és $G \setminus N$.

8.1.71. Tétel. Legyen N a G csoport rész-csoportja. A következő feltételek ekvivalensek:

- (1) N normálosztó;
- (2) $a^{-1}Na = N$ minden $a \in G$ -re;
- (3) $a^{-1}Na \subset N$ minden $a \in G$ -re;

Bizonyítás. (1)-ből következik (2), mert $a^{-1}Na = a^{-1}aN = N$. (2)-ből következik (1), mivel $Na = a(a^{-1}Na) = aN$. Nyilván (2)-ből következik (3). Ha (3) fennáll, akkor $a^{-1}Na \subset N$ -ban a helyére a^{-1} -et írva $aNa^{-1} \subset N$, amiből $N = a^{-1}(aNa^{-1})a \subset a^{-1}Na$, így (2)-t kaptuk. $\square$

8.1.72. Következmény. Normálosztók metszete is normálosztó.

Következik (3)-ból; a bizonyítás hasonló annak bizonyításához, hogy részcsoporthoz metszete részcsoporthoz. $\square$

8.1.73. Példa. A D_3 diédercsoportban egy adott τ a tükrözés által generált $H = \{e, \tau\}$ részcsoporthoz nem normálosztó, mert $H\varepsilon = \{\varepsilon, \tau\varepsilon\}$, de $\varepsilon H = \{\varepsilon, \varepsilon\tau\} = \{\varepsilon, \tau\varepsilon^2\}$. A forgatások által alkotott $\{e, \varepsilon, \varepsilon^2\}$ részcsoporthoz normálosztó, mert kettő az indexe.

→ **8.1.74. Feladat [3].** Normálosztó-e

- (1) $\mathbb{Z}$ -ben $3\mathbb{Z}$;
- (2) D_6 -ban a 120° -os forgatás által generált részcsoporthoz;
- (3) D_6 -ban a 180° -os forgatás és egy tükrözés által generált részcsoporthoz.

* **8.1.75. Feladat [6].** Normálosztó-e $\text{GL}(\mathbb{R}^n)$ -ben

- (1) az egy adott bázisban diagonális mátrixú transzformációk halmaza;
- (2) az identikus leképezés skalárszorosainak halmaza;
- (3) az egy adott bázisban felső háromszög mátrixú transzformációk halmaza.

* **8.1.76. Belső automorfizmusok.** Ha G csoport és $a \in G$ rögzített, akkor a G -n értelmezett $x \mapsto a^{-1}xa$ leképezés automorfizmusa G -nek, mert xy -hoz az $a^{-1}(xy)a$ elemet rendeli, ami $a^{-1}xa$ és $a^{-1}ya$ szorzata, tehát homomorfizmus, az egyszerűsítési szabály miatt kölcsönösen egyértelmű, és minden elem előáll képként, mert x az axa^{-1} képe. Az ilyen alakú automorfizmusokat *belső automorfizmusoknak* vagy *konjugálásoknak* nevezzük. Általában nem minden automorfizmus belső automorfizmus: például kommutatív esetben csak az identikus leképezés belső automorfizmus, de az inverzképezés is automorfizmus. Ha az x elemhez van olyan belső automorfizmus, amely y -ba viszi át, akkor azt mondjuk, hogy x és y *konjugáltak*. Ez nyilván ekvivalenciareláció, az ekvivalenciaosztályok a *konjugált elemosztályok*. Nyilván egy automorfizmusnál egy részcsoporthoz képe részcsoporthoz. Az előző tétel (2) pontja szerint a normálosztók pontosan azok a részcsoporthoz, amelyeknek a képe minden belső automorfizmusnál saját maga, azaz olyan részcsoporthoz, amelyek minden elemükhöz az azzal konjugáltakat is tartalmazzák. Ez az oka az invariáns részcsoporthoz elnevezésnek.

* **8.1.77. Centralizátor és centrum.** Egy G csoport egy adott x elemével felcserélhető elemek G -nek egy részcsoporthozját alkotják, ez az x *centralizátora*, jelölése $C(x)$. A $C = \bigcap_{x \in G} C(x)$ részcsoporthoz normálosztó is, hiszen G minden elemmel felcserélhető elemeit tartalmazza, ezeket pedig minden belső automorfizmus az egységelembe viszi; C a G csoport *centrumba*.

* **8.1.78. Osztályegyenlet.** Egy G csoportban az $x \in G$ elem konjugált elemosztályának annyi eleme van, amennyi $C(x)$ szerinti mellékosztály. Ha G véges csoport, akkor $\sum [G:C(x)]$ a G rendje, ahol az összegzés a különböző elemosztályokból választott egy-egy x -re értendő; ez az osztályegyenlet.

Bizonyítás. Az x két konjugáltja, $g^{-1}xg$ és $h^{-1}xh$ pontosan akkor egyenlő, ha $(hg^{-1})x = x(hg^{-1})$, azaz ha $hg^{-1} \in C(x)$. Ez azzal ekvivalens, hogy g és h ugyanazon $C(x)$ szerinti jobboldali mellékosztályba tartoznak. Tehát annyi különböző mellékosztály van, ahány konjugált. Ezzel az első állítást beláttuk. A konjugált elemosztályok elemszámának összege nyilván G rendje.

* **8.1.79. Példák.** (1) A Q kvaterniócsoportban a konjugált elemosztályok $\{1\}$, $\{-1\}$, $\{i, -i\}$, $\{j, -j\}$, $\{k, -k\}$ és $C(1) = C(-1) = Q$, $C(i) = C(-i) = \{1, -1, i, -i\}$, $C(j) = C(-j) = \{1, -1, j, -j\}$, $C(k) = C(-k) = \{1, -1, k, -k\}$, így $C = \{1, -1\}$.

(2) A D_3 diédercsoportban a konjugált elemosztályok $\{e\}$, $\{\varepsilon, \varepsilon^2\}$, $\{\tau, \tau\varepsilon, \tau\varepsilon^2\}$, és $C(e) = D_3$, $C(\varepsilon) = C(\varepsilon^2) = \{e, \varepsilon, \varepsilon^2\}$, $C(\tau) = \{e, \tau\}$, $C(\tau\varepsilon) = \{e, \tau\varepsilon\}$, $C(\tau\varepsilon^2) = \{e, \tau\varepsilon^2\}$, így $C = \{e\}$.

8.1.80. Tétel. Legyen G csoport. Ekkor

- (1) egy N normálosztó szerinti mellékosztályok a csoportnak a művelettel kompatibilis osztályozását alkotják;
- (2) egy N normálosztó szerinti mellékosztályok közötti művelet megegyezik az osztályok mint halmazok komplexusszorzásával;
- (3) minden, a művelettel kompatibilis osztályozás esetén az egységelem osztálya normálosztó, és az osztályozás ezen normálosztó szerinti mellékosztályokból áll.

Bizonyítás. Ha N normálosztó, $a' \in Na$ és $b' \in Nb$, akkor a részcsoporthoz szerinti mellékosztályokról tanultakat felhasználva $Na' = Na$ és $Nb' = Nb$, tehát

$$a'b' \in (Na')(Nb') = (Na)(Nb) = N(aN)b = N(Na)b = N^2ab = Nab,$$

azaz az osztályozás kompatibilis a művelettel, amivel beláttuk (1)-et. Másrészt

$$\{a'b' : a' \in Na, b' \in Nb\} = (Na)(Nb) = Nab,$$

tehát az osztályok szorzása megegyezik a komplexusszorzással, amivel beláttuk (2)-t.

(3) bizonyításához tegyük fel, hogy adott egy, a szorzással kompatibilis $\sim$ ekvivalenciareláció, és jelölje N az e egységelem osztályát. Mivel $a \in N$ esetén $e = a^{-1}a \sim a^{-1}e = a^{-1}$, kapjuk, hogy $N^{-1} \subset N$. Ha $a, b \in N$, akkor $ab \sim ee = e$, így $NN \subset N$, tehát N részcsoporthoz. Ha most $x \in N$ és g tetszőleges, akkor $g^{-1}xg \sim g^{-1}eg = e$, így $g^{-1}Ng \subset N$, tehát N normálosztó. Ha a és b ekvivalensek, akkor $a^{-1}ab^{-1}$ és $a^{-1}bb^{-1}$ is, azaz $a^{-1} \sim b^{-1}$, tehát az inverz képzés kompatibilis az osztályozással. Innen viszont $e = aa^{-1} \sim ab^{-1}$, tehát $ab^{-1} \in N$. Megfordítva, ha $ab^{-1} \in N$, azaz $ab^{-1} \sim e$, akkor $a = ab^{-1}b \sim eb = b$, és így az $\sim$ ekvivalenciarelációhoz tartozó osztályozás pontosan az N szerinti mellékosztályokból áll. $\square$

8.1.81. Következmény. Egy G csoportnak egy N normálosztó szerinti mellékosztályai (a komplexusszorzásra nézve csoportot alkotnak).

Bizonyítás. G -nek a mellékosztályok (a komplexusszorzással mint művelettel tekintett) halmazára való $a \mapsto Na$ leképezése művelettartó, így a homomorf képre tanultakból következik az állítás. $\square$

8.1.82. Faktorcsoport. Az előző következményben szereplő csoportot a G csoport N normálosztó szerinti faktorcsoportjának (vagy hányadoscsoportjának) nevezzük, és G/N -nel jelöljük. Ha G rendje véges, akkor G/N rendje $[G:N]$, az N indexe.

Általában a faktorstruktúrák azért fontosak, mert számos esetben lehetőség van arra, hogy ezekben áttekinthetőbben vizsgáljuk az eredeti struktúra bizonyos érdemi tulajdonságait. Bizonyos számítógépes algoritmusok felgyorsítása is ezen a módszeren alapul.

8.1.83. Példák. (1) Ha $N = G$, akkor G/N egyelemű. Ha $N = \{e\}$, akkor az osztályok egyeleműek, így G/N izomorf G -vel.

(2) Bármely $m \in \mathbb{Z}$ -re az $m\mathbb{Z}$ normálosztó $\mathbb{Z}$ additív Abel-csoportban, és a faktorcsoport $\mathbb{Z}_m$ additív csoportja.

(3) A kvaterniócsoportban a kételemű $\langle -1 \rangle$ részcsoport szerinti négyelemű faktorcsoport izomorf a Klein-féle csoporttal.

8.1.84. Homomorfizmus magja. Egy G csoportnak egy G' csoportba való φ homomorfizmusánál a *homomorfizmus magján* a G' csoport e' egységelemének a teljes inverz képét értjük, amit $\ker(\varphi)$ -vel jelölünk.

8.1.85. Homomorfizmus-tétel. Egy G csoport egy φ homomorfizmusánál a *homomorfizmus magja normálosztó*, és a $G/\ker(\varphi)$ faktorcsoport izomorf $G' = \varphi(G)$ -vel. A G bármely N normálosztója magja valamely homomorfizmusnak: G -nek G/N -re való kanonikus leképezése homomorfizmus, amelynek magja N .

Bizonyítás. A $\varphi^{-1}(a')$, $a' \in G'$ halmazrendszer a G egy osztályozása. Megmutatjuk, hogy kompatibilis a szorzással. Valóban, bármely $a \in \varphi^{-1}(a')$ -re és $b \in \varphi^{-1}(b')$ -re $\varphi(ab) = \varphi(a)\varphi(b) = a'b'$, azaz $ab \in \varphi^{-1}(a'b')$, függetlenül az a és b választásától. Így $e \in \varphi^{-1}(e')$ osztálya, ami $\ker(\varphi)$, normálosztó, és a szerinte vett osztályozás éppen a megadott osztályozás. Az $a' \mapsto \varphi^{-1}(a')$ bijektív leképezés homomorfizmus, és így G' izomorfizmusa $G/\ker(\varphi)$ -re.

A tétel második fele az előző tétel következményének bizonyítása alapján nyilvánvaló.

□

A homomorfizmustétel a 8.1.2 ábrán tanulmányozható egy konkrét példa segítségével: G az egész számok halmaza a $+$ művelettel, G' a $\{\uparrow, \downarrow\}$ halmaz a $\oplus$ kizáró vagy művelettel, a φ függvény pedig az $n \mapsto 2|n|$ logikai értékű leképezés, így $\ker(\varphi) = 2\mathbb{Z}$. A kanonikus leképezés G -ből $G/\ker(\varphi)$ -re κ , az izomorfizmus pedig ψ .

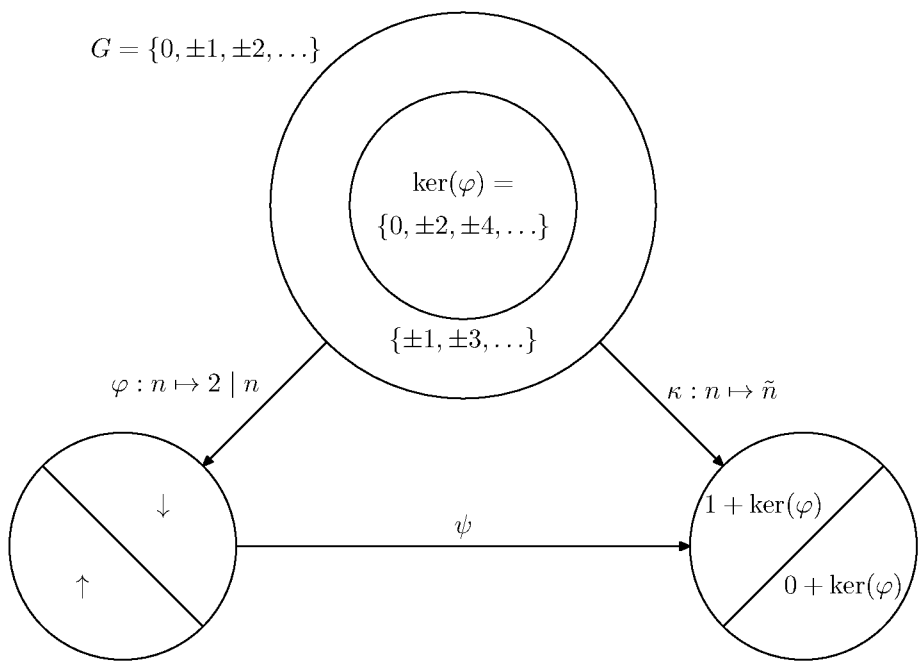
→ **8.1.86. Feladat [7].** Mutassuk meg, hogy izomorfak:

- (1) $(\mathbb{Z}/n\mathbb{Z}, +)$ és $(\mathbb{Z}_n, +)$;
- (2) $(\mathbb{C}/\mathbb{R}, +)$ és $(\mathbb{R}, +)$;
- (3) $(\mathbb{C} \setminus \{0\}/\mathbb{T}, \cdot)$ és $(\mathbb{R}^+, \cdot)$;
- (4) $(\mathbb{C} \setminus \{0\}/\mathbb{R}^+, \cdot)$ és $(\mathbb{T}, \cdot)$;
- (5) $(\mathbb{R}/\mathbb{Z}, +)$ és $(\mathbb{T}, \cdot)$;
- (6) $(\mathbb{Q}/\mathbb{Z}, +)$ és $(\mathbb{U}, \cdot)$;
- (7) $(\mathbb{Q} \setminus \{0\}/\mathbb{U}_2, \cdot)$ és $(\mathbb{Q}^+, \cdot)$;
- (8) $(\mathbb{R} \setminus \{0\}/\mathbb{U}_2, \cdot)$ és $(\mathbb{R}^+, \cdot)$;

* **8.1.87. Feladat [7].** Mutassuk meg, hogy $\mathbb{GL}(\mathbb{R}^1)$ és

$$N = \{x \mapsto x + b : x \in \mathbb{R}, b \in \mathbb{R}\}$$

részcsoporthai $(\mathbb{GA}(\mathbb{R}^1), \circ)$ -nek, de $\mathbb{GL}(\mathbb{R}^1)$ nem normálosztó, míg N normálosztó, és a faktorcsoport izomorf $\mathbb{GL}(\mathbb{R}^1)$ -gyel, azaz $(\mathbb{R} \setminus \{0\}, \cdot)$ -tal.



8.1.2 ábra: A homomorfizmustételhez.

* **8.1.88. Feladat [7].** Legyen F egy test, $n \in \mathbb{N}^+$. Mutassuk meg, hogy izomorfak:

- (1) $\mathrm{GL}(F^n)/\mathrm{SL}(F^n)$ és $(F^*, \cdot)$;
- (2) $\mathrm{O}(n)/\mathrm{SO}(n)$ és $(\mathbb{U}_2, \cdot)$;
- (3) $\mathrm{U}(n)/\mathrm{SU}(n)$ és $(\mathbb{T}, \cdot)$;
- (4) $\mathrm{SO}(2)$ és $(\mathbb{T}, \cdot)$.

8.1.89. Feladat [6]. Határozzuk meg az alábbi Abel-csoportok endomorfizmusait és automorfizmusait:

- (1) $(\mathbb{Z}, +)$;
- (2) $(\mathbb{Q}, +)$.

* **8.1.90. Projektív csoportok.** Legyen F egy test, $n \in \mathbb{N}^+$. A $\mathrm{GL}(F^n)$ csoportnak az identikus leképezés konstansszorosai szerinti faktorcsoporthát *projektív általános lineáris csoportnak* nevezzük, és $\mathrm{PGL}(F^n)$ -nel jelöljük, a $\mathrm{SL}(F^n)$ csoportnak az identikus leképezés konstansszorosai szerinti faktorcsoporthát *projektív speciális lineáris csoportnak* nevezzük, és $\mathrm{PSL}(F^n)$ -nel jelöljük.

* **8.1.91. Feladat [10].** Legyen F egy test, elemszáma q , egy prímszám, és $n \in \mathbb{N}^+$. Határozzuk meg $\mathrm{PGL}(F^n)$ és $\mathrm{PSL}(F^n)$ rendjét.

8.1.92. Direkt szorzat. Legyen G_i ($i \in I$) egy-egy binér művelettel ellátott halmazok egy indexelt családja. Az egyszerűség kedvéért mindegyik halmazon a műveletet jelöljük szorzással. Ekkor a

$$G = \times_{i \in I} G_i$$

Descartes-szorzatot ellátva az $(ab)_i = a_i b_i$ összefüggéssel definiált művelettel, a G -t a G_i , $i \in I$ család *direkt szorzatának* nevezzük.

A legfontosabb speciális eset az, amikor $I = \{1, 2, \dots, n\}$, ekkor a direkt szorzat elemei $a = (a_1, a_2, \dots, a_n)$, $a_i \in G_i$ alakú n -esek. A szorzás definíció szerint koordinátánként történik, így ha $b = (b_1, b_2, \dots, b_n)$ egy másik eleme a direkt szorzatnak, akkor $ab = (a_1 b_1, a_2 b_2, \dots, a_n b_n)$.

Nyilvánvaló, hogy ha minden G_i félcsoport, akkor G is, ha minden G_i kommutatív, akkor G is, ha minden G_i egységelemes, akkor G is, és ha minden G_i csoport, akkor G is. Ez utóbbi esetben, ha $J \subset I$, akkor az $a \mapsto a|_J$ projekció homomorfizmus, képe $\times_{i \in J} G_i$, magja pedig izomorf $\times_{i \in I \setminus J} G_i$ -vel.

A direkt szorzás segítségével a véges Abel-csoportok szerkezete teljesen leírható:

8.1.93. Véges Abel-csoportok alaptétele. *Egy véges Abel-csoport véges sok ciklikus csoport direkt szorzatával izomorf. A tényezők választhatók prímhatalvány rendűnek. A prímhatalvány rendek egyértelműen meghatározottak.*

* **Bizonyítás.** A tétel következik az alábbi, még általánosabb tételből:

* **8.1.94. Végesen generált Abel-csoportok alaptétele.** *Egy véges halmaz által generált Abel-csoport véges sok ciklikus csoport direkt szorzatával izomorf. A tényezők közül a véges rendűek választhatók prímhatalvány rendűnek. A végtelen rendű tényezők száma és az egyes prímhatalványrendek egyértelműen meghatározottak.*

* **Bizonyítás.** Megtalálható (általánosabb formában) Safarevics [76] könyvében, 47–48. oldal. $\square$

→ **8.1.95. Feladat [2].** Bizonyítsuk be, hogy a Klein-féle csoport nem izomorf $\mathbb{Z}_4$ -gyel, de izomorf $\mathbb{Z}_2$ önmagával vett direkt szorzatával.

8.1.96. Feladat [2]. Mutassuk meg, hogy $\mathbb{Z}_2^{\mathbb{N}}$ végtelen csoport, de minden elem rendje véges. Általánosítsuk az állítást.

8.1.97. Feladat [2]. Mutassuk meg, hogy ha A, B diszjunkt halmazok, akkor az $(\varphi(A \cup B), \triangle)$ Abel-csoport izomorf a $(\varphi(A), \triangle)$ és $(\varphi(B), \triangle)$ Abel-csoportok direkt szorzatával.

8.1.98. Feladat [3]. Legyenek G és H csoportok, $g \in G$, $h \in H$. A g és h elemek rendjének ismeretében hogyan adható meg a (g, h) elem $G \times H$ -beli rendje?

8.1.99. Feladat [3]. Mutassuk meg, hogy egy m rendű és egy n rendű ciklikus csoport direkt szorzata pontosan akkor ciklikus, ha m és n relatív prímek.

8.1.100. Feladat [5]. Mutassuk meg, hogy $(\mathbb{C} \setminus \{0\}/\mathbb{U}, \cdot)$ és $(\mathbb{R}^+, \cdot) \times (\mathbb{R}/\mathbb{Q}, +)$ izomorfak.

8.1.101. Feladat: diszkrét direkt szorzat [5]. Legyen G_i ($i \in I$) csoportok egy indexelt családja. Mutassuk meg, hogy azok a kiválasztási függvények, amelyek csak véges sok helyen vesznek fel egységelemtől különböző elemet értékként, egy normálosztót alkotnak a direkt szorzatban; ez a G_i ($i \in I$) indexelt család *diszkrét direkt szorzata*.

8.1.102. Cayley tétele. *Bármely G csoport izomorf valamely halmaz permutációinak $(a \circ \text{kompozícióval tekintett csoportja})$ egy részcsoportjával. A halmaz választható G -nek.*

Lehet, hogy a halmaz jóval kisebbnek is választható, például D_n már egy n -szög csúcsai permutációinak is részcsoportja, vagy egy kocka egybevágóságainak csoportja részcsoportja a lapok permutációcsoportjának.

Bizonyítás. Tekintsük G reguláris reprezentációját, azaz legyen $a \in G$, és az a -hoz rendelt p_a -ra legyen $p_a(x) = ax$, ha $x \in G$. A reprezentációról tanultakból tudjuk, hogy az $a \mapsto p_a$ hozzárendelés monomorfizmus. A p_a leképezések az egyszerűsítési szabály miatt kölcsönösen egyértelműek és G -re képeznek, mivel $a^{-1}x$ képe p_a -nál x . $\square$

8.1.103. Permutációcsoportok. Tetszőleges X halmaz összes permutációinak a $\circ$ művelettel vett csoportját az X szimmetrikus csoportjának neveztük, ezen csoportok részcsoportjai a *permutációcsoportok*. Az előző tétel mutatja, hogy ezek a fogalmak alapvető fontosságúak. A szimmetrikus csoport szerkezete csak az alaphalmaz elemeinek számától függ: ha φ az X halmaznak az Y halmazra való kölcsönösen egyértelmű leképezése, akkor tudjuk, hogy $f \mapsto \varphi \circ f \circ \varphi^{-1}$ megfeleltetés kölcsönösen egyértelmű leképezése (bijekciója) X összes permutációinak Y összes permutációira. Mivel a permutációk összetételére ez a megfeleltetés művelettartó is, hiszen

$$(\varphi \circ f \circ \varphi^{-1}) \circ (\varphi \circ g \circ \varphi^{-1}) = \varphi \circ f \circ g \circ \varphi^{-1},$$

így X és Y permutációinak csoportjai izomorfak. Mivel minket elsősorban a véges csoportok érdekelnek, az $\{1, 2, \dots, n\}$, $n \in \mathbb{N}$ alakú halmazok permutációinak vizsgálatára szorítkozhatunk. Az $\{1, 2, \dots, n\}$ halmaz összes permutációinak csoportját S_n -nel fogjuk jelölni, és n -ed fokú szimmetrikus csoportnak nevezzük. (Az elnevezés a szimmetrikus polinomokkal való kapcsolatra utal.) Nyilvánvalóan S_n rendje $n!$.

Bár az S_n elemei sorozatok, így egy $p \in S_n$ elemet jelölhetünk $p_1, p_2, \dots, p_n$ -nel, szokásosabb a hagyományos jelölés:

$$p = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix},$$

azaz minden elem alá odaírjuk a képét. Bármilyen más sorrendben is felírhatjuk az elemeket és alájuk a képüket, például ha $q \in S_n$,

$$q = \begin{pmatrix} 1 & 2 & \dots & n \\ q_1 & q_2 & \dots & q_n \end{pmatrix}$$

egy tetszőleges másik permutáció, akkor p írható

$$p = \begin{pmatrix} q_1 & q_2 & \dots & q_n \\ p_{q_1} & p_{q_2} & \dots & p_{q_n} \end{pmatrix}$$

alakban is. A két permutáció szorzata

$$\begin{aligned} p \circ q &= \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ q_1 & q_2 & \dots & q_n \end{pmatrix} \\ &= \begin{pmatrix} q_1 & q_2 & \dots & q_n \\ p_{q_1} & p_{q_2} & \dots & p_{q_n} \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ q_1 & q_2 & \dots & q_n \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \dots & n \\ p_{q_1} & p_{q_2} & \dots & p_{q_n} \end{pmatrix}. \end{aligned}$$

Egy

$$p = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix}$$

alakban írt permutációra legyen k az inverziók száma az alsó sorban, azaz az összes olyan $1 \leq i < j \leq n$ párok száma, amelyekre $p_i > p_j$. A permutációt *páros permutációnak*, illetve *páratlan permutációnak* nevezzük aszerint, hogy k páros vagy páratlan; ez a permutáció paritása.

Permutációkat egy másik alakban is felírhatunk. Ha $1 \leq i_1, i_2, \dots, i_k \leq n$ különböző természetes számok, jelölje $(i_1, i_2, \dots, i_k)$ azt a permutációt, amely i_1 -et i_2 -be, i_2 -t i_3 -ba stb., i_k -t i_1 -be viszi, minden más számot pedig fixen hagy. Egy ilyen permutációt k hosszúságú *ciklusnak* nevezzük. (A ciklus jelölés nem teljesen pontos, mert nem derül ki belőle, hogy mely S_n eleméről van szó.) Egy ciklus többféleképpen is felírható, bármelyik i_j -vel kezdetünk. Diszjunkt ciklusok nyilván felcserélhetőek. Minden permutáció felírható páronként diszjunkt ciklusok szorzataként, és ez az előállítás egyértelmű is, ha a sorrendtől és a felírásból nyilván elhagyható egy (vagy nulla) hosszúságú ciklusoktól eltekintünk.

A triviális egy (vagy nulla) hosszú ciklusoktól eltekintve a legegyszerűbb ciklusok a kettő hosszú ciklusok, ezeket *transzpozícióknak* nevezzük. Mivel

$$(i_1, i_2, i_3, i_4, \dots, i_k) = (i_1, i_3, i_4, \dots, i_k)(i_1, i_2),$$

minden permutáció felírható transzpozíciók szorzataként. Bár ez az előállítás nem egyértelmű, az alábbi állítás igaz:

8.1.104. Tétel. Egy $p \in S_n$ permutáció pontosan akkor páros, ha előállítható páros sok transzpozíció szorzataként, és pontosan akkor páratlan, ha páratlan sok transzpozíció szorzataként állítható elő.

Bizonyítás. Mivel az identikus permutáció páros, csak azt kell megmutatnunk, hogy ha egy permutációt jobbról szorzunk egy transzpozícióval, akkor megváltozik a permutáció paritása. Ha a

$$p = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix}$$

permutációt szorozzuk az (i, j) , $i < j$ transzpozícióval jobbról, akkor az eredmény a

$$\begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ p_1 & p_2 & \dots & p_j & \dots & p_i & \dots & p_n \end{pmatrix}$$

permutáció. Ha $k < i$ vagy $k > j$, akkor azon inverziók száma, amelyekben p_k részt vesz, nem változik. Ugyanez a helyzet, ha $i < k < j$, de p_k vagy nagyobb, mint $\max\{p_i, p_j\}$, vagy kisebb, mint $\min\{p_i, p_j\}$. Ha $i < k < j$ és $\min\{p_i, p_j\} < p_k < \max\{p_i, p_j\}$, akkor azon inverziók száma, amelyekben p_k részt vesz, kettővel változik. Marad még egy lehetséges inverzió, a p_i és p_j közötti. Mivel $p_i > p_j$ esetén ez az inverzió megszűnik, $p_i < p_j$ esetén pedig keletkezik, az állítást beláttuk. $\square$

8.1.105. Következmény. Az S_n csoportban szorzásnál a paritások „mod 2 összeadódnak”: egy páros és egy páratlan permutáció szorzata páratlan, két páros vagy két páratlan permutáció szorzata pedig páros. A páros permutációk 2 indexű normálosztót alkotnak S_n -ben, amit A_n -nel jelölünk és n -ed fokú alternáló csoportnak nevezzük. $\square$

Az alternáló csoport elnevezés az alternáló polinomokkal való kapcsolatra utal.

8.1.106. Példa. Az S_4 -ben

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & \end{pmatrix} = (1, 2, 3, 4) = (1, 3)(1, 2)(3, 4)$$

páratlan, míg

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = () = (1, 2)(2, 1) = (1, 3)(3, 1)$$

páros.

→ **8.1.107. Feladat [7].** Tekintsük a következő permutációkat:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

$$\delta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad \varepsilon = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

- (1) Bontsuk fel őket idegen ciklusok szorzatára.
- (2) Számítsuk ki az $\alpha\beta$, $\alpha^{-1}\beta$, $\alpha^2\beta$, $(\alpha\beta)^2$, $\alpha\beta\alpha^3$, $\varepsilon^{-1}\delta\gamma^{-1}$, $\gamma\delta^2\varepsilon$, ε^3 , $\delta^3\varepsilon^3$, $(\delta\varepsilon)^3$ permutációkat.

→ **8.1.108. Feladat [5].** Határozzuk meg a

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 4 & 2 & 7 & 5 & 6 & 1 \end{pmatrix}^{1111}$$

permutációt.

8.1.109. Feladat [7]. Oldjuk meg a σ permutációra az alábbi egyenleteket:

- (1) $(1\ 3\ 2)\sigma(3\ 4\ 1) = (2\ 3\ 4)$;
- (2) $(5\ 1\ 3)^{10}(2\ 3\ 4\ 6)^{10}\sigma^{-1}((1\ 2\ 3)(3\ 6\ 7)) = ()$;
- (3) $\sigma^2 = (1\ 2\ 3)$;
- (4) $\sigma^3 = (1\ 2\ 3)$;
- (5) $\sigma^4 = ()$ az S_4 -ben.

→ **8.1.110. Feladat [0].** Soroljuk fel a 2, 3, 8, 6, 1 sorozat öt inverzióját.

→ **8.1.111. Feladat [0].** Legkevesebb hány transzpozícióval kaphatjuk meg az ALGORITMUS szóból a LOGARITMUS szót?

→ **8.1.112. Feladat [5].** Keressük meg, hogy az alábbi csoportok közül melyek izomorfak: $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_3 \setminus \{0\}$, $\mathbb{Z}_5 \setminus \{0\}$, $\mathbb{Z}_8 \setminus \{0\}$, $\mathbb{Z}_{12} \setminus \{0\}$, S_2 , A_3 , S_3 , D_3 , D_4 , Q .

°* **8.1.113. Feladat [10].** Mutassuk meg, hogy az alábbi csoportok izomorfak:

- (1) S_3 , $\text{GL}(\mathbb{Z}_2^2)$, $\text{SL}(\mathbb{Z}_2^2)$ és $\text{PSL}(\mathbb{Z}_2^2)$;
- (2) A_4 és $\text{PSL}(\mathbb{Z}_3^2)$;
- (3) A_5 , $\text{PSL}(\mathbb{Z}_5^2)$ és $\text{PSL}(F^2)$, ahol F egy 4 elemű test;
- (4) $\text{PSL}(\mathbb{Z}_7^2)$ és $\text{PSL}(\mathbb{Z}_3^3)$;
- (5) A_6 és $\text{PSL}(F^2)$, ahol F egy 9 elemű test;
- (6) A_8 és $\text{PSL}(\mathbb{Z}_2^4)$.

→ **8.1.114. Feladat [2].** Az $\{1, 2, \dots, n\}$ halmaz mely permutációjára lesz az inverziók száma maximális? Mennyi ekkor az inverziók száma?

°* **8.1.115. Feladat [12].** Adjunk algoritmust, amely $O(n \log n)$ összehasonlítással a legrosszabb esetben is meghatározza az $\{1, 2, \dots, n\}$ halmaz egy (sorozatként megadott) permutációjában az inverziók számát.

→ **8.1.116. Feladat [4].** Adjunk meg a D_4 diédercsoporttal izomorf permutációcsoportot. Legalább hány eleműnek kell lennie a halmaznak, amelynek a permutációit tekintjük?

8.1.117. Feladat [6]. Adjunk meg a kvaterniócsoporttal izomorf permutációcsoportot. Igyekezzünk minél kevesebb elemű halmazt választani.

8.1.118. Feladat [3]. Mutassuk meg, hogy az S_n csoportban nem üres ciklusok rendje megegyezik a hosszukkal, és bármely permutáció rendje megegyezik a nem üres idegen ciklusokra való felbontásánál fellépő tényezők hosszának a legkisebb többszörösével.

* **8.1.119. Definíció.** Egy G csoport egy *normálláncán* részcsoportjainak egy olyan

$$G = G_0 \supset G_1 \supset G_2 \supset \dots \supset G_n = \{e\}$$

véges sorozatát értjük, amelyben G_i normálosztó G_{i-1} -ben, ha $i = 1, 2, \dots, n$. A G csoportot *feloldhatónak* nevezzük, ha van olyan normállánca, amelynek G_{i-1}/G_i *faktorai* Abel-csoportok.

A normállánc faktorai némi tájékoztatást nyújtanak a csoportról. Mivel a véges Abel-csoportok szerkezetét ismerjük, a feloldható véges csoportokról elég sok információnk van. Vannak azonban olyan csoportok, amelyeknek csak triviális normálosztója (azaz csak triviális homomorfizmusa) van, ezeket *egyszerű csoportnak* nevezzük. Egy előző tételből tudjuk, hogy az egyszerű véges Abel-csoportok az egyelemű csoport és a prímrendű ciklikus csoportok.

Legyen $n > 1$ természetes szám. Az előző következmény szerint $S_n \supset A_n \supset \{e\}$ egy normállánca S_n -nek. Megmutatható, hogy $n \geq 5$ esetén A_n nem kommutatív egyszerű csoport, így ez a normállánc nem is bővíthető tovább. Ennek felhasználásával az is belátható, hogy S_n nem feloldható, ha $n \geq 5$. A csoportok feloldhatóságát Galois vizsgálta először algebrai egyenletek gyökjelekkel való megoldhatóságával kapcsolatban.

Ma már a nem kommutatív véges egyszerű csoportok is ismertek (ez a csoportelmélet egyik legnagyobb diadala), ezeknek azonban már a felsorolása is olyan bonyolult, hogy itt nem lehet tárgyalni, annak bizonyítása pedig, hogy valóban ezek és csak ezek a véges egyszerű csoportok, több tízezer oldal több száz cikkben szétszórva. A véges egyszerű csoportok 17 végtelen sorozatba tartoznak (az egyik A_n , $n \geq 5$; egy másik a $\text{PSL}(F^n)$)

csoportok, amelyek egyszerűek, ha F egy véges test, kivéve, ha $n = 2$, $F = \mathbb{Z}_2$, illetve ha $n = 2$, $F = \mathbb{Z}_3$), továbbá van még 26 sporadikus (szórványos) véges egyszerű csoport. Ezek némelyikével még találkozni fogunk; a legnagyobb a „*Monster*”, amelynek

8080 17424 79451 28758 86459 90496 17107 57005 75436 80000 00000

eleme van.

* **8.1.120. Példa.** Megmutatható, hogy S_4 -ben

$$\{()\} \subsetneq \{(), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\} \subsetneq A_4 \subsetneq S_4$$

a normálosztók, ahol $()$ az identikus permutáció, így A_4 nem egyszerű csoport.

8.1.121. Feladat [3]. Döntsük el, hogy az alábbi csoportok közül melyik ciklikus:

- (1) S_3 ;
- (2) $\mathbb{Z}_7^\times$;
- (3) U_n ;
- (4) $(\wp(X), \triangle)$, ahol X tetszőleges halmaz.

8.1.122. Feladat [3]. Igazoljuk, hogy bármely csoport tetszőleges x, y elemeire

- (1) x rendje megegyezik x^{-1} rendjével;
- (2) x rendje megegyezik $y^{-1}xy$ rendjével;
- (3) xy rendje megegyezik yx rendjével;
- (4) ha x és y felcserélhetőek, akkor xy rendje osztja x rendjének és y rendjének a legkisebb közös többszörösét.

→ **8.1.123. Feladat [4].** Hány automorfizmusa van az egész számok additív csoportjának?

→ **8.1.124. Feladat [6].** Keressük meg egy 12 rendű ciklikus csoport, illetve S_3 összes részcsoporthát, az azok szerinti mellékosztályokat, összes normálosztóját, és az azok szerinti faktorcsoportokat.

8.1.125. Feladat [3]. Bizonyítsuk be, hogy ha egy csoport H és K véges részcsoporthainak rendje relatív prím, akkor a két részcsoporth metszete csak az egységelemet tartalmazza.

8.1.126. Feladat [4]. Mutassuk meg, hogy ha a G csoport rendje n , az m relatív prím n -hez, akkor bármely $g \in G$ -re az $x^m = g$ egyenletnek pontosan egy megoldása van G -ben.

8.1.127. Feladat [4]. Bizonyítsuk be, hogy

$$\{(), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

normálosztó S_4 -ben, és a szerinte vett faktorcsoporth izomorf S_3 -mal.

8.1.128. Feladat [4]. Igazoljuk, hogy az $(1, 1, 1)$ elem normálosztót generál az (additív) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ csoportban. Mivel lesz izomorf a faktorcsoporth?

8.1.129. Feladat [5]. Igazoljuk, hogy az alábbi leképezések csoporthomomorfizmust definiálnak, határozzuk meg mindegyiknek a magját és a mag szerinti faktorcsoportot:

- (1) $(\mathbb{Z}, +) \rightarrow S_3, n \mapsto (1\ 2\ 3)^n$;
- (2) $g^n \rightarrow h^{3^n}$, ahol g egy 15 elemű, h pedig egy 9 elemű ciklikus csoport generátora;
- (3) $G \times H \rightarrow H, (g, h) \mapsto h$, ahol G és H tetszőleges csoportok.

8.1.130. Feladat [9]. Határozzuk meg Q , S_3 , A_4 , D_4 , D_5 és D_6 részcsoportjait, normálosztóit és faktorcsoportjait.

* **8.1.131. Feladat [9].** Határozzuk meg D_3 , D_4 , Q , D_5 , S_5 , A_5 , és $\mathbb{GL}(\mathbb{Z}_2^2)$ konjugált osztályait és normálosztóit.

8.1.132. Feladat [8]. Határozzuk meg az összes legfeljebb tizedrendű csoportot izomorfia erejéig.

* **8.1.133. Feladat [22].** Határozzuk meg az összes legfeljebb 32 rendű csoportot izomorfia erejéig.

8.1.134. További feladatok. [3]: II.2–II.6, II.34, II.76, III.1–III.6, IV.1–IV.226; [17]: 129–137; [36]: 4.35–4.37; [83]: II.8.27–II.8.29, II.8.32, III.5.16, X.5.2, XII.6.1–XII.6.3, XII.6.7, XII.6.18–XII.6.21.

8.2 Gyűrűk és testek

8.2.1. Megjegyzés. Ebben a fejezetben a gyűrűkkel fogunk foglalkozni, amelyek mint tudjuk, egy alaphalmazból és rajta értelmezett két binér műveletből állnak. A csoportelméletben tanultak nagyban segítik az itt tárgyalt anyag megértését. Célszerű átnézni a 3. és 6. fejezetben bevezetett fogalmakat, mint például disztributivitás, általános disztributivitás, kommutatív gyűrű, egységelemes gyűrű, előjelszabály, ismételt összeadás, nullgyűrű, zérógyűrű, nullosztópár, nullosztómentes gyűrű, egyszerűsítés balról és jobbról, integritási tartomány, ferdetest, test, osztó, többszörös, egység, asszociált, legnagyobb közös osztó, legkisebb közös többszörös, relatív prímek. A legfontosabb példáink gyűrűkre az egész számok gyűrűje és $\mathbb{Z}_m$, ferdetestre a kvaterniók, testre pedig a racionális, valós és a komplex számok teste és $\mathbb{Z}_m$, ha m prím. További példákat nyerhetünk a függvények között értelmezett műveletek segítségével.

8.2.2. Megjegyzés. Egy egységelemes integritási tartomány nyilván pontosan akkor test, ha minden nem nulla eleme egység. Egy véges integritási tartomány test, mert egy rögzített nem nulla elemmel végigsorozva a nem nulla elemeket jobbról, illetve balról, mindegyiket megkapjuk, így a nem nulla elemek körében az $ax = b$ és az $ya = b$ egyenletek megoldhatók.

8.2.3. Példák. (1) Egy tetszőleges X halmazt egy R gyűrűbe képező összes függvények R^X halmaza a pontonkénti összeadással és szorzással gyűrű. Ha R kommutatív, akkor ez a gyűrű is kommutatív, ha R egységelemes, akkor az R^X gyűrű is egységelemes, de ha R is és X is legalább kételemű, akkor R^X nem nullosztómentes – így nem is test –, még akkor sem, ha R test.

(2) Tegyük fel, hogy $\alpha \in \mathbb{C} \setminus \mathbb{Q}$ olyan szám, amelyre $\alpha^2 + k\alpha + \ell = 0$, azaz $\alpha^2 = -k\alpha - \ell$ valamely k, ℓ egészekkel. Ekkor $\mathbb{Z}[\alpha] := \mathbb{Z} + \mathbb{Z}\alpha \subset \mathbb{C}$ egységelemes integritási tartomány, mert

$$\begin{aligned}(x + y\alpha)(x' + y'\alpha) &= xx' + (xy' + x'y)\alpha + yy'\alpha^2 \\ &= xx' + (xy' + x'y)\alpha - yy'(k\alpha + \ell) \in \mathbb{Z}[\alpha].\end{aligned}$$

A $\mathbb{Z}[\alpha]$ elemei egyértelműen írhatók $x + y\alpha$ alakban, ahol $x, y \in \mathbb{Z}$, mivel ha $x + y\alpha = x' + y'\alpha$, akkor $y = y'$ esetén $x = x'$, az $y \neq y'$ esetben viszont $\alpha = (x - x')(y' - y) \in \mathbb{Q}$ teljesülne. $\mathbb{Z}[i]$ nyilván a Gauss-egészek gyűrűje. Mint majd látni fogjuk, már ezen számgyűrűk között is vannak olyanok, amelyekben a faktorizáció irreducibilis elemekre nem egyértelmű, a prímelem és az irreducibilis elem fogalma nem esik egybe stb. Ilyen gyűrűket a Fermat-sejtéssel kapcsolatban kezdtek vizsgálni, és ezek vizsgálata vezetett az ideál fogalmának kialakulásához.

*** 8.2.4. Példa.** Megmutatjuk, hogy egy tetszőleges A Abel-csoport összes endomorfizmusai egységelemes gyűrűt alkotnak a pontonkénti összeadással és a függvények kompozíciójával, mint szorzással; ezt a gyűrűt A endomorfizmusgyűrűjének nevezzük. Valóban, ha $f, g: A \rightarrow A$ endomorfizmusok, akkor $g \circ f$ nyilván endomorfizmus, és $f + g$ is endomorfizmus, mivel A Abel-csoport, így

$$\begin{aligned}(f + g)(x + y) &= f(x + y) + g(x + y) = f(x) + f(y) + g(x) + g(y) \\ &= (f + g)(x) + (f + g)(y).\end{aligned}$$

Az összeadás nyilván kommutatív, asszociatív, az azonosan nulla leképezés nullelem, és az f additív inverze $-f$. Ha még $h: A \rightarrow A$ is endomorfizmus, akkor minden $x \in A$ -ra

$$\begin{aligned}((f + g) \circ h)(x) &= (f + g)(h(x)) = f(h(x)) + g(h(x)) \\ &= (f \circ h)(x) + (g \circ h)(x) = (f \circ h + g \circ h)(x),\end{aligned}$$

azaz teljesül a jobb oldali disztributivitás. A bal oldali disztributivitás hasonlóan adódik. Végül vegyük észre, hogy az identikus leképezés egységelem.

Konkrét példaként vizsgáljuk meg $\mathbb{Z}$ mint additív Abel-csoport endomorfizmusgyűrűjét. Ha $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$ egy endomorfizmus, akkor indukcióval $\varphi(n) = n\varphi(1)$, ha $n \in \mathbb{N}$, és $\varphi(-n) = -\varphi(n)$ miatt ez minden $n \in \mathbb{Z}$ -re fennáll. Ez azt jelenti, hogy $\varphi(1)$ egyértelműen meghatározza az endomorfizmust. Mivel minden $a \in \mathbb{Z}$ -re $\varphi(n) = na$ endomorfizmus, és $(\varphi_a \circ \varphi_b)(n) = \varphi_a(bn) = abn$, azt kapjuk, hogy $\mathbb{Z}$ mint additív Abel-csoport endomorfizmusgyűrűje izomorf a $\mathbb{Z}$ gyűrűvel.

→ **8.2.5. Feladat [0].** Írjuk fel a modulo 5 maradékosztályok testére vonatkozó összeadási és szorzási táblázatot.

→ **8.2.6. Feladat [6].** Igazoljuk, hogy a szokásos összeadással és a megadott szorzással testet kapunk:

$$(1) \quad \mathbb{Z}_2 \times \mathbb{Z}_2, (x, y) \cdot (x', y') := (xx' + yy', xy' + x'y + yy');$$

$$(2) \quad \mathbb{Z}_3 \times \mathbb{Z}_3, (x, y) \cdot (x', y') := (xx' - yy', xy' + x'y).$$

→ **8.2.7. Feladat [6].** Tegyük fel, hogy $\alpha \in \mathbb{C} \setminus \mathbb{Q}$ olyan szám, amelyre $\alpha^2 + r\alpha + s = 0$, azaz $\alpha^2 = -r\alpha - s$ valamely r, s racionális számokkal. Mutassuk meg, hogy ekkor $\mathbb{Q} + \mathbb{Q}\alpha \subset \mathbb{C}$ test.

* **8.2.8. Feladat [5].** Határozzuk meg $(\mathbb{Q}, +)$ endomorfizmusgyűrűjét.

8.2.9. Feladat [6]. Döntsük el, hogy az alábbi számhalmazok közül melyek alkotnak testet a valós számok szokásos műveleteivel:

- (1) $\{p + q\sqrt{2} + r\sqrt{3} : p, q, r \in \mathbb{Q}\};$
- (2) $\{p + q\sqrt{2} + r\sqrt{3} + s\sqrt{6} : p, q, r, s \in \mathbb{Q}\};$
- (3) $\{p + q\sqrt[3]{2} : p, q \in \mathbb{Q}\};$
- (4) $\{p + q\sqrt[3]{2} + r\sqrt[3]{4} : p, q, r \in \mathbb{Q}\}.$

8.2.10. Feladat [7]. Legyen R kommutatív egységelemes gyűrű, $a, b \in R$. Mutassuk meg, hogy ha $a^n = 0$ valamely $n \in \mathbb{N}$ -re, és b invertálható, akkor $a + b$ is invertálható.

8.2.11. Feladat [8]. Legyen R egységelemes gyűrű, $a, b \in R$. Mutassuk meg, hogy

- (1) $a, b, ab - 1$ invertálható, akkor $a - b^{-1}$ és $(a - b^{-1})^{-1} - a^{-1}$ is invertálhatóak és ez utóbbi inverze $aba - a$;
- (2) ha $1 - ab$ invertálható, akkor $1 - ba$ is.

8.2.12. Feladat [6]. Mutassuk meg, hogy ha egy gyűrűben egyetlen baloldali egységelem van, akkor az kétoldali egységelem.

8.2.13. Feladat [5]. Mutassuk meg, hogy ha egy egységelemes gyűrűben egy elemnek egyetlen balinverze van, akkor az jobbinverz is.

8.2.14. Feladat [10]. Legyen R véges gyűrű. Mutassuk meg, hogy

- (1) ha R egységelemes, akkor minden nem nulla elem vagy baloldali nullosztó, vagy invertálható;
- (2) ha van olyan $a \in R$, amely nem baloldali nullosztó és van olyan $b \in R$, amely nem jobboldali nullosztó, akkor R egységelemes.

8.2.15. Homomorfizmusok. Legyen R és R' két-két binér művelettel ellátott halmaz. Az egyszerűség kedvéért R -ben és R' -ben is az első műveletet összeadással, a másodikat pedig szorzással fogjuk jelölni. Az R -nek R' -be való összeadás- és szorzástartó $\varphi: R \rightarrow R'$ leképezését *homomorfizmusnak* fogjuk nevezni, és azt mondjuk, hogy $\varphi(R)$ az R *homomorf képe*. Ha a φ homomorfizmus kölcsönösen egyértelmű (injektív), akkor *monomorfizmusnak*, ha pedig R' -re képez (szürjektív), akkor egy R' -re való *epimorfizmusnak* nevezzük. Ha φ kölcsönösen egyértelmű és R' -re képez (bijektív), akkor φ *izomorfizmus* R és R' között. Ha R és R' között létezik izomorfizmus, akkor azt mondjuk, hogy izomorfak; ilyenkor algebrai szempontból nem lehet különbséget tenni közöttük.

Ha $R' = R$ ugyanazokkal a műveletekkel, akkor a homomorfizmusokat *endomorfizmusoknak*, az izomorfizmusokat pedig *automorfizmusoknak* is nevezzük.

Hasonlóan, mint a csoportoknál, adódik, hogy homomorfizmusok összetétele is homomorfizmus, izomorfizmusok összetétele izomorfizmus, izomorfizmus inverze is izomorfizmus, és $\mathbb{I}_R$ automorfizmus.

8.2.16. Példák. (1) Ha X tetszőleges nem üres halmaz, akkor a $(\triangle, \cap)$ műveletekkel mint összeadással és szorzással tekintett $\wp(X)$ hatványhalmaz kommutatív gyűrű, és ha $x \in X$, akkor az

$$A \mapsto \begin{cases} \uparrow, & \text{ha } x \in A, \\ \downarrow, & \text{ha } x \notin A \end{cases}$$

leképezése a $(\oplus, \wedge)$ műveletekkel tekintett $\{\uparrow, \downarrow\}$ kommutatív gyűrűbe epimorfizmus, és ha $X = \{x\}$, akkor izomorfizmus.

(2) Ha X tetszőleges nem üres halmaz, akkor a $(\triangle, \cap)$ műveletekkel mint összeadás-sal és szorzással tekintett $\wp(X)$ hatványhalmaz kommutatív gyűrű, és ha $x \in X$, akkor az

$$A \mapsto \begin{cases} \uparrow, & \text{ha } x \notin A, \\ \downarrow, & \text{ha } x \in A \end{cases}$$

leképezése a $(\iff, \vee)$ műveletekkel tekintett $\{\uparrow, \downarrow\}$ kommutatív gyűrűbe epimorfizmus, és ha $X = \{x\}$, akkor izomorfizmus.

(3) Ha $m \in \mathbb{Z}$, akkor $\mathbb{Z}$ -nek a $\mathbb{Z}_m$ gyűrűre való $x \mapsto \tilde{x} \bmod m$ leképezése epimorfizmus, $m = 0$ esetén izomorfizmus.

(4) A komplex konjugálás a komplex számok testének automorfizmusa.

→ **8.2.17. Feladat [6].** Határozzuk meg izomorfizmus erejéig a négyelemű egységelemes gyűrűket.

8.2.18. Tétel. *Gyűrű homomorf képe gyűrű.*

Bizonyítás. A csoportoknál tanultak alapján csak a disztributivitást kell belátni. Jelölje x képét x' . A homomorf kép tetszőleges három elemét felírhatjuk a', b', c' alakban. Így $a'(b' + c') = a'(b + c)' = (a(b + c))' = (ab + ac)' = (ab)' + (ac)' = a'b' + a'c'$, és hasonlóan $(b' + c')a' = b'a' + c'a'$. $\square$

Úgy a gyűrűknél, mint a testeknél fontos jellemző az elemek additív rendje, amely megfelelő feltétel teljesülése esetén minden nem nulla elemre megegyezik.

8.2.19. Tétel. *Egy R nullosztómentes gyűrűben a nem nulla elemek additív rendje megegyezik, és vagy végtelen, vagy prímszám.*

Bizonyítás. Ha egy nullosztómentes R gyűrűben egy nem nulla a elem additív rendje $n \in \mathbb{N}^+$, és b tetszőleges nem nulla elem, akkor $n(ab) = (na)b = 0b = 0$, másrészt pedig $n(ab) = a(nb)$, így $nb = 0$ kell legyen, azaz b rendje is véges, és legfeljebb annyi, mint a rendje. Mivel a és b szerepe felcserélhető, minden nem nulla elemnek ugyanannyi az additív rendje. Megmutatjuk, hogy ez a közös rend, ha nem végtelen, akkor csak prímszám lehet. Ugyanis, ha n a nem nulla a elem additív rendje, akkor $n > 1$, és ha $n = km$, akkor $0 = na = k(ma)$. Ha $m < n$, akkor $ma \neq 0$, tehát $k = n$, mert egyébként ma additív rendje kisebb lenne, mint n . $\square$

8.2.20. Gyűrű karakterisztikája. Az előző tétel szerint nullosztómentes gyűrűben a nem nulla elemek additív rendje megegyezik. Ha ez a közös érték végtelen, akkor azt mondjuk, hogy a *gyűrű karakterisztikája* nulla, ha pedig egy véges n érték, akkor azt mondjuk, hogy a *gyűrű karakterisztikája* n . Jelölése: $\text{char}(R)$.

Hasznos észrevétel, hogy ha $n = \text{char}(R) > 0$, és a gyűrű kommutatív, akkor bármely $a, b \in R$ esetén

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} = a^n + b^n,$$

mert n prím, és $0 < k < n$ esetén a binomiális együttható osztható n -nel. (Természetesen ugyanez több tagra is igaz.) Így $x \mapsto x^n$ endomorfizmus. Ezt a leképezést Frobenius-endomorfizmusnak nevezzük. Indukcióval minden $k \in \mathbb{N}^+$ -ra $x \mapsto x^{n^k}$ is endomorfizmus.

8.2.21. Feladat [5]. Mutassuk meg, hogy egy nem nulla karakterisztikájú integritási tartományban a Frobenius-endomorfizmus automorfizmus.

8.2.22. Részgyűrű, ideál. Legyen R egy halmaz a $(+, \cdot)$ binér műveletekkel. Az R egy S részhalmazát *részgyűrűnek*, illetve *résztestnek* nevezzük, ha maga is gyűrű, illetve test az adott műveletekkel. A számunkra legfontosabb eset az lesz, amikor R maga is gyűrű, illetve test. (Ilyenkor azt is mondjuk, hogy R az S *bővítése*.) A részcsoporthoz tanultak szerint egy $S \neq \emptyset$ részhalmaza R -nek pontosan akkor részgyűrű, ha $a, b \in S$ esetén $a - b \in S$ és $ab \in S$. Ezek a feltételek nyilván úgy is írhatók, hogy $S - S \subset S$, illetve $SS \subset S$. A részgyűrű fogalma a részcsoporthoz fogalmával analóg: olyan additív részcsoporthoz, amelyből még a szorzás sem vezet ki. Azt a szerepet, amelyet csoporthoz a részcsoporthoz közül a normálosztók játszottak, a gyűrűk esetében az ideálok veszik át. Az I részgyűrűt *jobbideálnak*, illetve *balideálnak* nevezzük, ha $a \in I$ és $r \in R$ esetén $ar \in I$, illetve $ra \in I$. Ha I egyszerre balideál és jobbideál is, akkor *ideálnak* nevezzük. A csoporthoz tanultak szerint az, hogy I jobbideál, illetve balideál, azzal ekvivalens, hogy $I - I \subset I$ és $IR \subset I$, illetve hogy $I - I \subset I$ és $RI \subset I$. Így az, hogy I ideál, azzal ekvivalens, hogy $I - I \subset I$, $IR \subset I$ és $RI \subset I$. Innen azonnal következik, hogy akárhány jobbideál, balideál, illetve ideál metszete ismét jobbideál, balideál, illetve ideál. Nyilván az egész R és a csak a nullelemet tartalmazó egyelemű részhalmaz ideál, ezek a *triviális ideálok*. Ha egy gyűrűben ezeken kívül nincs más ideál, akkor *egyszerű gyűrűnek* nevezzük. Az R -től különböző ideálokat *valódi ideálnak* nevezzük. Természetesen kommutatív gyűrűben a jobbideál és a balideál fogalma egybeesik az ideál fogalmával.

Egy $A \subset R$ részhalmaz által *generált ideálon* az összes, az A -t tartalmazó ideálok metszetét értjük. Jelölése: (A) . Tudjuk, hogy (A) ideál; ez a legszűkebb ideál, amely tartalmazza A -t. Ha $A = \{a_1, a_2, \dots, a_n\}$, akkor $(\{a_1, a_2, \dots, a_n\})$ helyett csak $(a_1, a_2, \dots, a_n)$ -et írunk. Ha egy I ideált egyetlen $a \in R$ generál, azaz $I = (a)$, akkor *főideálnak* nevezzük. (Hasonlóan definiálható az A által generált jobbideál, illetve balideál is.)

8.2.23. Példák. (1) A valós változós valós értékű függvények $\mathbb{R}^{\mathbb{R}}$ gyűrűjében részgyűrűt alkotnak például a korlátos függvények, a folytonos függvények, a korlátos folytonos függvények, a polinomfüggvények stb.

(2) Egy X lineáris tér önmagába való lineáris leképezései a pontonkénti összeadással és a függvényösszetétellel mint szorzással az Abel-csoportként tekintett X endomorfizmusai gyűrűjének egy részgyűrűjét alkotják.

(3) Ha az előző pontban szereplő X lineáris tér n dimenziós, akkor az önmagába való lineáris leképezéseinek az előző pontban megadott gyűrűje izomorf az $n \times n$ -es mátrixoknak a mátrixok összeadásával és szorzásával tekintett gyűrűjével.

8.2.24. Példák. (1) Az egész számok gyűrűjében egy m egész szám többszöröse ideált alkotnak. Ez nyilván főideál, amelyet m (vagy $-m$) generál.

(2) Ha X nem üres halmaz, és $x \in X$, akkor a $(\Delta, \cap)$ műveletekkel ellátott $\wp(X)$ gyűrűben $\{A \subset X : x \notin A\}$ főideál.

(3) A $\mathbb{Q} \times \{0\}$ halmaz ideál (a koordinátánkénti összeadással és szorzással ellátott) $\mathbb{Q} \times \mathbb{Q}$ -ban.

8.2.25. Példák. További érdekes példák ideálra: egy adott polinom többszörösei az egyhatározatlanú valós együtthatós polinomok gyűrűjében, a konstans tagot nem tartalmazó polinomok a kéthatározatlanú valós együtthatós polinomok gyűrűjében (ez utóbbi

nem főideál). Az $n \times n$ -es valós mátrixok nem kommutatív gyűrűjében azok a mátrixok, amelyekben az első sor, illetve az első oszlop kivételével minden más sor, illetve oszlop minden eleme nulla, jobbideált, illetve balideált alkotnak (de nem alkotnak ideált).

→ **8.2.26. Feladat [0].** Bizonyítsuk be, hogy $2\mathbb{Z}$ a $\mathbb{Z}$ -nek részgyűrűje. Ideál-e? Főideál-e?

→ **8.2.27. Feladat [0].** Bizonyítsuk be, hogy $4\mathbb{Z}$ a $2\mathbb{Z}$ -nek részgyűrűje. Ideál-e? Főideál-e?

→ **8.2.28. Feladat [2].** Bizonyítsuk be, hogy $\mathbb{Z}$ -ben $(18, 30) = (6)$, tehát főideál.

→ **8.2.29. Feladat [0].** Legyenek I és J az R gyűrű ideáljai. Bizonyítsuk be, hogy $I + J$ az $I \cup J$ által generált ideál.

8.2.30. Feladat [6]. Egy gyűrű ideáljai a tartalmazásra nézve részben rendezett halmazt alkotnak.

(1) Készítsük el a $\mathbb{Z}_{12}$, $\mathbb{Z}_{30}$ és $\mathbb{Z}_{24}$ gyűrűk ideáljainak Hasse-diagramját;

(2) Milyen $n \in \mathbb{N}^+$ -ra alkotnak $\mathbb{Z}_n$ ideáljai rendezett halmazt?

→ **8.2.31. Feladat [2].** Mutassuk meg, hogy $\mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k \subset \mathbb{H}$ egységelemes nullosztómentes nem kommutatív gyűrű.

8.2.32. Feladat [5]. Bizonyítsuk be, hogy bármely R gyűrűre $R \times \mathbb{Z}$ egységelemes gyűrű az $(r, m) + (s, n) = (r+s, m+n)$ összeadással és az $(r, m) \cdot (s, n) = (rs+ms+nr, mn)$ szorzással, és ebben $R \times \{0\}$ izomorf R -el. Mutassuk meg, hogy ha R egységelemes, akkor $R \times \mathbb{Z}$ -ben vannak nullosztók.

* **8.2.33. Reprezentációk.** Egy R gyűrűnek egy A Abel-csoport endomorfizmusgyűrűjébe való homomorfizmusát R reprezentációjának nevezzük. Ha a leképezés monomorfizmus, akkor *hű reprezentációról* beszélünk. Egy egységelemes gyűrűnek mint (multiplikatív) egységelemes félcsoportnak a reguláris reprezentációja a gyűrű *reguláris reprezentációja*; mint tudjuk, ez hű reprezentáció.

* **8.2.34. Feladat [5].** Bizonyítsuk be, hogy minden gyűrű izomorf egy Abel-csoport endomorfizmusgyűrűjének valamely részgyűrűjével.

* **8.2.35. Boole-gyűrűk.** Olyan gyűrűt, amelynek bármely a elemére $a^2 = a$, *Boole-gyűrűnek* nevezünk. Boole-gyűrűben minden a elemre $2a = 0$, hiszen $a + a = (a + a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a$, ahonnan $a + a = 0$ (és így $a = -a$). Minden Boole-gyűrű kommutatív, mert $a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$, ahonnan $ab = -(ba) = ba$.

A nullgyűrűtől különböző legegyszerűbb példa Boole-gyűrűre $\{\uparrow, \downarrow\}$ a $(\oplus, \wedge)$ műveletekkel. Tetszőleges X halmazra $\wp(X)$ példa Boole-gyűrűre a $(\Delta, \cap)$ műveletekkel. (Figyeljük meg a nagyfokú hasonlóságot a logikai műveletek és a halmazműveletek között: nem véletlen, hiszen mindkét esetben Boole-gyűrűben vagyunk.) Egy halmazhoz a karakterisztikus függvényét rendelve látjuk, hogy ez a gyűrű a $\{0, 1\}^X$ függvénygyűrűvel izomorf, ahol $\{0, 1\}$ a kételemű test. Természetesen egy Boole-gyűrű minden részgyűrűje is Boole-gyűrű.

* **8.2.36. Feladat [2].** Legyen R a 30 természetes szám osztóinak halmaza, $x \diamond y := \text{lkk}(x, y) / \text{lko}(x, y)$ és $x \star y := \text{lko}(x, y)$.

- (1) Mutassuk meg, hogy $(R, (\diamond, \star))$ Boole-gyűrű. Határozzunk meg egy vele izomorf halmazgyűrűt.
- (2) Általánosítsuk a feladatot 30 helyett tetszőleges négyzetmentes pozitív természetes számra.
- (3) Általánosítsuk a feladatot arra az esetre, amikor R az összes négyzetmentes pozitív természetes számok halmaza. Van-e olyan izomorf halmazgyűrű, amely valamely halmaz összes részhalmazából áll?

* **8.2.37. Feladat [10].** Egy X halmazt a $\cup$ és $\cap$ binér műveletekkel *hálónak* nevezünk, ha mindkét művelet kommutatív és asszociatív, és minden $a, b \in X$ esetén teljesülnek az $(a \cup b) \cap a$ és $(a \cap b) \cup a = a$ *elnyelési tulajdonságok*. Ha az X háló Y részhalmazából nem vezetnek ki a $\cap$ és $\cup$ műveletek, akkor Y az X *részhalója*. Ha a hálónak van az $\cup$ műveletre semleges eleme, azt *nullelemnek* nevezzük és 0-val jelöljük. Ha a hálónak van a $\cap$ műveletre semleges eleme, azt *egységelemnek* nevezzük és 1-gyel jelöljük. Ha az $a \in X$ -hez van olyan $a' \in X$, amelyre $a \cup a' = 1$ és $a \cap a' = 0$, akkor azt mondjuk, hogy a' az a *komplementere*.

- (1) Mutassuk meg, hogy $\{\uparrow, \downarrow\}$ az $\cup := \vee$ és $\cap := \wedge$ logikai műveletekkel háló, amelyben van 0 és 1, és mindkét elemnek van egyértelmű komplementere.
- (2) Mutassuk meg, hogy bármely X halmazra $\wp(X)$ a szokásos metszet- és unióképzéssel háló, amelyben van 0 és 1, és minden elemnek van egyértelmű komplementere.
- (3) Az előző példában szereplő hálók részhálói között keressünk olyanokat, amelyekben nincs 0, amelyekben nincs 1, illetve amelyekben van 0 és 1, de rajtuk kívül egyetlen elemnek sincs komplementere.
- (4) Mutassuk meg, hogy hálóban minden $a \in X$ -re $a \cup a = a$ és $a \cap a = a$, azaz mindkét művelet *idempotens*.
- (5) Mutassuk meg, hogy egy hálóban $a \cap b = a$ pontosan akkor teljesül, ha $a \cup b = b$.
- (6) Mutassuk meg, hogy ha egy hálóban van nullelem, akkor $0 \cap a = 0$ minden $a \in X$ -re.
- (7) Mutassuk meg, hogy ha egy hálóban van egységelem, akkor $1 \cup a = 1$ minden $a \in X$ -re.

* **8.2.38. Feladat [6].** Egy X hálót *disztributívnak* nevezünk, ha minden $a, b, c \in X$ -re teljesülnek az $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$ és $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$ disztributivitások.

- (1) Mutassuk meg, hogy az előző feladatban szereplő három példa disztributív háló.
- (2) Mutassuk meg, hogy egy hálóban bármelyik disztributivitásból következik a másik.

* **8.2.39. Feladat [9].** Mutassuk meg, hogy egy háló egy speciális részbenrendezett halmaz:

- (1) tegyük fel, hogy X részbenrendezett halmaz, amelyben bármely $\{a, b\} \subset X$ -re létezik $\sup\{a, b\}$ és $\inf\{a, b\}$; mutassuk meg, hogy az $a \cup b := \sup\{a, b\}$ és $a \cap b := \inf\{a, b\}$ definíciókkal hálót kapunk, és ha X -ben van legkisebb elem, az lesz a 0, ha van legnagyobb elem, az lesz az 1;

- (2) megfordítva, tegyük fel, hogy X háló, és mutassuk meg, hogy $a \leq b := a \cap b = a$ részben rendezés, amelyre bármely $\{a, b\} \subset X$ -re létezik $\sup\{a, b\}$ és $\inf\{a, b\}$ és azok $a \cup b$ illetve $a \cap b$, így hálóban mindig adott egy természetes részbenrendezés, és erre a nullelem a legkisebb elem, az egységelem pedig a legnagyobb elem.

* **8.2.40. Feladat [6].** Határozzuk meg egy 5 elemű halmazon azokat a páronként nem hasonló részben rendezéseket, amelyek hálót adnak. Van-e nullelem, egységelem, illetve disztributív-e a háló? Határozzuk meg az elemek komplementereit. Rajzoljuk fel a Hasse-diagramokat.

° * **8.2.41. Feladat [3].** Tekintsük az $\{1, 2, 4, 6, 12\}$ halmazt és az $\{1, 4, 6, 12\}$ részhalmazát az „osztója” részben rendezéssel. Mutassuk meg, hogy mindkettő háló, de az utóbbi nem részhálója az előbbinek. Rajzoljuk fel a Hasse-diagramokat.

* **8.2.42. Feladat [9].** Olyan disztributív hálót, amelyben minden elemnek van komplementere, *Boole-algebrának* nevezzük.

- (1) Mutassuk meg, hogy disztributív hálóban egy elemnek legfeljebb egy komplementere létezhet.
- (2) Mutassuk meg, hogy Boole-algebrában, a komplementert vesszővel jelölve, $(a \cup b)' = a' \cap b'$ és $(a \cap b)' = a' \cup b'$.
- (3) Mutassuk meg, hogy egy Boole-algebrából az $ab := a \cap b$ és $a + b := (a \cap b') \cup (b \cap a')$ műveletekkel egységelemes Boole-gyűrűt kapunk.

* **8.2.43. Feladat [8].** Mutassuk meg, hogy Boole-gyűrűből az $a \cap b := ab$ és $a \cup b := a + b - ab$ definíciókkal disztributív hálót kapunk, amelyben van nullelem és pontosan akkor van egységelem, ha a gyűrű egységelemes. Ekkor a kapott háló Boole-algebra, és $a' = 1 + a$.

* **8.2.44. Feladat [8].** Mutassuk meg, hogy az alábbi részbenrendezések hálót adnak, és vizsgáljuk meg, hogy mikor van nullelem, egységelem, mikor disztributív a háló, illetve hogy mikor kapunk Boole-algebrát:

- (1) egy rendezett halmaz;
- (2) egy $n \in \mathbb{N}$ szám osztói az oszthatósággal;
- (3) $\mathbb{N}$ az oszthatósággal;
- (4) egy X halmazra $\mathbb{R}^X$ a pontonként kisebb vagy egyenlővel;
- (5) egy X halmazra $[0, 1]^X$ a pontonként kisebb vagy egyenlővel.

* **8.2.45. Feladat [8].** Keressünk az előző feladatban szereplő hálókkal izomorf részhálóját $\mathcal{P}(X)$ -nek az unió- és metszetheképzéssel alkalmas X -re, ha van ilyen.

* **8.2.46. Feladat: Stone tétele [20].** Bizonyítsuk be, hogy minden disztributív háló izomorf valamely X halmazra $\wp(X)$ egy részhálójával, és minden Boole-algebra izomorf valamely X halmazra $\wp(X)$ egy részhálójával, amely tartalmazza X -et és az $\emptyset$ -t.

8.2.47. Mellékosztályok. Legyen R egy gyűrű és legyen I egy additív részcsoporthja R -nek. Vezessük be az $a \sim b$, ha $a - b \in I$ relációt. Tudjuk, hogy ez az összeadással kompatibilis ekvivalenciareláció, az $a \in R$ ekvivalenciaosztálya az $I + a$ halmaz. Az ekvivalenciaosztályokat az R gyűrű I szerinti *mellékosztályainak* vagy *maradékosztályainak* nevezzük.

8.2.48. Tétel. Egy R gyűrű egy I ideál szerinti mellékosztályai a gyűrűnek mindkét művelettel kompatibilis osztályozását alkotják. Minden, mindkét művelettel kompatibilis osztályozás esetén a nulla osztálya ideál, és az osztályozás ezen ideál szerinti mellékosztályokból áll.

Bizonyítás. Ha I ideál, akkor – mivel az összeadással R kommutatív csoport – a csoportelméletből tudjuk, hogy az osztályozás kompatibilis az összeadással, és az osztályok összeadása megegyezik a komplexus összeadással. Az ideáltulajdonságból arra is következtetni tudunk, hogy az osztályozás a szorzással is kompatibilis, hiszen

$$(1) \quad (I + a)(I + b) = II + aI + Ib + ab \subset I + ab.$$

Most tegyük fel, hogy adott egy, az összeadással és a szorzással is kompatibilis ekvivalenciareláció. A csoportoknál tanultakat alkalmazva kapjuk, hogy ez az R valamely I additív részcsoporthoz szerinti ekvivalenciareláció, tehát ez ekvivalenciaosztályok az I szerinti mellékosztályok. Tetszőleges C osztálynak az I osztállyal vett szorzata egy osztály részhalmaza. Ennek tartalmaznia kell a nullát is, mert $0 \in I$, így csak $CI \subset I$ lehetséges. Ez minden C osztályra fennáll, tehát $RI \subset I$. Hasonlóan $IR \subset I$, tehát I ideál. $\square$

8.2.49. Következmény. Egy R gyűrűnek egy I ideál szerinti mellékosztályai az összeadásra és a szorzásra nézve gyűrűt alkotnak.

Bizonyítás. Ha $\sim$ a megfelelő ekvivalenciareláció, akkor $x \mapsto \tilde{x}$ mindkét műveletre nézve művelettartó. $\square$

8.2.50. Faktorgyűrű. Az előző következményben szereplő gyűrűt az R gyűrű I ideál szerinti *maradékosztály-gyűrűjének* (vagy *faktorgyűrűjének*, illetve *hányadosgyűrűjének*) nevezzük, és R/I -vel jelöljük.

8.2.51. Példa. Ha $R = \mathbb{Z}$ és $I = m\mathbb{Z}$, akkor $R/I = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

* **8.2.52. Megjegyzés.** Az előző tétel (1) összefüggésében az egyenlőség általában nem teljesül, tehát a maradékosztályok szorzása nem biztos, hogy megegyezik a komplexusszorzással. Tekintsünk egy példát. Legyen $R = \mathbb{Z}$, $I = 8\mathbb{Z}$, $a = b = 4$, ekkor

$$(I + a)(I + b) = (8\mathbb{Z} + 4)(8\mathbb{Z} + 4) = 64\mathbb{Z}^2 + 32\mathbb{Z} + 32\mathbb{Z} + 16 = 64\mathbb{Z} + 32\mathbb{Z} + 16 \subset 16\mathbb{Z},$$

ami csupa 16-tal osztható számot tartalmaz, viszont $8\mathbb{Z} + 16$ minden 8-cal oszthatót, tehát kapjuk, hogy

$$(8\mathbb{Z} + 4)(8\mathbb{Z} + 4) \subset 16\mathbb{Z} \subsetneq 8\mathbb{Z} + 16.$$

8.2.53. Homomorfizmus magja. Egy R gyűrűnek egy R' gyűrűbe való φ homomorfizmusánál a *homomorfizmus magján* az R' gyűrű nullelemének a teljes inverz képét értjük. A φ magját most is $\ker(\varphi)$ -vel jelöljük.

8.2.54. Homomorfizmus-tétel. Egy R gyűrű egy φ homomorfizmusánál a homomorfizmus magja ideál. Ha R képe R' , akkor az $R/\ker(\varphi)$ maradékosztály-gyűrű izomorf R' -vel. Az R bármely I ideálja magja valamely homomorfizmusnak, például R kanonikus leképezése R/I -re homomorfizmus, amelynek magja I .

Bizonyítás. Azt, hogy a $\varphi^{-1}(a')$, $a' \in R'$ halmazrendszer az R egy, az összeadással kompatibilis osztályozása, tudjuk a csoportelméletből. Ha $a', b' \in R'$, akkor a $\varphi^{-1}(a')$ bármely a elemére és a $\varphi^{-1}(b')$ bármely b elemére $\varphi(ab) = \varphi(a)\varphi(b) = a'b'$, azaz $ab \in \varphi^{-1}(a'b')$, így az osztályozás a szorzással is kompatibilis. Tehát ez az osztályozás egy I ideál szerinti osztályozás. Az ideál a nulla teljes inverz képe. Az $a' \mapsto \varphi^{-1}(a')$ leképezés bijektív és művelettartó, tehát izomorfizmusa R' -nek $R/\ker(\varphi)$ -re.

A tétel második fele az előző tétel 8.2.49 következményének bizonyítása alapján nyilvánvaló. $\square$

A 8.1.2 ábrán látható példa a gyűrűk homomorfizmustételének szemléltetésére is alkalmas: G az egész számok gyűrűje, G' a $\{\uparrow, \downarrow\}$ halmaz az $\oplus$ „kizáró vagy”-gyal mint összeadással és az $\wedge$ „és” művelettel mint szorzással, a φ függvény pedig az $n \mapsto 2|n$ logikai értékű leképezés, így $\ker(\varphi) = 2\mathbb{Z}$. A kanonikus leképezés G -ből $G'/\ker(\varphi)$ -re κ , az izomorfizmus pedig ψ .

8.2.55. Példa. Ha $R = \mathbb{Z}$ és $m \in \mathbb{Z}$, akkor egy egész számhoz a modulo m vett maradékosztályát rendelő leképezés homomorfizmus, amelynek magja $I = m\mathbb{Z}$, képe pedig $R/I = \mathbb{Z}_m$. Tetszőleges R gyűrűre $R/\{0\}$ izomorf R -el, R/R pedig a nulgyűrű.

→ **8.2.56. Feladat [0].** Gyűrűhomomorfizmusok-e az alábbi leképezések? Ha igen, adjuk meg a magjukat:

- (1) $\mathbb{C} \rightarrow \mathbb{R}, x + iy \mapsto x$;
- (2) $R \times R' \rightarrow R \times R, (r, r') \mapsto (r, r)$, ahol R, R' tetszőleges gyűrűk;
- (3) $\mathbb{Z}_n \rightarrow \mathbb{Z}_{2n}, \tilde{m} \mapsto \tilde{m}$, ha $0 \leq m < n$;
- (4) $\mathbb{Z}_{2n} \rightarrow \mathbb{Z}_n, \tilde{m} \mapsto \tilde{m}$, ha $0 \leq m < n$ és $\tilde{m} \mapsto \widetilde{m-n}$, ha $n \leq m < 2n$.

→ **8.2.57. Feladat [2].** Bizonyítsuk be, hogy $\mathbb{Z}_{12}$ -nek a 0, 3, 6, 9 osztályai egy részgyűrűjét alkotják. Ideál-e? Főideál-e? Ha ideál, a faktorgyűrű test-e?

→ **8.2.58. Feladat [2].** Döntsük el, hogy a Gauss-egészek gyűrűjében a megadott halmazok ideált alkotnak-e, és ha igen, határozzuk meg a faktorgyűrűt:

- (1) $\mathbb{Z}$;
- (2) $2\mathbb{Z} + i2\mathbb{Z}$;
- (3) $4\mathbb{Z} + i6\mathbb{Z}$.

→ **8.2.59. Feladat [2].** Igazoljuk, hogy ha $d|n$, akkor $\mathbb{Z}_n$ -nek a d osztálya által generált ideál szerinti faktorgyűrűje izomorf $\mathbb{Z}_{n/d}$ -vel.

→ **8.2.60. Feladat [4].** Az alábbi faktorgyűrűk közül melyek izomorfak: $\mathbb{Z}_4/(\tilde{0})$, $\mathbb{Z}_8/(\tilde{4})$, $\mathbb{Z}_{16}/(\tilde{4})$, $2\mathbb{Z}/(8)$, $2\mathbb{Z}_{16}/(\tilde{8})$, $\mathbb{Z}/(4)$, $4\mathbb{Z}/(16)$.

→ **8.2.61. Feladat [6].** (1) Lehet-e egy nullosztómentes, de nem egységelemes gyűrű faktorgyűrűje egységelemes?

- (2) Lehet-e egy nullosztómentes gyűrű faktorgyűrűje nem nullosztómentes?
- (3) Lehet-e egy nem nullosztómentes gyűrű faktorgyűrűje nullosztómentes?

- **8.2.62. Feladat** [8]. (1) Határozzuk meg a $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_{360}$ gyűrűhomomorfizmusokat.
 (2) Adott $n \in \mathbb{N}$ esetén hány $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_n$ gyűrűhomomorfizmus van?
 (3) Adott $m, n \in \mathbb{N}$ esetén határozzuk meg a $\varphi: \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ gyűrűhomomorfizmusokat.
 (4) Határozzuk meg a $\mathbb{Z}_n$ gyűrű endomorfizmusait és automorfizmusait.

8.2.63. Direkt szorzat. Legyen $G_i, i \in I$ két binér művelettel ellátott halmazok egy indexelt családja. Az egyszerűség kedvéért mindegyik halmazon az első műveletet jelöljük összeadással, a másodikat pedig szorzással. Ekkor a

$$G = \times_{i \in I} G_i$$

Descartes-szorzatot ellátva az $(a + b)_i = a_i + b_i$ és $(ab)_i = a_i b_i$ összefüggéssel definiált műveletekkel, a G -t a G_i család *direkt szorzatának* nevezzük. A direkt szorzat a hatvány általánosítása.

A legfontosabb speciális eset, amikor $I = \{1, 2, \dots, n\}$, ekkor a direkt szorzat elemei $a = (a_1, a_2, \dots, a_n)$, $a_i \in G_i$, ha $i \in I$ alakú n -esek. Mivel az összeadás és a szorzás definíció szerint koordinátánként történik, ha $b = (b_1, b_2, \dots, b_n)$ egy másik eleme a direkt szorzatnak, akkor $a + b = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$ és $ab = (a_1 b_1, a_2 b_2, \dots, a_n b_n)$.

Nilvánvaló, hogy ha minden G_i gyűrű, akkor G is, ha minden G_i kommutatív, akkor G is, ha minden G_i egységelemes, akkor G is, de soha nem test, még csak nem is nullosztómentes, ha I legalább két G_i nem nullgyűrű. Ha $J \subset I$, akkor az $a \mapsto a|_J$ projekció homomorfizmus, képe $\times_{i \in J} G_i$, magja pedig izomorf $\times_{i \in I \setminus J} G_i$ -vel.

* **8.2.64. Példa.** Ha az $n, m \in \mathbb{N}^+$ számok relatív prímek, akkor a kínai maradéktételből kapjuk, hogy a $\mathbb{Z}_m \times \mathbb{Z}_n$ gyűrű izomorf a $\mathbb{Z}_{mn}$ gyűrűvel. Speciálisan $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ izomorf $\mathbb{Z}_{nm}^*$ -gal. Egyébként, mivel $\mathbb{Z}_n^*$ rendje $\varphi(n)$, minden elemének rendje osztja $\varphi(n)$ -et, azaz bármely $a \in \mathbb{Z}_n^*$ -ra $a^{\varphi(n)}$ a $\mathbb{Z}_n^*$ egységeleme; ez Euler tétele.

8.2.65. Tétel. Egy R kommutatív egységelemes gyűrűben az $a \in R$ elem által generált főideálra $(a) = aR$. Speciálisan a nulla által generált főideál $\{0\}$, az egységelem által generált főideál pedig R .

Bizonyítás. A jobb oldalon álló halmaz tartalmazza a -t, és elemei közül nyilván nem vezet ki a kivonás és az R elemeivel való szorzás, így (a) része a jobb oldali halmaznak. Másrészt, ha a benne van egy I ideálban, akkor minden $ar = ra, r \in R$ alakú elem is. $\square$

8.2.66. Következmény. Egy R egységelemes integritási tartomány a, b elemeire

- (1) $(a) \subset (b)$ akkor és csak akkor, ha $b|a$;
- (2) $(a) = (b)$ akkor és csak akkor, ha a és b asszociáltak;
- (3) $(a) = R$ akkor és csak akkor, ha a egység. $\square$

8.2.67. Gauss-gyűrűk. Az egész számok körében az oszthatósággal kapcsolatban nyert eredményeket szeretnénk átvinni gyűrűkre is. Központi szerepet játszik a számelmélet alaptételének megfelelő egyértelmű faktorizáció irreducibilis elemekre. Egy R egységelemes integritási tartományt *Gauss-gyűrűnek* (vagy *egyértelmű faktorizációs tartománynak*) nevezzük, ha minden nullától és egységtől különböző elem sorrendtől és egységektől eltekintve egyértelműen felírható irreducibilis elemek (véges) szorzataként, azaz ha a nem nulla és nem egység, akkor felírható $a = p_1 p_2 \cdots p_n$ alakban, ahol $p_1, p_2, \dots, p_n$

(nem feltétlenül különböző) irreducibilis elemek, és ha $a = q_1 q_2 \cdots q_m$ egy másik előállítás irreducibilis elemek szorzataként, akkor $m = n$, és van olyan $\sigma \in S_n$ permutáció, hogy q_{σ_i} és p_i asszociáltak, ha $i = 1, 2, \dots, n$. Az előállítás felírható

$$a = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

alakban is, ahol ε egység, $p_1, p_2, \dots, p_k$ páronként nem asszociált irreducibilis elemek, a kitevők pedig $\mathbb{N}^+$ (vagy $\mathbb{N}$) elemei. (Ebbe az alakba az egységek is beleférnek, ha $k = 0$.) A felbontásból leolvashatók a osztói, ezek

$$(1) \quad d = \varepsilon' p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

alakúak, ahol ε' egység és $\beta_j \in \mathbb{N}$, $\beta_j \leq \alpha_j$, ha $j = 1, 2, \dots, k$, hiszen ha $a = cd$, akkor c és d irreducibilis tényezőkre való felbontásának szorzata a irreducibilis tényezőkre való felbontása kell hogy legyen. Ha több elemünk van, és mindnek adott az irreducibilis tényezőkre való felbontása, akkor – hasonlóan mint $\mathbb{Z}$ -ben – közös osztóik, valamint közös többszöröseik is leolvashatók, és látjuk, hogy létezik legnagyobb közös osztó és legkisebb közös többszörös.

Egy Gauss-gyűrűben minden irreducibilis elem prímelem, mert ha a nullától és egységtől különböző p irreducibilis elemre $p|ab$, akkor vagy $ab = 0$, amiből valamelyik nulla, vagy pedig $ab = pd$ valamely $d \neq 0$ elemre, amiből d -t felírva (1) alakban, az ab egy olyan előállítását kapjuk irreducibilis elemek szorzataként, amelyben szerepel p . Ha most felírjuk az a és a b felbontását (1) alakban, valamelyikben szerepelnie kell p -nek, mert egyébként ab faktorizációja nem lenne egyértelmű.

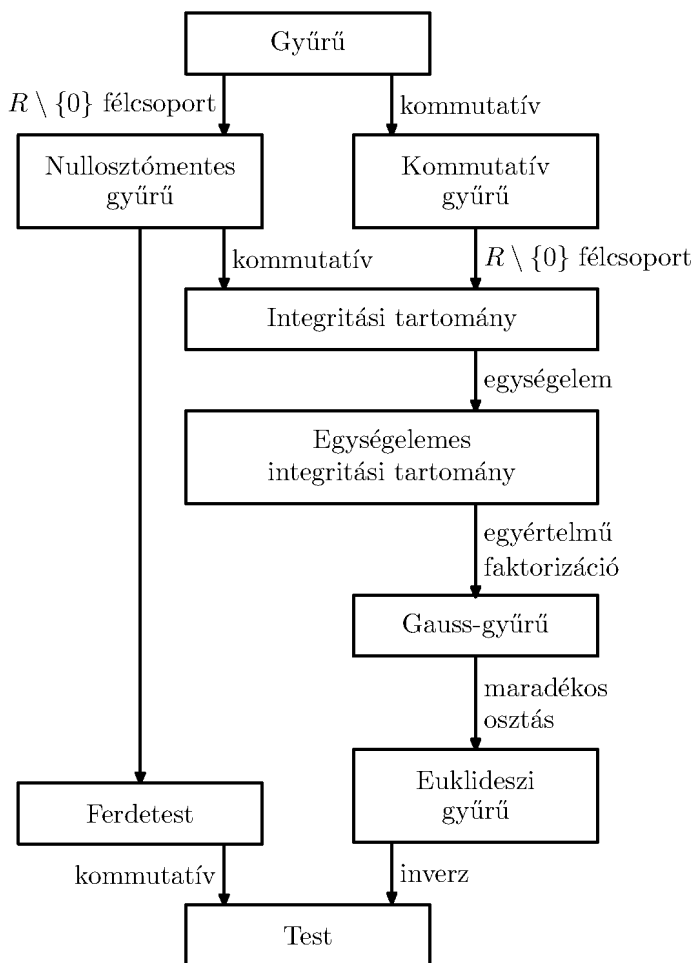
* **8.2.68. Példa.** Vannak olyan egységelemes integritási tartományok, amelyek nem Gauss-gyűrűk. Könnyű látni, hogy az $R = \mathbb{Z} + i\sqrt{5}\mathbb{Z} \subset \mathbb{C}$ halmaz részgyűrűje $\mathbb{C}$ -nek. Minden $c = a + i\sqrt{5}b \in R$, $a, b \in \mathbb{Z}$ -re $|c|^2 = a^2 + 5b^2$ természetes szám, és 5-tel osztva 0, 1 vagy 4 maradékot ad. Mivel $d|c$ esetén az abszolút érték multiplikativitása miatt nyilván $|d|^2 |c|^2$, és az 1 egységelemre $|1|^2 = 1$, az egységek ± 1 . A $9 = 3 \cdot 3 = (2 + \sqrt{5}i)(2 - \sqrt{5}i)$ felbontásokban $|3|^2 = 9$, aminek nincs olyan nem triviális osztója, amelyre 5-tel osztva a maradék 0, 1 vagy 4 lenne. Hasonlóan $|2 \pm \sqrt{5}i|^2 = 9$, így 3 , $2 + \sqrt{5}i$ és $2 - \sqrt{5}i$ irreducibilisek R -ben és nem prímek, valamint az irreducibilis elemekre bontás nem egyértelmű.

8.2.69. Euklideszi gyűrűk. A legegyszerűbb gyűrűk, amelyekről be fogjuk látni, hogy Gauss-gyűrűk, az euklideszi gyűrűk. Egy R egységelemes integritási tartományt *euklideszi gyűrűnek* nevezünk, ha a nem nulla elemein értelmezve van egy $\mathbb{N}$ -beli értékű φ függvény úgy, hogy

- (1) ha $a, b \in R$, $b \neq 0$, akkor van olyan $q, r \in R$, hogy $a = bq + r$ és $r = 0$, vagy $r \neq 0$ és $\varphi(r) < \varphi(b)$;
- (2) $\max\{\varphi(a), \varphi(b)\} \leq \varphi(ab)$ minden $a, b \in R$, $a \neq 0$, $b \neq 0$ esetén.

(Tulajdonképpen az (R, φ) párt kellene euklideszi gyűrűnek neveznünk.) Megfigyelhetjük, hogy φ az egész számok körében az abszolút érték által játszott szerepet általánosítja: $\mathbb{Z}$ az $n \mapsto |n|$ függvénnyel nyilván euklideszi gyűrű. Mint ez a példa is mutatja, a definícióban szereplő r általában nem egyértelmű: itt például lehet a legkisebb nemnegatív maradék, a legkisebb abszolút értékű maradék, stb.

Sok más példa is adható. A legfontosabb a test feletti egyhatározatlanú polinomok gyűrűje, ahol φ a fokszám; ezzel részletesen foglalkozni fogunk. A polinomoknál olyan gyűrűre is látunk majd példát, amely Gauss-gyűrű, de nem tehető euklideszi gyűrűvé.



8.2.1 ábra: Kétműveletes algebrai struktúrák.

8.2.70. Állítás. *Euklideszi gyűrűben pontosan azok az elemek az egységek, amelyekre φ minimális értéket vesz fel. Az a, b nem nulla elemekre $b|a$ esetén egyrészt $\varphi(b) \leq \varphi(a)$, másrészt egyenlőség pontosan akkor teljesül, ha a és b asszociáltak.*

Az nem igaz (példát majd a test feletti polinomok adnak), hogy ha $\varphi(b) = \varphi(a)$, akkor a és b asszociáltak.

Bizonyítás. Ha $\varphi(\varepsilon)$ minimális, akkor az e egységelemet osztva ε -nal, az r maradék csak nulla lehet, így ε egység. Ha $b|a$, akkor a (2) tulajdonság miatt $\varphi(b) \leq \varphi(a)$. Ha ε egység, $a \in R$ pedig olyan elem, amelyre $\varphi(a)$ minimális, akkor $\varepsilon|a$ miatt $\varphi(\varepsilon)$ is minimális. Ha a és b asszociáltak, akkor $\varphi(a) \leq \varphi(b)$, és fordítva is. Végül tegyük fel, hogy $b|a$ és $\varphi(b) = \varphi(a)$. Felírva b -t $aq + r$ alakban, meg kell mutatnunk, hogy $r \neq 0$ lehetetlen. Mivel $r = b - aq = b + bc(-q) = b(e - cq)$, azt kapnánk, hogy $\varphi(r) \geq \varphi(b)$, ami ellentmondás.

□

8.2.71. Példa: Gauss-egészek. A komplex síkbeli egységnyezetrács elemei, azaz a $G = \mathbb{Z} + i\mathbb{Z} = \{n + im : n, m \in \mathbb{Z}\} \subset \mathbb{C}$ halmaz elemei, az úgynevezett Gauss-egészek euklideszi gyűrűt alkotnak a $\varphi(z) = |z|^2$ függvénnyel. Az, hogy (2) fennáll, következik abból, hogy szorzat abszolút értéke az abszolút értékek szorzata. A másik tulajdonság belátásához jelölje q a G halmaz a/b -hez legközelebbi (egyik) elemét. Ekkor $|a/b - q|^2 < 1$, mivel az abszolút érték legfeljebb $\sqrt{1/2}$. Innen $|b|^2|a/b - q|^2 < |b|^2$, azaz $|a - bq|^2 < |b|^2$, tehát (1) teljesül. Az egységek nyilván ± 1 és $\pm i$.

8.2.72. Feladat [7]. Tegyük fel, hogy $\alpha \in \mathbb{C} \setminus \mathbb{Q}$ olyan szám, amelyre $\alpha^2 + k\alpha + \ell = 0$, azaz $\alpha^2 = -k\alpha - \ell$ valamely k, ℓ egészekkel. Ekkor $\mathbb{Z}[\alpha]$ -beli oszthatóság vizsgálatához hasznos lesz a $\varphi(x + y\alpha) = |x^2 + kxy + \ell y^2|$, ha $x, y \in \mathbb{Z}$ függvény. Mutassuk meg, hogy

- (1) $\varphi(z) = 0$ pontosan akkor, ha $0 = z \in \mathbb{Z}[\alpha]$;
- (2) $\varphi(zw) = \varphi(z)\varphi(w)$, ha $z, w \in \mathbb{Z}[\alpha]$;
- (3) $z \in \mathbb{Z}[\alpha]$ pontosan akkor egység, ha $\varphi(z) = 1$;
- (4) ha α nem valós, akkor $\varphi(z) = |z|^2$.

8.2.73. Feladat [11]. Mutassuk meg, hogy $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$ és $\mathbb{Z}[(1 + \sqrt{5})/2]$ euklideszi gyűrűk az előző feladatban megadott φ függvénnyel, és hogy $\mathbb{Z}[\sqrt{2}]$ -ben végtelen sok egység van. Keressünk más valós számokat, amelyekre $\mathbb{Z}[\alpha]$ a megadott φ függvénnyel euklideszi gyűrű.

8.2.74. Feladat [10]. Mutassuk meg, hogy $\mathbb{Z}[i\sqrt{2}]$, $\mathbb{Z}[(1 + i\sqrt{3})/2]$, $\mathbb{Z}[(1 + i\sqrt{7})/2]$ és $\mathbb{Z}[(1 + i\sqrt{11})/2]$ euklideszi gyűrűk a $\varphi(z) = |z|^2$ függvénnyel. Mindegyikben határozzuk meg az egységeket.

8.2.75. Bővített euklideszi algoritmus. A következő eljárás egy R euklideszi gyűrűben meghatározza az $a, b \in R$ elemek egy d legnagyobb közös osztóját, valamint az $x, y \in R$ elemeket úgy, hogy $d = ax + by$ teljesüljön. (Az eljárás során végig $ax_n + by_n = r_n$, $n = 0, 1, \dots$)

- (1) [Inicializálás.] Legyen $x_0 \leftarrow e$, a gyűrű egységeleme, $y_0 \leftarrow 0$, $r_0 \leftarrow a$, $x_1 \leftarrow 0$, $y_1 \leftarrow e$, $r_1 \leftarrow b$, $n \leftarrow 0$.
- (2) [Vége?] Ha $r_{n+1} = 0$, akkor $x \leftarrow x_n$, $y \leftarrow y_n$, $d \leftarrow r_n$, és az eljárás véget ért.
- (3) [Ciklus.] Legyen $r_n = q_{n+1}r_{n+1} + r_{n+2}$, ahol $r_{n+2} = 0$ vagy $\varphi(r_{n+2}) < \varphi(r_{n+1})$, legyen $x_{n+2} \leftarrow x_n - q_{n+1}x_{n+1}$, $y_{n+2} \leftarrow y_n - q_{n+1}y_{n+1}$, $n \leftarrow n + 1$, és menjünk (2)-re.

Bizonyítás. Mivel a $\varphi(r_1), \varphi(r_2), \dots$ természetes számok szigorúan monoton csökkenő sorozata, az eljárás véget ér, mert egyébként $\mathbb{N}$ nem lenne jólrendezett. Indukcióval $ax_n + by_n = r_n$, így $d = ax + by$. Innen a és b közös osztói mind osztói d -nek. Mivel $r_{n+1} = 0$, vagy $n = 0$, és ekkor $d = a$ és $b = 0$, vagy pedig $n > 0$, és $r_{n-1}, r_{n-2}, \dots, r_1, r_0$ mind többszörösei r_n -nek, mert $r_{n-1} = q_n r_n$, $r_{n-2} = q_{n-1} r_{n-1} + r_n$, és így tovább, speciálisan $a = r_0$ és $b = r_1$ többszörösei d -nek, tehát d legnagyobb közös osztó. $\square$

8.2.76. Tétel. Egy euklideszi gyűrű egy eleme pontosan akkor felbonthatatlan, ha prímelem.

Bizonyítás. Az egyik irányt már általánosan is beláttuk. Tegyük fel, hogy p felbonthatatlan, és legyen $p|ab$. Tegyük fel, hogy $p \nmid a$. Ekkor p és a legnagyobb közös osztói csak az egységek. A bővített euklideszi algoritmussal kaphatunk olyan x, y elemeket, hogy

$px + ay = \varepsilon$ egység. Szorozva b -vel és ε multiplikatív inverzével, $pbx\varepsilon^{-1} + aby\varepsilon^{-1} = b$. Mivel p osztója a bal oldalnak, a jobb oldalnak is. $\square$

8.2.77. Tétel. *Euklideszi gyűrű minden nem nulla és nem egység eleme sorrendtől és asszociáltságtól eltekintve egyértelműen felírható felbonthatatlan elemek szorzataként, azaz euklideszi gyűrű Gauss-gyűrű.*

Bizonyítás. Először a felbontás létezését bizonyítjuk. Ha az adott a elem nem irreducibilis, akkor 8.2.70 szerint felírható két olyan, mondjuk b és c elem szorzataként, amelyekre $\max\{\varphi(b), \varphi(c)\} < \varphi(a)$. Indukcióval folytatjuk ezt az eljárást: ha a kapott szorzatnak van reducibilis tényezője, akkor ezekből kiválasztva egy olyat, amelyre φ maximális, azt helyettesítsük két tényező szorzatával. Minden lépésben vagy a maximális φ érték csökken, vagy azon tényezők száma, amelyekre a maximális φ érték vétetik fel, ha több ilyen volt. Az eljárás a természetes számok jólrendezettsége miatt véges sok lépésben csupa irreducibilis tényezőből álló felbontáshoz vezet.

A felbontás egyértelműségének bizonyításához tegyük fel, hogy van olyan a , amely két lényegesen különböző módon bontható fel, és legyen a olyan ezek közül, amelyre $\varphi(a)$ minimális:

$$a = p_1 p_2 \cdots p_j = q_1 q_2 \cdots q_k.$$

Mivel $p_1 | a$, azaz $p_1 | q_1 q_2 \cdots q_k$, van olyan i , hogy $p_1 | q_i$. Ekkor viszont p_1 és q_i asszociáltak, mert q_i irreducibilis. Egyszerűsítve a közös tényezővel egy olyan a' elemet kapnánk, amelyre $\varphi(a') < \varphi(a)$, és felbontása nem egyértelmű. $\square$

* **8.2.78. Tétel.** *Euklideszi gyűrűben minden ideál főideál.*

Bizonyítás. Legyen R euklideszi gyűrű, I pedig egy ideálja. Ha $I = \{0\}$, akkor $I = (0)$. Egyébként legyen a az I egy olyan eleme, amelyre $\varphi(a)$ minimális. Mivel $(a) \subset I$, csak a fordított tartalmazást kell megmutatni. Ha valamely $b \in I$ nem lenne többszöröse a -nak, akkor maradékos osztással egy olyan $r \in I$ elemet kapnánk, amelyre $\varphi(r) < \varphi(a)$. $\square$

* **8.2.79. Feladat [13].** Mutassuk meg, hogy $\mathbb{Z}[(1+i\sqrt{19})/2]$ főideálgyűrű, azaz benne minden ideál főideál, de a $\varphi(z) = |z|^2$ függvénnyel nem euklideszi gyűrű.

* **8.2.80. Definíció.** Egy R gyűrű egy I valódi ideálját *maximális ideálnak* nevezzük, ha nincs nála bővebb valódi ideál, azaz ha a valódi ideálok között a tartalmazásra nézve maximális.

* **8.2.81. Következmény.** *Egy euklideszi gyűrű egy nem triviális ideálja pontosan akkor maximális, ha egy irreducibilis elem generálja.*

Bizonyítás. Ha $I = (a)$ maximális, akkor a nem nulla és nem egység, valamint semmilyen b sem lehet nem triviális osztója, mert erre $(a) \subsetneq (b) \subsetneq R$ teljesülne. Megfordítva, ha a irreducibilis, akkor $(0) \subsetneq (a) \subsetneq R$, és ha egy I ideálra $(a) \subsetneq I \subsetneq R$, akkor annak b generátorára $b|a$, de b nem egység és nem is asszociáltja a -nak, ami lehetetlen. $\square$

* **8.2.82. Tétel.** *Legyen R kommutatív egységelemes gyűrű, I az R egy ideálja. Az R/I faktorgyűrű akkor és csak akkor test, ha I maximális ideál.*

Bizonyítás. Először tegyük fel, hogy I maximális ideál, és tekintsük R/I egy nem nulla $I + a$ elemét, azaz legyen $a \notin I$. Az $S = \{x + ay : x \in I, y \in R\}$ halmaz nyilván ideál. Mivel I valódi része S -nek, $S = R$, így alkalmas $x \in I$ -re és $y \in R$ -re $e = x + ay$. Ez azt jelenti, hogy $\tilde{e} = I + e = I + x + ay = I + ay \supset (I + a)(I + y)$, azaz a kapott y osztálya R/I -ben a osztályának inverze.

Megfordítva, tegyük fel, hogy R/I test, S pedig olyan ideál, amely valódi módon tartalmazza I -t, azaz létezik olyan a , amelyre $a \in S$ de $a \notin I$. Mivel R/I test, az $\tilde{a}\tilde{x} = \tilde{b}$ egyenlet bármely $b \in R$ -re megoldható, azaz van olyan $x \in R$, hogy $I + ax = I + b$. De $I + ax \subset S$, így $b \in S$. Mivel b tetszőleges, $S = R$. $\square$

* **8.2.83. Definíció.** Egy R gyűrű egy I ideálját *prímideálnak* nevezzük, ha $ab \in I$ esetén $a \in I$ vagy $b \in I$. Euklideszi gyűrűben ez azt jelenti, hogy az ideál generátorai prímelemek.

* **8.2.84. Tétel.** Legyen R kommutatív egységelemes gyűrű, I az R egy ideálja. Az R/I faktorgyűrű akkor és csak akkor integritási tartomány, ha I az R egy valódi prímideálja.

Bizonyítás. Maradékosztályokra áttérve az, hogy I prímideál, azzal ekvivalens, hogy $\tilde{a}\tilde{b} = \tilde{0}$ esetén $\tilde{a} = \tilde{0}$ vagy $\tilde{b} = \tilde{0}$, amiből következik az állítás; az $I \neq R$ feltétel azt zárja ki, hogy R/I zérógyűrű legyen. $\square$

* **8.2.85. Következmény.** Kommutatív egységelemes gyűrűben minden maximális ideál prímideál.

Bizonyítás. Test integritási tartomány is. $\square$

* **8.2.86. Tétel.** Egy kommutatív egységelemes egyszerű gyűrű akkor és csak akkor test, ha nem nullgyűrű.

Bizonyítás. Ha van olyan $a \neq 0$ elem, amely nem invertálható, akkor az $(a) = aR$ főideál nem tartalmazza az egységelemet, így R -nek van nem triviális ideálja. Megfordítva, ha R test, $I \neq \{0\}$ egy ideál, $a \in I$, $a \neq 0$, akkor bármely $b \in R$ -re $b = aa^{-1}b \in I$, tehát $I = R$. $\square$

8.2.87. Hányadostest. Legyen R a nullgyűrűtől különböző integritási tartomány. Az $R \times (R \setminus \{0\})$ halmazon vezessük be az $(a, b) \sim (a', b')$, ha $ab' = a'b$ ekvivalenciarelációt, az $(a, b) + (a', b') = (ab' + a'b, bb')$ összeadást és az $(a, b)(a', b') = (aa', bb')$ szorzást. A műveletek kompatibilisek az ekvivalenciarelációval, és az ekvivalenciaosztályok testet alkotnak, amelyet az R hányadostestének nevezünk.

A bizonyítás ugyanaz, mint a racionális számok bevezetésénél.

* **Bizonyítás.** Triviális, hogy $\sim$ reflexív és szimmetrikus. Ha $(a, b) \sim (a', b')$ és $(a', b') \sim (a'', b'')$, akkor $ab' = ba'$ és $a'b'' = b'a''$. A két összefüggést összeszorozva $aa'b'b'' = ba'b'a''$. Ha $a' \neq 0$, akkor $a'b'' \neq 0$, így egyszerűsítve azt kapjuk, hogy $ab'' = ba''$, azaz $(a, b) \sim (a'', b'')$. Ha $a' = 0$, akkor $b' \neq 0$ miatt $a = 0$ és $a'' = 0$, és ekkor is $(a, b) \sim (a'', b'')$.

Az összeadás kompatibilis az ekvivalenciarelációval, mert ha $(a, b) \sim (a', b')$, akkor $ab' = ba'$, amiből $ab'b''b'' = ba'b''b''$, innen viszont

$$\begin{aligned}(ab'' + ba'')b'b'' &= ab'b''b'' + ba'a''b'' = ba'b''b'' + ba'a''b'' \\ &= (a'b'' + b'a'')bb'',\end{aligned}$$

tehát

$$(a, b) + (a'', b'') = (ab'' + ba'', bb'') \sim (a'b'' + b'a'', b'b'') = (a', b') + (a'', b''),$$

és a párok összeadása triviálisan kommutatív, így elég ezt belátni. Mivel a párok összeadása könnyen kiszámolhatóan asszociatív is, az ekvivalenciosztályok összeadása is kommutatív és asszociatív. A $(0, b)$ alakú párok halmaza nullelem, ezt jelöljük nullával. Az (a, b) pár osztályának additív inverze a $(-a, b)$ pár osztálya. Így $R \times (R \setminus \{0\})$ ekvivalenciosztályainak halmaza az összeadással Abel-csoport.

A szorzás is kompatibilis az osztályozással, mert ha $(a, b) \sim (a', b')$, akkor $ab' = ba'$, amiből $aa''b'b'' = ba'a''b''$, így

$$(a, b) \cdot (a'', b'') = (aa'', bb'') \sim (a'a'', b'b'') = (a', b') \cdot (a'', b'').$$

Mivel a párok szorzása láthatóan kommutatív, beláttuk a szorzás kompatibilitását az osztályozással. Mivel a párok szorzása asszociatív is, az osztályoké is asszociatív. Egyszerű számolás mutatja, hogy $(a, b) \cdot ((a'b') + (a''b''))$ és $(a, b) \cdot (a'b') + (a, b) \cdot (a''b'')$ ekvivalens párok, így az osztályok szorzása disztributív. Ezzel beláttuk, hogy $R \times (R \setminus \{0\})$ ekvivalenciosztályainak halmaza kommutatív gyűrű. A (b, b) alakú párok halmaza a multiplikatív egységelem az osztályok halmazában. Ha $(a, b) \approx (0, b')$, akkor $a \neq 0$, ekkor viszont az (a, b) pár osztályának multiplikatív inverze a (b, a) pár osztálya. Ezzel a bizonyítást befejeztük. $\square$

8.2.88. Következmény. Az előző tétel jelöléseivel, az R integritási tartomány beágyazható a hányadostestébe: bármely rögzített $b \neq 0$ -ra $x \in R$ -hez a (bx, b) osztályát rendelve ugyanazt a monomorfizmust kapjuk. $\square$

* **8.2.89. Algebrai struktúrák.** Nem csak egy vagy két műveletet tekinthetünk egy halmazon, hanem tetszőlegesen sokat, és ezek nem csak nullér, unér és binér műveletek lehetnek, hanem akárhány változósak (például a vegyes szorzás ternér művelet). Így az *algebrai struktúra* általános fogalmához jutunk. Számos fogalom és konstrukció (részstruktúra, faktorstruktúra, direkt szorzat, stb.) átvihető tetszőleges algebrai struktúrákra is, de ezzel itt nem foglalkozunk.

→ **8.2.90. Feladat [3].** Határozzuk meg a $\mathbb{Z}_m$ hányadostestét.

→ **8.2.91. Feladat [3].** Határozzuk meg a Gauss-egészek hányadostestét.

→ **8.2.92. Feladat [5].** Adjunk meg a $\mathbb{Z}[\sqrt{5}]$ integritási tartományban a ± 1 elemektől különböző egységeket.

→ **8.2.93. Feladat [7].** Az $R = \{m/n : m, n \in \mathbb{Z}, 2 \nmid n\}$ integritási tartományra

(1) mutassuk meg, hogy Gauss-gyűrű;

(2) adjunk meg olyan függvényt, amellyel euklideszi gyűrű.

→ **8.2.94. Feladat [5].** Legyen x és y egy Gauss-gyűrű két, egymáshoz relatív prím eleme. Mutassuk meg, hogy ha az xy szorzat egy elem négyzetének az asszociáltja, akkor x és y is az.

8.2.95. Feladat [7]. Egy testet *prímtestnek* nevezünk, ha nincs valódi részteste. Mutassuk meg, hogy bármely test összes résztesteinek a metszete prímtest. Határozzuk meg az összes prímtestet.

8.2.96. Feladat [7]. Mutassuk meg, hogy a $\{p + q\sqrt{2} : p, q \in \mathbb{Q}\}$ gyűrűnek két automorfizmusa van: az identitás és a $\varphi(p + q\sqrt{2}) = p - q\sqrt{2}$ leképezés.

8.2.97. Feladat [7]. Határozzuk meg a $\{p + q\sqrt[3]{2} + r\sqrt[3]{4} : p, q, r \in \mathbb{Q}\}$ gyűrű automorfizmusait.

8.2.98. További feladatok. [3]: II.10, II.11, V.1–V.3, V.5–V.7, V.9–V.44, V.47, V.52, V.54–V.74, V.76, V.77, V.78, V.80–V.108, V.111–V.119, V.121–V.124, V.128–V.140, V.145, V.151–V.153, V.155–V.157, V.162, V.164, V.166–V.170, V.172–V.180, V.184–V.189, V.193–V.195, V.197–V.203, VI.1; [57]: 1.1-1.–1.1-4; [69]: 2.11.13–2.11.26; [83]: VII.5.5, VII.5.8, VII.5.18, XIII.3.3.

8.3 Polinomok

8.3.1. Polinomok. Legyen R gyűrű. Az (egyhatározatlanú) polinomokról az az elképzelésünk, hogy $\sum_{i=0}^n f_i x^i$ alakú véges összegek, ahol x a „határozatlan”, $n \in \mathbb{N}$, $f_i \in R$, ha $0 \leq i \leq n$, az összeadás és szorzás pedig tagonként történik. A definíció könnyen pontosá tehető az alábbi módon: ha $f = (f_0, f_1, \dots)$ és $g = (g_0, g_1, \dots)$ is R -beli végtelen sorozatok, azaz $R^{\mathbb{N}}$ elemei, akkor összegüket az $f + g = (f_0 + g_0, f_1 + g_1, \dots)$ sorozatként, szorzatukat pedig azon $h = (h_0, h_1, \dots)$ sorozatként definiálva, amelyre

$$h_k = \sum_{i=0}^k f_i g_{k-i} = \sum_{j=0}^k f_{k-j} g_j = \sum_{i+j=k} f_i g_j,$$

könnyen ellenőrizhető, hogy egy gyűrűt kapunk. Nyilván, ha R kommutatív, akkor ez a gyűrű is kommutatív, ha R egységelemes az 1 egységelemmel, akkor a sorozatok gyűrűje is az, benne az $(1, 0, 0, \dots)$ sorozat egységelem. Végül, ha az R gyűrű nullosztómentes, akkor a sorozatok gyűrűje is, mivel ha m , illetve n a legkisebb index, amelyre $f_m \neq 0$, illetve $g_n \neq 0$, akkor $h_{m+n} = f_m g_n \neq 0$.

Az R feletti *egyhatározatlanú polinomokon* olyan R -beli $f = (f_0, f_1, \dots)$ sorozatokat értünk, amelyeknek csak véges sok tagja nem nulla, a fenti műveletekkel; vegyük észre, hogy ha $i > m$ esetén $f_i = 0$, és $j > n$ esetén $g_j = 0$, akkor $k > m + n$ esetén a $h_k = \sum_{i+j=k} f_i g_j$ összegnek minden tagja nulla, így polinomok szorzata polinom és nyilván polinomok összege is polinom, azaz a polinomok a fenti gyűrűnek részgyűrűjét alkotják.

Nyilvánvaló, hogy az $a \mapsto (a, 0, 0, \dots)$ leképezés R -nek a polinomok gyűrűjébe való monomorfizmusa, értékészletének elemei a *konstans polinomok*, ezeket R elemeivel azonosíthatjuk.

A továbbiakban az $f = (f_0, f_1, \dots, f_n, 0, 0, \dots)$ polinomot kényelmi okokból a szokásos $f = f_0 x^0 + f_1 x^1 + f_2 x^2 + \dots + f_n x^n$ alakba írjuk. Ez a jelölés emlékeztet arra, hogy a műveleteket hogyan kell elvégezni. Általában x^0 -t nem írjuk ki, x^1 helyett pedig x -et írunk, így az $f_0 + f_1 x + f_2 x^2 + \dots + f_n x^n$ alakot kapjuk. Az f_i neve az i -ed fokú *tagegyütthatója*. A nulladfokú tag együtthatója a polinom *konstans tagja*. Az $f = f_0 + f_1 x + f_2 x^2 + \dots + f_n x^n$ felírásból a nulla együtthatójú tagokat szokás elhagyni,

illetve a felírásához további nulla együtthatójú tagok adhatók hozzá, így a felírás nem egyértelmű. Egyértelművé válik azonban, ha kikötjük, hogy $f_n \neq 0$ legyen, és minden n -nél alacsonyabb fokú tag is szerepeljen. Ekkor f_n a polinom *főegyütthatója*, n pedig a polinom *foka*, jelölése $\deg(f)$. (Egy másik lehetőség a felírás egyértelművé tételére, hogy minden nulla együtthatójú tagot elhagyunk.)

A nulla polinom egyértelmű felírása az üres összeg, nincs főegyütthatója és fokát a $-\infty$ szimbólumnak definiáljuk. A konstans polinomok a legfeljebb nulladfokú polinomok. A legfeljebb elsőfokú polinomok a *lineáris polinomok*. Azokat a polinomokat, amelyek $f_i x^i$ alakba írhatók, *monomoknak* nevezzük.

Az R feletti egyháthatározatlanú polinomok gyűrűjét $R[x]$ -szel jelöljük. Természetesen x helyett bármilyen más betű is szerepelhet. Néha egy $f \in R[x]$ polinomra inkább az $f(x)$ jelölést fogjuk használni.

Ha R egységelemes az 1 egységelemmel, akkor az $f_i x^i$ tag helyett $f_i = 1$ esetén x^i -t szokás írni. Speciálisan $x = (0, 1, 0, 0, \dots)$, és indukcióval kapjuk, hogy ha $n \in \mathbb{N}$, akkor x^n olyan sorozat, amelyben az n indexű tag az 1 egységelem, az összes többi tag pedig nulla. Ha egy polinom főegyütthatója R egységeleme, akkor *főpolinomnak* (vagy *normált polinomnak*) nevezzük.

Ha az R gyűrű nullosztómentes, akkor két nem nulla polinom szorzatának a főegyütthatója a főegyütthatók szorzata, foka pedig a fokok összege: ha $f = \sum_{i=0}^m f_i x^i$, $f_m \neq 0$, $g = \sum_{i=0}^n g_i x^i$, $g_n \neq 0$, $h = fg$, akkor a $h_k = \sum_{i+j=k} f_i g_j$ összegnek $k = m + n$ esetén egyetlen nem nulla tagja van, $f_m g_n$. Tehát h nem nulla polinom, így $R[x]$ is nullosztómentes. (Egyébként mivel a nulla polinom fokát $-\infty$ -nek választottuk, $\deg(fg) = \deg(f) + \deg(g)$ mindig teljesül.) Mivel R izomorf a konstans polinomok részgyűrűjével, $\text{char}(R) = \text{char}(R[x])$, hiszen minden nem nulla elemnek ugyanannyi az additív rendje.

Figyeljük meg, hogy a polinomok definíciója lényegében megfelel a számítógépes tárolási módjuknak, azzal az eltéréssel, hogy nyilván nem tárolhatunk végtelen sok nullát: vagy az n fokszámot és az együtthatók $f_0, f_1, \dots, f_n$ tömbjét tároljuk, vagy a nem nulla együtthatókra az (i, f_i) párok egy láncolt listáját.

*** 8.3.2. Formális hatványsorok.** Ha R egy gyűrű, akkor az R -beli végtelen sorozatok gyűrűjét az előző definícióban definiált műveletekkel $R[[x]]$ -szel jelöljük, elemeit *formális hatványsoroknak* nevezzük, és az $f = (f_0, f_1, \dots)$ elemet $\sum_{i=0}^{\infty} f_i x^i$ alakban írjuk.

→ **8.3.3. Feladat [0].** Adjuk meg $\mathbb{Z}_{72}$ fölött $8x^2 + 12$ és $18x + 36$ szorzatát.

→ **8.3.4. Feladat [2].** Határozzuk meg $\mathbb{H}$ felett az $f = (3 + 2i - j + 5k)x^2 - (2 - 3i + k)$ és $g = 2ix - (4 - 5k)$ polinomokra $fg - gf$ -et.

→ **8.3.5. Feladat [2].** Határozzuk meg a $\mathbb{Z}$ feletti $3x^8 + 5x^6 - 11x^3 + 7x^2 - 15x + 8$ és $16x^7 - 13x^6 + 6x^3 - 13x + 21$ polinomok szorzatában a 0-ad, 9-ed, 14-ed, 15-öd és 20-ad fokú tag együtthatóját!

→ **8.3.6. Feladat [2].** Oldjuk meg az előző feladatot $\mathbb{Z}_{24}$ felett. Mennyi a szorzatpolinom fokszáma?

8.3.7. Polinomfüggvények. A polinomok definíciójánál használt jelölésekkel egy $f = f_0 + f_1 x + \dots + f_n x^n$ polinomnak az $r \in R$ helyen felvett *helyettesítési értékén* az $f(r) = f_0 + f_1 r + \dots + f_n r^n \in R$ elemet értjük. Ha f helyettesítési értéke az r helyen nulla, akkor azt mondjuk, hogy r az f *gyöke*. Az $r \mapsto f(r)$ leképezést az f polinomhoz tartozó

polinomfüggvénynek hívjuk. Felhívjuk a figyelmet arra, hogy a polinomokat nem R -en értelmezett függvényként definiáltuk, tehát a polinomok nem R -en értelmezett függvények. (Szokás megkülönböztetésként az f polinomhoz tartozó polinomfüggvényt például f -vel jelölni.)

A megkülönböztetés azért fontos, mert előfordulhat, hogy két különböző polinomhoz ugyanaz a polinomfüggvény tartozik. Például, ha az R gyűrű véges, de nem a nullgyűrű, akkor végtelen sok polinom van $R[x]$ -ben, míg csak véges sok R -et R -be képező függvény létezik. Konkrétabban, ha p prímszám, $R = \mathbb{Z}_p$, akkor a Fermat-tétel szerint bármely $n \in \mathbb{Z}$ -re $n^p \equiv n \pmod{p}$, azaz minden $r \in \mathbb{Z}_p$ -re $r^p = r$, így a $\mathbb{Z}_p$ feletti x^p és x polinomokhoz ugyanaz a polinomfüggvény tartozik.

A később bizonyítandó tételekből azonban az következni fog, hogy ha R végtelen egységelemes integritási tartomány, akkor $R[x]$ két különböző eleméhez nem tartozik ugyanaz a polinomfüggvény. Ekkor a polinomokat azonosíthatjuk a polinomfüggvényekkel.

Megjegyezzük, hogy ha R kommutatív egységelemes gyűrű, akkor bármely $c \in R$ -re a $\vartheta_c: f \mapsto f(c)$ leképezése $R[x]$ -nek R -re epimorfizmus.

8.3.8. A maradékos osztás tétele polinomokra. Legyen R egységelemes integritási tartomány, $f, g \in R[x]$, $g \neq 0$, és tegyük fel, hogy g főegyütthatója egység R -ben. Ekkor egyértelműen léteznek olyan $q, r \in R[x]$ polinomok, amelyekre $f = gq + r$, ahol $\deg(r) < \deg(g)$.

Vegyük észre, hogy főpolinommal lehet maradékosan osztani.

Bizonyítás. Először q és r létezését bizonyítjuk a fokszám szerinti indukcióval. Ha $\deg(f) < \deg(g)$, akkor $q = 0$ és $r = f$ választható. Indukcióval, ha f főegyütthatója f_n , a g főegyütthatója pedig g_k , legyen $f^* = f - f_n g_k^{-1} g x^{n-k}$. Mivel $\deg(f^*) < \deg(f)$, az indukciós feltevés szerint $f^* = gq^* + r^*$, ahonnan $r = r^*$, $q = f_n g_k^{-1} x^{n-k} + q^*$ választással kapjuk az előállítást.

Az egyértelműség onnan következik, hogy $gq + r = gq^* + r^*$ esetén $g(q - q^*) = r^* - r$; innen, ha valamelyik oldal nem nulla, akkor a másik sem, de a bal oldal fokszáma legalább $k = \deg(g)$, a jobb oldal fokszáma pedig ennél kisebb. $\square$

8.3.9. Következmény: gyöktényező leválasztása. Ha $f \neq 0$ és c az f gyöke, akkor valamely $q \neq 0$ polinomra $f = (x - c)q$.

Bizonyítás. A maradékos osztás tételét alkalmazva $g = x - c$ választással $f = (x - c)q + r$. Ha $r \neq 0$ lenne, akkor $\deg(r) = 0$ miatt a c helyen az egyik oldal helyettesítési értéke nulla, a másiké nem nulla lenne. $\square$

8.3.10. Következmény. Ha $f \neq 0$, akkor f -nek legfeljebb $\deg(f)$ gyöke van.

Mint látni fogjuk, R kommutativitása és nullosztómentessége is szükséges.

Bizonyítás. A fokszám szerinti indukcióval dolgozunk. Ha $\deg(f) = 0$, igaz az állítás. Ha $\deg(f) > 0$, és c egy gyök, akkor $f = (x - c)g$, ahol $1 + \deg(g) = \deg(f)$. Ha d az f egy gyöke, akkor vagy $d - c = 0$, azaz $d = c$, vagy d gyöke g -nek, ahonnan következik az állítás. $\square$

8.3.11. Következmény. Ha két, legfeljebb n -ed fokú polinom $n + 1$ különböző helyen ugyanazt az értéket veszi fel, akkor megegyezik.

Bizonyítás. Egyébként a különbségpolinom olyan legfeljebb n -ed fokú nem nulla polinom lenne, amelynek $n + 1$ gyöke van. $\square$

8.3.12. Következmény. Ha R végtelen, akkor két különböző polinomhoz nem tartozik ugyanaz a polinomfüggvény.

Bizonyítás. Egyébként a különbségpolinomnak végtelen sok gyöke lenne. $\square$

8.3.13. Következmény. Ha R test, akkor a $0 \neq f \mapsto \deg(f)$ függvénnyel $R[x]$ euklideszi gyűrű.

Bizonyítás. Testben minden nem nulla elem egység, így minden nem nulla g -re alkalmazható az előző tétel, továbbá ha f, g nem nulla polinomok, akkor $\deg(fg) = \deg(f) + \deg(g) \geq \max\{\deg(f), \deg(g)\}$. $\square$

8.3.14. Megjegyzés. Vegyük észre, hogy a maradékos osztás tétele algoritmust is ad a maradékos osztás elvégzésére. Ez az algoritmus annak eldöntésére is alkalmazható, hogy g osztója-e f -nek. Ha ugyanis $f = gh$, akkor h főegyütthatója az az egyetlen R -beli h_{n-k} elem, amelyre $f_n = g_k h_{n-k}$ és az $f^* = f - h_{n-k} x^{n-k} g$, $h^* = h - h_{n-k} x^{n-k}$ jelölésekkel $f^* = gh^*$. Ha tehát az osztás során a k -nál nem alacsonyabb fokú közbülső maradék főegyütthatója nem osztható g főegyütthatójával, vagy az algoritmus végén a maradék nem nulla, akkor $g \nmid f$, egyébként pedig megkapjuk h -t.

* **8.3.15. Megjegyzés: pszeudoosztás.** Vegyük észre, hogy a maradékos osztás tételében, ha $n = \deg(f) \geq \deg(g) = m$, a g főegyütthatója nem egység, de osztója f főegyütthatójának, akkor egy osztási lépést el tudunk végezni. Speciálisan, ha f -et megszorozzuk a g polinom g_m főegyütthatójával, akkor egy osztási lépést el tudunk végezni, ha pedig g_m^{n-m+1} -gyel szorozzuk, akkor kaphatunk egy

$$g_m^{n-m+1} f(x) = q(x)g(x) + r(x)$$

előállítást, ahol $\deg(r) < \deg(g)$. Ez a *pszeudoosztás*, q a *pszeudohányados*, r pedig a *pszeudomaradék*.

8.3.16. Megjegyzés: Horner-elrendezés. A maradékos osztás tételét alkalmazva az f és a $g = x - c$ polinomra azt kapjuk, hogy $f = (x - c)q + r$, ahol r konstans, értéke $f(c)$. Így $n - 1$ szorzással és ugyanannyi összeadással megkaphatjuk $f(c)$ -t.

8.3.17. Megjegyzés. Az, hogy egy polinomnak hány gyöke van, függ attól, hogy milyen gyűrű felett tekintjük, azaz hol keressük a gyököt. Például az $1 + x^2$ polinomot $\mathbb{Z}$, $\mathbb{Q}$, illetve $\mathbb{R}$ felett tekintve nincs gyöke, $\mathbb{C}$ felett két gyöke van, i és $-i$, ha $\mathbb{Z}_p$ felett tekintjük, ahol p prímszám, akkor $p = 2$ esetén egy gyöke van, $p = 3$ esetén nincs gyöke és $p = 5$ esetén két gyöke van. A kvaterniók ferdetestében végtelen sok gyök van: minden $x = bi + cj + dk$, $b, c, d \in \mathbb{R}$ kvaternióra, amelyre $b^2 + c^2 + d^2 = 1$, teljesül, hogy $1 + x^2 = 0$. A nem nullosztómentes $\mathbb{Z}_{65}$ -ben 8, 18, 47, 57 mind gyökei $1 + x^2$ -nek.

→ **8.3.18. Feladat [3].** Osszuk el az első polinomot a másodikkal maradékosan $\mathbb{Q}$, $\mathbb{Z}_7$ és $\mathbb{Z}_6$ felett, ha lehet:

- (1) $42x^4 - 7x^3 + 13x^2 + 43x - 12$, $x^2 - x + 1$;
- (2) $x^3 - 3x^2 - x - 1$, $3x^2 - 2x + 1$;

- (3) $5x^4 + 2x - 3, 2x^2 - 3x + 4;$
- (4) $x^3, 2x + 3;$
- (5) $x^2 + 3x - 2, 6x^4 + 5x^2 - 3x + 2;$
- (6) $x^3 + x^2 + 3x + 2, 2x^2 + 4.$

→ **8.3.19. Feladat [3].** Határozzuk meg a -t és b -t úgy, hogy $x^4 + 3x^2 + ax + b$ osztható legyen $x^2 - 2ax + 2$ -vel $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, illetve $\mathbb{C}$ felett.

→ **8.3.20. Feladat [6].** Határozzuk meg az alábbi $\mathbb{Q}[x]$ -beli polinomok legnagyobb közös osztóját:

- (1) $(x-1)^3(x+2)^2(x-3)(x-4)$ és $(x-1)^5(x+2)(x+5);$
- (2) $x^m - 1$ és $x^n - 1;$
- (3) $x^m + 1$ és $x^n + 1.$

→ **8.3.21. Feladat [5].** Ha lehet, oldjuk meg az u, v ismeretlen polinomokra nézve $\mathbb{R}[x]$ -ben az alábbi egyenleteket:

- (1) $(3x^3 - 2x^2 + x + 2)u + (x^2 - x + 1)v = 1;$
- (2) $(x^4 - x^3 - 4x^2 + 4x + 1)u + (x^2 - x - 1)v = x.$

→ **8.3.22. Feladat [5].** Ha lehet, oldjuk meg az u, v ismeretlen polinomokra nézve $\mathbb{Z}_2[x]$ -ben az alábbi egyenleteket:

- (1) $(x^5 + x^2 + 1)u + (x^4 + x^2 + x)v = 1;$
- (2) $(x^4 + 1)u + (x^3 + x^2 + x + 1)v = x^3 + x + 1.$

→ **8.3.23. Feladat [6].** Határozzuk meg a legalacsonyabb fokú olyan $h \in K[x]$ polinomot, amely az f -fel osztva u , a g -vel osztva pedig v maradékot ad, ha

- (1) $f = x^3 + 1, g = x^3 + x^2 - 2, u = -x^2, v = x^2 - 2x + 2, K = \mathbb{Q};$
- (2) $f = x^2 - 2x + 1, g = x^3 - 3x^2 + 2, u = x, v = x^2 + x + 1, K = \mathbb{R};$
- (3) $f = x^3 + x^2 + 1, g = x^3 + x + 1, u = x + 1, v = x^2 + x + 1, K = \mathbb{Z}_2.$

→ **8.3.24. Feladat [4].** Mutassuk meg, hogy a Horner-elrendezés lényegében az

$$f(c) = \left(\dots ((f_n c + f_{n-1})c + f_{n-2})c + \dots + f_1 \right) c + f_0$$

összefüggéssel ekvivalens. (Innen kapta az „elrendezés” nevet.)

→ **8.3.25. Feladat [4].** Az $x - c$ -vel való maradékos osztás segítségével határozzuk meg az alábbi $\mathbb{C}[x]$ -beli polinomok helyettesítési értékét a megadott helyen:

- (1) $x^4 - 3x^3 + 6x^2 - 10x + 16, c = 4;$
- (2) $x^5 + (1 + 2i)x^4 - (1 + 3i)x^2 + 7, c = -2 - i;$
- (3) $x^4 - 3ix^3 - 4x^2 + 5ix - 1, c = 1 + 2i.$

→ **8.3.26. Feladat [4].** Az $x - c$ -vel való ismételt maradékos osztás segítségével írjuk fel az alábbi $\mathbb{C}[x]$ -beli polinomokat $x - c$ hatványai segítségével:

- (1) $x^4 + 2x^3 - 3x^2 - 4x + 1, c = -1;$
- (2) $x^5, c = 1.$

* **8.3.27. Körosztási polinomok.** Ha $n \in \mathbb{N}^+$, legyenek $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}$ az n -edik egységgyökök. Az ε_k pontosan akkor primitív n -edik egységgyök, ha n és k relatív prímek: valóban, $\varepsilon_k^\ell = \varepsilon_1^{k\ell} = \varepsilon_j$ pontosan akkor teljesül valamely $\ell \in \mathbb{Z}$ -re, ha $k\ell \bmod n = j$; ha k és n relatív prímek, akkor ez az egyenlet megoldható minden $j \in \mathbb{Z}$ -re, ha pedig nem relatív prímek, akkor például $j = 1$ -re nem megoldható. Legyen

$$\Phi_n(x) = \prod_{0 \leq k < n, \text{Inko}(k, n) = 1} (x - \varepsilon_k),$$

az n -edik *körosztási polinom*; ennek foka $\varphi(n)$. Például $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, $\Phi_4(x) = x^2 + 1$, $\Phi_5(x) = x^4 - x^3 + x^2 - x + 1$, $\Phi_6(x) = x^2 - x + 1$ stb. Mivel bármely ε_k egységgyök m rendjére $m|n$, és erre az m -re (de csak erre) ε_k primitív m -edik egységgyök,

$$\prod_{m|n} \Phi_m(x) = \prod_{0 \leq k < n} (x - \varepsilon_k) = x^n - 1;$$

például $\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = x^6 - 1$. Innen egyébként $\sum_{m|n} \varphi(m) = n$. Teljes indukcióval megmutatjuk, hogy Φ_n egész együtthatós: $\Phi_1(x) = x - 1$ egész együtthatós, és ha minden $m < n$ -re Φ_m egész együtthatós, akkor $x^n - 1 = \Phi_n(x)p_n(x)$ miatt, ahol

$$p_n(x) = \prod_{m|n, m < n} \Phi_m(x)$$

egész együtthatós főpolinom, $x^n - 1$ -et osztva $p_n(x)$ -szel, kapjuk, hogy Φ_n is egész együtthatós. Mivel $m|n$ esetén $x^m - 1 | p_n(x)$, az is adódik, hogy

$$\Phi_n(x) \left| \frac{x^n - 1}{x^m - 1} = \left(\sum_{j=0}^{n/m-1} x^{mj} \right).$$

* **8.3.28. Wilson tétele.** Ha p prímszám, akkor $(p-1)! \equiv -1 \pmod{p}$.

Bizonyítás. A $p = 2$ eset triviális. Ha $p > 2$, akkor a $\mathbb{Z}_p$ feletti $x^{p-1} - 1 - \prod_{i=1}^{p-1} (x - i)$ polinom nulla kell legyen, mert $1, 2, \dots, p-1$ gyökei, foka pedig legfeljebb $p-2$. Így speciálisan a konstans tag is nulla kell legyen $\mathbb{Z}_p$ -ben. $\square$

8.3.29. Polinom algebrai deriváltja. Legyen R gyűrű. Egy $f = f_0 + f_1x + f_2x^2 + \dots + f_nx^n \in R[x]$ polinom *algebrai deriváltján* vagy röviden *deriváltján* az $f' = f_1 + 2f_2x + 3f_3x^2 + \dots + nf_nx^{n-1} \in R[x]$ polinomot értjük.

Egységelemes integritási tartomány felett az $f \mapsto f'$ algebrai deriválás rendelkezik az alábbi tulajdonságokkal:

- (1) konstans polinom deriváltja a nulla polinom;
- (2) az x polinom deriváltja az egységelem;
- (3) $(f + g)' = f' + g'$, ha $f, g \in R[x]$ (*additivitás*);
- (4) $(fg)' = f'g + fg'$, ha $f, g \in R[x]$ (*szorzat differenciálási szabálya*);

ez utóbbi tulajdonság belátásához az additivitás és a disztributivitás miatt csak azt kell észrevenni, hogy monomok szorzatára igaz az összefüggés.

* **8.3.30. Megjegyzés.** Megfordítva, ha R egységelemes integritási tartományra egy $f \mapsto f'$ leképezése $R[x]$ -nek önmagába rendelkezik az előző definícióban szereplő (1)–(4) tulajdonságokkal, akkor i szerinti indukcióval az $f_i x^i$ monomra

$$(f_i x^{i-1} \cdot x)' = (i-1)f_i x^{i-2} x + f_i x^{i-1} = i f_i x^{i-1},$$

amiből az $f' = f_1 + 2f_2 x + 3f_3 x^2 + \dots + n f_n x^{n-1}$ formula következik tetszőleges polinomra, azaz $f \mapsto f'$ az algebrai deriválás.

8.3.31. Tétel. Legyen R egységelemes integritási tartomány, $f, g \in R[x]$ és $n \in \mathbb{N}^+$. Ha $g^n | f$, akkor $g^{n-1} | f'$.

Bizonyítás. Indukcióval $(g^n)' = n g^{n-1} g'$, ha $n \in \mathbb{N}^+$. Ha $f = g^n h$, akkor

$$f' = n g^{n-1} g' h + g^n h' = g^{n-1} (n g' h + g h'). \quad \square$$

8.3.32. Következmény. Ha R test (és így $R[x]$ -ben van legnagyobb közös osztó), $f \neq 0$, és d az f és az f' egyik legnagyobb közös osztója, akkor $q = f/d$ négyzetmentes, azaz egyetlen legalább elsőfokú g polinomnak a négyzetével sem osztható.

Bizonyítás. Adott g -re legyen $n \in \mathbb{N}$ a legnagyobb természetes szám, amelyre $g^n | f$. Mivel $n > 0$ esetén $g^{n-1} | f'$, így $g^{n-1} | d$. Ha $g^2 | q$ teljesülne, akkor ebből $g^{n+1} | f$ következne. $\square$

8.3.33. Többszörös gyökök. Legyen R egységelemes integritási tartomány, $f \in R[x]$, $f \neq 0$ és $n \in \mathbb{N}^+$. Azt mondjuk, hogy $c \in R$ az f egy n -szeres gyöke, ha $(x-c)^n | f$, de $(x-c)^{n+1} \nmid f$. (Szokásos az $(x-c)^n \parallel f$ jelölés is.) Ez azzal ekvivalens, hogy $f = (x-c)^n g$, ahol g -nek c nem gyöke.

8.3.34. Tétel. Legyen R egységelemes integritási tartomány, $f \in R[x]$, $n \in \mathbb{N}^+$ és $c \in R$ az f egy n -szeres gyöke. Ekkor c az f' -nek legalább $(n-1)$ -szeres gyöke, és ha $\text{char}(R) \nmid n$ (például ha $\text{char}(R) = 0$), akkor pontosan $(n-1)$ -szeres gyöke.

Bizonyítás. Ha $f = (x-c)^n g$, akkor $f' = (x-c)^{n-1} ((x-c)g' + ng)$. Innen látszik, hogy c legalább $(n-1)$ -szeres gyöke f' -nek. A zárójelben álló kifejezés értéke a c helyen $ng(c)$, ami $g(c) \neq 0$ miatt nem nulla, ha $\text{char}(R) \nmid n$. $\square$

8.3.35. Megjegyzés. A derivált gyöke nyilván nem feltétlenül gyöke a polinomnak (például $x^2 + 1$ -nek 0 nem gyöke, de a deriváltjának igen). Másrészt a polinom n -szeres gyöke lehet a deriválnak több, mint $n-1$ -szeres gyöke is: ha p prím, $a \in \mathbb{Z}_p$, $n \in \mathbb{N}$, $p \nmid n$, akkor $f = (x-a)^p ((x-a)^n + 1) \in \mathbb{Z}_p[x]$ -nek az a egy p -szeres gyöke, míg $f' = n(x-a)^{p+n-1}$ -nek $(p+n-1)$ -szeres gyöke.

→ **8.3.36. Feladat [2].** Hányszoros gyöke 2 az $x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8 \in \mathbb{Z}[x]$ polinomnak?

→ **8.3.37. Feladat [3].** Határozzuk meg az a együtthatót úgy, hogy -1 legalább kétszeres gyöke legyen az $x^5 - ax^2 - ax + 1 \in \mathbb{R}[x]$ polinomnak.

→ **8.3.38. Feladat [3].** Keressük meg az alábbi $\mathbb{C}[x]$ -beli polinomok többszörös gyökeit:

- (1) $x^6 - 6x^4 - 4x^3 + 9x^2 + 12x + 4$;
- (2) $x^5 - 10x^3 - 20x^2 - 15x - 4$.

→ **8.3.39. Feladat [3].** Adjunk meg az alábbi $\mathbb{C}[x]$ -beli polinomokhoz olyan polinomot, amelynek ugyanazok a gyökei, de mindegyik egyszerűs:

$$(1) \quad x^6 - 15x^4 + 8x^3 + 51x^2 - 72x + 27;$$

$$(2) \quad x^5 - 6x^4 + 16x^3 - 24x^2 + 20x - 8.$$

8.3.40. Irreducibilis polinomok és testbővítések. A 8.3.13 következmény szerint test feletti egyhatározatlanú polinomok euklideszi gyűrűt alkotnak, így bennük a prímelem és az irreducibilis elem fogalma egybeesik, és minden nem nulla polinom irreducibilis polinomok szorzatára bomlik, lényegében egyértelműen. Az egységek a nem nulla konstans polinomok. Bármely test felett az elsőfokú polinomok irreducibilisek.

Legyen F test, és $f \in F[x]$ egy n -ed fokú ($n \in \mathbb{N}^+$) főpolinom. A $\tilde{F} = F[x]/(f)$ gyűrűben minden mellékosztályban a legalacsonyabb fokú polinom fokszáma kisebb, mint n , és csak egy n -nél alacsonyabb fokú polinom van (mivel a mellékosztály bármely két polinomjának különbsége többszöröse f -nek); ez meghatározható úgy, hogy a mellékosztály tetszőleges g elemére vesszük az f -fel való osztásánál adódó r maradékot: mivel $g = qf + r$, $g - r \in (f)$. A műveleteket végezhetjük ezekkel a reprezentánsokkal: ha a szorzat foka nem kisebb, mint n , akkor osztunk f -fel, és vesszük a maradékot. Jelölje $\tilde{x}$ az $x \in F[x]$ polinom osztályát $F[x]/(f)$ -ben. A $\tilde{F}$ gyűrű elemei egyértelműen felírhatók $a_0 + a_1\tilde{x} + \dots + a_{n-1}\tilde{x}^{n-1}$ alakban, ahol $a_0, a_1, \dots, a_{n-1} \in F$. Így F részteste $\tilde{F}$ -nak, másszóval $\tilde{F}$ bővítése F -nek. Az így megkapható testbővítéseket *algebrai testbővítéseknek* nevezzük.

Ha f irreducibilis főpolinom, akkor $\tilde{F} = F[x]/(f)$ test; ez következik abból, hogy az (f) főideál maximális ideál, de közvetlenül is belátható: ha $g \notin (f)$, azaz f nem osztja g -t, akkor alkalmazva a bővített euklideszi algoritmust, olyan $u, v \in F[x]$ polinomokat kapunk, amelyekre $d = fu + gv$, ahol d az f és g egyik legnagyobb közös osztója, egy nullad fokú polinom, azaz nem nulla konstans. Szorozva $1/d$ -vel azt kapjuk, hogy $1 = fu/d + gv/d$, azaz v/d osztálya a g osztályának az inverze, tehát $\tilde{F}$ minden nem nulla elemének van inverze. Az F részteste a $\tilde{F}$ testnek. (A $\tilde{F}[x]$ -belinek is tekinthető f polinom $\tilde{F}[x]$ -ben már nem irreducibilis, $\tilde{x}$ egy gyöke.)

Legyen p egy prímszám. A fenti konstrukciót alkalmazva a $\mathbb{Z}_p$ véges testre és egy f irreducibilis főpolinomra, egy p^n elemű véges testet kapunk. Azt, hogy az n -ed fokú $f \in \mathbb{Z}_p[x]$ polinom irreducibilis-e, például úgy is megvizsgálhatjuk, hogy minden, legfeljebb $\lfloor n/2 \rfloor$ fokszerű polinommal megpróbáljuk elosztani. (Ennél sokkal hatékonyabb eljárást is fogunk tanulni.)

8.3.41. Példák. (1) Tekintsük az $\mathbb{R}[x]$ polinomgyűrűben az R felett irreducibilis $x^2 + 1$ polinom által generált $(x^2 + 1)$ főideált. Minden mellékosztályban a legalacsonyabb fokú polinom lineáris, és a mellékosztályban pontosan egy lineáris polinom van. A faktorgyűrű műveleteivel a mellékosztályok $\mathbb{C}$ -vel izomorf testet alkotnak.

(2) Tekintsük a $\mathbb{Z}_2[x]$ polinomgyűrűben az $x^2 + x + 1$ irreducibilis polinom által generált $(x^2 + x + 1)$ főideált. Minden mellékosztályban a legalacsonyabb fokú polinom lineáris, és a mellékosztályban pontosan egy lineáris polinom van. A faktorgyűrű szorzásával a mellékosztályok egy négyelemű testet alkotnak.

→ **8.3.42. Feladat [3].** Adjuk meg a $\mathbb{Q}[x]/(x^6 - 3x - 3)$ gyűrűben

(1) az $(x^3 + 1)(x^5 - 1)$ polinom osztályának legalacsonyabb fokú reprezentánsát;

(2) az $x^3 + 3x^2 - 5$ polinom osztálya inverzének a legalacsonyabb fokú reprezentánsát.

→ **8.3.43. Feladat [2].** Hány másodfokú reducibilis főpolinom van $\mathbb{Z}_7$ felett?

→ **8.3.44. Feladat [4].** Felbontható-e $\mathbb{Z}_3$ felett az $x^7 + 2x^4 + x^2 + 2x + 2$ polinom?

→ **8.3.45. Feladat [5].** A $\mathbb{Z}_2$ gyűrű felett

(1) állapítsuk meg, hogy irreducibilisek-e az $x^4 + 1$, $x^3 + x^2 + 1$, illetve $x^4 + x + 1$ polinomok;

(2) adjuk meg az összes, legfeljebb harmadfokú irreducibilis polinomot;

(3) bontsuk irreducibilis polinomok szorzatára az $x^7 + 1$ polinomot.

8.3.46. Feladat [4]. Bontsuk fel az $x^8 + x^6 + x^5 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$ polinomot irreducibilis polinomok szorzatára.

→ **8.3.47. Feladat [3].** Konstruáljunk négyelemű testet, és írjuk fel a műveleti táblákat.

8.3.48. Feladat [3]. Konstruáljunk nyolcelemű testet az $x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ polinom segítségével.

8.3.49. Feladat [4]. Keressük meg $\mathbb{Z}_3$ felett az összes másodfokú irreducibilis főpolinomot. Mindegyikkel konstruáljunk véges testet.

8.3.50. Feladat [4]. Keressük meg $\mathbb{Z}_2$ felett az összes negyedfokú irreducibilis főpolinomot. Mindegyikkel konstruáljunk véges testet.

→ **8.3.51. Feladat [2].** Döntsük el, hogy $\mathbb{Z}[x]$ -ben a megadott halmazok ideált alkotnak-e, és ha igen, határozzuk meg a faktorgyűrűt:

(1) polinomok, amelyek konstans tagja páros;

(2) polinomok, amelyek elsőfokú tagjának együtthatója páros.

8.3.52. Feladat [6]. Mutassuk meg, hogy

(1) $\mathbb{R}[x]/(x^2 + 1)$ izomorf $\mathbb{C}$ -vel;

(2) $\mathbb{Z}[x]/(x^2 + 1)$ izomorf a Gauss-egészekkel;

(3) $\mathbb{Z}[x]/(x^2 - d)$ izomorf $\mathbb{Z}[\sqrt{d}]$ -vel, ha d nem négyzetszám;

(4) $\mathbb{Z}[x]/(m)$ izomorf $\mathbb{Z}_m[x]$ -szel;

(5) $\mathbb{Z}[x]/(m, x)$ izomorf $\mathbb{Z}_m$ -mel;

(6) $F[x]/(x + 1)$ izomorf F -fel tetszőleges testre.

8.3.53. Feladat [6]. Izomorfak-e az alábbi gyűrűk?

(1) $\mathbb{R}[x]/(x^2 + 2)$ és $\mathbb{C}$;

(2) $\mathbb{R}[x]/(x^2 - 1)$ és $\mathbb{C}$;

(3) $\mathbb{R}[x]/(x^2 - 1)$ és $\mathbb{R} \times \mathbb{R}$;

(4) $\mathbb{Z}[i]/(3)$ és $\mathbb{Z}_3[x]/(x^2 + 1)$.

8.3.54. Véges testek elemszáma. Bármely véges test elemeinek száma prímszám, ahol a prímszám a test karakterisztikája.

° **Bizonytás.** Ha p az F véges test karakterisztikája és e az egységeleme, akkor F vektortér a $\{0, e, 2e, \dots, (p-1)e\}$ részteste felett, és ha n -dimenziós, akkor F -nek p^n eleme van. $\square$

8.3.55. Megjegyzések. (1) Abból, hogy egy test karakterisztikája egy p prímszám, nem következik, hogy a test véges. Például $\mathbb{Z}_p[x]$ hányadostestének karakterisztikája p .

(2) Ha $n > 1$, akkor egy p^n elemű véges test nem izomorf $\mathbb{Z}_{p^n}$ -el, sem $\mathbb{Z}_p^n$ -el, bár mindegyiknek ugyanannyi eleme van, mert az utóbbiak nem nullosztómentes gyűrűk (de nem izomorfak, mert $\mathbb{Z}_{p^n}$ additív csoportja ciklikus, míg $\mathbb{Z}_p^n$ -ben minden nem nulla elem additív rendje p).

8.3.56. Feladat [4]. Hány k -adik hatvány, illetve egy k -adik hatványnak hány k -adik gyöke van egy q elemű testben, ha

$$(1) \quad q = 49, k = 15;$$

$$(2) \quad q = 125, k = 24;$$

$$(3) \quad q = 4096, k = 1024.$$

°* **8.3.57. Alkalmazás: A Rijndael és AES blokkrejtjelzők.** A $w^8 + w^4 + w^3 + w + 1$ polinom könnyen ellenőrizhetően irreducibilis $\mathbb{Z}_2$ felett. A 256 elemű $\mathbb{Z}_2[w]/(w^8 + w^4 + w^3 + w + 1)$ testet Rijndael-testnek is nevezik: ezt a testet használja a Joan Daemen és Vincent Rijmen belga kriptográfusok által tervezett Rijndael-rendszer. A test elemei mellékosztályok, a mellékosztályokat a bennük szereplő egyetlen 8-nál alacsonyabb fokú polinommal reprezentáljuk. A rendszer titkos kulcsú szimmetrikus rejtjelező, gyors a rejtjelezés és a fejtés, és a klasszikus, Shannontól származó elveken alapul: a kulcstól is függő helyettesítéseket és keveréseket alkalmaz a rejtjelzendő blokkra számos menetben egymás után. Alapvetően 32 bites szavakat használ. A rejtjelzendő blokk b és a kulcs k (szavakban megadott) mérete is 4, 5, 6, 7 vagy 8 szó lehet, egymástól függetlenül. Ha r menetet használunk, akkor először a k szavas kulcsot kiterjesztjük egy $r+1$ darab b szavas segédkulcs-sorozattá (lásd később). Egy W szót tekinthetünk egy (B_0, B_1, B_2, B_3) bájtnégyesnek, ahol a bájtok a memóriacímeik növekvő sorrendjében következnek. A teljes blokkot tekinthetjük egy bájtmátrixnak, amelynek egyes oszlopait a szavak bájtjai alkotják, a sorindexek 0, 1, 2, 3. Egy tetszőleges B bájtot tekinthetünk egy $(b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7)$ bitsorozatnak, egy $b_0 + b_1 2 + b_2 2^2 + \dots + b_7 2^7$ számnak, illetve a Rijndael-test egy, a $b_0 + b_1 w + \dots + b_7 w^7$ polinommal reprezentált elemének.

A rejtjelezés r menetből áll, ahol $r \geq 10$, ha $b = k = 4$, egyébként ha $b, k \leq 6$, akkor $r \geq 12$, és minden más esetben $r \geq 14$. A menetek előtt bitenkénti kizáró vagy műveletet végzünk a blokk és az első segédkulcs között. Az egyes menetek az alábbi négy lépésből állnak:

(1) Bájtonkénti S helyettesítés: A blokkra bájtonként elvégezzük az S helyettesítést, ahol $S(x) = Cx^{-1} + c$; itt x^{-1} azt jelenti, hogy az x bájtot a Rijndael-test egy elemével azonosítva kiszámítjuk a multiplikatív inverzét (a nulla bájt inverzét nullának tekintjük).

Az eredményül kapott x' bájttra kiszámítjuk az

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = C \begin{pmatrix} x'_0 \\ x'_1 \\ x'_2 \\ x'_3 \\ x'_4 \\ x'_5 \\ x'_6 \\ x'_7 \end{pmatrix} + c$$

összefüggéssel adott y bájtot $\mathbb{Z}_2$ feletti mátrixszorzással és vektorösszeadással, ahol

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad \text{és} \quad c = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix},$$

és $S(x) = y$. A helyettesítés inverze $x = S^{-1}(y) = (C^{-1}(y - c))^{-1}$; a C mátrix modulo 2 inverze

$$C^{-1} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

(2) Sorkeverés: A blokknak megfelelő bájt mátrix sorait ciklikusan balra léptetjük, minden sort annyi bájttal, amennyi a sor indexe. Ha $b > 6$, akkor a 2, illetve 3 indexű sort 3-mal, illetve 4-gyel léptetjük. A transzformáció invertálása nyilvánvaló.

(3) Oszlopkeverés: A bájt mátrixban minden oszlopot egy harmadfokú polinomnak tekintünk a z változóban a Rijndael-test felett. Az együtthatókat az oszlop bájtjai adják, a 0 indexű sorban van a konstans tag. Ezt a polinomot szorozzuk a Rijndael-test feletti $(w^2 + w)z^3 + z^2 + z + w$ polinommal, és az eredményt redukáljuk modulo $z^4 + 1$, ennek a (Rijndael-testbeli) együtthatói adják a keverés eredményét. Az invertálás azon alapul, hogy az előző polinomnak modulo $z^4 + 1$ van inverze: $(w^3 + w + 1)z^3 + (w^3 + w^2 + 1)z^2 + (w^3 + 1)z + w^3 + w^2 + w$.

(4) Segédkulcs hozzáadása: bitenként kizáró vagy műveletet végzünk a kapott szavak és a következő segédkulcs szavai között. Az invertálás ugyanez.

Az utolsó, r -edik menetben az oszlopkeverési lépés kimarad. A dekódolás nyilván a rejtjelzési lépések inverzeinek fordított sorrendben történő elvégzésével történik.

Le kell még írunk a segédkulcsok képzését. A segédkulcsok tömbje $(r+1)b$ szóból áll, ezt a szósortozatot olvassuk az elejétől kezdve, mindig b szót, ezek a segédkulcsok. A tömböt a következőképpen töltjük fel: az első k helyre kerülnek az eredeti kulcs szavai. A további W_i , $i = 0, 1, \dots, (r+1)b - k - 1$ szavakat a következőképpen képezzük: általában W_i az előtte álló, és a k -val előtte álló szóra alkalmazott bitenkénti kizáró vagy művelettel adódik. A $k \leq 6$ esetben ettől csak akkor térünk el, ha $i \equiv 0 \pmod{k}$; ekkor a két szó közötti kizáró vagy művelet előtt az előző szó bájtoit ciklikusan eggyel balra léptetjük (a 0 indexű bájtt a 3 indexű bájtt helyére kerül), bájtonként alkalmazzuk az S helyettesítést, majd a 0 indexű bájthoz bitenkénti kizáró vagy művelettel hozzáadjuk a Rijndael-test $w^{[i/k]}$ által reprezentált eleme mint bájtt bitjeit. Ha $k > 6$, akkor még egy eltérés van: ha $i \equiv 4 \pmod{k}$, akkor a két szó közötti kizáró vagy művelet előtt az előző szóra bájtonként alkalmazzuk az S helyettesítést.

Az AES (Advanced Encryption Standard) USA-szabvány rejtjelező a Rijndael speciális esete: $b = 4$ és $k = 4$, $r = 10$ vagy $k = 6$, $r = 12$ vagy $k = 8$, $r = 14$.

8.3.58. Tétel. *Véges test nem nulla elemeinek multiplikatív csoportja ciklikus. Ha a véges testnek q eleme van, akkor bármely c elemére $c^q = c$.*

Az állítás a Fermat-tétel általánosítása. A tétel alapján a véges testben végzett szorzáshoz használhatunk „logaritmustáblát”.

* **Bizonyítás.** Legyen a nem nulla elemek multiplikatív csoportja G , és legyen a G rendje n . Ha $d|n$, és van olyan $g \in G$, amelynek rendje d , akkor ez egy $H = \{1, g, g^2, \dots, g^{d-1}\}$ ciklikus részcsoportot generál. Mivel testben az $x^d = 1$ egyenletnek legfeljebb d megoldása van, azok mind a H részcsoportban vannak. Speciálisan, minden d rendű eleme G -nek eleme, sőt, generátora H -nak, és $\varphi(d)$ ilyen van. Így d rendű g eleme G -nek 0 vagy $\varphi(d)$ darab van. Ha valamely $d|n$ -re nulla lenne, az ellentmondana annak, hogy $\sum_{d|n} \varphi(d) = n$ (lásd például a 8.3.27 pontot). Így van n rendű elem is – éppen $\varphi(n)$ számú –, tehát G ciklikus. $\square$

* **8.3.59. Tétel.** *Legyen F egy q elemű véges test. Egy F feletti d -ed fokú irreducibilis polinom akkor és csakis akkor osztja $x^{q^n} - x$ -et, ha $d|n$.*

Bizonyítás. Elég azt az esetet tekinteni, amikor az irreducibilis polinom főpolinom. Legyen f egy d -ed fokú irreducibilis főpolinom, és tekintsük az $\tilde{F} = F[x]/(f)$ véges testet, amelynek q^d eleme van. Ennek bármely y elemére $y^{q^d} = y$. Innen k szerinti indukcióval

$$y^{q^{dk}} = y^{(q^{d(k-1)} \cdot q^d)} = (y^{q^{d(k-1)}})^{q^d} = y^{q^d} = y$$

minden $y \in \tilde{F}$ -ra. Így $d|n$, $dk = n$ esetén $y^{q^n} = y$ az $\tilde{F}$ -ban van, ami speciálisan $y = \tilde{x}$ választással azt is jelenti, hogy az F feletti $x^{q^n} - x$ polinom osztható f -el.

Megfordítva, legyen ξ a $\tilde{F}$ nem nulla elemei multiplikatív ciklikus csoportjának tetszőleges generátora. Legyen p az $\tilde{F}$ karakterisztikája; tudjuk, hogy q egy p -hatvány. Azok az $\eta \in \tilde{F}$ elemek, amelyekre $\eta^{q^n} = \eta$, az összeadásra nézve zárt halmazt alkotnak, mert $(\eta_1 + \eta_2)^{p^k} = \eta_1^{p^k} + \eta_2^{p^k}$, és q^n is p -hatvány. Nyilván az ilyen η elemek halmaza a szorzásra is zárt. Így ha f osztja az $x^{q^n} - x$ polinomot $F[x]$ -ben, akkor $\tilde{F}$ -ban $\tilde{x}^{q^n} = \tilde{x}$, amiből, mivel ξ is az $\tilde{x}$ polinomja, $\xi^{q^n} = \xi$ is teljesül. De ha $n = kd + r$, $0 \leq r < d$, akkor

$$\xi = \xi^{q^n} = \xi^{(q^{dk} \cdot q^r)} = (\xi^{q^{dk}})^{q^r} = \xi^{q^r},$$

ami $r > 0$ esetén ellentmondana annak, hogy ξ generátorelem. $\square$

8.3.60. Következmény. Az F feletti n -ed fokú irreducibilis főpolinomok száma legalább $(q^n - q^{\lfloor n/2 \rfloor} \lfloor \log n \rfloor)/n > 0$.

Az informatikában szokásos módon $\log$ a kettes alapú logaritmus.

* **Bizonyítás.** Mivel $x^{q^n} - x$ deriváltja a -1 polinom, bármely irreducibilis főpolinomnak legfeljebb az első hatványa osztja $x^{q^n} - x$ -et. Bármely d valódi osztója n -nek osztója n/p_i -nek valamely p_i prímtényezőjére n -nek. Így azon irreducibilis főpolinomok, amelyek osztói $x^{q^n} - x$ -nek, de fokuk kisebb, mint n , mind osztói valamely $x^{q^{n/p_i}} - x$ polinomnak, amelynek foka legfeljebb $q^{\lfloor n/2 \rfloor}$. Mivel az n különböző prímosztóinak száma legfeljebb $\lfloor \log n \rfloor$, azon irreducibilis főpolinomok, amelyek osztói $x^{q^n} - x$ -nek, de fokuk kisebb, mint n , szorzatának a foka legfeljebb $q^{\lfloor n/2 \rfloor} \lfloor \log n \rfloor$. Így a pontosan n -ed fokú irreducibilis főpolinomok szorzatának a foka legalább $q^n - q^{\lfloor n/2 \rfloor} \lfloor \log n \rfloor$, tehát számuk legalább $(q^n - q^{\lfloor n/2 \rfloor} \lfloor \log n \rfloor)/n$. Hátravan még annak bizonyítása, hogy a számláló pozitív. Mivel $n = \lceil n/2 \rceil + \lfloor n/2 \rfloor$, azt kell megmutatnunk, hogy $q^{\lfloor n/2 \rfloor} > \lfloor \log n \rfloor$. Ezt nyilván elég $q = 2$ -re belátni. Azt fogjuk megmutatni, hogy még $2^{n/2} > \log n$ is teljesül. Ez könnyen ellenőrizhető $n = 1, 2, 3, 4, 5, 6, 7$ esetén, egyébként pedig indukcióval következik, mert

$$\frac{\log(n+1)}{\log n} < \frac{\log(2n)}{\log n} = \frac{1 + \log n}{\log n} = 1 + 1/\log n \leq 1 + 1/3 = \frac{4}{3} < \sqrt{2},$$

ha $n \geq 8$.

8.3.61. Következmény. Bármely $q = p^n$ (p prím, $n \in \mathbb{N}^+$) prímhatalványra létezik q elemű véges test.

Bizonyítás. Alkalmazzuk az 8.3.40 pontot és előző következményt $F = \mathbb{Z}_p$ -re.

* **8.3.62. Feladat [3].** Hány másodfokú irreducibilis polinom van egy q elemű véges test felett?

* **8.3.63. Feladat [10].** Adjunk pontos formulát a μ számelméleti függvény segítségével egy q elemű véges test feletti irreducibilis főpolinomok számára.

8.3.64. Irreducibilis polinomok $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ és $\mathbb{Z}$ felett. A komplex számtest felett az algebra alaptétele szerint minden $\mathbb{C}[x]$ -beli nem konstans polinomnak van gyöke, így a gyöktényező leválasztására vonatkozó állítás szerint pontosan az elsőfokú polinomok az irreducibilisek, és egy n -ed fokú $f_0 + f_1x + \dots + f_nx^n$ polinomot a tényezők sorrendjétől eltekintve egyértelműen felírhatunk

$$f_n(x - c_1)^{\alpha_1}(x - c_2)^{\alpha_2} \dots (x - c_k)^{\alpha_k}$$

gyöktényező alakban, ahol a különböző $c_1, c_2, \dots, c_k$ komplex számok a különböző gyökök, az $\alpha_1, \alpha_2, \dots, \alpha_k$ pozitív természetes számok pedig az egyes gyökök multiplicitásai, $\alpha_1 + \alpha_2 + \dots + \alpha_k = n$.

A valós számtest felett irreducibilisek az elsőfokú polinomok és azok a másodfokú polinomok, amelyeknek nincs valós gyöke. Megmutatjuk, hogy más irreducibilis polinom nincs. Egy a valós számtest feletti, azaz valós együtthatós $f = f_0 + f_1x + \dots + f_nx^n$ polinom tekinthető komplex együtthatósak is, így az algebra alaptétele szerint $n \geq 1$

esetén van olyan $c \in \mathbb{C}$, hogy $f_0 + f_1c + \cdots + f_nc^n = 0$. Ha c valós, akkor f reducibilis. Ha $c \notin \mathbb{R}$, akkor konjugálással $f_0 + f_1\bar{c} + \cdots + f_n\bar{c}^n = 0$, tehát c konjugáltja is gyök. A $g_c = (x - c)(x - \bar{c}) = x^2 - 2\Re(c)x + |c|^2$ valós együtthatós polinommal $\mathbb{R}$ felett maradékosan osztva, $f = g_cq + r$. Az r csak nulla lehet, mert egyébként legfeljebb elsőfokú lenne, és így nem lehetne nem valós komplex gyöke. Tehát a valós számtest felett minden $f_0 + f_1x + \cdots + f_nx^n$ polinom legfeljebb másodfokú irreducibilis polinomok szorzatára bontható lényegében egyértelműen.

A racionális számtest felett bonyolultabb a helyzet. Vannak polinomok, például $x^2 - 2$, amelyek $\mathbb{Q}$ felett irreducibilisek, bár $\mathbb{R}$ felett nem. Meg fogjuk mutatni, hogy $\mathbb{Q}[x]$ -ben minden $n \in \mathbb{N}^+$ -ra van olyan n -ed fokú polinom, amely irreducibilis.

A $\mathbb{Z}[x]$ gyűrű nem tehető euklideszi gyűrűvé. Ha ugyanis euklideszi gyűrűvé tudnánk tenni, akkor a 2 és x polinomok legnagyobb közös osztója, amely létezik és 1, előállítható lenne $1 = 2u + xv$ alakban valamely $u, v \in \mathbb{Z}[x]$ polinomokkal, ami nem lehetséges, mert a jobb oldal konstans tagja páros.

A $\mathbb{Q}[x]$ -beli és $\mathbb{Z}[x]$ -beli faktorok között kapcsolat van, bár nem ugyanazok. Például a $6x^2 + 12x + 12$ polinom $\mathbb{Z}[x]$ -ben nem felbonthatatlan, felírható $2 \cdot 3 \cdot (x^2 + 2x + 2)$ alakban, míg $\mathbb{Q}[x]$ -ben felbonthatatlan, itt ugyanis 2 és 3 már egységek, így $6x^2 + 12x + 12$ asszociáltja az $x^2 + 2x + 2$ polinomnak, amelynek nincs racionális gyöke, mert még valós sincs.

Általánosabban, legyen R egy Gauss-gyűrű, K pedig a hányadosteste. Minden $R[x]$ -beli polinom tekinthető $K[x]$ -belinek is. Egy $K[x]$ -beli polinom együtthatói nevezőinek szorzatával beszorozva a polinomot, egy vele $K[x]$ -ben asszociált polinomot kapunk, ami már $R[x]$ -beli. Ugyancsak asszociált főpolinomot kapunk $K[x]$ -ben, ha a főegyütthatóval végigosztjuk a polinomot. Nyilván $R[x]$ -ben általában nem tudjuk a főegyütthatóval végigosztani a polinomot. Az R irreducibilis elemei irreducibilisek $R[x]$ -ben is, míg $K[x]$ -ben egységek. Ettől eltekintve, az $R[x]$ -beli és $K[x]$ -beli felbonthatóság lényegében ekvivalens: ha egy $R[x]$ -beli polinom előáll $R[x]$ -ben két nem konstans, tehát alacsonyabb fokú polinom szorzataként, akkor nyilván $K[x]$ -ben is. A megfordítást, azt, hogy a két reducibilitás egybeesik, Gauss tétele adja. Az így kapott kapcsolat $R[x]$ és $K[x]$ között nagyon fontos: néha azt használjuk ki, hogy $K[x]$ euklideszi gyűrű, tehát Gauss-gyűrű, máskor meg az R -beli oszthatóságot. (A K -beli oszthatóság triviális.)

*** 8.3.65. Primitív polinomok.** Legyen R egy Gauss-gyűrű. Ekkor $R[x]$ egy polinomját *primitív polinomnak* nevezzük, ha együtthatóinak az egységelem legnagyobb közös osztója. (Test felett minden nem nulla polinom ilyen.) Az $R[x]$ -beli irreducibilis polinomok nyilván primitívek.

Minden $0 \neq f \in R[x]$ polinom előállítható $f = df^*$ alakban, ahol f^* primitív polinom és $0 \neq d \in R$; az előállításához emeljük ki f együtthatóinak legnagyobb közös osztóját. Az előállítás nyilván lényegében egyértelmű, d és f^* egységfaktorok erejéig egyértelműen meghatározottak.

*** 8.3.66. Gauss lemmája.** Legyen R egy Gauss-gyűrű, $f, g \in R[x]$ pedig nullától különböző primitív polinomok. Ekkor fg is primitív polinom.

Bizonyítás. Tegyük fel, hogy fg nem primitív polinom. Ekkor van olyan $p \in R$ prímelem, amely osztja fg minden együtthatóját. Legyen i , illetve j a legkisebb olyan index, amelyre $p \nmid f_i$, illetve $p \nmid g_j$. Mivel az fg polinom $i + j$ -edik együtthatója

$$f_0g_{i+j} + \cdots + f_ig_j + \cdots + f_{i+j}g_0,$$

és ebben az összegben p minden más tagot oszt, osztania kell $f_i g_j$ -t is, tehát $p|f_i$ vagy $p|g_j$, ami ellentmondás. $\square$

* **8.3.67. Lemma.** Legyen R egy Gauss-gyűrű, K pedig a hányadosteste. Minden $0 \neq f \in K[x]$ polinom felírható $f = af^*$ alakban, ahol $0 \neq a \in K$ és $f^* \in R[x]$ egy primitív polinom. A felírás lényegében egyértelmű: a és f^* egy R -beli egységfaktor illetve reciproka erejéig egyértelműen meghatározott.

Bizonyítás. Írjuk fel f együtthatóit R -beli elemek hányadosaiként. Végigszorozva f -et az együtthatói nevezőinek c szorzatával, majd kiemelve a kapott $R[x]$ -beli polinom együtthatóinak d legnagyobb közös osztóját, kapjuk az előállítást $a = d/c$ -vel. Ha $f = bg^*$ egy másik előállítás, akkor b -t felírva d'/c' , $c', d' \in R$ alakban, azt kapjuk, hogy $dc'f^* = d'cg^*$, amiből az $R[x]$ -beli polinomok lényegében egyértelmű előállítása miatt következik az egységfaktor erejéig való egyértelműség. $\square$

8.3.68. Gauss tétele. Legyen R egy Gauss-gyűrű, K pedig a hányadosteste.

- (1) Ha egy $f \in R[x]$ polinom előállítható két nem konstans g, h polinom szorzataként $K[x]$ -ben, akkor $R[x]$ -ben is előállítható két g^*, h^* polinom szorzataként, amelyekre g és g^* , illetve h és h^* asszociáltak $K[x]$ -ben, azaz egymásnak K -beli konstansszorosai.
- (2) $R[x]$ is Gauss-gyűrű.

* **Bizonyítás.** Tegyük fel, hogy $f = gh$, ahol $g, h \in K[x]$ nem konstans polinomok. Írjuk fel f -et df^* alakban, ahol $f^* \in R[x]$ primitív polinom, $d \in R$. Felírva g -t ag^{**} , a h -t pedig bh^{**} alakban, ahol $g^{**}, h^{**} \in R[x]$ primitív polinomok, $df^* = f = gh = abg^{**}h^{**}$. Mivel Gauss lemmája szerint $g^{**}h^{**}$ is primitív polinom, és az előző lemma szerint pedig f előállítása primitív polinom segítségével lényegében egyértelmű, valamely R -beli ε egységgel $f^* = \varepsilon g^{**}h^{**}$ és $\varepsilon d = ab$, ahol $a, b \in K$. Így azt kapjuk, hogy $f = df^* = d\varepsilon g^{**}h^{**}$, és például $g^* = d\varepsilon g^{**}$, $h^* = h^{**}$ választással kapjuk f kívánt felbontását. Figyeljük meg, hogy ha f primitív polinom volt, akkor g^* és h^* is azok.

(2) bizonyításához vegyük észre, hogy egy konstans pontosan akkor egység R -ben, ha mint konstans polinom egység $R[x]$ -ben, és pontosan akkor irreducibilis R -ben, ha mint konstans polinom irreducibilis $R[x]$ -ben, továbbá $R[x]$ nem konstans irreducibilis polinomjai primitívek.

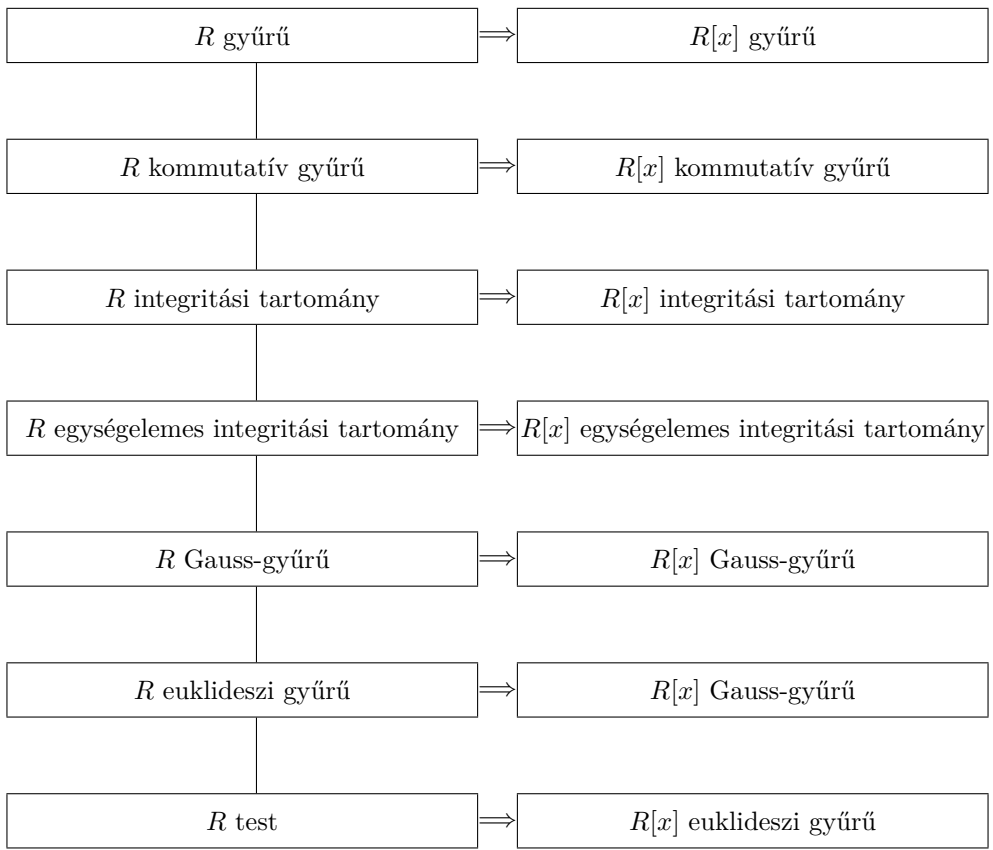
Legyen $0 \neq f \in R[x]$, és írjuk fel f -et df^* alakban, ahol $d \in R$ és $f^* \in R[x]$ primitív polinom. Az (1) bizonyításának utolsó mondata szerint, indukcióval, f -et előállíthatjuk $f_1 f_2 \cdots f_n$ alakban, ahol $f_1, f_2, \dots, f_n$ primitív irreducibilis polinomok, d -t pedig $\varepsilon p_1 \cdots p_m$ alakban, ahol $p_1, \dots, p_m$ irreducibilis elemek, ε pedig egység R -ben.

Az egyértelműség bizonyításához tegyük fel, hogy

$$\varepsilon p_1 \cdots p_m f_1 \cdots f_n = f = \varepsilon' q_1 \cdots q_r g_1 \cdots g_s,$$

ahol $\varepsilon, \varepsilon'$ egységek, $p_1, \dots, p_m$ és $q_1, \dots, q_r$ pedig irreducibilis elemek R -ben (és így $R[x]$ -ben), $f_1, \dots, f_n$ és $g_1, \dots, g_s$ pedig legalább elsőfokú, R felett irreducibilis polinomok, így primitívek és az első lépés szerint irreducibilisek K felett is. Így a fellépő polinomok f -nek egy K feletti irreducibilis faktorizációját is megadják, tehát $s = n$, és (megfelelő átindexelés után) alkalmas $0 \neq \varepsilon_i \in K$ elemekkel $f_i = \varepsilon_i g_i$. Az előző lemma szerint minden ε_i egység R -ben. Így

$$\varepsilon p_1 \cdots p_m = \varepsilon'' q_1 \cdots q_r$$



8.3.1 ábra: Gyűrűk és polinomgyűrűk.

valamely $\varepsilon'' \in R$ egységgel. Mivel R Gauss-gyűrű, kapjuk az állítást. $\square$

*** 8.3.69. Legnagyobb közös osztó számolása Gauss-gyűrű feletti polinomgyűrű esetén.** Legyen R Gauss-gyűrű. Megmutatjuk, hogyan kaphatunk hatékony algoritmus legnagyobb közös osztó számítására $R[x]$ -ben, ha R -ben van hatékony algoritmusunk a négy alapműveletre és a legnagyobb közös osztó számolására. Először is vegyük észre, hogy ha $f, g \in R[x]$, $0 \neq f = af^*$, $0 \neq g = bg^*$, ahol f^* az f , g^* pedig a g primitív része, akkor f minden osztója, ha nulladfokú, akkor osztója a -nak, ha pedig primitív, akkor osztója f^* -nak. Innen a és b egy legnagyobb közös osztójának valamint f^* és g^* legnagyobb közös osztójának a szorzata f és g egy legnagyobb közös osztója, hiszen bármilyen h közös osztót felírva ch^* alakban, ahol h^* a h primitív része, c az egyik, h^* a másik tényezőnek osztója. Elég tehát primitív polinomok legnagyobb közös osztójának a meghatározásával foglalkozni.

Legyenek $f, g \in R[x]$ primitív polinomok, $\deg(f) \geq \deg(g) \geq 0$. Egy, az f -hez és g -hez tartozó *polinom maradék sorozat* egy olyan $r_0, r_1, \dots, r_k \in R[x]$ polinomsorozat, amelyre $r_0 = f$, $r_1 = g$, $r_k | r_{k-1}$, és valamely $\alpha_i, \beta_i \in R$, $q_i \in R[x]$ elemekkel

$$\alpha_j r_{j-1}(x) = q_j(x) r_j(x) + \beta_j r_{j+1}(x), \quad j = 1, 2, \dots, k-1.$$

Vegyük észre, hogy $f = r_0$ és $g = r_1$ bármely legnagyobb közös osztója, mivel primitív polinom, relatív prím β_1 -hez, így osztója r_2 -nek; indukcióval folytatva, osztója minden r_j -nek. Megfordítva, r_k primitív része osztója r_{k-1} primitív részének, és mivel relatív prím α_{k-1} -hez, r_{k-2} -nek is stb., tehát osztója g -nek és f -nek is. Így akármilyen polinom maradék sorozat esetén r_k primitív része f és g egy legnagyobb közös osztója.

Polinom maradék sorozatot könnyen kaphatunk pszeudoosztással, azaz ha ϱ_j jelöli r_j főegyütthatóját, és $\delta_j = \deg(r_{j-1}) - \deg(r_j)$, akkor $\alpha_j = \varrho_j^{\delta_j+1}$, $\beta_j = 1$ ($j = 1, 2, \dots, k-1$) választással. Ennek a választásnak az a hátránya, hogy az együtthatók általában gyorsan nőnek, például $R = \mathbb{Z}$ esetén hosszuk akár exponenciálisan is nőhet. Egy másik lehetőség, hogy minden lépésben pszeudoosztást alkalmazunk (azaz α_j választása változatlan), de r_{j+1} -et a pszeudomaradék primitív részének választjuk, ami meghatározza β_j -t. Ekkor az együtthatók a lehető leglassabban nőnek, de minden lépésben ki kell számolnunk a pszeudomaradék együtthatóinak legnagyobb közös osztóját. Egy közbenső, sokkal jobb lehetőség a *szubrezultáns algoritmus*: itt is pszeudoosztás alkalmazunk (tehát α_j választása változatlan), de $\beta_j = \gamma_j \eta_j^{\delta_j}$, ahol $\gamma_1 = 1$, $\eta_1 = 1$, és $\gamma_j = \varrho_{j-1}$, $\eta_j = \gamma_j^{\delta_{j-1}} / \eta_{j-1}^{\delta_{j-1}-1}$, ha $1 < j < k$; természetesen meg kell mutatnunk, hogy az η_j definíciójában szereplő osztás elvégezhető, és az r_j -vel való pszeudoosztásnál kapott pszeudomaradék osztható β_j -vel. Az ezek bizonyításához szükséges eszközökről kapta az algoritmus a nevét. Megmutatható, hogy itt az együtthatók nem nőnek túl gyorsan, például az $R = \mathbb{Z}$ esetben hosszuk alig több, mint lineárisan nő. A részleteket illetően lásd Knuth [46] könyvét, 4.6.1.

→ **8.3.70. Feladat** [0]. Felbontható-e $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ illetve $\mathbb{C}$ felett a $6x + 10$ polinom?

→ **8.3.71. Feladat** [3]. A $3x^4 - 5x^3 + 3x^2 + 4x - 2$ polinom egyik gyöke $1+i$. Határozzuk meg a többi gyökét.

→ **8.3.72. Feladat** [3]. Adjunk meg olyan minimális fokszámú valós együtthatós polinomot, amelynek

- (1) az 1 kétszeres, a 2, 3 és $1+i$ pedig egyszeres gyöke;
- (2) az i háromszoros, a $-1-i$ egyszeres gyöke.

→ **8.3.73. Feladat** [6]. Adjuk meg az alábbi polinomok irreducibilis felbontását $\mathbb{C}$ illetve $\mathbb{R}$ felett:

- (1) $x^6 - 27$;
- (2) $x^6 + 27$;
- (3) $x^8 - 16$;
- (4) $x^8 + 16$;
- (5) $x^{10} - x^5 + 1$;
- (6) $x^{22} + x^{11} - 6$;
- (7) $x^4 + 4x^3 + 4x^2 + 1$;
- (8) $x^{2n} - 2x^n + 2$;
- (9) $x^{2n} + x^n + 1$;
- (10) $x^{2n} - 2x^n - 3$.

→ **8.3.74. Feladat [3].** Határozzuk meg a $4x^6 - 8x^5 - 3x^4 - 11x^3 + 18x^2 + 28x + 8$ polinom racionális többszörös gyökeit, és adjuk meg mindegyiknek a multiplicitását.

→ **8.3.75. Feladat [3].** Az alábbi polinomokat bontsuk fel irreducibilis polinomok szorzatára $\mathbb{Z}$ és $\mathbb{Q}$ felett:

(1) $3x^5 + 2x^3 - 12x^2 - 10x + 14;$

(2) $20x^4 + 26x^3 + 65x^2 + 91.$

8.3.76. Feladat [6]. Bizonyítandók a következő azonosságok:

(1)

$$x^{2n} - 1 = (x^2 - 1) \prod_{k=1}^{n-1} (x^2 - 2x \cos(k\pi/2) + 1);$$

(2)

$$x^{2n+1} - 1 = (x - 1) \prod_{k=1}^n (x^2 - 2x \cos(2k\pi/(2n+1)) + 1);$$

(3)

$$x^{2n+1} + 1 = (x + 1) \prod_{k=1}^n (x^2 + 2x \cos(2k\pi/(2n+1)) + 1);$$

(4)

$$x^{2n} + 1 = \prod_{k=0}^{n-1} (x^2 - 2x \cos((2k+1)\pi/(2n)) + 1).$$

* **8.3.77. Schönemann–Eisenstein-tétel.** Ha az R Gauss-gyűrű feletti legalább elsőfokú f primitív polinomhoz van olyan $p \in R$ prímelem, amely nem osztója a főegyütthatónak, de osztója minden más együtthatónak, p^2 viszont nem osztója a konstans tagnak, akkor f irreducibilis. Hasonlóan, ha az R Gauss-gyűrű feletti legalább elsőfokú f polinomhoz van olyan $p \in R$ prímelem, amely nem osztója a konstans tagnak, de osztója minden más együtthatónak, p^2 viszont nem osztója a főegyütthatónak, akkor f irreducibilis.

Bizonyítás. Az első esetre végezzük el a bizonyítást, a másik eset bizonyítása teljesen hasonló. Tegyük fel, hogy $f = gh$. Mivel p nem osztja az f főegyütthatóját, sem a g , sem a h főegyütthatóját nem osztja. Legyen m a legkisebb olyan index, amelyre $p \nmid g_m$, és legyen n a legkisebb olyan index, amelyre $p \nmid h_n$. Ha $k = m + n$, akkor

$$p \nmid f_k = \sum_{i+j=k} h_i g_j,$$

mivel p osztja a jobb oldalon álló összeg minden tagját, kivéve azt a tagot, amelyben $i = m$ és $j = n$. Így $m + n = \deg(f)$, ahonnan $m = \deg(g)$ és $n = \deg(h)$. Viszont m és n nem lehet egyszerre pozitív, különben $p^2 \mid f_0 = h_0 g_0$ teljesülne. Így az egyik polinom konstans, és ha nem lenne egység, akkor f nem lenne primitív. $\square$

* **8.3.78. Következmény.** Ha p prímelem, $n \in \mathbb{N}^+$, akkor $f = x^n + p$ irreducibilis R és (a Gauss-tétel miatt) a hányadosteste felett. $\square$

Speciálisan, ha p prímszám, akkor $x^n + p$ irreducibilis $\mathbb{Z}$ és $\mathbb{Q}$ felett.

* **8.3.79. Megjegyzések.** (1) Ha R test, a Schönemann–Eisenstein-tétel nyilván nem alkalmazható irreducibilis polinomok konstruálására, hiszen ekkor R -ben nincs olyan elem, amely nem nulla és nem egység, így nincsenek prímek.

(2) Néha az irreducibilitás bizonyításához a Schönemann–Eisenstein-tétel nem alkalmazható közvetlenül, csak némi kerülővel. Például a

$$\sum_{j=0}^{n-1} x^j = \frac{x^n - 1}{x - 1} \in \mathbb{Z}[x]$$

polinomok reducibilisek, ha n összetett szám, mert ha $n = km$, akkor nyilván

$$\sum_{j=0}^{n-1} x^j = \left(\sum_{j=0}^{k-1} x^{mj} \right) \left(\sum_{j=0}^{m-1} x^j \right).$$

Ha viszont n prímszám, akkor a fenti polinom irreducibilis. Ennek bizonyításához vegyük észre, hogy ha a polinom felbontható lenne, akkor x helyére $x + 1$ -et írva, az így kapott polinom is az lenne, de ez

$$\frac{\sum_{j=0}^n \binom{n}{j} x^j - 1}{x} = \sum_{j=0}^{n-1} \binom{n}{j+1} x^j,$$

amire már alkalmazható a Schönemann–Eisenstein-tétel, mert ha n prím, akkor

$$\binom{n}{j+1}$$

többszöröse n -nek, ha $n - 1 > j \geq 0$, egyenlő n -el, ha $j = 0$, és 1, ha $j = n - 1$.

→ **8.3.80. Feladat [3].** Irreducibilis-e az $x^5 + 5$ polinom $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, illetve $\mathbb{Z}_5$ felett?

8.3.81. Feladat [5]. Legyen $f \in \mathbb{Z}[x]$ a $\mathbb{Z}$ felett irreducibilis főpolinom, $\alpha \in \mathbb{C}$ az f egy gyöke $\mathbb{C}$ felett, $n = \deg(f)$. Mutassuk meg, hogy

$$\mathbb{Z}[\alpha] := \left\{ \sum_{j=0}^{n-1} a_j \alpha^j : a_0, a_1, \dots, a_{n-1} \in \mathbb{Z} \right\}$$

gyűrű.

8.3.82. Lagrange-interpoláció. A polinomok osztására vonatkozó tétel következményei között, 8.3.11-ben láttuk, hogy ha az R egységelemes integritási tartománynak $c_0, c_1, \dots, c_n$ különböző elemei, $d_0, d_1, \dots, d_n$ pedig tetszőleges elemei R -nek, akkor legfeljebb egy olyan legfeljebb n -ed fokú f polinom létezik, amelyre $f(c_j) = d_j$, ha $j = 0, 1, \dots, n$. Ha R test, akkor mindig létezik is ilyen polinom, és az alábbi *Lagrange interpolációs eljárással* megkapható. Legyen

$$l_j(x) = \frac{\prod_{i \neq j} (x - c_i)}{\prod_{i \neq j} (c_j - c_i)}$$

a j -edik *Lagrange interpolációs alappolinom*, és legyen $f(x) = \sum_{j=0}^n d_j l_j(x)$.

8.3.83. Titokmegosztás. A Lagrange-interpoláció *titokmegosztásra* is felhasználható. Legyen $m, n \in \mathbb{N}^+$, $m < n$. Tegyük fel, hogy egy $t \in \mathbb{N}$, $t < T$ titkot n részre akarunk szétosztani úgy, hogy bármelyik m részből a titok visszaállítható legyen, de kevesebből semmi információt ne lehessen kapni a titokról. Válasszunk egy, a t maximális lehetséges T értékénél (és n -nél is) nagyobb p prímet és véletlen $a_1, a_2, \dots, a_{m-1} \in \mathbb{Z}_p$ együtthatókat, majd számítsuk ki a $\mathbb{Z}_p$ feletti $t + a_1x^1 + a_2x^2 + \dots + a_{m-1}x^{m-1}$ polinom $y_1, y_2, \dots, y_n$ értékeit az $1, 2, \dots, n$ helyeken. Ezen y_j -k a *titokrészek*: bármelyik m titokrészből a polinom megkapható Lagrange-interpolációval, így adódik a konstans tag, azaz a titok, de kevesebb részből könnyen láthatóan nem.

→ **8.3.84. Feladat [4].** Adjuk meg azt az $\mathbb{R}[x]$ -beli interpolációs polinomot, amely az adott helyeken az adott értékeket veszi fel:

- (1) a $0, 1, 2, 3, 4$ helyen $1, 2, 3, 4, 6$;
- (2) a $-1, 0, 1, 2, 3$ helyen $6, 5, 0, 3, 2$.

8.3.85. Kronecker-eljárás. Ha R egy (végtelen) Gauss-gyűrű, amelyben rendelkezésünkre áll egy eljárás, amellyel akármelyik elem osztóit meg tudjuk határozni, valamint vannak eljárások a műveletek elvégzésére (például, ha $R = \mathbb{Z}$), akkor egy $f \in R[x]$ polinomnak meghatározhatjuk az irreducibilis faktorait. Ha $f = gh$, akkor bármely $c \in R$ -re $f(c) = g(c)h(c)$, így $g(c) \mid f(c)$. Legyen K az R hányadosteste. Választva különböző $c_0, c_1, \dots, c_n$ elemet R -ben, bármely R -beli $d_j \mid f(c_j)$, $j = 0, 1, \dots, n$ értékekhez Lagrange-interpolációval meghatározhatjuk azt az egyetlen $g \in K[x]$ polinomot, amelyre $\deg(g) \leq n$ és $g(c_j) = d_j$, azaz $g(c_j) \mid f(c_j)$, $j = 0, 1, \dots, n$. Ha $g \in R[x]$ és osztja f -et, akkor megtaláltuk f egy osztóját, és f helyett a hányadossal folytatjuk. (Néha érdemes az osztás előtt ellenőrizni még néhány $c \in R$ -re, hogy $g(c) \mid f(c)$ teljesül-e. Azt is megnézhetjük, hogy g főegyütthatója osztja-e f főegyütthatóját, bár ezt az osztási algoritmus is az első lépésben ellenőrzi.) Ha $n = 0$ -val indulunk, és egyesével növeljük n -et, akkor csak irreducibilis polinomosztókat fogunk találni (mert egy reducibilis, legalább elsőfokú osztó irreducibilis tényezőit előbb megtaláljuk). Ha $n \leq \lfloor \deg(f)/2 \rfloor$ -ig nem találtunk osztót, akkor f irreducibilis. Az elsőfokú faktorok megadják a K -beli, és ezáltal az R -beli gyököket is. (Sok R gyűrűre a gyökkeresésre, a faktorizálásra, és az irreducibilitás bizonyítására is léteznek sokkal hatékonyabb eljárások is.)

→ **8.3.86. Feladat [5].** Keressük meg az alábbi egész együtthatós polinomok racionális gyökeit:

- (1) $x^4 - 2x^3 - 8x^2 + 13x - 24$;
- (2) $x^4 + 4x^3 - 2x^2 - 12x + 9$;
- (3) $10x^4 - 13x^3 + 15x^2 - 18x - 24$;
- (4) $6x^4 + 19x^3 - 7x^2 - 26x + 12$.

→ **8.3.87. Feladat [5].** Igazoljuk, hogy az alábbi polinomok irreducibilisek $\mathbb{Z}[x]$ -ben:

- (1) $x^4 - 8x^3 + 12x^2 - 6x + 2$;
- (2) $x^5 - 12x^3 + 36x - 12$;
- (3) $x^4 - x^3 + 2x + 1$.

→ **8.3.88. Feladat [5].** Határozzuk meg a $6x^4 + 17x^3 + 13x^2 - 9x - 6$ polinom irreducibilis felbontását $\mathbb{Z}[x]$ -ben.

→ **8.3.89. Feladat [5].** Számítsuk ki az alábbi polinomok legnagyobb közös osztóját $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ és $\mathbb{Z}_3$ felett. Van-e közös gyökük az egyes esetekben?

- (1) $x^4 + x^3 - 3x^2 - 4x - 1$ és $x^3 + x^2 - x - 1$;
- (2) $x^5 + x^4 - x^3 - 2x - 1$ és $3x^4 + 2x^3 + x^2 + 2x - 2$;
- (3) $7x^4 - 28x^3 + 7$ és $11x^3 - 33x^2 + 11$;
- (4) $x^6 + 2x^4 - 4x^3 - 3x^2 + 8x - 5$ és $x^5 + x^2 - x + 1$.

* **8.3.90. Cardano-képlet.** Keressünk gyökképletet kettőnél magasabb fokú komplex együtthatós polinomok gyökeinek meghatározására. A főegyütthatóval végigosztva feltehetjük, hogy az 1. Ha $y^n + f_1 y^{n-1} + f_2 y^{n-2} + \dots + f_n = 0$, akkor $y = x - f_1/n$ (invertálható) helyettesítéssel az egyenlet $x^n + g_2 x^{n-2} + g_3 x^{n-3} + \dots + g_n = 0$ alakú lesz, így elég azt az esetet vizsgálni, amikor a második legmagasabb fokú tag nulla. A másodfokú esetben a helyettesítés után a megoldás triviális.

A harmadfokú esetben az $x^3 + px + q = 0$ egyenlet megoldásait keressük $x = u + v$ alakban. Mivel $x^3 = (u + v)^3 = u^3 + v^3 + 3uv(u + v)$, azaz $x^3 - 3uvx - (u^3 + v^3) = 0$, ha sikerül u -t és v -t úgy választani, hogy $uv = -p/3$ és $u^3 + v^3 = -q$ teljesüljön, akkor készen vagyunk. Az első egyenletből $u^3 v^3 = -p^3/27$, így u^3 és v^3 a $z^2 + qz - p^3/27$ másodfokú egyenlet, az úgynevezett *karakterisztikus egyenlet* gyökei, például

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \quad v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Így végül is a megoldásokat a

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Cardano-képlet adja, ahol a kilenc lehetséges köbgyök párból azt a hármat kell választani, amelyeknek a szorzata $-p/3$. Egyszerű számolás mutatja, hogy ezek valóban megadják $x^3 + px + q$ gyöktényezősz felbontását.

A negyedfokú esetben a bal oldalt az $\alpha \in \mathbb{C}$ paraméter bevezetésével átalakítva az $x^4 + px^2 + qx + r = 0$ egyenletet

$$(1) \quad \left(x^2 + \frac{p}{2} + \alpha\right)^2 - \left(2\alpha x^2 - qx + \left(\alpha^2 + p\alpha - r + \frac{p^2}{4}\right)\right) = 0$$

alakra hozhatjuk. Ha sikerül az α paramétert úgy választani, hogy a nagy zárójelben álló polinomja x -nek teljes négyzet legyen, akkor az egyenlet két másodfokú egyenletre esik szét, így megoldható. Ehhez az kell, hogy ezen polinomnak egyetlen gyöke legyen, azaz fenn kell állnia a

$$q^2 - 8\alpha \left(\alpha^2 + p\alpha - r + \frac{p^2}{4}\right) = 0$$

összefüggésnek. Ezt a harmadfokú egyenletet megoldva három alkalmas α értéket is kapunk.

Magasabb fokú egyenletre nem adható hasonló gyökképlet. Ha $n \geq 5$, akkor még olyan egész együtthatós n -ed fokú polinom is létezik, amelynek gyökei nem írhatók fel racionális számok, a négy alpművelet és gyökvonások segítségével, azaz még „*saját gyökképlete*” sincs, ilyen például $x^5 - 4x + 2$. Az első ilyen jellegű eredmény Abeltől származik, aki ezzel a problémával kapcsolatban kezdte el vizsgálni csoportok kommutativitását. A kérdéskört Galois tisztázta teljesen, aki megmutatta, hogy az egyenlet négy alpművelettel és gyökjelekkel való megoldhatósága attól függ, hogy a gyökök bizonyos permutációiból alkotott csoport, az egyenlet Galois-csoportja feloldható-e. Speciális esetekben tehát sikerülhet meghatározni a gyököket, például sokszor segít egy új változó bevezetése $y = h(x)$ alakban, ahol h polinom; ez a *Tschirnhaus-transzformáció*. Például az $x^4 + ax^2 + b = 0$ egyenletből $y = x^2$ helyettesítéssel másodfokú egyenlet lesz. A Tschirnhaus-transzformációt használtuk e pont elején is a második legmagasabb fokú tag „eltüntetésére”.

* **8.3.91. Feladat [5].** Határozzuk meg $(x-1)(x-3)(x+4)$ transzformáltját az $y = x^2 - x - 1$ helyettesítésnél.

* **8.3.92. Feladat [7].** Transzformáljuk a megadott polinomokat a megadott helyettesítéssel:

$$(1) \quad x^3 - 3x - 4, y = x^2 + x + 1;$$

$$(2) \quad x^3 + 2x^2 + 2, y = x^2 + 1;$$

$$(3) \quad x^4 - x - 2, y = x^3 - 2;$$

$$(4) \quad x^4 - x^3 - x^2 + 1, y = x^3 + x^2 + x + 1.$$

* **8.3.93. Testbővítések.** Ha F a K részteste, azaz K az F test bővítése, akkor nyilván K vektortér F felett. Ennek a vektortérnek a dimenzióját a *bővítés fokának* nevezzük és $[K:F]$ -fel jelöljük; ha véges, akkor *véges bővítésről* beszélünk.

Legyen $\alpha \in K$. Mivel résztestek metszete is résztest, a K összes, F -et és α -t tartalmazó résztestének a metszete maga is részteste K -nak: nyilván ez az

$$F(\alpha) = \{p(\alpha)/q(\alpha) : p, q \in F[x], q(\alpha) \neq 0\}$$

részhalmaza K -nak.

Ha van olyan $0 \neq p \in F[x]$ polinom, amelynek α gyöke, akkor azt mondjuk, hogy α *algebrai* F felett. Az α egy *minimálpolinomja* F felett egy minimális fokú ilyen polinom. Egy minimálpolinom minden olyan $F[x]$ -beli polinomnak osztója, amelynek α gyöke, mert egyébként a minimálpolinommal osztva a kapott maradék egy, a minimálpolinomnál alacsonyabb fokú polinom lenne, amelynek α gyöke. Így a minimálpolinomok egymás asszociáltjai $F[x]$ -ben. A minimálpolinomok nyilván irreducibilisek. Fokszámuk az α *foka* F felett.

* **8.3.94. Tétel.** Legyen K az F test bővítése. Ha $\alpha \in K$ algebrai F felett, a foka n , és f egy minimálpolinomja α -nak, akkor $F(\alpha)$ izomorf $F[x]/(f)$ -fel, és $F(\alpha)$ minden eleme egyértelműen írható fel $\sum_{j=0}^{n-1} r_j \alpha^j$ alakban, ahol $r_0, r_1, \dots, r_{n-1} \in F$.

Bizonyítás. A $g \mapsto g(\alpha)$ leképezés olyan homomorfizmusa az $F[x]$ gyűrűnek K -ba, amelynek magja (f) , így értékkészlete egy $F[x]/(f)$ -fel izomorf test. Az értékkészlete tartalmazza F -et és α -t, így $F(\alpha)$ -t is. Mivel $F(\alpha)$ nyilván tartalmazza a $\sum_{j=0}^{n-1} r_j \alpha^j$

alakú összegeket, csak azt kell megmutatnunk, hogy az értékkészlet minden eleme ebben a halmazban van. Legyen $g \in F[x]$ tetszőleges, és írjuk fel $g = qf + r$ alakban; nyilván $g(\alpha) = r(\alpha) = \sum_j r_j \alpha^j$. $\square$

* **8.3.95. Feladat: testbővítések [11].** Legyen K az F test bővítése.

- (1) Mutassuk meg, hogy ha $[K:F]$ véges és V véges dimenziós vektortér K felett, akkor F felett is az, és V dimenziója F felett a V tér K feletti dimenziójának és $[K:F]$ -nek a szorzata.
- (2) Mutassuk meg, hogy $\alpha \in K$ pontosan akkor algebrai F felett, ha F egy $L \subset K$ véges bővítésének az eleme, és hogy ekkor α foka osztja L fokát.
- (3) Mutassuk meg, hogy ha $\alpha \in K$ -ra és $n \in \mathbb{N}^+$ -ra α^n algebrai F felett, akkor α is.
- (4) Mutassuk meg, hogy K -nak az F felett algebrai elemei testet alkotnak.

* **8.3.96. Feladat [5].** Mutassuk meg, hogy $\sqrt{2} + \sqrt{3}$ algebrai $\mathbb{Q}$ felett, és foka 4.

* **8.3.97. Feladat [0].** Mi a kapcsolat a $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(1 + \sqrt{2})$ és a $\mathbb{Q}(\sqrt{8})$ testek között?

* **8.3.98. Feladat [3].** Ellenőrizzük, hogy a $x^3 - 6x^2 + 9x + 3$ polinom irreducibilis $\mathbb{Q}$ felett. Legyen $\alpha \in \mathbb{C}$ a polinom egy gyöke. Fejezzük ki a $\mathbb{Q}(\alpha)$ test $\mathbb{Q}$ feletti $1, \alpha, \alpha^2$ bázisában az alábbi elemeket:

- (1) $3\alpha^5 - 2\alpha$;
- (2) $1/(\alpha + 1)$.

* **8.3.99. Feladat [5].** Határozzuk meg $\sqrt{2 - \sqrt[3]{2}}$ minimálpolinomját $\mathbb{Q}$ felett.

* **8.3.100. Feladat [6].** A következő testbővítések közül melyik algebrai (itt A az összes szám algebrai számok teste):

- (1) $\mathbb{R} \subset \mathbb{C}$;
- (2) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5})$;
- (3) $\mathbb{Q} \subset A$;
- (4) $\mathbb{Q}(\sqrt{5}) \subset A$;
- (5) $\mathbb{Q}(\sqrt{5}) \subset \mathbb{R}$;
- (6) $\mathbb{Q}(\pi) \subset \mathbb{R}$.

* **8.3.101. Feladat [6].** Határozzuk meg $\mathbb{Q}$ alábbi algebrai bővítéseinek fokát:

- (1) $\mathbb{Q}(\sqrt{7})$;
- (2) $\mathbb{Q}(i\sqrt{5})$;
- (3) $\mathbb{Q}(1 + i\sqrt{3})$;
- (4) $\mathbb{Q}(i + \sqrt{5})$;
- (5) $\mathbb{Q}(r + i\sqrt{s})$, ahol $r, s \in \mathbb{Q}$, $\sqrt{s} \notin \mathbb{Q}$.

* **8.3.102. Feladat [5].** Mutassuk meg, hogy ha $\alpha \in \mathbb{C}$ algebrai $\mathbb{Q}$ felett és foka n , akkor $\sqrt{\alpha}$ is algebrai, és foka osztója $2n$ -nek. Igaz-e, hogy $\sqrt{\alpha}$ foka mindig pontosan $2n$? Általánosítsuk az állítást.

* **8.3.103. Feladat [6].** Mutassuk meg, hogy ha $\alpha \in \mathbb{C}$ algebrai és foka n , akkor α^2 is algebrai, és foka osztója $\mathbb{Q}$ felett n -nek. Igaz-e, hogy α^2 foka mindig pontosan n ? Általánosítsuk az állítást.

* **8.3.104. Feladat: szerkeszthetőség [12].** (Laczkovich [49] könyve nyomán.) Legyen adott a síkban két különböző pont, A és B . Rögzítsünk egy koordinátarendszert, amelyben az A koordinátái $(0, 0)$, a B koordinátái pedig $(1, 0)$. Azt mondjuk, hogy a d valós szám *szerkeszthető*, ha az adott pontokat felhasználva, körzővel és vonalzóval meg tudunk szerkeszteni két olyan pontot, amelyek távolsága $|d|$. Mutassuk meg, hogy

- (1) a szerkeszthető valós számok testet alkotnak;
- (2) a racionális számok szerkeszthetők;
- (3) egy pont (azaz egy komplex szám) pontosan akkor szerkeszthető, ha a koordinátái szerkeszthetők;
- (4) ha $a > 0$ szerkeszthető, akkor $\sqrt{a}$ is szerkeszthető;
- (5) egy valós szám pontosan akkor szerkeszthető, ha megkapható a racionális számokból az összeadás, kivonás, szorzás, osztás és a négyzetgyökvonás véges sokszori alkalmazásával;
- (6) a szerkeszthető valós számok foka $\mathbb{Q}$ felett kettőhatvány;
- (7) $\cos 20^\circ$ nem szerkeszthető, így a *szögharmadolás* (tetszőleges szög harmadának szerkesztése) megoldhatatlan;
- (8) $\sqrt[3]{2}$ nem szerkeszthető, így a *kockakettőzés* (adott élhosszúságú kockához kétszer akkora térfogatú kocka élhosszának megszerkesztése) megoldhatatlan.
- (9) Legyenek t és ε olyan komplex számok, amelyekre $t = \varepsilon + \varepsilon^{-1}$. Mutassuk meg, hogy ha t egy n -ed fokú algebrai szám, akkor ε szintén algebrai, és foka osztója $2n$ -nek.
- (10) Mutassuk meg, hogy ha p páratlan prím, és a szabályos p -szög szerkeszthető, akkor p Fermat-prím, azaz $2^{2^n} + 1$ alakú valamely $n \in \mathbb{N}$ -re. (Használjuk az előző pontot $t = 2 \cos(2\pi/p)$ -re.)
- (11) Mutassuk meg, hogy ha p páratlan prím, akkor a szabályos p^2 -szög nem szerkeszthető.
- (12) Mutassuk meg, hogy ha a szabályos n -szög szerkeszthető, akkor $n = 2^k p_1 p_2 \cdots p_m$, ahol $p_1, p_2, \dots, p_m$ különböző Fermat-prímek. (Gauss bebizonyította, hogy szabályos n -szög pontosan akkor szerkeszthető, ha $n = 2^k p_1 p_2 \cdots p_m$, ahol $p_1, p_2, \dots, p_m$ különböző Fermat-prímek, ezzel megoldva a szabályos 17-szög szerkesztését is.)

* **8.3.105. Feladat [3].** Bizonyítandó, hogy $\cos \alpha$ pontosan akkor szerkeszthető, ha $\cos(\alpha/2)$ szerkeszthető.

* **8.3.106. Feladat [3].** Bizonyítandó, hogy ha $\cos \alpha$ és $\cos \beta$ szerkeszthetők, akkor $\cos(\alpha + \beta)$ és $\cos(\alpha - \beta)$ is.

* **8.3.107. Feladat [4].** Határozzuk meg azokat a k egészeket, amelyekre $\cos k^\circ = \cos(k\pi/180)$ szerkeszthető.

8.3.108. Feladat [7]. Fejezzük ki képlettel a

- (1) $\cos 12^\circ = \cos(\pi/15)$ számot;
- (2) $\cos 3^\circ = \cos(\pi/60)$ számot.

8.3.109. Feladat [10]. Fejezzük ki képlettel a $\cos 1^\circ = \cos(\pi/180)$ számot.

8.3.110. Véges testek alaptétele. Bármely $q = p^n$ (p prím, $n \in \mathbb{N}^+$) prímszámra a q elemű véges testek izomorfak.

Már láttuk, hogy bármely q prímszámra van q elemű véges test. Mivel a tétel szerint lényegében csak egy q elemű véges test van, beszélhetünk a q elemű véges testről. Ezt $\mathbb{F}_q$ -val jelöljük. Természetesen ha q prím, akkor $\mathbb{F}_q = \mathbb{Z}_q$.

* **Bizonyítás.** Legyen F egy tetszőleges q elemű véges test, p pedig az F karakterisztikája. Ekkor, mint tudjuk, $q = p^n$, és az egységelem többszöröse egy $\mathbb{Z}_p$ -vel izomorf résztestet alkotnak F -ben. Ezt $\mathbb{Z}_p$ -vel azonosítva, $\mathbb{Z}_p$ az F részteste. Legyen f egy n -ed fokú irreducibilis főpolinom $\mathbb{Z}_p$ felett. Ez osztója $\mathbb{Z}_p$ felett a $g(x) = x^{p^n} - x = x^q - x$ polinomnak. A g polinom F felett elsőfokú polinomok szorzatára bomlik, mert minden $y \in F$ gyöke, így q különböző gyöke van. De akkor az irreducibilis tényezőkre való felbontás egyértelműsége miatt f is elsőfokú tényezők szorzatára bomlik F felett. Jelölje α az f egyik gyökét F felett. Mivel $\mathbb{Z}_p(\alpha)$ -nak 8.3.40 szerint $q = p^n$ eleme van, $\mathbb{Z}_p(\alpha) = F$. Mivel $\mathbb{Z}_p(\alpha)$ izomorf $\mathbb{Z}_p[x]/(f)$ -fel, az F izomorf $\mathbb{Z}_p[x]/(f)$ -fel. $\square$

8.3.111. Wedderburn tétele. Véges ferdetest kommutatív, tehát test.

* **Bizonyítás.** Legyen K véges ferdetest, és ha $x \in K$, legyen $C_K(x) = \{y \in K : xy = yx\}$, valamint $C_K = \bigcap_{x \in K} C_K(x)$. Könnyen ellenőrizhető, hogy minden $C_K(x)$, és így C_K is ferdetest, sőt, C_K kommutatív is, azaz test. Legyen q a C_K elemeinek száma. Mivel minden $C_K(x)$ vektortér C_K felett, elemszámuk q^{n_x} valamely $n_x \in \mathbb{N}^+$ -ra. Speciálisan $K = C_K(0)$ elemszáma is q -hatvány, mondjuk q^n . Azt fogjuk megmutatni, hogy $n = 1$. Mivel K vektortér a bővebb $C_K(x)$ ferdetest felett is, és a lineáris függőség, függetlenség, bázis és dimenzió fogalma ekkor is érvényes marad, $n_x | n$ minden $x \in K$ -ra. Tekintsük most a $K^\times$ multiplikatív csoportot. Ekkor a $C(x)$ centralizátor $x \neq 0$ esetén $C_K(x) \setminus \{0\}$, és így a C centrum $C_K \setminus \{0\}$. Az osztályegyenlet szerint

$$q^n - 1 = q - 1 + \sum [K^\times : C(x)] = q - 1 + \sum \frac{q^n - 1}{q^{n_x} - 1};$$

az összegzés a nem egyelemű konjugált elemosztályok egy-egy x reprezentánsára értendő, $q - 1$ pedig az egyelemű konjugált elemosztályok száma, ami nyilván $C = C_K \setminus \{0\}$ elemszáma. A Φ_n körosztási polinom q helyen felvett értéke osztja a bal oldalt, és a jobb oldali összeg minden tagját, így $q - 1$ -et is. Ha azonban $n > 1$, akkor ez ellentmondás, mert $\Phi_n(x) = \prod (x - \varepsilon_k)$, ahol a szorzat az összes primitív n -edik ε_k egységgyökre értendő, így $|\Phi_n(q)| = \prod |q - \varepsilon_k|$, és a jobb oldalon minden tényező abszolút értéke nagyobb, mint $q - 1$. Tehát $n = 1$ és így $K = C_K$. $\square$

* **8.3.112. Polinomfaktorizálás véges testek felett.** Első lépésként az $\mathbb{F}_q$ feletti f polinomot ($q = p^n$, p prím, $n \in \mathbb{N}^+$) a 8.3.32 következményben megadott lépés ismétlésével (azaz a polinomot osztva $d = \text{lko}(f, f')$ -vel, majd ugyanezt elvégezve d -re stb.) négyzetmentes tényezők szorzatára bontjuk; gondot okozhat, hogy az f és f' polinomok legnagyobb közös osztója f is lehet, ha $f' = 0$. Ez akkor fordulhat elő, ha $f_0 + f_1 x^p + f_2 x^{2p} + \dots + f_m x^{mp}$ alakú az f , azaz csak olyan monomokban lép fel nem nulla

együttható, amelyekben a kitevő p többszöröse. Ekkor $g_j = f_j^{q/p}$ választással $g_j^p = f_j^q = f_j$, és a $g = g_0 + g_1x + \dots + g_mx^m$ polinomra

$$g(x)^p = g_0^p + (g_1x)^p + \dots + (g_mx^m)^p = f(x),$$

így elég g -t faktorizálni.

Második lépésként egy már négyzetmentes f polinomot felírunk $f_1f_2 \dots$ (véges) szorzat alakban, ahol f_d a pontosan d -ed fokú irreducibilis tényezők szorzata: Először számoljuk ki $f(x)$ és $x^q - x$ legnagyobb közös osztóját, az f_1 polinomot. Az f_1 az elsőfokú irreducibilis tényezőinek szorzata. Ha f_1 nem konstans, f -et helyettesítjük f/f_1 -el, majd kiszámoljuk az új f és $x^{q^2} - x$ legnagyobb közös osztóját, az f_1 polinomot, stb. A d -edik lépésben az aktuális f és $x^{q^d} - x$ legnagyobb közös osztóját, az $f_d(x)$ polinomot számoljuk ki, ez a d -ed fokú irreducibilis tényezők szorzata. Megállhatunk, ha d nagyobb lesz, mint az aktuális f fokszámának a fele, ekkor f már irreducibilis.

Harmadik lépésként az f_d polinomokat „széthasítjuk”, azaz megpróbáljuk kéttényezős szorzattá alakítani. Ha f_d fokszáma d , akkor nyilván irreducibilis, megállhatunk. Ha valamelyik f_d fokszáma nagyobb, mint d , akkor egy valószínűségi módszert használhatunk a „széthasítására”. Ez azon alapul, hogy tetszőleges $t(x)$ „tesztpolinomra” $t(x)^{q^d} - t(x)$ többszöröse $x^{q^d} - x$ -nek; valóban, mivel F karakterisztikája p és q a p hatványa,

$$t(x)^{q^d} = (\sum_{j=0}^k t_j x^j)^{q^d} = \sum_{j=0}^k t_j^{q^d} (x^j)^{q^d} = \sum_{j=0}^k t_j (x^{q^d})^j,$$

ahonnan $F[x]/(x^{q^d} - x)$ -ben számolva

$$\tilde{t}^{q^d} = \sum_{j=0}^k t_j (\tilde{x}^{q^d})^j = \sum_{j=0}^k t_j \tilde{x}^j = \tilde{t}, \text{ azaz } \tilde{t}^{q^d} - \tilde{t} = \tilde{0}.$$

Ha most a $t(x)^{q^d} - t(x)$ polinomnak vesszük egy felbontását, akkor valószínű, hogy f_d irreducibilis osztói nem mind ugyanabban a tényezőben lesznek, és legnagyobb közös osztó képzéssel „hasíthatunk”. Páratlan q esetén a nyilvánvaló

$$t(x)^{q^d} - t(x) = (t(x)^{(q^d-1)/2} - 1)(t(x)^{(q^d-1)/2} + 1)t(x)$$

faktorizálás használható; megmutatható, hogy ha a t tesztpolinomot véletlenszerűen választjuk az összes $2d$ -nél alacsonyabb fokú polinomok közül, akkor f_d és $t(x)^{(q^d-1)/2} - 1$ legnagyobb közös osztója legalább $1/2 - 1/(2q^d)$ eséllyel nem triviális (azaz foka nagyobb, mint nulla, de kisebb mint f_d foka). A „hasítással” kapott részeket természetesen ha kell, újabb véletlen t választásával megpróbáljuk tovább „hasítani”. (A gyakorlatban sokszor már azzal is célt érünk, ha t -t véletlen elsőfokú főpolinomnak választjuk.) Páros (azaz kettőhatvány) q esetén a

$$t(x)^{q^d} - t(x) = T(t(x))(T(t(x)) - 1)$$

faktorizálás használható, ahol

$$T(x) = x + x^2 + x^4 + x^8 + \dots + x^{q^d/2};$$

ez úgy adódik, hogy a nyilvánvaló $x^2 - x = x(x-1)$ faktorizálásba x helyére $T(x)$ -et írunk, és felhasználjuk, hogy $T(x)^2 - T(x) = x^{q^d} - x$ (mivel $T(x)^2 = T(x^2)$, így $T(x)^2 - T(x)$ -ben két tag kivételével minden kiesik), majd x helyére $t(x)$ -et helyettesítünk.

* **8.3.113. Magasabb fokú kongruenciák.** Az

$$f_0 + f_1x + f_2x^2 + \cdots + f_nx^n \equiv 0 \pmod{m}$$

polinomiális kongruencia megoldásait keressük, ahol $f_0, f_1, \dots, f_n \in \mathbb{Z}$ és $m \in \mathbb{N}$, $m > 1$. A kínai maradéktétel segítségével a kongruencia minden megoldását megkaphatjuk, ha az m kanonikus felbontásában szereplő prímszámok tényezőit véve modulusnak, meghatározzuk a megoldásokat. Hasznos észrevétel, hogy a gyökök nem a polinomtól, hanem csak a hozzá tartozó polinomfüggvénytől függenek: ha p prímszám, $\alpha \in \mathbb{N}^+$, akkor minden $x \in \mathbb{Z}$ -re

$$x^{j+\varphi(p^\alpha)} \equiv x^j \pmod{p^\alpha}, \quad \text{ha } j \geq \alpha,$$

hiszen a különbségben $p|x$ esetén az egyik, egyébként a másik tényező nulla; ennek a segítségével redukálhatjuk a kongruencia fokát. Az $\alpha = 1$ eset elintézhető az előző pont alapján, hiszen ekkor egy $\mathbb{Z}_p$ feletti polinom gyöktényezőit kell meghatároznunk. Végül az $\alpha > 1$ eset az alábbi feladat felhasználásával rekurzióval visszavezethető az $\alpha = 1$ esetre. Ez egyszeres gyök esetén az alábbi Hensel-lemmával is megtehető. A rekurzió és a Hensel-lemma is lényegében abban áll, hogy a megoldásokat p alapú számrendszerben keressük, egyenként növelve a jegyek számát.

* **8.3.114. Feladat [7].** Mutassuk meg, hogy ha $c, t, p \in \mathbb{Z}$, $\alpha \in \mathbb{N}^+$, $f(x) \in \mathbb{Z}[x]$, akkor

$$f(c + tp^\alpha) \equiv f(c) + tp^\alpha f'(c) \pmod{p^{\alpha+1}},$$

tehát

$$\frac{f(c + tp^\alpha) - f(c)}{p^\alpha} \equiv tf'(c) \pmod{p},$$

és így ha p prím és c az f egy gyöke modulo p^α , akkor $f'(c) \not\equiv 0 \pmod{p}$ esetén f -nek modulo $p^{\alpha+1}$ pontosan egy olyan c' gyöke létezik, amely kongruens c -vel modulo p^α , ha pedig $f'(c) \equiv 0 \pmod{p}$, akkor f -nek modulo $p^{\alpha+1}$ vagy nincs gyöke, vagy minden olyan c' gyöke, amely kongruens c -vel modulo p^α .

* **8.3.115. Hensel-lemma.** Legyen p prímszám, $\alpha \in \mathbb{N}^+$, $f, g_\alpha, h_\alpha, u, v \in \mathbb{Z}[x]$, $\deg(u) < \deg(h_\alpha)$, $\deg(v) < \deg(g_\alpha)$, és tegyük fel, hogy $\deg(f) = \deg(g_\alpha) + \deg(h_\alpha)$, az f főegyütthatója a g_α és h_α főegyütthatójának szorzata, valamint teljesülnek az

$$f(x) \equiv g_\alpha(x)h_\alpha(x) \pmod{p^\alpha}, \quad u(x)g_\alpha(x) + v(x)h_\alpha(x) \equiv 1 \pmod{p}$$

kongruenciák. Ekkor léteznek olyan $g_{\alpha+1}, h_{\alpha+1} \in \mathbb{Z}[x]$ polinomok, amelyre

$$g_{\alpha+1}(x) \equiv g_\alpha(x) \pmod{p^\alpha} \quad \text{és} \quad h_{\alpha+1}(x) \equiv h_\alpha(x) \pmod{p^\alpha},$$

továbbá a fenti feltételek mind teljesülnek $\alpha + 1$ -gyel α helyett. A $g_{\alpha+1}$ és $h_{\alpha+1}$ polinomok egyértelműek modulo $p^{\alpha+1}$.

A bizonyítás konstruktív, algoritmust ad $g_{\alpha+1}$ és $h_{\alpha+1}$ meghatározására. Nyilván tetszőleges $u, v \in \mathbb{Z}[x]$ -re $u(x)g_\alpha(x) + v(x)h_\alpha(x) \equiv 1 \pmod{p}$ csak akkor teljesülhet, ha g_α és h_α relatív prím modulo p . Megfordítva, a bizonyítás során azt is látni fogjuk, hogy ekkor $\deg(u) < \deg(h_\alpha)$ és $\deg(v) < \deg(g_\alpha)$ mindig elérhető.

Bizonyítás. Ha létezik $g_{\alpha+1}$ és $h_{\alpha+1}$, akkor a főegyütthatók szorzatára és a fokszá-
mokra vonatkozó feltétel szerint csak

$$g_{\alpha+1} = g_{\alpha} + p^{\alpha} \bar{g} \quad \text{illetve} \quad h_{\alpha+1} = h_{\alpha} + p^{\alpha} \bar{h}$$

alakú lehet, ahol $\bar{g}, \bar{h} \in \mathbb{Z}[x]$, $\deg(\bar{g}) < \deg(g_{\alpha})$, $\deg(\bar{h}) < \deg(h_{\alpha})$. Az

$$u(x)g_{\alpha+1}(x) + v(x)h_{\alpha+1}(x) \equiv 1 \pmod{p}$$

feltétel ekkor nyilván teljesül, az

$$f(x) \equiv g_{\alpha+1}(x)h_{\alpha+1}(x) = (g_{\alpha}(x) + p^{\alpha}\bar{g}(x))(h_{\alpha}(x) + p^{\alpha}\bar{h}(x)) \pmod{p^{\alpha+1}}$$

feltétel pedig azzal ekvivalens, hogy

$$\bar{h}(x)g_{\alpha}(x) + \bar{g}(x)h_{\alpha}(x) \equiv w(x) \pmod{p},$$

ahol

$$w(x) = \frac{f(x) - g_{\alpha}(x)h_{\alpha}(x)}{p^{\alpha}} \in \mathbb{Z}[x].$$

Tetszőleges $q(x) \in \mathbb{Z}[x]$ -re

$$(1) \quad (u(x)w(x) + q(x)h_{\alpha}(x))g_{\alpha}(x) + (v(x)w(x) - q(x)g_{\alpha}(x))h_{\alpha}(x) \equiv w(x) \pmod{p}.$$

Legyen ezért q a vw polinomnak a g_{α} polinommal $\mathbb{Z}_p$ felett való osztásánál fellépő
hányados, $\bar{g} = vw - qg_{\alpha}$ és $\bar{h} = uw + qh_{\alpha}$, mindkettő $\mathbb{Z}_p$ felett kiszámolva. Mivel
 $\bar{g}$ a vw polinomnak g_{α} -val való osztásánál fellépő maradék, $\deg(\bar{g}) < \deg(g_{\alpha})$. Mivel
 $\deg(w) < \deg(f) = \deg(g_{\alpha}) + \deg(h_{\alpha})$, azt kapjuk, hogy $\deg(\bar{h}) < \deg(h_{\alpha})$, mivel egyéb-
ként az (1) kongruencia nem teljesülhetne a foksámok eltérése miatt.

Ha $\bar{\bar{g}}$ és $\bar{\bar{h}}$ másik megoldás, akkor

$$(\bar{h}(x) - \bar{\bar{h}}(x))g_{\alpha}(x) \equiv (\bar{\bar{g}}(x) - \bar{g}(x))h_{\alpha}(x) \pmod{p}.$$

Mivel $\mathbb{Z}_p$ felett g_{α} és h_{α} relatív prímek, g_{α} osztja $\bar{\bar{g}} - \bar{g}$ -t. Mivel ennek fokszáma kisebb,
mint g_{α} fokszáma, csak nulla lehet. Innen a másik oldal is nulla, így $\bar{h} = \bar{\bar{h}}$ is következik.
 $\square$

*** 8.3.116. Megjegyzés.** A Hensel-lemma felhasználható egész együtthatós polinomok
faktorizálására. Először is, akármilyen nem nulla, akár komplex együtthatós n -ed fokú

$$f = f_0 + f_1x + \cdots + f_nx^n$$

polinomra, ha $f = gh$, $\deg(g) = m$, $g = g_0 + g_1x + \cdots + g_mx^m$, akkor

$$|g_j| \leq \binom{m-1}{j} \|f\| + \binom{m-1}{j-1} |f_n|, \quad \text{ha} \quad j = 0, 1, \dots, m,$$

ahol $\|f\|$ az $|f_0|^2 + |f_1|^2 + \dots + |f_n|^2$ összeg négyzetgyöke. (Lásd Knuth [46], 4.6.2–20 feladat.)

Már tudjuk, hogy elég csak egy $f \in \mathbb{Z}[x]$ négyzetmentes polinom faktorizálásával foglalkozni, hiszen ha $\deg(f) > 1$ és $d = \text{lnc}(f, f')$, akkor $f = d \cdot (f/d)$ egy alacsonyabb fokúakra való felbontás, és f/d négyzetmentes. Csak primitív polinomok faktorizálásával fogunk foglalkozni. (Az együtthatók legnagyobb közös osztójának faktorizálása ennél nehezebb feladat!) Ha az f négyzetmentes primitív polinom felírható nem triviális módon gh alakban, ahol $g, h \in \mathbb{Z}[x]$, akkor g és h primitív polinomok, relatív prímek, továbbá $f \equiv gh \pmod{p^\alpha}$ minden p príme és $\alpha \in \mathbb{N}^+$ -ra. Keressünk egy prímet, amely nem osztja az f főegyütthatóját. A prímet válasszuk úgy, hogy $f \pmod{p}$ négyzetmentes legyen (megmutatható, hogy ez mindig teljesül, ha p nem osztója egy, csak az f polinomtól függő számnak, az f úgynevezett *diszkrimináns*ának: lásd Knuth [46], 4.6.2–23 és 4.6.1–12 feladatok). Szorozzuk meg $f(x)$ -et f_n -nel, és alakítsuk szorzattá az $f^* = f_n f(x)$ polinomot modulo p . Mindkét tényezőt végigszorozva egy $\mathbb{Z}_p$ -beli egységgel, elérhetjük, hogy mindkét tényezőben a főegyüttható f_n -nel kongruens modulo p . A főegyütthatókat mindkét tényezőben kicserélve f_n -re, a kapott $g_1(x)$, $h_1(x)$ polinomokra teljesülnek a Hensel-lemma feltételei $\alpha = 1$ -re. A Hensel-lemma segítségével „felemelve” ezt a felbontást egy modulo p^α vett felbontássá, megtalálhatjuk $f^*(x)$ egy $g^*(x)h^*(x)$ szorzattá bontását, amelyre $g^*(x) \equiv g_1(x) \pmod{p}$ és $h^*(x) \equiv h_1(x) \pmod{p}$, ha van ilyen. Az α kitevőt olyan nagynak kell választani, hogy p^α nagyobb legyen g^* és h^* együtthatói abszolút értéke egy korlátjának a kétszeresénél, és célszerű a maradékosztályokat a legkisebb abszolút értékű maradékukkal reprezentálni, mert ekkor közvetlenül g^* és h^* együtthatóit kapjuk. A g^* és h^* primitív részét véve, f egy szorzatfelbontását kapjuk, és így nyilván minden szorzatfelbontás kiadódik, hiszen mindegyiknek van valamilyen képe modulo p .

8.3.117. Feladat [4]. Oldjuk meg az alábbi kongruenciákat:

- (1) $x^3 + 2x - 3 \equiv 0 \pmod{9}$;
- (2) $x^3 + 2x - 3 \equiv 0 \pmod{5}$;
- (3) $x^3 + 2x - 3 \equiv 0 \pmod{45}$;
- (4) $x^3 + 4x + 8 \equiv 0 \pmod{15}$;
- (5) $x^3 - 9x^2 + 23x - 15 \equiv 0 \pmod{503}$;
- (6) $x^3 - 9x^2 + 23x - 15 \equiv 0 \pmod{143}$.

* **8.3.118. Feladat [4].** Oldjuk meg az alábbi kongruenciákat:

- (1) $x^5 + x^4 + 1 \equiv 0 \pmod{3^4}$;
- (2) $x^3 + x + 57 \equiv 0 \pmod{5^3}$;
- (3) $x^2 + 5x + 24 \equiv 0 \pmod{36}$;
- (4) $x^3 + 10x^2 + x + 3 \equiv 0 \pmod{3^2}$;
- (5) $x^3 + x^2 - 4 \equiv 0 \pmod{7^3}$;
- (6) $x^3 + x^2 - 5 \equiv 0 \pmod{7^3}$.

8.3.119. Feladat [4]. Oldjuk meg az alábbi kongruenciákat:

- (1) $x^{11} + x^8 + 5 \equiv 0 \pmod{7}$;
- (2) $x^{20} + x^{13} + x^7 + x \equiv 0 \pmod{7}$;

$$(3) \quad x^{15} - x^{10} + 4x - 3 \equiv 0 \pmod{7};$$

$$(4) \quad 2x^3 + 5x^2 + 6x + 1 \equiv 0 \pmod{13};$$

$$(5) \quad x^{14} + 12x^2 \equiv 0 \pmod{13}.$$

* **8.3.120. Feladat [4].** Oldjuk meg modulo 540 az

$$x^{79} + 3x^{78} + 2x^{77} + 539x^7 + 537x^6 + 538x^5 + x^2 + 447x \equiv 0$$

kongruenciát.

8.3.121. Racionális törtfüggvények. Ha R integritási tartomány, akkor $R[x]$ is, így képezhetjük a hányadostestét; ezt $R(x)$ -szel jelöljük, és az elemeit R feletti *racionális függvényeknek* nevezzük.

→ **8.3.122. Feladat [5].** Mutassuk meg, hogy $\mathbb{Z}[x]$ hányadosteste izomorf $\mathbb{Q}(x)$ -szel.

8.3.123. Parciális törtekre bontás. Legyen K test, $g_1, g_2, \dots, g_n \in K[x]$ legalább elsőfokú páronként relatív prím polinomok, $g = g_1 g_2 \cdots g_n$. Ekkor léteznek olyan

$$f_1, f_2, \dots, f_n \in K[x]$$

polinomok, amelyekkel (a hányadostestben)

$$\frac{1}{g} = \frac{f_1}{g_1} + \frac{f_2}{g_2} + \cdots + \frac{f_n}{g_n}.$$

A tételt az integrálásnál használjuk $\mathbb{R}$ illetve $\mathbb{C}$ feletti polinomokra.

Bizonyítás. Indukcióval bizonyítunk. Ha $n = 1$, az állítás nyilvánvaló. Ha $n = 2$, akkor a kiterjesztett euklideszi algoritmussal kaphatunk olyan f_1, f_2 polinomokat, amelyekre $f_1 g_2 + f_2 g_1 = 1$, amit $g_1 g_2$ -vel osztva kapjuk az állítást. Végül az általános eset úgy következik, hogy a $g_1, g_2, \dots, g_{n-2}, g_{n-1} g_n$ polinomokra alkalmazva az indukciós feltevést, kapunk egy

$$\frac{1}{g} = \frac{f_1}{g_1} + \frac{f_2}{g_2} + \cdots + \frac{f_{n-2}}{g_{n-2}} + \frac{f^*}{g_{n-1} g_n}$$

előállítást, majd az $n = 2$ speciális esetből kapott

$$\frac{1}{g_{n-1} g_n} = \frac{f_{n-1}^*}{g_{n-1}} + \frac{f_n^*}{g_n}$$

előállítás mindkét oldalát szorozzuk f^* -gal, és ezt írjuk az utolsó tag helyére. $\square$

8.3.124. Következmény. Ha $h \in K[x]$, akkor léteznek olyan $h_j \in K[x]$ polinomok, amelyekkel

$$\frac{h}{g} = \frac{h_1}{g_1} + \frac{h_2}{g_2} + \cdots + \frac{h_n}{g_n}.$$

Bizonyítás. Szorozzuk a tételben kapott előállítás mindkét oldalát h -val. $\square$

8.3.125. Következmény. Az előző következményben kapott előállítás felírható

$$\frac{h}{g} = p + \frac{h_1}{g_1} + \frac{h_2}{g_2} + \cdots + \frac{h_n}{g_n}$$

alakban is, ahol $p \in K[x]$, és $\deg(h_j) < \deg(g_j)$, ha $j = 1, \dots, n$.

Bizonyítás. Minden tagban osszuk maradékosan a számlálót a nevezővel. $\square$

8.3.126. Megjegyzés. Ha a $g_1, g_2, \dots, g_n$ polinomokat a g -nek irreducibilis polinomok szorzataként történő előállításából kaptuk, akkor az előző következményben szereplő törtek u/v^k alakúak, ahol $\deg(u) < \deg(v^k)$. Ezek a törtek felírhatók

$$\frac{u}{v^k} = \frac{u_k}{v^k} + \frac{u_{k-1}}{v^{k-1}} + \cdots + \frac{u_1}{v}$$

alakban, ahol $\deg(u_j) < \deg(v)$, ha $j = 1, \dots, k$. Ez $k = 1$ esetén nyilvánvaló, egyébként pedig k szerinti indukcióval következik, ha u -t maradékosan osztjuk v -vel, majd mindkét oldalt végigosztjuk v^k -vel.

→ **8.3.127. Feladat [6].** Bontsuk parciális törtekre az alábbi racionális törtfüggvényeket $\mathbb{R}$, illetve $\mathbb{C}$ felett:

(1)

$$\frac{x^2 + 1}{x(x^2 - 1)}, \quad \frac{2}{(x - 1)(x - 2)(x - 3)}, \quad \frac{x^5 - x^3 - x^2}{x^2 - 1};$$

(2)

$$\frac{x^2}{(x - 1)^2(x + 1)}, \quad \frac{4}{(x^2 - 1)^2}, \quad \frac{x^6 - x^2 + 1}{(x - 1)^3};$$

(3)

$$\frac{x^2 + 1}{(x^2 + x + 1)^2}, \quad \frac{x^4 + 1}{x^3(x^2 + 1)}, \quad \frac{2}{x^4 + 2x^3 + 2x^2 + 2x + 1};$$

(4)

$$\frac{8}{x^4 + 4}, \quad \frac{2x^4}{x^4 + x^2 + 1}, \quad \frac{1 - x^2}{1 - 2x \cos \varphi + x^2};$$

(5)

$$\frac{3x^3 + 15x + 6}{x^4 + x^3 + 3x^2 + 2x + 2}, \quad \frac{2x^3 + 4x}{x^4 + x^2 + 4}, \quad \frac{3x^2 - 3}{x^3 - 3x + 1}.$$

8.3.128. Többhatározatlanú polinomok. Legyen R gyűrű, $n \in \mathbb{N}$. Az R feletti n -határozatlanú polinomok gyűrűjét n szerinti rekurzióval definiáljuk: ha $n = 0$, legyen $R[x_1, x_2, \dots, x_n] = R$, az egyhatározatlanú polinomok gyűrűjét már definiáltuk, ha pedig $n > 1$, akkor legyen $R[x_1, x_2, \dots, x_n] := R[x_1, x_2, \dots, x_{n-1}][x_n]$, azaz az n határozatlanú polinomok olyan polinomjai x_n -nek, amelynek együtthatói az $x_1, x_2, \dots, x_{n-1}$ határozatlanok polinomjai. Nyilván $x_1, x_2, \dots, x_n$ helyett bármilyen más betűk is szerepelhetnek. Néha egy $f \in R[x_1, x_2, \dots, x_n]$ polinomra inkább az $f(x_1, x_2, \dots, x_n)$ jelölést fogjuk használni. A rekurzív definíció miatt azok a tulajdonságok, amelyek öröklődnek a gyűrűről a polinomgyűrűre, a többhatározatlanú polinomok gyűrűjére is öröklődnek.

Könnyen látható, hogy az n -határozatlanú polinomok

$$\sum_{i_1, i_2, \dots, i_n} f_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

alakú véges összegek, ahol $x_1, x_2, \dots, x_n$ a „határozatlanok” és $f_{i_1, i_2, \dots, i_n} \in R$. Az $a \in R$ elemhez hozzárendelve azt az f polinomot, amelyre $f_{0,0,\dots,0} = a$ és $f_{i_1, i_2, \dots, i_n} = 0$ egyébként, az R egy olyan leképezését kapjuk a polinomok gyűrűjébe, amely nyilván monomorfizmus, értékkészletének elemei a *konstans polinomok*, ezeket R elemeivel azonosíthatjuk. Az

$$f_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

tagot *monom*nak nevezzük, $f_{i_1, i_2, \dots, i_n}$ az *együtthatója*, $(i_1, i_2, \dots, i_n)$ a *multifoka*, $i_1 + \dots + i_n$ pedig a *foka*. Az n -határozatlanú polinomok jelölésére a hagyományos

$$(1) \quad f = \sum_{i_1 + i_2 + \dots + i_n \leq m} f_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

felírást fogjuk használni. Gyakran az x_j^0 alakú tényezőket nem írjuk ki, x_j^1 helyett pedig x_j -t írunk. Az (egyetlen) nulladfokú tag együtthatója a polinom *konstans tagja*. Mivel az (1) felírásból a nulla együtthatójú tagokat szokás elhagyni, illetve a felírásához további nulla együtthatójú tagok adhatók hozzá, a felírás nem egyértelmű. Egyértelművé válik azonban, ha kikötjük, hogy m minimális legyen, és minden m -nél nem magasabb fokú tag – egyszer – szerepeljen. Ez a minimális m a polinom *foka*, jelölése $\deg(f)$. (Egy másik lehetőség a felírás egyértelművé tételére, hogy minden nulla együtthatójú tagot elhagyunk.) A nulla polinom egyértelmű felírása az üres összeg, és fokát $-\infty$ -nek definiáljuk. A konstans polinomok a legfeljebb nulladfokú polinomok. A legfeljebb elsőfokú polinomok a *lineáris polinomok*. Ha egy polinom minden (nem nulla) tagjának ugyanaz a k a foka, akkor k -adfokú *homogén polinom*nak nevezzük.

A definícióból adódik, hogy az összeadás és szorzás tagonként történik: ha

$$g = \sum_{i_1 + i_2 + \dots + i_n \leq m} g_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

egy másik polinom, akkor összegük az

$$f + g = \sum_{i_1 + i_2 + \dots + i_n \leq m} (f_{i_1, i_2, \dots, i_n} + g_{i_1, i_2, \dots, i_n}) x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

polinom, szorzatuk pedig az a $h = fg$ polinom, amelyre

$$h_{k_1, k_2, \dots, k_n} = \sum_{i_1 + j_1 = k_1, \dots, i_n + j_n = k_n} f_{i_1, i_2, \dots, i_n} g_{j_1, j_2, \dots, j_n}.$$

Vegyük észre, hogy ha f legfeljebb m -edfokú, g legfeljebb l -edfokú, akkor h legfeljebb $m + l$ -edfokú. Ha az R gyűrű nullosztómentes, akkor az $R[x_1, x_2, \dots, x_n]$ gyűrű is nullosztómentes, és két polinom szorzatának a foka a fokok összege.

Ha R egységelemes az 1 egységelemmel, akkor $R[x_1, \dots, x_n]$ is egységelemes, benne az $f_{0,0,\dots,0} = 1$ és egyébként $f_{i_1,i_2,\dots,i_n} = 0$ összefüggéssel definiált polinom egységelem. Az

$$f_{i_1,i_2,\dots,i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

tag szokásos írásmódja $f_{i_1,i_2,\dots,i_n} = 1$ esetén

$$x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}.$$

Számítógépen vagy az m fokszámot és az együtthatók $f_{i_1,i_2,\dots,i_n}$, $i_j \leq m$, ha $j = 1, 2, \dots, n$ tömbjét tároljuk, vagy a nem nulla együtthatókra az

$$((i_1, i_2, \dots, i_n), f_{i_1,i_2,\dots,i_n})$$

párok egy láncolt listáját.

* **8.3.129. Multiindexek.** Többhatározatlanú polinomok felírása tömörebbé tehető az alábbi módon: az $\mathbb{N}^n$ elemeit általában *multiindexeknek* fogjuk nevezni. Multiindexek összegét koordinátáinként definiáljuk. Ha $i = (i_1, i_2, \dots, i_n)$, akkor legyen $|i| = i_1 + i_2 + \cdots + i_n$ és $x^i = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$. Ezzel a jelöléssel az f polinom $\sum_{|i| \leq m} f_i x^i$ véges összegként írható. (Tulajdonképpen f egy olyan $\mathbb{N}^n$ -et R -be képező függvénnyel azonosítható, amely véges sok helyen vesz fel nem nulla értéket.) Az $f_i x^i$ monom multifoka i , foka $|i|$.

Ha $f = \sum_i f_i x^i$ és $g = \sum_i g_i x^i$ polinomok, akkor összegük a $\sum_i (f_i + g_i) x^i$ polinom, szorzatuk pedig az a $h = fg$ polinom, amelyre $h_k = \sum_{i,j \in \mathbb{N}^n, i+j=k} f_i g_j$, ha $k \in \mathbb{N}^n$.

* **8.3.130. Formális hatványsorok.** Ha R egy gyűrű, akkor az R feletti n *határozatlanú formális hatványsorok* $R[[x_1, x_2, \dots, x_n]]$ gyűrűjét mint $R[[x_1, x_2, \dots, x_{n-1}]][[x_n]]$ -et definiáljuk (az $n = 0$ esetben legyen $R[[x_1, x_2, \dots, x_n]] = R$; az $n = 1$ esetet már definiáltuk), elemeit $\sum_{i \in \mathbb{N}^n} f_i x^i$ alakban írjuk.

8.3.131. Tétel. Ha R egy Gauss-gyűrű, $n \in \mathbb{N}$, akkor $R[x_1, x_2, \dots, x_n]$ is Gauss-gyűrű.

Bizonyítás. Gauss tételének felhasználásával indukcióval következik, mivel

$$R[x_1, x_2, \dots, x_n] = R[x_1, x_2, \dots, x_{n-1}][x_n]. \quad \square$$

8.3.132. Megjegyzés. Ha $n > 1$, akkor $R[x_1, x_2, \dots, x_n]$ nem tehető euklideszi gyűrűvé, még akkor sem, ha R test, mert 1 az x_1 és x_2 polinomok legnagyobb közös osztója, de semmilyen $p_1(x_1, x_2)$, $p_2(x_1, x_2)$ polinomokkal nem áll elő $x_1 p_1(x_1, x_2) + x_2 p_2(x_1, x_2)$ alakban, mert mindkét szorzat konstans tagja nulla.

* **8.3.133. Szimmetrikus polinomok.** Legyen R egységelemes integritási tartomány. Az $f \in R[x_1, x_2, \dots, x_n]$ polinomot *szimmetrikus polinomnak* nevezzük, ha bármely két határozatlan megcserélésekor ugyanaz marad. (Ha ilyenkor a polinom ellentettjére változik, akkor *alternálónak* nevezzük.)

Tekintsük például az

$$f = (z - x_1)(z - x_2) \cdots (z - x_n) \in R[x_1, x_2, \dots, x_n, z]$$

polinomot. Ezt $z^n - s_1 z^{n-1} + s_2 z^{n-2} - \dots + (-1)^n s_n$ alakba írva, $s_1, s_2, \dots, s_n$ az $x_1, x_2, \dots, x_n$ változóknak nyilván szimmetrikus polinomjai, mert

$$s_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k}$$

alakba írhatók; ezek az *elemi szimmetrikus polinomok*. Nyilván s_k egy k -ad fokú homogén polinom. Szimmetrikus polinomok például a

$$\sigma_k = \sum_{i=1}^n x_i^k, \quad k = 0, 1, \dots$$

hatványösszegek is.

Egy $f_i x^i \in R[x_1, x_2, \dots, x_n]$ nem nulla monom *súlyán* az $i_1 + 2i_2 + 3i_3 + \dots + ni_n$ számot értjük; ez függ a határozatlanok sorrendjétől is. Az $f \neq 0$ polinom *súlyán* a benne nem nulla együtthatóval fellépő $f_i x^i$ monomok súlyainak maximumát értjük; a nulla polinom súlya $-\infty$.

*** 8.3.134. Szimmetrikus polinomok alaptétele.** Az R egységelemes integritási tartomány feletti minden $f \in R[x_1, x_2, \dots, x_n]$ szimmetrikus polinomhoz található olyan egyértelműen meghatározott $F \in R[y_1, y_2, \dots, y_n]$ polinom, amelyre

$$f(x_1, \dots, x_n) = F(s_1(x_1, \dots, x_n), \dots, s_n(x_1, \dots, x_n)),$$

ahol $s_1, s_2, \dots, s_n$ az $x_1, x_2, \dots, x_n$ határozatlanok elemi szimmetrikus polinomjai. Ha f fokszáma d , akkor F súlya is d .

Bizonyítás. Az előállítás létezését n szerinti indukcióval bizonyítjuk. Ha $n = 1$, az egész állítás nyilvánvaló. Ha $n - 1$ -re van előállítás, akkor n -re ugyanezt d szerinti teljes indukcióval bizonyítjuk. Ha f konstans polinom, azaz ha $d \leq 0$, akkor ez triviális. Tegyük fel, hogy az előállítás minden d -nél alacsonyabb fokú polinomra létezik. Legyen $f(x_1, \dots, x_n)$ foka d . Ekkor van olyan $F^*(y_1, \dots, y_{n-1})$ polinom, amelynek súlya nem nagyobb, mint d , és amelyre

$$f(x_1, \dots, x_{n-1}, 0) = F^*(s_1^*, s_2^*, \dots, s_{n-1}^*),$$

ahol $s_1^*, s_2^*, \dots, s_{n-1}^*$ az $x_1, x_2, \dots, x_{n-1}$ határozatlanok elemi szimmetrikus polinomjai. Mivel definíció szerint

$$(z - x_1) \dots (z - x_{n-1}) = z^{n-1} - s_1^* z^{n-2} + \dots + (-1)^{n-1} s_{n-1}^*,$$

az összefüggést z -vel szorozva

$$(z - x_1) \dots (z - x_{n-1}) z = z^n - s_1^* z^{n-1} + \dots + (-1)^{n-1} s_{n-1}^* z,$$

azaz az s_j^* polinomok úgy állnak elő a megfelelő $s_j \in R[x_1, \dots, x_n]$ elemi szimmetrikus polinomokból, hogy x_n helyére nullát írunk.

Megmutatjuk, hogy $F^*(s_1, \dots, s_{n-1})$ foka $x_1, \dots, x_n$ -ben legfeljebb d . Ugyanis $F^*(y_1, \dots, y_{n-1})$ -ben csak olyan $F_{i_1, \dots, i_{n-1}}^* y_1^{i_1} \cdots y_{n-1}^{i_{n-1}}$ monomok léphetnek fel, amelyekre $i_1 + 2i_2 + \cdots + (n-1)i_{n-1} \leq d$. Az $y_i \leftarrow s_i$ helyettesítés során ez a monom az

$$F_{i_1, \dots, i_{n-1}}^* s_1^{i_1} s_2^{i_2} \cdots s_{n-1}^{i_{n-1}}$$

polinomba megy át, ami, figyelembe véve, hogy s_j foka j , az $x_1, \dots, x_n$ határozatlanoknak legfeljebb d -ed fokú polinomja.

Tekintsük most az

$$f^*(x_1, \dots, x_n) = f(x_1, \dots, x_n) - F^*(s_1, \dots, s_{n-1})$$

legfeljebb d -ed fokú polinomot. Ez az $x_1, \dots, x_n$ határozatlanok szimmetrikus polinomja, mert a különbség első tagja szimmetrikus polinom, a második tagja pedig szimmetrikus polinomok polinomja, így szintén szimmetrikus polinom. Fennáll továbbá, hogy $f^*(x_1, \dots, x_{n-1}, 0) = 0$, így x_n osztója $f^*(x_1, \dots, x_n)$ -nek, azaz f^* -nak nincsenek olyan tagjai, amelyekben x_n a nulladik hatványon szerepel. Az f^* szimmetrikussága miatt tetszőleges j -re $f^*(x_1, \dots, x_{j-1}, 0, x_{j+1}, \dots, x_n) = 0$ is fennáll. Innen az következik, hogy f^* minden tagjában x_j legalább az első hatványon szerepel. Tehát $s_n = x_1 \cdots x_n$ osztója az f^* polinomnak:

$$f^*(x_1, \dots, x_n) = s_n f^{**}(x_1, \dots, x_n),$$

ahol f^{**} szimmetrikus polinom, és a foka legfeljebb $d - n < d$. Indukciós feltevésünk szerint van olyan legfeljebb $d - n$ súlyú $F^{**}(y_1, \dots, y_n)$ polinom, amelyre

$$f^{**}(x_1, \dots, x_n) = F^{**}(s_1, \dots, s_n),$$

tehát

$$f^*(x_1, \dots, x_n) = s_n F^{**}(s_1, \dots, s_n).$$

Innen

$$f(x_1, \dots, x_n) = F^*(s_1, \dots, s_n) + s_n F^{**}(s_1, \dots, s_n),$$

és a jobb oldalon álló mindkét tag, tehát összegük is, legfeljebb d súlyú $x_1, \dots, x_n$ -ben. Így

$$F(s_1, \dots, s_n) = F^*(s_1, \dots, s_n) + s_n F^{**}(s_1, \dots, s_n)$$

választható.

Indukcióval megmutatjuk, hogy az elemi szimmetrikus polinomok *algebrailag függetlenek* R felett, ami azt jelenti, hogy tetszőleges $F(y_1, \dots, y_n)$ nem nulla polinomra $F(s_1, \dots, s_n) \in R[x_1, \dots, x_n]$ nem nulla polinom. Ha két előállítás különbségére alkalmazzuk, akkor ebből azonnal következik a tételben szereplő előállítás egyértelműsége.

Ha $s_1, \dots, s_n$ nem lennének algebrailag függetlenek, akkor létezne egy minimális fokszerű $F(y_1, y_2, \dots, y_n)$ polinom, amelyre

$$F(s_1, \dots, s_n) = 0.$$

Tekintsük F -et mint $R[y_1, \dots, y_{n-1}][y_n]$ elemét, és legyen

$$F(y_1, \dots, y_n) = F_0(y_1, \dots, y_{n-1}) + F_1(y_1, \dots, y_{n-1})y_n + \cdots + F_d(y_1, \dots, y_{n-1})y_n^d.$$

Itt $F_0 \neq 0$, mert egyébként y_n osztója lenne F -nek, mondjuk

$$F(y_1, \dots, y_n) = y_n G(y_1, \dots, y_n)$$

következne, amiből viszont

$$F(s_1, \dots, s_n) = s_n G(s_1, \dots, s_n),$$

és így $G(s_1, \dots, s_n) = 0$ következne. Mivel $G(y_1, \dots, y_n)$ foka kisebb $F(y_1, \dots, y_n)$ fokánál, ez ellentmondana F fokszáma minimalitásának. Az $y_j \leftarrow s_j$ helyettesítés után

$$F(s_1, \dots, s_n) = F_0(s_1, \dots, s_{n-1}) + F_1(s_1, \dots, s_{n-1})s_n + \dots + F_d(s_1, \dots, s_{n-1})s_n^d.$$

Tekintsük ezt mint $x_1, \dots, x_n$ polinomját, és vegyük az $x_n = 0$ helyen. Mivel ekkor $s_n = 0$, azt kapjuk, hogy

$$0 = F_0(s_1^*, \dots, s_{n-1}^*).$$

Mivel $F_0 \neq 0$, nem triviális összefüggést találtunk $x_1, x_2, \dots, x_{n-1}$ elemi szimmetrikus polinomjai, azaz $s_1^*, s_2^*, \dots, s_{n-1}^*$ között, ami ellentmond indukciós feltevésünknek. $\square$

*** 8.3.135. Newton képletei.** Ha az R egységelemes integritási tartomány felett az $x_1, x_2, \dots, x_n$ határozatlanok elemi szimmetrikus polinomjai $s_1, s_2, \dots, s_n$, és σ_i , $i = 1, 2, \dots$ a megfelelő hatványösszegek, akkor fennállnak a

$$\begin{aligned} \sigma_1 - s_1 &= 0, \\ \sigma_2 - s_1\sigma_1 + 2s_2 &= 0, \\ &\vdots \\ \sigma_{n-1} - s_1\sigma_{n-2} + \dots + (-1)^{n-2}s_{n-2}\sigma_1 + (-1)^{n-1}(n-1)s_{n-1} &= 0 \end{aligned}$$

és

$$(2) \quad \sigma_{k+n} - s_1\sigma_{k+n-1} + \dots + (-1)^n s_n \sigma_k = 0 \quad (k = 0, 1, \dots)$$

egyenletek.

Bizonyítás. Tekintsük az

$$f(z) = (z - x_1) \cdots (z - x_n) = z^n + a_1 z^{n-1} + \dots + a_n, \quad a_k = (-1)^k s_k$$

polinomot. Mivel $f(x_i) = 0$ ($i = 1, 2, \dots, n$),

$$\sum_{i=1}^n x_i^k f(x_i) = 0, \quad \text{ha } k \geq 0.$$

Ez azt jelenti, hogy

$$\sum_{i=1}^n (x_i^{k+n} + a_1 x_i^{k+n-1} + \dots + a_n x_i^k) = \sigma_{k+n} + a_1 \sigma_{k+n-1} + \dots + a_n \sigma_k = 0,$$

tehát a (2) egyenletek fennállnak.

Legyen $h_i(z) = \prod_{j \neq i} (z - x_j)$. Ekkor

$$f(z) = (z - x_i)h_i(z).$$

Másrészt, felhasználva, hogy

$$z^j - x_i^j = (z - x_i) \left(z^{j-1} + z^{j-2}x_i + \cdots + zx_i^{j-2} + x_i^{j-1} \right),$$

és, hogy $f(x_i) = 0$, ha a_0 a gyűrű egységeleme, azt kapjuk, hogy

$$\begin{aligned} f(z) &= f(z) - f(x_i) = (a_n - a_n) + a_{n-1}(z - x_i) + \cdots + a_0(z^n - x_i^n) \\ &= (z - x_i) \sum_{k=0}^{n-1} a_k \sum_{j=0}^{n-k-1} x_i^j z^{n-k-j-1}. \end{aligned}$$

Innen $h_i(z)$ az utolsó kifejezés $z - x_i$ utáni része. Ezt, valamint a szorzat differenciálási szabályából adódó $f'(z) = \sum_{i=1}^n h_i(z)$ összefüggést felhasználva

$$\begin{aligned} f'(z) &= \sum_{i=1}^n h_i(z) = \sum_{i=1}^n \sum_{k=0}^{n-1} a_k \sum_{j=0}^{n-k-1} x_i^j z^{n-k-j-1} \\ &= \sum_{k=0}^{n-1} \sum_{j=0}^{n-k-1} \sum_{i=1}^n a_k x_i^j z^{n-k-j-1} \\ &= \sum_{t=0}^{n-1} z^{n-t-1} \sum_{j+k=t} a_k \sum_{i=1}^n x_i^j \\ &= \sum_{t=0}^{n-1} \left(\sum_{k+j=t} a_k \sigma_j \right) z^{n-i-1}, \end{aligned}$$

ahol $\sigma_0 = na_0$. Mivel másrészt $f'(z) = \sum_{t=0}^{n-1} (n-t)a_t z^{n-t-1}$, az együtthatók összehasonlításával

$$(n-t)a_t = \sum_{k+j=t} a_k \sigma_j, \quad t = 1, \dots, n-1.$$

Ez az (1)-ben szereplő $n-1$ egyenlet. $\square$

→ **8.3.136. Feladat** [5]. Mutassuk meg, hogy minden $f: \{\uparrow, \downarrow\}^n \rightarrow \{\uparrow, \downarrow\}$ logikai függvény valamely, az $(\{\uparrow, \downarrow\}, (\oplus, \wedge))$ gyűrű feletti n határozatlanú polinomhoz tartozó polinomfüggvény. (Ez a logikai függvény *Zsegalkin-polinomja*.)

* **8.3.137. Feladat** [4]. Határozzuk meg a d paraméter értékét, ha $2x^3 - x^2 - 7x + d$ két gyökének összege 1.

* **8.3.138. Feladat** [4]. Számítani szeretnénk a $8x^3 - 12x^2 - 2x + 3$ gyökei?

* **8.3.139. Feladat** [4]. A Newton-formulák felhasználásával számítsuk ki az alábbi polinomok gyökeinek négyzetösszegét:

- (1) $x^3 + 2x - 3$;
- (2) $x^5 - 5x^3 + 5x - 2$.

* **8.3.140. Feladat [4].** Mutassuk meg, hogy $\mathbb{C}[x, y]/(x)$ izomorf $\mathbb{C}[y]$ -nal.

8.3.141. További feladatok megoldásokkal. [28], [29]: 1.1–1.3, 1.6, 1.9–1.14, 1.16–1.27, 1.29–1.31, 1.33–1.37, 1.39–1.169, 2.6–2.15, 2.17–2.41, 2.38, 2.44–2.122, 3.1–3.16, 1.3.25–3.46, 3.62–3.64.

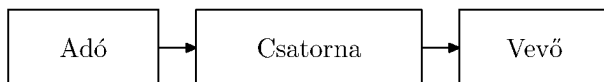
8.3.142. További feladatok. [3]: V.4, V.8, V.45, V.48–V.51, V.53, 1.V.75, V.79, V.109, V.110, V.120, V.125–V.127, V.190–V.192, V.106, 1.VI.2–VI.4, VI.6–VI.26, VI.53–V.87; [17]: 75–80, 538–569, 1.582–660, 663–685, 755–817, 856–867; [57]: 1.2–5–1.6–29, 1.1.6–32–1.6–37, 2.0–1–2.0–2, 2.0–4–2.0–5, 2.0–10–2.0–15, 2.0–18, 1.2.0–28, 2.0–30, 2.0–32, 3.1–1–3.2–9; [69]: 2.2.1–2.2.4, 1.2.6.4–2.6.5, 2.8.1, 2.9.1–2.9.19, 9.1.1–9.1.4; [83]: 1.IX.4.6–IX.4.9, IX.4.16–IX.4.22, IX.4.26, XIII.3.8.

Kódolás

Ebben a fejezetben a kódolás alapjaival foglalkozunk. Elsőként nagyon sematikusán áttekintjük, hogy hogyan történik az adatok átvitele. Ezután két kérdéssel foglalkozunk részletesebben: a gazdaságos, valamint a hibakorlátozó kódolással. A rejtjelzéssel itt nem foglalkozunk.

9.1 Kommunikáció és kódolás

A *kommunikáció* során információt hordozó *adatokat* viszünk át egy *csatornán* keresztül az *információforrástól*, az *adótól* az információ címzettjéhez, a *vevőhöz*. Ezt vázlatosan a 9.1.1 ábra mutatja.



9.1.1 ábra: Kommunikáció.

Az ábra szerint az információ átvitele térben történik. Valójában minden információátvitel térben és időben történik, és egyes esetekben az egyik, míg más esetekben a másik dimenzió a domináns. Ha telefonálunk, akkor a távolság a fontosabb, ugyanakkor az információ adathordozóra való rögzítése és egy későbbi időpontban való visszaolvasása esetén a helyváltozás kevésbé fontos. A továbbiakban általában úgy beszélünk az adatátvitelről, mintha az térben történne, de ebbe mindig beleértjük az időbeliséget is.

A modellel kapcsolatban felmerül néhány kérdés:

- (1) mi az információ, és hogyan mérhető az információ;
- (2) hogyan történik az információ átvitele;
- (3) milyen kapcsolat van az elküldött és a vett adat között.

9.1.1. Információ, bit, entrópia. Az információról mindenkinek van valamilyen intuitív fogalma. A nagyszámú definíció közül itt azt említjük meg, amely szerint az *információ* új ismeret. Az információt Shannon nyomán az általa megszüntetett bizonytalansággal mérjük. Tegyük fel, hogy egy információforrás nagy számú, összesen n üzenetet bocsát ki. Az összes ténylegesen előforduló különböző üzenet legyen $a_1, a_2, \dots, a_m$ ($m \in \mathbb{N}^+$). Ha az a_i üzenet k_i -szer fordul elő, akkor azt mondjuk, hogy *gyakorisága* k_i , *relatív gyakorisága* pedig $p_i = k_i/n > 0$. A $p_1, p_2, \dots, p_m$ szám- m -est az üzenetek *eloszlásának* nevezzük. Nyilván $\sum_{i=1}^m p_i = 1$. Az a_i üzenet *egyedi információtartalmának* célszerű definíciója $I_i = -\log_r p_i$, ahol r egy 1-nél nagyobb valós szám. A logaritmus alapja az *információ egységét* határozza meg. Amennyiben az alap 2, akkor az információ egysége a *bit*, és ilyenkor $\log_r p_i$ helyett egyszerűen $\log p_i$ -t írunk. (Az informatikában általánosan elterjedt szokás a kettes alapú logaritmust egyszerűen $\log$ -gal jelölni.) Többnyire

nem az egyes üzenetek egyedi információtartalma, hanem az üzenetforrás által kibocsátott üzenetek $H_r(p_1, \dots, p_m) = -\sum_{i=1}^m p_i \log_r p_i$ *átlagos információtartalma* érdekes, ez a forrás *entrópiája*, amely csak az üzenetek eloszlásától függ, de tartalmuktól nem.

Általánosabban, egy m tagú *eloszlás* egy pozitív valós számokból álló $p_1, p_2, \dots, p_m$ sorozat, amelyre $\sum_{i=1}^m p_i = 1$. Az eloszlás *entrópiáját* a

$$H_r(p_1, \dots, p_m) = -\sum_{i=1}^m p_i \log_r p_i$$

összefüggéssel értelmezzük. A fogalom nem csak a kódolásnál hasznos, hanem például bináris kereséseknél is. (Van összefüggés a fizikai értelemben vett entrópiával is.)

* **9.1.2. Segédttétel.** Legyen $p_1, \dots, p_m$ egy eloszlás. Egy $I \subset \mathbb{R}$ intervallumon szigorúan konvex $f: I \rightarrow \mathbb{R}$ függvényre az

$$f\left(\sum_{i=1}^m p_i q_i\right) \leq \sum_{i=1}^m p_i f(q_i), \quad \text{ha } q_1, \dots, q_m \in I$$

Jensen-egyenlőtlenség *teljesül*, és *egyenlőség pontosan akkor áll fenn*, ha $q_1 = \dots = q_m$.

Bizonyítás. Ha $m = 1$, akkor nincs mit bizonyítani. Az $m = 2$ esetben az állítás a szigorú konvexitás definíciója. Indukcióval, legyen $p = \sum_{i=1}^m p_i$. Ekkor $p + p_{m+1} = 1$, és így

$$\begin{aligned} \sum_{i=1}^{m+1} p_i f(q_i) &= p \sum_{i=1}^m \frac{p_i}{p} f(q_i) + p_{m+1} f(q_{m+1}) \\ &\geq p f\left(\sum_{i=1}^m p_i q_i / p\right) + p_{m+1} f(q_{m+1}) \\ &\geq f\left(\sum_{i=1}^{m+1} p_i q_i\right), \end{aligned}$$

valamint az egyenlőségek pontosan akkor teljesülnek, ha $q_1 = q_2 = \dots = q_m$ és $q_{m+1} = \sum_{i=1}^m p_i q_i / p = q_m$. $\square$

9.1.3. Tétel. Bármilyen eloszláshoz tartozó entrópiára

$$H_r(p_1, p_2, \dots, p_m) \leq \log_r m,$$

és *egyenlőség pontosan akkor teljesül*, ha $p_1 = p_2 = \dots = p_m = 1/m$.

Az m elemű eloszlás átlagos információtartalmának maximuma tehát $\log m$ bit. Az r -től független $H_r(p_1, p_2, \dots, p_m) / \log_r m$ hányados a *relatív entrópia*.

* **Bizonyítás.** Mivel $r > 1$ esetén $-\log_r$ szigorúan konvex függvény,

$$\begin{aligned} -H_r(p_1, \dots, p_m) &= \sum_{i=1}^m p_i \log_r p_i = -\sum_{i=1}^m p_i \log_r (1/p_i) \\ &\geq -\log_r \left(\sum_{i=1}^m p_i / p_i\right) = -\log_r m. \quad \square \end{aligned}$$

→ **9.1.4. Feladat [1].** Határozzuk meg az adott eloszlás entrópiáját és relatív entrópiáját:

- (1) 0,34, 0,18, 0,17, 0,16, 0,15;
- (2) 0,6, 0,1, 0,09, 0,08, 0,07, 0,06;
- (3) 0,4, 0,4, 0,1, 0,03, 0,03, 0,02, 0,02;
- (4) 0,3, 0,2, 0,2, 0,1, 0,1, 0,05, 0,05.

9.1.5. Feladat [1]. Az adott eloszlásra határozzuk meg a H_3 és H_4 entrópiát és a relatív entrópiát:

- (1) 0,03, 0,12, 0,13, 0,02, 0,08, 0,3, 0,21, 0,01, 0,05, 0,01, 0,04;
- (2) 0,11, 0,03, 0,21, 0,01, 0,08, 0,27, 0,14, 0,13, 0,02;
- (3) 0,9, 0,1;
- (4) 0,57, 0,43;

9.1.6. Feladat [1]. Határozzuk meg a H_4 entrópiát és a relatív entrópiát, ha a gyakoriságok 84, 118, 100, 31, 52, 213, 71, 60, 17, 84, 138, 32.

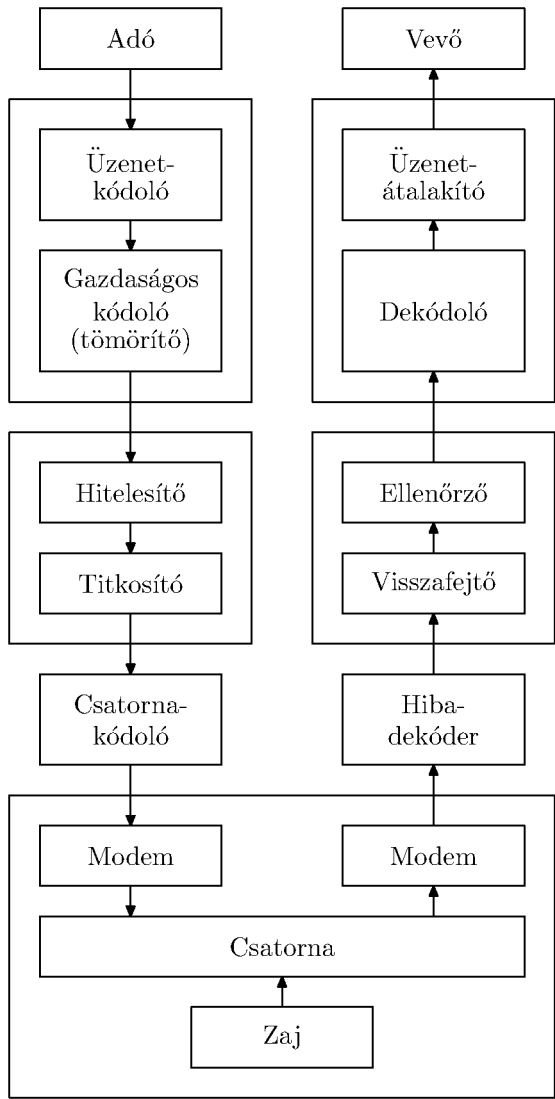
9.1.7. Kódolás. Azt, hogy hogyan történik az információ átvitel, és hogy milyen kapcsolat van az elküldött és a vett adat között, együtt tárgyaljuk. Ahhoz, hogy az adatot továbbítani tudjuk, először is olyan alakra kell hozni, hogy képesek legyünk a céljainknak megfelelően kezelni. A *kódolás* a legáltalánosabb értelemben az üzenetek halmazának egy másik halmazba való leképezését jelenti. Ha a leképezés injektív, akkor azt mondjuk, hogy a kódolás *felbontható, egyértelműen dekódolható*, vagy *veszteségmentes*, egyébként *veszteséges*, mert információvesztéssel jár.

Gyakran az üzenetet valamilyen karakterkészlet elemeiből alkotott sorozattal adjuk meg. Ez az eljárás is egy kódolás, ilyen például az írás. Kódolás tehát a kínai írás, a japán írás, az óegyiptomi írás és hasonlóan kódolás a latin betűs írás is. Minden esetben arról van szó, hogy egy kódolandó üzenetet meghatározott módon felbontunk egymáshoz csatlakozó, előre rögzített olyan elemi részekre – nem teljesen pontosan fogalmazva rendre „szavakra”, „szótagokra”, „fogalmakra”, illetve „hangokra” –, hogy minden üzenet előálljon ilyen elemi részek egymás után fűzésével, de egyetlen üzenetet se lehessen kétféleképpen felbontani ezekre az elemi részekre, „betűkre”. Az ilyen részeknek megadjuk a kódját, és a teljes üzenetet úgy kódoljuk, hogy az előbbi részek kódját egymás után írjuk. A kódoláshoz tehát megadjuk az elemi részek kódját, amelyet egy szótár tartalmaz, és ezek segítségével kódoljuk az üzeneteket. Az ilyen kódolást *betűnkénti kódolásnak* nevezzük (mert léteznek más kódok is). A betűket gyakran számokká kódoljuk: jelenleg elterjedt az úgynevezett *ASCII-kód*, amellyel 128 különböző jel kódolható, illetve ennek a kódnak a kiterjesztései, amelyekkel 256 vagy 65536 jelet lehet kódolni. Néha számokat akarunk betűkké kódolni (például hogy ASCII fájlként küldhessük el): egy módszer, hogy a 32...63 számokat változatlanul hagyjuk, a 0...31 számokhoz pedig hozzáadunk 64-et, majd az ASCII-kód szerinti betűt tekintjük.

A valóságban az egyes üzenetek különböző gyakorisággal fordulnak elő. Ez a felismerés vezetett ahhoz a gondolathoz, hogy célszerű a gyakrabban előforduló üzeneteket rövidebb kóddal megadni. Egy ilyen kódolás *tömörítést* végez, amelynek során csökkentjük az eredeti jelsorozatban meglévő *redundanciát*. A redundancia, vagy más néven a *terjengősség* azt jelenti, hogy a mondandónkat lényegesen hosszabban fejezzük ki, mint amennyire az szükséges lenne. Például a **nyilvánosság** szó 12 betűből áll, holott legfeljebb 5 betű $(26^6 - 1)/25 = 12\,356\,631$ lehetőséget biztosít, így az összes magyar szó

kódolására elég lenne (a tekintett szót már a nyilvánosság mássalhangzókból is kitalálhatjuk).

Az elsőként említett kódolást nevezzük *üzenetkódolás*nak, míg a másodikat *gazdaságos kódolás*nak. A két lépést együttesen *forráskódolás*nak nevezzük.



9.1.2 ábra: A kommunikáció folyamata.

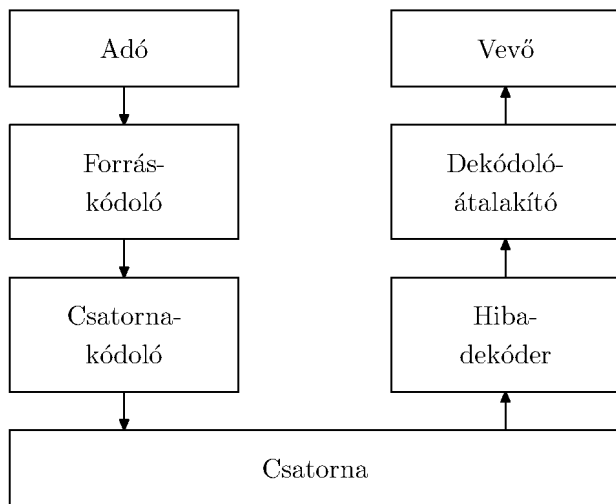
A csatornán áthaladó jel torzulást szenved, így a vétel helyére nem pontosan az a jelsorozat érkezik, mint amit a csatorna bemenetére betápláltak. Amennyiben bármilyen jelsorozat egy lehetséges üzenet, akkor a módosulást nem vesszük észre, a vétel helyén semmilyen módon nem tudjuk eldönteni egy vett jelsorozatról, hogy az megegyezik-e

az eredetileg elküldött üzenettel, vagy egy másik üzenet változott meg, és így kaptuk a vett jelsorozatot. A biztonságosabb átvitel érdekében úgynevezett *hibakorlátozó kódolást* végzünk a csatorna bemenetén. Ezzel a kódolással szándékosan viszünk redundanciát a kódolt üzenetbe. Gondoljuk meg, hogy az élő nyelvek redundanciájának köszönhetően zajban is megértjük, amit egy előadó mond, jóllehet az általunk hallott hang nem azonos azzal, ami eredetileg elhangzott. A megfelelő hibakorlátozó kód kiválasztása függ a csatornától is, ezért ezt a kódolást *csatornakódolásnak* nevezzük.

Végezetül a kódolt üzenetet ténylegesen, fizikailag is át kell vinni a csatornán. Az átvitelhez olyan alakra kell transzformálni az üzenetet, amely forma fizikailag alkalmas a nagy távolságra történő továbbításra. Ilyen például, ha leírjuk az üzenetet, és levél formájában küldjük el, vagy ha elektromos jellé alakítjuk át, és például telefonvonalon keresztül továbbítjuk. Ezt a berendezést most – kissé pontatlanul – *modemnek* (*modulátor-demodulátor*) fogjuk nevezni.

Bár a közvetlen témánkhoz nem szorosan kapcsolódik, ám mindenképpen a kommunikációval kapcsolatos a titkosság és a hitelesség kérdése, vagyis az adatátvitel során, amennyiben szükséges, gondoskodni kell az üzenet *titkosításáról* és *hitelesítéséről* is. Az utóbbit például digitális aláírással lehet megvalósítani. A titkosítást és hitelesítést a tömörítés után kell végezni, mert titkosított üzenet a gyakorlatban már nem tömöríthető.

Az előbbiek alapján a kommunikáció részletesebben a 9.1.2 ábra szerint valósítható meg. Az ábrán is jelzett összevonások, valamint a rejtjelezéssel kapcsolatos részek elhagyása után a 9.1.3 ábra szerinti egyszerűbb modellt kapjuk.



9.1.3 ábra: Kommunikáció titkosítás nélkül.

9.2 Forráskódolás

9.2.1. Betűnkénti kódolás. Mint már említettük, a betűnkénti kódolás során az eredeti üzenetet meghatározott módon egymáshoz átfedés nélkül csatlakozó részekre bontjuk, egy-egy ilyen részt egy szótár alapján kódolunk, és az így kapott kódokat az eredeti

sorrendnek megfelelően egymáshoz láncoljuk. (Feltesszük, hogy az üzenet véges, és a végét érzékeljük.) Az általánosság csorbítása nélkül feltehetjük, hogy a szótár alapján kódolandó elemi üzenetek egy A ábécé (a *kódolandó ábécé*) betűi, és egy-egy ilyen betű kódja egy másik (az előbbitől nem feltétlenül különböző) B ábécé, a *kódoló ábécé* vagy *kódábécé* betűivel felírt *szó*, vagyis ezen ábécéből vett betűk véges hosszúságú sorozata, a sorozat elemeit egyszerűen egymás mellé írva. A továbbiakban mindkét ábécéről feltesszük, hogy nem üres és véges. Ha a B ábécé egyelemű, kételemű, háromelemű stb., akkor rendre *unáris*, *bináris*, *ternáris*, stb., *kódról* beszélünk. Az A ábécé betűivel felírható összes (legalább egy betűt tartalmazó) szó halmazát A^+ , míg az egyetlen betűt sem tartalmazó *üres szó*val (jele: $\emptyset$ vagy λ) kibővített halmazt A^* jelöli. Az előbbieket alapján a betűnkénti kódolást egy $\varphi: A \rightarrow B^*$ leképezés határozza meg, amelyet természetes módon terjesztünk ki egy $\psi: A^* \rightarrow B^*$ leképezéssé: ha $a_1a_2 \dots a_n = \alpha \in A^*$ (tehát $n \in \mathbb{N}$, és $a_i \in A$, ha $1 \leq i \leq n$), akkor α kódja $\psi(\alpha) = \varphi(a_1)\varphi(a_2) \dots \varphi(a_n)$; $\text{rng}(\psi)$ elemei a *kódszavak*. Nyilván, ha φ nem injektív, vagy az üres szó benne van az értékkészletében, akkor a kapott ψ kódolás nem injektív, azaz nem felbontható, ezért betűnkénti kódolásnál általában fel fogjuk tenni, hogy φ injektív és B^+ -ba képez.

9.2.2. Példa. Tipikus példa betűnkénti kódolásra a 9.2.1 táblázatban látható *Morse-kód*. (Jól jöhet, ha börtönbe kerülünk.)

betű	kód	betű	kód	betű	kód
A	.-	J	.-....	S	...
B		K	---.	T	—
C	.-.-.	L		U	...—
D	---.	M	---	V	—
E	.	N	—.	W	...--
F		O	----	X	---..
G		P		Y	---..
H		Q	----.	Z	---..
I	..	R	...-		
szám	kód	szám	kód	írásjel	kód
0	-----	5		.	-
1	-	6	-----	,	-----
2	...--	7	-----	?	...--
3	---..	8	-----	:	-----
4	-	9	-----	-	-----

9.2.1 táblázat: Morse-kód.

Itt az angol ábécé (csak nagybetűkkel) a kódolandó ábécé, míg a kódoló ábécé két betűt tartalmaz, a *pontot* és a *vonást* (hang esetén „*tí*” és „*tá*”), és például az *sms* szó kódja „...—...”. Az így adódó kódokat nem tudnánk dekódolni, mert nem injektív a megfeleltetés. Például a *vb* szó kódja megegyezik az előbbi kóddal. A valóságban természetesen az egyes jelek, továbbá az egyes betűk adása között meghatározott szünetet tartanak, és a kódolás így már egyértelmű lesz: konkrétan egy vonás háromszor olyan hosszú, mint egy pont, és minden jel után egy egységnyi szünet következik, majd a betű kódja végén még további két egységnyi szünet van (egy pont átviteléhez szükséges időt tekintve egységnek). Ha egy egységnyi hosszúságú jelet egy 1-es, és egy egységnyi hosszúságú szünetet egy 0 jelöl, akkor például a B kódja, amely az eredeti, ponttal és vonással

megadott rendszerben „—”, most 111010101000 lesz. Ezzel a kiegészítéssel már egyértelműen dekódolható a vett üzenet, hiszen minden betű kódja három nullára végződik, és nincs olyan betű, amelynél a kódszó belsejében vagy az elején lenne három nulla. Ennél a kódnál a három nullának önmagában is van jelentése, ez a szóköz kódja, vagyis ez választja el egymástól az egymás után következő szavak kódját (így egy szó kódjának a végén hat darab nulla áll). Ekkor sms kódja 10101000111011100010101000000, míg vb kódja 101010111000111010101000000, így a két kód jól megkülönböztethető és a kódolás egyértelműen megfejthető.

9.2.3. Prefix, szuffix, infix. Legyen α , β és γ az A ábécével felírt három szó. Ekkor α *prefixe* (vagy *előtagja*) és γ *szuffixe* (vagy *utótagja*) az $\alpha\gamma$ szónak, β pedig *infixe* (vagy *belső tagja*) $\alpha\beta\gamma$ -nak. Szavak egy halmaza *prefixmentes halmaz*, ha nincs benne két olyan különböző szó, hogy egyik a másik prefixe.

Ha α egy szó, akkor az üres szó és α mind prefixe, mind szuffixe, mind pedig infixe α -nak. Ezek az α *triviális prefixei*, *triviális szuffixei* és *triviális infixei*. A prefix, szuffix, illetve infix *valódi prefix*, *valódi szuffix*, illetve *valódi infix*, ha nem egyezik meg α -val.

9.2.4. Kódfa. A betűnkénti kódolás szemléletesen és egyértelműen adható meg egy irányított fa segítségével. Legyen $\varphi: A \rightarrow B^*$ egy betűnkénti kódolás. Tetszőleges szóhalmaz, így a φ értékkészletében lévő kódszavak összes prefixeinek halmaza is részbenrendezett a „prefixe” relációra. Készítsük el ennek a relációnak a Hasse-diagramját. Nyilván egy irányított fát kapunk, amelynek gyökere az üres szó, és minden szó a hosszának megfelelő szinten van. A fa éleit színezzük úgy B elemeivel, hogy ha $\beta = \alpha b$ valamely $b \in B$ -re, akkor az α -ból β -ba vezető él színe legyen b . Nyilván bármely csúcs esetén a csúcsból kivezető élek mind különböző színűek. A kódfa valamely csúcsát, amely nem levél, *teljes csúcsnak* illetve *csónka csúcsnak* nevezzük attól függően, hogy tartozik-e minden színhez a csúcsból kiinduló, az adott színnel színezett él. A kódfa csúcsait is kiszínezhetjük: az $a \in A$ kódjának megfelelő csúcs színe legyen a , azon csúcsok színe, amelyek nincsenek φ értékkészletében, legyen „üres”. Vegyük észre, hogy levél színe nem lehet „üres”.

Az előbbi konstrukciót meg is fordíthatjuk. Tekintsünk egy véges élszínezett irányított fát, ahol a színek halmaza B , és az egy csúcsból kiinduló élek mind különböző színűek az A véges ábécének a fa csúcsaira való leképezésével együtt, amelynél minden levél fellép képként. Az $a \in A$ betű kódja legyen az a szó, amelyet úgy kapunk, hogy a gyökértől az a -nak megfelelő csúcsig haladó irányított úton összeolvassuk az élek színeit.

9.2.5. Prefix kód, egyenletes kód és vesszős kód. Tegyük fel, hogy az injektív $\varphi: A \rightarrow B^+$ leképezés $\text{rng}(\varphi)$ értékkészlete B^+ prefixmentes részhalmaza. Ekkor a φ által meghatározott $\psi: A^* \rightarrow B^*$ betűnkénti kódolás nyilván könnyen dekódolható, mert ha egymás után érkeznek a kódábécé betűi, és nézzük az addig beérkezett szimbólumokból összeálló szót, akkor amint ez kiadja a kódolandó ábécé valamely betűjének kódját, azonnal dekódolható is, hiszen a folytatásával kapott jelsorozat már egyetlen betűnek sem lehet a kódja. Ezen dekódolási módszer miatt szokás az ilyen kódot *prefix kódnak* nevezni. (A *prefixmentes kód* elnevezés is használatos, mivel a dekódolás $\text{rng}(\varphi)$ prefixmentességén múlik.) Prefix kód nyilván felbontható.

Egy betűnkénti kód *egyenletes kód* vagy *fix hosszúságú kód*, ha a betűk kódjainak hossza azonos. Mivel egy ilyen kód nyilván prefix, ezért felbontható, így mindig van felbontható kód.

Egy betűnkénti kód *vesszős kód*, ha van olyan ϑ szó, a *vessző*, hogy ϑ minden kódszónak szuffixe, de egyetlen kódszó sem áll elő $\alpha\vartheta\beta$ alakban nem üres β szóval. Egy vesszős kód prefix kód, mert a vessző egyértelműen jelzi a beérkezett jelsorozatban egy-egy kódszó végét, és ha ezt folytatjuk, akkor már biztosan nem kapunk kódszót, hiszen ebben a meghosszabbított sorozatban a vessző valódi infix lenne. Ha egy betűnkénti kódban nincs vessző, akkor a *kód vesszőmentes*.

A Morse-kódnál láttuk, hogy az eredeti, csak ponttal és vonással megadott betűnkénti kód nem felbontható, míg az 1-gyel és 0-val való átírás után kapott szabály szerinti kód vesszős, ahol a 000 jelsorozat a vessző.

Egy betűnkénti kód pontosan akkor prefix kód, ha a kódfájának csak a levelei kódszavak.

9.2.6. Példák. A fenti jelölésekkel legyen $A = \{a, b, c\}$, $B = \{0, 1\}$, és ψ a φ -ből képzett leképezés.

(1) Legyen $\varphi(a) = 00$, $\varphi(b) = 1$ és $\varphi(c) = 01$. A kódszavak halmaza prefixmentes, így ez egy prefix kód, tehát egyértelműen dekódolható.

(2) Legyen $\varphi(a) = 10$, $\varphi(b) = 11$ és $\varphi(c) = 01$. Ez egyenletes kód, így egyben prefix kód.

(3) Legyen $\varphi(a) = 0010$, $\varphi(b) = 10$ és $\varphi(c) = 010$. Ennél a kódnál minden kódszó 10-ra végződik, vagyis 10 mindegyiknek szuffixe, de az 10 egyetlen kódszónak sem valódi prefixe, és nem is valódi infix. Ez a kód tehát vesszős kód, így prefix kód.

(4) Legyen $\varphi(a) = 10$, $\varphi(b) = 1$ és $\varphi(c) = 01$. Ekkor $\psi(ab) = \varphi(a)\varphi(b) = 101 = \varphi(b)\varphi(c) = \psi(bc)$, tehát ez a kód nem dekódolható: bár φ injektív, ψ nem.

(5) Legyen $\varphi(a) = 10$, $\varphi(b) = 1$ és $\varphi(c) = 00$. Ez a kód egyértelműen megfejthető, tehát ψ injektív. Tegyük ugyanis fel, hogy valameddig már dekódoltuk a beérkezett kódolt üzenetet, és most érkezik egy újabb jel. Ha ez a jel 0, akkor utána csak egy 0 következhet, és ez a 00 csupán a c kódja lehet. Ha viszont ez a jel 1, akkor ezt még nem tudjuk dekódolni. Amennyiben ez után az 1 után ismét 1 következik, akkor már tudjuk, hogy az első 1 egy b kódja, de a második 1-et még nem tudjuk dekódolni. Mindaddig, amíg csak 1-ek követik egymást, az utolsóként beérkező 1 kivételével valamennyit egyértelműen dekódoljuk b -ként. Abban az esetben, ha az 1 után vége van az adásnak, akkor ezt az utolsóként maradt 1-et szintén egyértelműen b -ként dekódoljuk. Ha viszont az 1 után 0 következik, akkor mindaddig, amíg vagy egy 1 nem érkezik, vagy vége nincs az adásnak, nem tudunk dekódolni. Amikor viszont vagy egy 1 érkezik, vagy vége van az adásnak, akkor hátulról visszafelé végrehajtható a dekódolás: minden két-két 0-t c -nek dekódolunk, és a végén vagy egy egyedül álló 1 marad, ami a b kódja, vagy 10 lesz a maradék, ami viszont az a kódja. Könnyen ellenőrizhető, hogy másként az előbbi jelsorozat nem dekódolható. Ez tehát egy felbontható, de nem prefix kód.

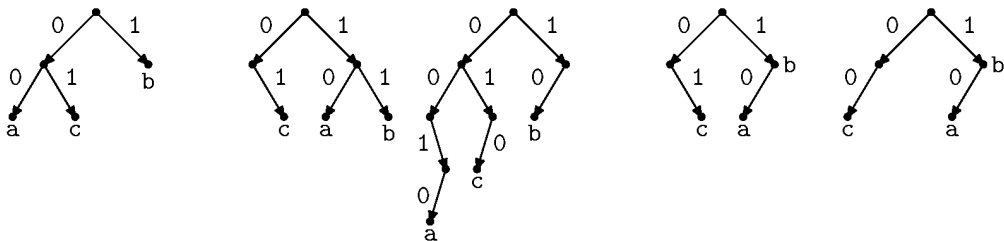
A 9.2.2 ábra mutatja a fenti kódokhoz tartozó kódfákat. Az első három kód prefix, és ezeknél a kódoknál csak a levelek kódszavak.

→ **9.2.7. Feladat [5].** Az adott kódokról döntsük el, hogy melyik felbontható, prefix, vesszős, illetve egyenletes. Rajzoljuk fel a kódfát is.

(1) $\{0, 10, 110, 1110, 1011, 1101\}$;

(2) $\{1, 011, 010, 001, 000, 110\}$;

(3) $\{0, 10, 110, 1110, 11110, 111110\}$;



9.2.2 ábra: Példák kódfákra.

(4) $\{111, 110, 101, 100, 011, 010\};$

(5) $\{1, 01, 0011, 0010, 0001, 0000\};$

(6) $\{1, 01, 011, 0111, 01111, 011111\}.$

9.2.8. Feladat [2]. Tetszőleges, r betűs kódábécét használó kód minden kódszavának elejére hozzáírjuk ugyanazt az $r + 1$ -edik szimbólumot. Felbontható-e az új kód? Prefix-e az új kód?

9.2.9. Tétel: McMillan-egyenlőtlenség. Legyen $A = \{a_1, \dots, a_n\}$ és B két ábécé, B elemeinek száma $r \geq 2$, és $\varphi: A \rightarrow B^+$ injektív leképezés. Ha a φ által meghatározott betűnkénti kódolás felbontható, akkor $l_j = |\varphi(a_j)|$ jelöléssel

$$\sum_{j=1}^n r^{-l_j} \leq 1.$$

Fordítva, ha $l_1, \dots, l_n$ olyan pozitív egész számok, hogy $\sum_{j=1}^n r^{-l_j} \leq 1$, akkor van az A -nak a B elemeivel való olyan felbontható, sőt prefix kódolása, hogy az a_j betű kódjának hossza l_j .

A fenti tételben szereplő egyenlőtlenség a *McMillan-egyenlőtlenség*, amely lényegében véve azt fejezi ki, hogy egy felbontható betűnkénti kódban az átlagos szóhosszúság nem lehet túlságosan kicsi (mert ha a szóhosszúság kicsi, akkor r megfelelő negatív kitevős hatványa nagy, viszont az összeg értéke nem haladhatja meg az 1-et). A tétel második része azt mutatja, hogy egy felbontható, de nem prefix kódznak nincs nagy jelentősége, hiszen ugyanolyan hosszakkal készíthető prefix kód is, amely „online” dekódolást tesz lehetővé. A második rész bizonyítása konstruktív: algoritmust ad a kód megkonstruálására.

* **Bizonyítás.** Tekintsük a $\varphi: A \rightarrow B^+$ injektív leképezés által meghatározott felbontható kódot. Jelöljük C -vel $\text{rng}(\varphi) \subset B^+$ -t, és legyen $M = \sum_{j=1}^n r^{-l_j}$ a tételbeli összeg. Indukcióval megmutatjuk, hogy $\sum_{\alpha \in C^i} r^{-|\alpha|} = M^i$, ha $i \in \mathbb{N}$. Ha $\alpha \in C^{i+1} = C^i \times C$, akkor α megadható $\alpha = \alpha_1 \alpha_2$ alakban, ahol $\alpha_1 \in C^i$ és $\alpha_2 \in C$. Ha a kód felbontható, akkor ez a felbontás egyértelmű, és

$$\begin{aligned} \sum_{\alpha \in C^{i+1}} r^{-|\alpha|} &= \sum_{\alpha_1 \in C^i} \sum_{\alpha_2 \in C} r^{-|\alpha_1 \alpha_2|} = \sum_{\alpha_1 \in C^i} \sum_{\alpha_2 \in C} r^{-(|\alpha_1| + |\alpha_2|)} \\ &= \sum_{\alpha_1 \in C^i} \sum_{\alpha_2 \in C} r^{-|\alpha_1|} r^{-|\alpha_2|} = \sum_{\alpha_1 \in C^i} r^{-|\alpha_1|} \sum_{\alpha_2 \in C} r^{-|\alpha_2|} \\ &= M^i M = M^{i+1}, \end{aligned}$$

ahol az első egyenlőségnél használtuk ki, hogy a kód felbontható. Ezt az összeget másképp is ki tudjuk számítani, ha az összegben szereplő tagokat a kitevőkben szereplő hosszak növekvő sorrendjében írjuk, és az azonos kitevőhöz tartozó tagokat összevonjuk. Legyen $w_k^{(i)}$ a C^i -beli k hosszúságú szavak száma és L a C -beli szavak hosszának maximuma. Ekkor a C^i -beli szavak hosszának maximuma iL , és

$$M^i = \sum_{\alpha \in C^i} r^{-|\alpha|} = \sum_{k=1}^{iL} w_k^{(i)} r^{-k} \leq \sum_{k=1}^{iL} r^k r^{-k} = iL,$$

mert r szimbólummal maximum r^k különböző k hosszúságú szó írható fel. A fentiek szerint minden pozitív egész i -re $M^i \leq iL$, vagyis $M^i/i \leq L$. Ha $M > 1$ lenne, akkor $M^i/i \rightarrow \infty$ miatt, vagy közvetlenül, az $i \geq 2$ esetén érvényes

$$L \geq \frac{M^i}{i} = \frac{(1 + (M-1))^i}{i} = \frac{1}{i} \sum_{j=0}^i \binom{i}{j} (M-1)^j > \frac{1}{i} \binom{i}{2} (M-1)^2 = (i-1) \frac{(M-1)^2}{2}$$

egyenlőtlenségből az arkhimédészi rendezettség miatt ellentmondást kapnánk.

A tétel második állításának bizonyításához feltehetjük, hogy $l_1 \leq l_2 \leq \dots \leq l_n$, és legyen $1 \leq k \leq n$ -re $c_k = \sum_{j=1}^{k-1} r^{-l_j}$. Ez a sorozat szigorúan monoton nő, az első eleme 0, és a $\sum_{j=1}^n r^{-l_j} \leq 1$ feltétel alapján minden tagja kisebb 1-nél. Így minden k -ra $r^{l_k} c_k = \sum_{j=1}^{k-1} r^{l_k - l_j} < r^{l_k}$, és a bal oldalon egy nem negatív egész szám áll, hiszen a hosszak rendezése következtében az összeg tagjainak kitevője nem negatív egész szám. Így $r^{l_k} c_k$ felírható az r alapú számrendszerben pontosan l_k hosszon (a felírás kezdődhet nullával is). Ez lesz az a_k kódja, a számjegyeket kicserélve B betűire. (Másként, az 1-nél kisebb c_k nem negatív valós szám r -alapú számrendszerben pontosan felírható törtrészében l_k jeggyel, és ezek a jegyek az a_k kódját adják.) Amennyiben $1 \leq i < k \leq n$, akkor

$$r^{l_k} (c_k - c_i) = \sum_{j=1}^{k-1} r^{l_k - l_j} - \sum_{j=1}^{i-1} r^{l_k - l_j} = \sum_{j=i}^{k-1} r^{l_k - l_j} \geq r^{l_k - l_i},$$

ezért a megfelelő kódok első l_i számjegye közül legalább egy különböző, tehát a megadott kód prefix kód. $\square$

→ **9.2.10. Feladat [5].** Az adott kódokról döntsük el, hogy melyik felbontható.

- (1) $\{1021, 121, 2021, 021, 221, 1121, 0121, 0221\}$;
- (2) $\{01, 02, 10, 11, 12, 20, 21, 22\}$.

→ **9.2.11. Feladat [3].** Van-e ternáris illetve kvaternáris prefix kód, ha az egybetűs szavak száma 0, a kétbetűsöké 2, a hárombetűsöké 18, a négybetűsöké 100 és az ötbetűsöké 75?

→ **9.2.12. Feladat [3].** Lehet-e felbontható egy ternáris kód, ha az 1, 2, 3, 4, 5 illetve 6 betűs szavak száma rendre 2, 3, 0, 0, 4, 1.

9.2.13. Feladat [3]. Adja meg a kódábécé minimális elemszámát, ha az 1, 2, 3, 4, 5, illetve 6 betűs szavak száma rendre

- (1) 0, 0, 3, 0, 2, 2;
- (2) 2, 3, 0, 0, 4, 1.

9.2.14. Átlagos szóhosszúság, optimális kód. A gazdaságos kódolás szempontjából döntő a kód átlagos szóhosszúsága. Legyen $A = \{a_1, \dots, a_n\}$ a kódolandó ábécé, $p_1, \dots, p_n$ a betűk eloszlása, $\varphi: A \rightarrow B^+$ egy betűnkénti kódolás, l_i az a_i kódjának hossza. Ekkor $\bar{l} = \sum_{i=1}^n p_i l_i$ a kód átlagos szóhosszúsága. Ha adott elemszámú ábécével és eloszlással egy felbontható betűnkénti kód átlagos szóhosszúsága minimális, akkor *optimális kódnak* nevezzük. Első pillantásra nem világos, hogy van-e optimális kód, mivel valós számok egy részhalmazában nem feltétlenül van minimális elem. Válasszunk azonban egy tetszőleges felbontható kódot, és legyen ennek átlagos szóhosszúsága l . Mivel $p_i l_i > l$ esetén a kód nem lehet optimális, elég azon kódokat tekintenünk, amelyekre $l_i \leq l/p_i$, ha $i = 1, \dots, n$. Ilyen kód csak véges sok van, így van köztük minimális átlagos hosszúságú. Mint az előző tételből tudjuk, ez választható prefix kódnak is. Algoritmust fogunk adni az optimális kód megkonstruálására.

9.2.15. Shannon tétele zajmentes csatornára. Az előző definíció jelöléseivel legyen B elemeinek száma r . Ha a betűnkénti kódolás felbontható, akkor $H_r(p_1, \dots, p_n) \leq \bar{l}$, ahol H_r az eloszlás entrópiája.

* **Bizonyítás.** A McMillan-egyenlőtlenséget, $-\log_r$ szigorú konvexitását és a 9.1.2 segédtelet használva,

$$\begin{aligned} \bar{l} - H_r(p_1, \dots, p_n) &= \sum_{i=1}^n p_i l_i + \sum_{i=1}^n p_i \log_r p_i \\ &= -\sum_{i=1}^n p_i \log_r r^{-l_i} - \sum_{i=1}^n p_i \log_r \frac{1}{p_i} \\ &= -\sum_{i=1}^n p_i \log_r \frac{r^{-l_i}}{p_i} \geq -\log_r \left(\sum_{i=1}^n r^{-l_i} \right) \\ &\geq -\log_r 1 = 0. \quad \square \end{aligned}$$

9.2.16. Tétel: Shannon-kód létezése. Az előző tétel jelöléseivel, $n > 1$ esetén van olyan prefix kód, amelyre $\bar{l} < H_r(p_1, \dots, p_n) + 1$.

Az előző tétellel együtt ez azt jelenti, hogy van olyan kód, amelynek átlagos szóhossza kevesebb, mint 1-gyel haladja meg az elméleti alsó határt. A bizonyítás konstruktív, a 9.2.9 tétel bizonyításával együtt algoritmust is ad a kód meghatározására.

* **Bizonyítás.** Válasszunk olyan $l_1, \dots, l_n$ természetes számokat, amelyekre $r^{-l_i} \leq p_i < r^{-l_i+1}$, ha $i = 1, \dots, n$. Ekkor $\sum_{i=1}^n r^{-l_i} \leq \sum_{i=1}^n p_i = 1$, így a 9.2.9 tétel szerint van prefix kód az adott l_i hosszakkal. Mivel $l_i < 1 - \log_r p_i$, erre

$$\bar{l} = \sum_{i=1}^n p_i l_i < \sum_{i=1}^n p_i (1 - \log_r p_i) = 1 + H_r(p_1, \dots, p_n). \quad \square$$

9.2.17. Tétel: optimális kód konstrukciója. Az előző tétel jelöléseivel legyen $n > 1$. Tekintsünk egy optimális prefix kódot és a kódját, és legyen a kódszavak hosszának maximuma L . Ekkor

(1) ha $p_i > p_j$, akkor $l_i \leq l_j$;

- (2) a kódfában csak az $L - 1$ -edik szinten lehet csonka csúcs, és még a csonka csúcsokból is legalább két él indul ki.

Továbbá

- (3) van olyan optimális prefix kód, amelynek kódfájában legfeljebb egy csonka csúcs van;
 (4) egy optimális prefix kód kódfájában pontosan akkor nincs csonka csúcs, ha $r \equiv n \pmod{r-1}$, azaz

$$r = 2 + ((n - 2) \bmod (r - 1)),$$

ha pedig egy csonka csúcs van, akkor annak m kifokára $m \equiv n \pmod{r-1}$, azaz

$$m = 2 + ((n - 2) \bmod (r - 1));$$

- (5) ha $n \leq r$, akkor egybetűs kódszavakat választva optimális prefix kódot kapunk;
 (6) legyen $\beta_1, \dots, \beta_n$ az r -elemű kódábécével megadott, a $p_1, \dots, p_n$ eloszláshoz tartozó optimális prefix kód, amelynek a kódfájában nincs csonka csúcs. Ha $2 \leq m \leq r$, és valamely $1 \leq k \leq n$ -re a $p_{n+1}, \dots, p_{n+m}$ pozitív valós számokra $\sum_{i=1}^m p_{n+i} = p_k$, továbbá

$$\max\{p_{n+1}, \dots, p_{n+m}\} \leq \min\{p_1, \dots, p_n\},$$

akkor

$$\beta_1, \dots, \beta_{k-1}, \beta_{k+1}, \dots, \beta_n, \beta_k b_1, \dots, \beta_k b_m,$$

ahol $b_1, \dots, b_m$ a B különböző elemei, a

$$p_1, \dots, p_{k-1}, p_{k+1}, \dots, p_n, p_{n+1}, \dots, p_{n+m}$$

„finomított” eloszláshoz tartozó optimális prefix kód.

A következő pontban megmutatjuk, hogy (4)–(6) segítségével hogyan konstruálhatunk optimális prefix kódot.

Bizonyítás. Ha (1) nem teljesülne, akkor

$$0 < (p_i - p_j)(l_i - l_j) = (p_i l_i + p_j l_j) - (p_i l_j + p_j l_i),$$

és innen $p_i l_j + p_j l_i < p_i l_i + p_j l_j$, azaz a két betű, a_i és a_j kódját felcserélve csökken az átlagos szóhosszúság.

Ha (2) nem teljesül, és a j -edik szinten van csonka csúcs, ahol $j < L - 1$, akkor egy L -edik szinten lévő levelet a hozzá vezető éllel áthelyezve erre a csonka csúcsra, és esetleg az áthelyezett élt átszínezve, a levélhez tartozó betű kódjának hossza L -ről $j + 1$ -re változik, vagyis csökken az átlagos szóhosszúság. Ha valamely csonka csúcsot csak egy él hagy el, akkor elhagyva ezt az élt, és az ennek az élnek a másik végén lévő csúcsból kiinduló részfat áthelyezve az előbbi csúcsba, az áthelyezett részfa leveleihez tartozó kódszavak hossza eggyel csökken, és így az átlagos szóhosszúság is csökken.

(3)-hoz, legyen egy optimális kód kódfájában két különböző csonka csúcs. Az előbbieket szerint ezek azonos szinten vannak, így egyikükről az egyik élhez tartozó levelet az éllel együtt áthelyezve a másik csonka csúcsra, és esetleg ezt az élt átszínezve, az átlagos

szóhosszúság nem változik. Ilyen áthelyezések sorozatával viszont vagy a fogadó csúcs telítődik, tehát a csonka csúcsok száma csökken, vagy a másik csonka csúcson legfeljebb egy él maradna, ami az előbbi pont alapján optimális kód kódfáján lehetetlen..

Hogy belássuk (4)-et, tekintsünk egy n levelet tartalmazó kódfát. Töröljük ebben a fában az egyik csúcshoz tartozó összes levelet, a csonka csúcsához tartozó levelekkel kezdve, ha van csonka csúcs. Ha m számú levelet töröltünk, akkor az új fában $m - 1$ -gyel kevesebb levél lesz. Folytassuk az eljárást mindaddig, amíg a végén csak a gyökér marad meg. Ha összesen s lépést hajtottunk végre, akkor $m - 1 + (s - 1)(r - 1) = n - 1$, vagyis $n = (s - 1)(r - 1) + m$, és $2 \leq m \leq r$.

Az (5)-ben megadott kód nyilván optimális prefix kód. (6)-ban az a_k betű kódját helyettesítjük m kódszóval úgy, hogy a prefix tulajdonság megmarad. (Ezzel a kódolandó ábécé méretét $m - 1$ betűvel növeljük, az átlagos kódhossz pedig p_k -val nő.) Jelölje a kapott kódot φ . Tegyük fel, hogy az állítás nem igaz, és legyen φ^* a

$$p_1, \dots, p_{k-1}, p_{k+1}, \dots, p_n, p_{n+1}, \dots, p_{n+m}$$

eloszláshoz tartozó valamely optimális prefix kód. Ekkor φ^* átlagos hossza kisebb, mint φ átlagos hossza. Az általánosság csorbitása nélkül feltehetjük, hogy φ^* kódfájában is legfeljebb egy csonka csúcs van. A φ kód konstrukciójából, illetve (4)-ből mindkét kódban egyszerre van csonka csúcs, és ha van, akkor a kifoka ugyanannyi, m , ha pedig nincs, akkor $m = r$. Mivel φ^* optimális kód, ezért (1) és (2) szerint az m darab legkisebb valószínűséghez tartozó kódszó a legmagasabb szinten van a kódfában, és ugyanezen a legmagasabb szinten vannak azok a kódszavak, amelyek az esetleges csonka csúcs gyermekeihez tartoznak. Mivel kódszavak cseréje, ha azok azonos szinten vannak, nem változtatja meg a kód átlagos hosszát, ezért feltehetjük, hogy mindkét kódban az m legkisebb valószínűségű kódszóhoz tartozó levél ugyanahhoz a csúcsához tartozik. Ezeket törölve, mindkét kód átlagos hossza ugyanannyival változik. Így a φ^* -ból kapott kód átlagos hossza kisebb lesz, mint a φ -ból kapott kódé, ami lehetetlen, hiszen feltettük, hogy a φ -ból kapott kód optimális kód. $\square$

9.2.18. Huffman-kód. Optimális kódot ad az úgynevezett *Huffman-kód*, amelyet az előző tétel (4)–(6) pontjai alapján tudunk megszerkeszteni. Rendezzük a relatív gyakoriságok csökkenő sorrendjében a betűket, majd osszuk el $n - 2$ -t $r - 1$ -gyel, és legyen m a maradék plusz 2. Első lépésben helyettesítsük a sorozat m utolsó betűjét egy újabb betűvel, amelyhez az elhagyott betűk relatív gyakoriságainak az összegét rendeljük, és az így kapott gyakoriságoknak megfelelően helyezzük el az új betűt a sorozatban. (Célszerű kupac struktúrát használni.) Ezek után ismételjük meg az előző redukiót, de most már minden lépésben r betűvel csökkentve a kódolandó halmazt, mígnem már csak r betű marad (feltehetjük, hogy induláskor több, mint r betű volt, ellenkező esetben a redukió elmarad). Most a redukált ábécé legfeljebb r betűt tartalmaz, és ha volt redukió, akkor pontosan r betűt. Ezeket a kódoló ábécé elemeivel kódoljuk, majd a redukióknak megfelelően visszafelé haladva, az ott összevont betűk kódját az összevonásként kapott betű már meglévő kódjának a kódoló ábécé különböző betűivel való kiegészítésével kapjuk.

9.2.19. Példa. Mutatunk egy példát a Huffman- és a Shannon-kódra. Mindkét esetben ugyanazon forrást fogjuk kódolni, így összehasonlítható a két kód hatékonysága.

Legyen a kódolandó ábécé 10-elemű (mondjuk az angol ábécé első 10 betűjével jelölve), az egyes betűk relatív gyakorisága rendre 0,17, 0,02, 0,13, 0,02, 0,01, 0,31, 0,02,

0,17, 0,06, 0,09, és a kódoló ábécé $\{0, 1, 2\}$. Mivel $10 - 2 = 4 \cdot (3 - 1) + 0$, az első lépésben $0 + 2 = 2$ betűt kell összefogni, majd a további lépésekben hárm-at-hárm-at (9.2.3 táblázat; az „új betűket” párokkal, illetve hárm-asokkal jelöljük). Amikor már csak 3 betűből áll az ábécé, akkor ezt a három betűt rendre 0-val, 1-gyel és 2-vel kódoljuk, majd visszafelé haladva előállítjuk a kívánt kódot (9.2.4 táblázat).

f	0,31	f	0,31	f	0,31
a	0,17	a	0,17	a	0,17
h	0,17	h	0,17	h	0,17
c	0,13	c	0,13	c	0,13
j	0,09	j	0,09	j	0,09
i	0,06	i	0,06	((g, e), b, d)	0,07
b	0,02	(g, e)	0,03	i	0,06
d	0,02	b	0,02		
g	0,02	d	0,02		
e	0,01				
f	0,31	(a, h, c)	0,47		
(j, ((g, e), b, d), i)	0,22	f	0,31		
a	0,17	(j, ((g, e), b, d), i)	0,22		
h	0,17				
c	0,13				

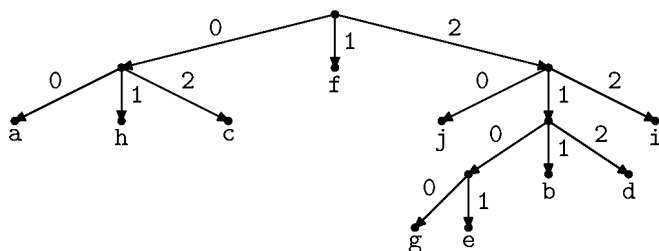
9.2.3 táblázat: Huffman-kód, redukciós lépések.

(a, h, c)	$\mapsto 0$	a	$\mapsto 00$		
		h	$\mapsto 01$		
		c	$\mapsto 02$		
f	$\mapsto 1$	j	$\mapsto 20$		
(j, ((g, e), b, d), i)	$\mapsto 2$	((g, e), b, d)	$\mapsto 21$	(g, e)	$\mapsto 210$
				g	$\mapsto 2100$
				e	$\mapsto 2101$
				b	$\mapsto 211$
				d	$\mapsto 212$
		i	$\mapsto 22$		

9.2.4 táblázat: Huffman-kód, kódfelépítés.

A kód átlagos szóhosszúsága $\approx 1,79$, míg az entrópia értéke $\approx 1,73$, így a kód átlagos szóhosszúsága igen jól megközelíti az elméletileg elérhető legkisebb értéket. A 9.2.5 ábra a kódfát mutatja.

Ugyanezen ábécét fogjuk most a Shannon-kóddal kódolni. Most is sorba kell rendezni az ábécét a relatív gyakoriságok csökkenő sorrendjében. Meghatározzuk a szükséges



9.2.5 ábra: Huffman-kód fája.

szóhosszúságokat. Mivel 0,31, 0,17, 0,13 kisebbek, mint $1/3$, de nem kisebbek, mint $1/9$, **f**, **a**, **h** és **c** kódhossza 2. Hasonlóan **j** és **i** kódhossza 3, míg **b**, **d** és **g** kódhossza 4, végül **e** kódhossza 5. Az **f** kódja 00, az **a** kódja 01, a **h** kódja 02, és ez utóbbihoz hármasszerű számrendszerben 1-et adva kapjuk **c** kódját, amely így 10. Ehhez 1-et adva 11-et kapunk, de **j** kódjának hossza 3, ezért ezt még jobbról ki kell egészíteni egy darab 0-val, tehát **j** kódja 110. Hasonlóan haladva megkapjuk a teljes kódot, amelyet a 9.2.6 táblázat mutat. Most a kód átlagos szóhosszúsága 2,30, amely nagyobb, mint a Huffman-kódnál volt (1,79), de kisebb, mint 2,73, az entrópia plusz 1.

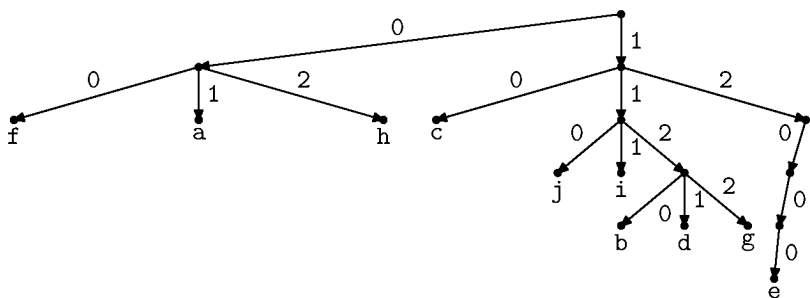
betű	gyakoriság	kód
f	0,31	00
a	0,17	01
h	0,17	02
c	0,13	10
j	0,09	110
i	0,06	111
b	0,02	1120
d	0,02	1121
g	0,02	1122
e	0,01	12000

9.2.6 táblázat: Példa Shannon-kódra.

A 9.2.7 ábra mutatja a kód kódfáját.

Megadjuk az ékezet nélküli latin betűk magyar nyelvben való előfordulásának relatív gyakoriságaihoz tartozó bináris Huffman- és Shannon-kódot (9.2.8 táblázat) (a Shannon-kódnál a **Q** betű kódjának hosszát az egyébként előforduló hosszak maximumának vettük; általában is a nagyon kis gyakoriságokat kicsit megnövelve, korlátozhatjuk a kódszavak hosszát, nem sokat rontva a kódon). Az adott eloszláshoz tartozó entrópia értéke $\approx 4,1289$, míg a Huffman-kód átlagos szóhosszúsága 4,1528, a Shannon-kódé pedig 4,5989. Ugyanakkor a Morse-kód 0-val és 1-gyel való kódolásánál az átlagos szóhosszúság ugyanezekkel a gyakoriságokkal 12,299. Látható, hogy mekkora javulás érhető el. Ennek egyik oka, hogy a vessző határozottan növeli az átlagos szóhosszúságot.

9.2.20. Adaptív Huffman-kód. Néha olyan esetekben akarunk Huffman-kódot használni, amikor nem áll módunkban előre megállapítani a relatív gyakoriságokat. Ilyenkor



9.2.7 ábra: A Shannon-kód kód fája.

betű	valószínűség	Huffman-kód	Shannon-kód
A	0,1247	100	0010
B	0,0190	000011	101100
C	0,0065	01101110	10111101
D	0,0197	000010	101011
E	0,1407	001	000
F	0,0078	0110110	10111100
G	0,0326	01100	10011
H	0,0165	011010	101101
I	0,0444	1110	01111
J	0,0105	0000000	10111100
K	0,0541	1100	01110
L	0,0605	1010	01100
M	0,0352	01001	10010
N	0,0638	0111	0101
O	0,0683	0101	0100
P	0,0096	0000001	10111101
Q	0,0000	0110111111	10111110001001
R	0,0367	01000	10001
S	0,0600	1011	01101
T	0,0761	0001	0011
U	0,0226	11011	101001
V	0,0199	000001	101010
W	0,0009	011011110	10111110000
X	0,0001	0110111110	10111110001000
Y	0,0261	11010	101000
Z	0,0437	1111	10000

9.2.8 táblázat: Bináris kódok magyar szöveghez.

úgy járhatunk el, hogy az ábécé minden betűjének adunk valamilyen (pozitív) „kezdeti gyakoriságot” (például 1-et), ehhez előállítjuk a Huffman kód kód fáját, majd a továbbiakban minden betű továbbítása után megnöveljük a gyakoriságát eggyel és megfelelően

átalakítjuk a kódfát. A vevő oldalon ugyanazt az algoritmust használjuk a kódfa átalakítására, mint az adó oldalon.

→ **9.2.21. Feladat [5].** Az adott ternáris kódról mutassuk meg, hogy felbontható, és konstruáljunk hozzá olyan ternáris prefix kódot, amelynek kódhosszai ugyanazok:

$$\{011, 0011, 110, 111, 2020, 20201, 220, 2212\}.$$

9.2.22. Feladat [4]. Az adott, egyértelműen dekódolható bináris kódhoz konstruáljunk olyan bináris prefix kódot, amelynek kódhosszai ugyanazok:

(1) $\{01, 10, 100, 111, 011\}$;

(2) $\{1, 10, 00, 0100\}$;

(3) $\{10, 101, 111, 1011\}$.

→ **9.2.23. Feladat [1].** Az adott eloszlásokhoz határozzuk meg a bináris illetve ternáris Huffman-kódot. Hasonlítsuk össze az átlagos kódhosszat az entrópiával.

(1) 0,34, 0,18, 0,17, 0,16, 0,15;

(2) 0,6, 0,1, 0,09, 0,08, 0,07, 0,06;

(3) 0,4, 0,4, 0,1, 0,03, 0,03, 0,02, 0,02;

(4) 0,3, 0,2, 0,2, 0,1, 0,1, 0,05, 0,05.

* **9.2.24. Feladat [1].** Az előző feladat eloszlásaihoz határozzuk meg a bináris illetve ternáris Shannon-kódot. Hasonlítsuk össze az átlagos kódhosszat a Huffman-kód átlagos kódhosszával és az entrópiával.

9.2.25. Feladat [1]. Az adott eloszlásokhoz határozzuk meg a ternáris illetve kvaternáris Huffman-kódot. Hasonlítsuk össze az átlagos kódhosszat az entrópiával.

(1) 0,03, 0,12, 0,13, 0,02, 0,08, 0,3, 0,21, 0,01, 0,05, 0,01, 0,04;

(2) 0,11, 0,03, 0,21, 0,01, 0,08, 0,27, 0,14, 0,13, 0,02.

* **9.2.26. Feladat [1].** Az előző feladat eloszlásaihoz határozzuk meg a ternáris illetve kvaternáris Shannon-kódot. Hasonlítsuk össze az átlagos kódhosszat a Huffman-kód átlagos kódhosszával és az entrópiával.

9.2.27. Feladat [1]. Határozzuk meg a kvaternáris Huffman-kódot, ha a gyakoriságok 84, 118, 100, 31, 52, 213, 71, 60, 17, 84, 138, 32.

* **9.2.28. Feladat [1].** Az előző feladat gyakoriságaival határozzuk meg a kvaternáris Shannon-kódot. Hasonlítsuk össze az átlagos kódhosszat a Huffman-kód átlagos kódhosszával és az entrópiával.

9.2.29. Feladat [1]. Az adott eloszlásokhoz határozzuk meg a kvaternáris Huffman-kódot. Hasonlítsuk össze az átlagos kódhosszat az entrópiával.

(1) 0,2, 0,2, 0,19, 0,12, 0,11, 0,09, 0,09;

(2) 0,4, 0,2, 0,2, 0,1, 0,1;

(3) 0,34, 0,18, 0,17, 0,16, 0,15;

(4) 0,6, 0,1, 0,09, 0,08, 0,07, 0,06.

* **9.2.30. Feladat [1].** Az előző feladat eloszlásaihoz határozzuk meg a kvaternáris Shannon–kódot. Hasonlítsuk össze az átlagos kódhosszat a Huffman-kód átlagos kódhosszával és az entrópiával.

9.2.31. A kódolandó ábécé kiterjesztése. Egyszerű módon el tudjuk érni, hogy egy felbontható kódban az egy betűre jutó átlagos szóhosszúság tetszőlegesen megközelítse az entrópia értékét, azaz az elméleti alsó határt. Ehhez az eredeti ábécéből elkészítjük az összes kétbetűs, hárombetűs stb. szót, és egy-egy ilyen szót tekintünk egy új ábécé egy-egy betűjének, ahol egy-egy ilyen új betűhöz a benne szereplő betűk relatív gyakoriságainak szorzatát rendelve kapjuk a megfelelő eloszlást. Az így kapott kód az eredeti kód *kétszeres, háromszoros* stb. *kiterjesztése*. Ha m betű egybefogásából áll a kiterjesztett ábécé, akkor van olyan kód, amelynek egy betűre jutó átlagos szóhosszúsága

$$\bar{l} < -\sum_{i=1}^n p_i \log_r p_i + \frac{1}{m}$$

(azaz 1 helyett csak $1/m$ -mel van az elméleti alsó határ felett), ahol n az eredeti ábécé betűinek száma, és a p_i -k az eredeti ábécé betűinek relatív gyakoriságai. A módszer szépséghibája, hogy például a kétszeres kiterjesztésnél azonos számot rendel **ty**-hoz és **yt**-hez, holott a magyar nyelvben a két betűkombináció még megközelítőleg sem azonos gyakorisággal fordul elő. Ha a párok valódi gyakoriságait tekintjük, még jobb kódot kapunk. A kiterjesztésnek határt szab, hogy a kódolandó ábécé, így a kódtábla is nagyon nagy lesz, ezért a gyakorlatban nem használják.

→ **9.2.32. Feladat [1].** Az adott eloszlásokhoz határozzuk meg a ternáris illetve kvaternáris Huffman-kódot. Hasonlítsuk össze az átlagos kódhosszat az entrópiával. Ugyanezt végezzük el a kétszeres, háromszoros és négyszeres kiterjesztésre is, feltételezve, hogy az egyes ismétlések variációk relatív gyakorisága a megfelelő relatív gyakoriságok szorzata.

(1) 0,9, 0,1;

(2) 0,57, 0,43,

* **9.2.33. Feladat [1].** Az előző feladat eloszlásaihoz határozzuk meg a ternáris illetve kvaternáris Shannon–kódot. Hasonlítsuk össze az átlagos kódhosszat a Huffman-kód átlagos kódhosszával és az entrópiával.

9.2.34. Szótárkódok. A betűnkénti kódolás nem képes kihasználni, ha az egymás után következő betűk egymástól nem függetlenek, vagyis egy betű megjelenése nem független attól, hogy előtte milyen betűket bocsátott ki az adó. Egy élő nyelvű szöveg általában ilyen: a magyar nyelvben a **t** után sokkal gyakoribb az **y**, mint például az **r** után. A korábban említett kiterjesztés sem megoldás erre a problémára. Egy másik probléma, hogy amennyiben egy üzenet nem tipikus, várhatóan benne a betűk előfordulásának relatív gyakorisága eltér a szokásostól, akkor egy rögzített kódtábla, amely a tipikus szövegek betűgyakorisága alapján épül fel, nem ad jó kódot még a Huffman-kód esetén sem. Ha viszont egy ilyen esetben a konkrét szöveg statisztikája alapján hozzuk létre a kódtáblát, akkor azt is továbbítani kell.

Vannak rövid szövegek esetén hasznos „ad hoc” megoldások. Például 256 elemű bővített ASCII kód esetén egy „*escape*” karaktert fenntartva, azzal átléphetünk egy másik kódtáblába, amelyben csak a 32–94 kódú ASCII karakterek szerepelnek, de a felső bit

A *szótárkódok* alapgondolata, hogy egy $\varphi \in A^* \rightarrow B^*$ *szótárt* használunk fel a kódolásra, amelynek értelmezési tartománya tartalmazza A -t, azaz a kódolandó ábécét. A szótár lehet állandó (statikus) vagy változó (dinamikus). Az alábbiakban ilyen kódokat mutatunk be.

gugogogogol

5gugogogogol96

Ha van olyan betű az ábécében, amely biztosan nem fordulhat elő a szövegben, például a @, akkor azt használhatjuk „escape” karakternek, jelezve, hogy az utána következő számjegy nem része a szövegnek, hanem az „escape” előtti betű legalább egyszer ismétlődik (0 számjegy 1 ismétlés stb.). Ezzel a szöveg

└─@6gugogogogo└─@9└─@8

␣@6gugogogogol␣#09

└─@6gugogogogol#

299

Látszólag gondot okoz „escape” karakterek hiánya. Ha azonban a futamkódolás eredményére egy prefix kódolást alkalmazunk, akkor annyi „escape” karaktert képezhetünk, amennyit akarunk. Sőt, az escape karaktert és az utána következő számot egybefoghatjuk, és ezekhez a párokhoz rendelhetünk egy prefix kódszót, vagy akár a betűt, az escape karaktert és az utána következő számot fogjuk össze, és ehhez a hármashoz rendelünk prefix kódszót. Fax üzenetek kódolására elterjedt ez a fajta kód. Csak fekete és fehér képelemek vannak, egy sor általában 1664 képelem, soronként olvasunk. A futamhosszakat kvázi „64 alapú” számrendszerben adjuk meg: 0, 1, 2, . . . , 63 és 64, 128, 192, 256, . . . , 2560. Külön kód van a fehér és a fekete képelemsorozatok számára. Ha a képelemek száma legalább 64, akkor először a magasabb helyiértékű számjegyet küldjük át. Minden sor fehér képelemsorozattal kezdődik, és „sor vége” karakter zárja le. Ennek kódja (mindkét kódtáblában) 000000000001. Semmilyen más kód nem kezdődik 7-nél több nullával, így ha a vevő 8 nullát talál, akkor a következő egyesig olvas. Ez biztosítja, hogy egy átviteli hiba esetén legfeljebb egy sor megy tönkre. A kódhosszakat a 9.2.9 táblázat tartalmazza; a kódhosszak alapján a megfelelő Huffman-kód már algoritmussal felépíthető, bár itt nincs minden kódhossz kihasználva.

fehér futam hossza	bináris kód hossza	feketé futam hossza	bináris kód hossza	tetszőleges színű futam hossza	bináris kód hossza
0	8	0	10	1792, . . . , 1920	11
1	6	1	3	1984, . . . , 2560	12
2, . . . , 7	4	2, 3	2		
8, . . . , 11	5	4	3		
12, . . . , 17	6	5, 6	4		
18, . . . , 28	7	7	5		
29, . . . , 63	8	8, 9	6		
64, 128	5	10, . . . , 12	7		
192	6	13, 14	8		
256	7	15	9		
320, . . . , 640	8	16, . . . , 18	10		
704, . . . , 1600	9	19, . . . , 25	11		
1664	6	26, . . . , 63	12		
1728	9	64	10		
		128, . . . , 448	12		
		512, . . . , 1728	13		

9.2.9 táblázat: Fax kódolás kódtáblája.

* **9.2.36. LZ77.** Ennek a szótár típusú kódolásnak az ötletét Lempel és Ziv egy 1977-ben megjelent cikke tartalmazza. A még nem kódolt szövegből egy l hosszúságú „ablakot” figyelünk, míg a már kódolt szövegnek az ablakot megelőző legfeljebb L hosszúságú része a „szótár” (az első L lépésben a szótár rövidebb). Az ablakban elhelyezkedő szöveg egy legalább m hosszú prefixét keressük a szótárban, a szótár végétől kezdve. Ha több prefixet is találunk, a leghosszabbat választjuk, és ha az több helyen is előfordul, akkor a szótár

végéhez legközelebb álló előfordulást. Ilyenkor az (n, d) pár kerül a kódolt szövegbe, ahol n a talált prefix hossza, $m \leq n \leq l$, a d pedig a távolság a szótár utolsó betűjétől, $0 \leq d < L$. Ha nem találunk legalább m hosszú prefixet, akkor az ablak első betűje kerül a kódszövegbe. Például, ha a kódolandó ASCII szöveg `gugogogogo1`, $l = 8$, $L = 16$, $m = 2$, akkor a kód `gugo(8,1)1` lesz. Ha n helyett $n - m + 128$ értékét írjuk a szövegbe, akkor a kód a hexadecimálisan `67 75 67 6F 86 1 6C` lesz. A kódszöveget általában tovább kódoljuk egy prefix kódolással.

* **9.2.37. A gzip parancs.** Ez a parancs a „deflate” tömörített adatformátumot használja egyes blokkokra, de ha nem sikerül eléggé tömöríteni, a program úgy is dönthet, hogy egy részt csak átmásol. A *deflate* adatformátum részletes leírását lásd: Network Working Group RFC 1951. (*RFC*: Request for Comment.) Sok más hasonló program és a *zlib* tömörített könyvtárformátum (lásd RFC 1950) használja a deflate formátumot. A deflate formátum az LZ77 eljárást kombinálja két prefix kóddal:

A deflate első lépése egy LZ77-változat, amely bájt sorozaton dolgozik $l = 258$, $L = 2^{15}$, $m = 3$ paraméterekkel. Az eredeti eljárás annyiban módosul, hogy az ablak második betűjével kezdődő infixekre is végeznek keresést a szótárban, és ha itt nagyobb n hosszt sikerül elérni, akkor az első bájt változtatás nélkül kerül a kimenetre. (A parancs paraméterezésével „lebutíthatjuk” a keresést, és a program gyorsabb lesz, de kevésbé tömörít; a dekódolás nem változik.)

A második lépés a prefix kódolások alkalmazásából áll. A kódtáblák lehetnek előre definiáltak vagy változóak. Az n hosszat az $n \mapsto n - m + 257$ transzformációval a $257 \dots 512$ tartományba viszik át; a blokk végét 256 jelzi. Az előre definiált kódtáblákat a 9.2.10 táblázat tartalmazza. Az `xx...x`-szel jelölt részek bináris számlálók. Ha változó kódtáblát használunk, akkor azt is át kell küldeni. Ezt úgy oldják meg hatékonyan, hogy a kódfa helyett csak a kódhosszakat tárolják sorrendben, az elő nem forduló esetekhez nulla hosszat adva meg. A kódhosszakból, a kódábécé betűit bármely rögzített sorrendben kiosztva, a kódfa már felépíthető. Maximum 15-re korlátozzák a kódhosszakat és futamkódolják, majd prefixkódolják, és csak ennek a prefix kódnak a kódhossztábláját viszik át.

* **9.2.38. LZW-kódok.** Lempel és Ziv módszereinek egyik továbbfejlesztése Welch-től származik. A kódszavak prefix kódot alkotnak, például fix hosszúságúak. Kiinduláskor a kódtábla (az adó- és a vevőoldalon is) csak a kódolandó szöveg ábécéjének betűihez tartozó kódszavakat tartalmazza, és ez bővül a kódolás valamint a dekódolás során úgy, hogy újabb és újabb betűsorozatok kódját adjuk meg. Tegyük fel, hogy valameddig már kódoltuk az eredeti szöveget, és kezdjük el olvasni a kódolandó szöveget ettől a ponttól kezdve. Az első olvasott betű kódját tartalmazza a kódtábla. Olvassuk ki a következő betűt. Ha az első két betűből álló szöveg is szerepel a kódtáblában, akkor olvassuk ki a harmadik betűt, és ezt folytassuk mindaddig, amíg egy olyan betűhöz nem érünk, hogy a megelőző betűig terjedő szövegnek már van kódja, de az utolsó betűvel kiegészített szövegnek még nincs. Legyen a kiolvasott szöveg $a_1 \dots a_n a_{n+1}$, ahol $n \in \mathbb{N}^+$. Az előbbiek szerint tehát $a_1 \dots a_n$ -nek már létezik kódja, de $a_1 \dots a_n a_{n+1}$ -nek még nem. Ekkor elküldjük az n -hosszúságú szöveg ismert kódját, és amennyiben a kódtáblában még van szabad hely, akkor a soron következő kódszót $a_1 \dots a_n a_{n+1}$ -hez rendeljük, azaz a kódtáblát kibővítjük az $a_1 \dots a_n a_{n+1}$ -ből és a kódjából álló rendezett párral. Amennyiben betelt a kódtábla, akkor nem bővítjük tovább.

betű vagy hossz	bináris kód	távolság	bináris kód
0...143	00110000...10111111	0...3	00000...00011
144...255	110010000...111111111	4...5	00100x
256...264	0000000...0001000	6...7	00101x
265...266	0001001x	8...11	00110xx
267...268	0001010x	12...15	00111xx
269...270	0001011x	16...23	01000xxx
271...272	0001100x	24...31	01001xxx
273...276	0001101xx	32...47	01010xxxx
277...280	0001110xx	48...63	01011xxxx
281...284	0001111xx	64...95	01100xxxxx
285...288	0010000xx	96...127	01101xxxxx
289...296	0010001xxx	128...191	01110xxxxxx
297...304	0010010xxx	192...255	01111xxxxxx
305...312	0010011xxx	256...383	10000xxxxxxxx
313...320	0010100xxx	384...511	10001xxxxxxxx
321...336	0010101xxxx	512...767	10010xxxxxxxx
337...352	0010110xxxx	768...1023	10011xxxxxxxx
353...368	0010111xxxx	1024...1535	10100xxxxxxxx
369...384	11000000xxxx	1536...2047	10101xxxxxxxx
385...416	11000001xxxx	2048...3071	10110xxxxxxxx
417...448	11000010xxxx	3072...4095	10111xxxxxxxx
449...480	11000011xxxx	4096...6143	11000xxxxxxxx
481...511	11000100xxxx	6144...8191	11001xxxxxxxx
512	11000101	8192...12287	11010xxxxxxxx
		12288...16383	11011xxxxxxxx
		16384...24575	11100xxxxxxxx
		24576...32767	11101xxxxxxxx

9.2.10 táblázat: Kódtábla gzip-hez.

A dekódolás hasonlóan történik. Az első vett kódszó biztosan egyetlen betű kódja, amelynek így a vevő oldalán is ismert a megfejtése. Ismét tegyük fel, hogy már valameddig eljutott az adás, és egy újabb kódszó érkezik. Ha az előző kódszónak megfelelő betűsorozat $a_1 \dots a_n$, és a most vett kódszó dekódolásában az első betű u , akkor az adónál a most elküldött kódszó előtt a kódtábla soron következő eleme nyilván az $a_1 \dots a_n u$ betűsorozatot fogja kódolni, vagyis a vevő is ezt a jelsorozatot rendeli a kódtábla soron következő eleméhez, és így a továbbiakban már ezt a kódot is tudja dekódolni. Egyetlen esetben lehet probléma a dekódolásnál. Ha a kódolásnál a már kódolt szöveg után az $a_1 \dots a_n a_{n+1} \dots a_{n+m}$ szöveg olyan, hogy $a_1 \dots a_n$ -nek már van kódja, de $a_1 \dots a_n a_{n+1}$ -nek még nincs, és $a_{n+1} \dots a_{n+m} = a_1 \dots a_n a_{n+1}$, akkor az $a_1 \dots a_n$ kódjának elküldése után az adónál bekerül a kódtáblába $a_1 \dots a_n a_{n+1}$ kódja, és így a következő kódolandó szöveghez, $a_1 \dots a_n a_{n+1}$ -hez már lesz bejegyzés, tehát tudjuk kódolni (de a következő

betűvel meghosszabbított szöveg még biztosan nem kódolható, hiszen ellenkező esetben az algoritmusunk alapján már az előző lépésben tudtuk volna $a_1 \dots a_n a_{n+1}$ -et kódolni). Ugyanakkor a vétel helyén $a_1 \dots a_n a_{n+1}$ kódját az előző, $a_1 \dots a_n$ -hez tartozó kód dekódolása, valamint a most beérkezett, az $a_1 \dots a_n a_{n+1}$ kódjának visszafejtésekor kapott szöveg első betűje alapján tudnánk meghatározni, ami lehetetlen, hiszen az aktuális dekódoláshoz a még ismeretlen, éppen most meghatározandó szöveget kellene ismerni. A dekódolás azonban mégis elvégezhető, mert ha a vett kódszó még nem szerepel a vétel helyén a kódtáblában, az csak azért lehetséges, mert a kódolandó szöveg a fent leírt alakú, tehát $a_{n+1} \dots a_{n+m} = a_1 \dots a_n a_{n+1}$, amiből viszont következik, hogy $a_{n+1} = a_1$, tehát a kódtáblában még nem található, éppen most beérkezett, dekódolandó szöveg $a_1 \dots a_n a_1$, így el tudjuk végezni a dekódolást, és tovább tudjuk építeni a vevőnél is a kódtáblát.

* **9.2.39. Példa az LZW-kódra.** Legyen a kód hexadecimális (azaz az ábécé 16 elemű), a kódszavak hossza 2 (így a kódtábla maximális mérete 256 bejegyzés), és az alaphelyzetben (azaz 128 betűre) használjunk ASCII-kódot. Például c kódja 63, így a kódtáblában az egyik bejegyzés a (c, 63) pár. Kódoljuk most is a gugogogogol szöveget.

Mivel g kódja 67, ugyanakkor gu még nem szerepel a kódtáblában, így elküldjük a 67-es kódszót, és a kódtáblába beírjuk (gu, 80)-at (mert 128 hexadecimálisan 80). A továbbiakban az uogogogol szöveget kell kódolnunk. Az u kódja ismert, de ug kódja még nem. Küldjük el u kódját, ami 75, és a kódtáblába írjuk be az (ug, 81) párt. Maradt a gogogogol szöveg. Ismert g kódja, de ismeretlen a go szöveg, tehát megy a 67-es kódszó, és a táblába beírjuk a (go, 82) párt. Most az ogogogol szöveg bal szélénél tartunk. Tudjuk o kódját, de még ismeretlen az og kódja. A 6F-es kód elküldésén kívül az (og, 83) bejegyzéssel megadjuk og kódját. A gogogol szöveg maradt. Tudjuk g és go kódját, de még nincs kódja a gog hármasnak, így elküldjük 82-t, és a táblába bekerül a (gog, 84) pár. Következik a gogol kódolása. Már tudjuk kódolni g-t, go-t, gog-ot, de még nem találkoztunk gogo-val, így el tudjuk küldeni a 84-es kódszót, és felveszük a kódtáblába (gogo, 85)-öt. Még ol van hátra. Ebből csak az o-t tudjuk kódolni, az elküldött kód 6F, és bővül a kódtábla a (ol, 86) párral. Végül egyetlen karakter, az l maradt, amelynek a kódja 6C. Ezt elküldjük, és a táblába már semmit nem kell bejegyeznünk.

Most nézzük a dekódolást. Az érkező kódszavak sorozata 67 75 67 6F 82 84 6F 6C. Mivel 67-ből g-t, 75-ből u-t dekódolunk, a kódtáblába bejegyezzük a (gu, 80) párt. A 67-ből ismét g-t dekódolunk, a táblába bekerül az (ug, 81) pár. Mivel 6F az o kódja, tehát az eddig visszafejtett szöveg gugo, és a táblába (go, 82)-t írunk. Következik a 82 dekódolása. A kódtáblában a (go, 82) bejegyzés található, így az eddig dekódolt teljes szöveg gugogo. Mivel az előző kódszó 6F, míg a most dekódolt szöveg első karaktere g volt, ezért a kódtáblába (og, 83) kerül. Most 84-et kell dekódolnunk, ám a táblánkban ilyen kód nincs. Ebből arra következtetünk, hogy a 84 megfejtése az utolsó dekódolt szöveg, jobbról kiegészítve az előbb dekódolt karaktersorozat bal szélső karakterével, vagyis a konkrét esetben 84 megfejtése gog, és gyorsan beírjuk a kódtáblába a (gog, 84) párt. A hátralévő kód fejtése már könnyű, az elsőé az o, és a kódtábla bővül a (gogo, 85) beírással, majd 6C megfejtése l, és a kódtáblába feljegyezzük az (ol, 86) párt.

Az előbbi kódolást és dekódolást mutatja a 9.2.11 és 9.2.12 táblázat.

A 9.2.11 táblázatban az 1. oszlopban a még nem kódolt szöveg, a 2. oszlopban az adott menetben kódolt szövegrész található. A 3. oszlop mutatja az elküldött kódszót, míg a 4. a táblába kerülő bejegyzést.

gugogogogol	g	67	(gu, 80)
ugogogogol	u	75	(ug, 81)
gogogogol	g	67	(go, 82)
ogogogol	o	6F	(og, 83)
gogogol	go	82	(gog, 84)
gogol	gog	84	(gogo, 85)
ol	o	6F	(ol, 86)
l	l	6C	

9.2.11 táblázat: Példa LZW kódra, kódolás.

67	(g, 67)	g	
75	(u, 75)	u	(gu, 80)
67	(g, 67)	g	(ug, 81)
6F	(o, 6F)	o	(go, 82)
82	(go, 82)	go	(og, 83)
84	(gog, 82)	gog	(gog, 84)
6F	(o, 6F)	o	(gogo, 85)
6C	(l, 6C)	l	(ol, 86)

9.2.12 táblázat: Példa LZW kódra, dekódolás.

A 9.2.12 táblázat 1. oszlopában az éppen vett kódszó látható, utána jön a tábla megfelelő bejegyzése, majd a dekódolt szövegrész. A 4. oszlopban található a tábla aktuális bejegyzése.

Programozásnál zavaró lehet, hogy a párok első koordinátája változó hosszúságú betűsorozat. Ezt könnyen kiküszöbölhetjük úgy, hogy csak az utolsó betűt tároljuk, és egy pointert a prefixre, ami már a táblában van. Ha a kód egyenletes kód, a dekódolásnál a φ függvény inverzét táblázatban tárolhatjuk. A kódolás során a φ függvényt mint párok halmazát kezeljük. Ez hash-transzformációval valósítható meg hatékonyan.

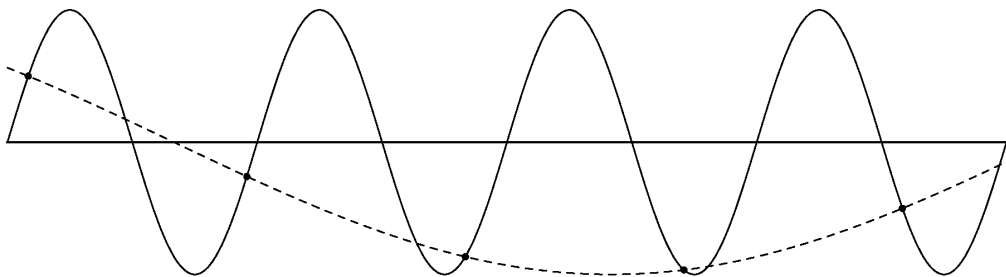
* **9.2.40. A compress parancs.** LZW-típusú kódot használ a *compress* parancs. Az újdonság, hogy a kódhosszat dinamikusan változtatjuk. Kezdetben a kódhossz 9 bit, és a bájtok kódjait tartalmazza. Ha betelik a szótár, 10 bitre növeljük a kódhosszat. A kódhossz maximális értéke paraméterezhető, de maximum 16 bit. Ha elértük a maximális kódhosszat, és betelt a szótár, a program akkor is figyel, hogy mekkora tömörítést sikerült elérni. Ha ez egy adott érték alá megy, eldobjuk a szótárat, és új szótár építésébe kezdünk.

* **9.2.41. Digitalizálás.** Egy valós értékű függvényt (fizikai vagyis *analóg jelet*) számítógépben közvetlenül nem tudunk reprezentálni, ezért mintavételezéssel sorozattá alakítjuk, majd a kapott valós számokat egész számokká alakítva kvantáljuk. A két lépés együtt a *digitalizálás*.

Egy $t \mapsto F(t)$ függvényt (amelyet legtöbbször az idő függvényének gondolunk, bár ez nem szükségszerű) *mintavételezéssel* alakíthatunk (mindkét irányban végtelen) sorozattá: legyen $f_k = F(\tau_0 + k\tau)$, ha $k \in \mathbb{Z}$, ahol $\tau_0 \in \mathbb{R}$ és $0 < \tau \in \mathbb{R}$ rögzítettek. A mintavételezés *periódusideje* τ , ennek reciproka, $1/\tau$ a *mintavételi frekvencia*, azaz az időegységre eső

minták száma. Természetesen, ha az F jel csak egy véges intervallumon van értelmezve, akkor a minta is véges sorozat lesz.

Tekintsük példaként a $t \mapsto \sin(2\pi(t - \tau_0)/T)$ periodikus jelet, amelynek periódusa T (azaz $F(t + T) = F(t)$ minden $t \in \mathbb{R}$ -re), frekvenciája így $1/T$. Ennek τ mintavételi periódusidővel való mintavételezésével az $f_k = \sin(2\pi k\tau/T)$, $k \in \mathbb{Z}$ sorozatot kapjuk. Észrevehetjük, hogy ha egy ilyen szinuszos jel frekvenciája a mintavételi frekvencia fele, azaz ha $2/T = 1/\tau$, akkor $f_k = \sin(\pi k) = 0$, ami megegyezik az azonosan nulla jel mintavételezésével kapott sorozattal. Ez azt mutatja, hogy a mintavételi frekvencia felénél nem kisebb frekvenciájú jelösszetevők a mintavételnél elveszhetnek. Ezért a mintavételi frekvencia az átvinni kívánt jel legmagasabb frekvenciájú összetevője frekvenciájának több mint kétszerese kell hogy legyen: ez *Shannon mintavételi törvénye*. (Lásd a 9.2.13 ábrát is.)



9.2.13 ábra: Az alulmintavételezés hatása.

Kétdimenziós $(x, y) \mapsto F(x, y)$ jelnél, például képnél, kétdimenziós mintavételezést alkalmazunk:

$$f_{i,j} = F(\xi_0 + i\xi, \eta_0 + j\eta).$$

Háromdimenziós $(x, y, t) \mapsto F(x, y, t)$ jelnél, például mozgóképnél, a mintavételezés is háromdimenziós:

$$f_{i,j,k} = F(\xi_0 + i\xi, \eta_0 + j\eta, \tau_0 + k\tau).$$

A mintavételezéssel kapott jel még nem tárolható a számítógépben: kerekítéssel digitalizálni kell. Általában egészen kerekítünk valamilyen szabály szerint. A kerekítés előtt rendszerint egy szigorúan monoton $v \mapsto q(v)$ *kvantálási függvényt* alkalmazunk a mintavételezéssel kapott értékekre, majd kerekítünk, ez a tulajdonképpeni *kvantálás*. A kvantálási függvény gyakran lineáris, $q(v) = av + b$ alakú. Minél nagyobb a , annál kisebb változás elég v -ben, hogy másik egész számot kapjunk a kerekítés után, tehát annál finomabb a kvantálás, azaz annál közelebbi jelszinteket tudunk megkülönböztetni. A b konstanssal például elérhetjük, hogy a kvantált értékek nemnegatívak legyenek, b tehát szinteltolást jelent.

A kvantálás sajnos azt is jelenti, hogy „zajt” viszunk be a jelbe. A hang (egységnyi felületre eső) teljesítménye a hangnyomás négyzetével arányos. A mikrofon a hangnyomással arányos feszültséget hoz létre, a villamos teljesítmény ennek a négyzetével arányos, tehát arányos a hangteljesítménnyel. Fülünk érzékenysége logaritmikus jellegű: bármely két hang között akkor érzünk ugyanolyan hangosságkülönbséget, ha teljesítményük aránya ugyanaz az érték. Ezért hangjel kvantálásánál logaritmikus jellegű kvantálási függvényt

érdemes alkalmazni, mert ekkor ugyan hangosabb jelnél a kvantálási zaj is hangosabb lesz, de a teljesítményük aránya ugyanaz marad, így egyformán érezzük zajosnak a különböző intenzitású részeket. Például a telefontársaságok Észak-Amerikában és Japánban a

$$v \mapsto \operatorname{sgn}(v) \frac{\log(1 + \mu|v|)}{\log(1 + \mu)}$$

függvényt használják rendszerint $\mu = 255$ választással, míg a világ többi részén a

$$v \mapsto \begin{cases} \operatorname{sgn}(v) \frac{A|x|}{1 + \ln A}, & \text{ha } 0 \leq |x| < 1/A, \\ \operatorname{sgn}(v) \frac{1 + \ln |Ax|}{1 + \ln A}, & \text{ha } 1/A \leq |x| \leq 1 \end{cases}$$

függvényt, általában $A = 87,6$ választással; ez mindkét esetben úgy értendő, hogy a fenti függvényeket mint $[-1, 1]$ -et önmagába képező függvényeket kell tekinteni, és alkalmazásuk előtt és után is konstanssal való szorzást alkalmazunk. (Az első függvény valamivel kisebb alapzajt, a második valamivel jobb dinamikát biztosít.) Az is lehet, hogy egy már (lineárisan, finoman) kvantált jelet kvantálunk újra nemlineáris kvantálással. (Például digitális telefontól a fenti függvényekkel tulajdonképpen 14 bites lineárisan kvantált értéket kvantálnak újra, hogy 8 bites értéket kapjanak, valamivel növelve a zajt, de csökkentve az átvíendő bitek számát.) Természetesen amikor a digitalizált jelet visszaalakítjuk analóg jellé, a kvantálási függvény inverzét kell alkalmaznunk.

Általában a digitalizálás mindkét lépésében – a mintavételezésnél és a kvantálásnál is – elvész az információ egy része, így általában minden digitalizálást használó kódolás eleve veszteséges.

Néhány tömörítő eljárás *vektorkvantálást* használ: összetartozó mennyiségeket (például egy színes képpont színekoordinátáit) együtt vektornak tekintünk, és egy vektorokat tartalmazó kódtáblából keressük ki a hozzá legközelebbi vektort.

* **9.2.42. DFT és IDFT.** Tekintsünk egy $T > 0$ periódus szerint periodikus valós változós komplex értékű F függvényt (azaz $F(t + T) = F(t)$ minden $t \in \mathbb{R}$ -re), legyen a mintavételi frekvencia az $1/T$ „alapfrekvencia” n -szerese, ahol $n \in \mathbb{N}^+$, azaz legyen $\tau = T/n$, és legyen (kényelmi okokból) $\tau_0 = 0$. A mintavételezéssel kapott $f_j = F(\tau_0 + j\tau)$ ($j \in \mathbb{Z}$) sorozat n szerint periodikus, azaz $f_{j+n} = f_j$ minden $j \in \mathbb{Z}$ -re, így egy $\mathbb{Z}_n$ -en értelmezett f függvénynek is tekinthető, vagyis az $f_0, f_1, \dots, f_{n-1}$ értékek egyértelműen jellemzik; a $\tau_0 + j\tau$, $j = 0, 1, \dots, n-1$ pontok az *alappontok* (elég lenne az is, hogy a $j \bmod n$ teljes maradékrendszer legyen). Ezt a függvényt szeretnénk „eltolt szinuszos” jelek lineáris kombinációjaként előállítani:

Tekintsük a $H_k(t) = \cos(2\pi kt/T) + i \sin(2\pi kt/T)$, $k \in \mathbb{Z}$ ugyancsak T szerint periodikus komplex értékű függvényeket. A H_k függvénynek a fenti módon való mintavételezésével az ω_n^{jk} , $j \in \mathbb{Z}$ sorozatot kapjuk, ahol $\omega_n = \cos(2\pi/n) + i \sin(2\pi/n)$ az első n -edik egységgyök. Legyen $\hat{f}_k = \sum_{j=0}^{n-1} f_j \omega_n^{-jk}$ (azaz az

$$(f_0, f_1, \dots, f_{n-1})$$

és az

$$(\omega_n^0, \omega_n^k, \dots, \omega_n^{(n-1)k})$$

$\mathbb{C}^n$ -beli vektorok belső szorzata), ha $k \in \mathbb{Z}$. A $\hat{f}_k$, $k \in \mathbb{Z}$ sorozat is n szerint periodikus, hiszen $\omega_n^n = 1$, így

$$\hat{f}_{k+n} = \sum_{j=0}^{n-1} f_j \omega_n^{-j(k+n)} = \sum_{j=0}^{n-1} f_j \omega_n^{-jk} = \hat{f}_k.$$

Tehát az f sorozathoz az $\hat{f}$ sorozatot rendelő leképezés a $\mathbb{Z}_n$ -en értelmezett komplex értékű függvények n -dimenziós komplex (azaz $\mathbb{C}$ feletti) vektorterét önmagába képezi le. Ezt a leképezést nevezzük *diszkrét Fourier-transzformációnak*, *DFT*-nek. A diszkrét Fourier-transzformáció olyan fontos leképezés, hogy gyors végrehajtására integrált áramköröket gyártanak, számos műszaki alkalmazással (jelanalízis, digitális szűrés, stb.), és szoros kapcsolatban áll az analízisben tanulmányozott Fourier-sorokkal és Fourier-transzformációval. A DFT nyilván lineáris.

Vegyük észre, hogy

$$\sum_{j=0}^{n-1} (\omega_n^k)^j = \frac{(\omega_n^k)^n - 1}{\omega_n^k - 1}$$

0, ha $\omega_n^k \neq 1$, és a szumma nyilván n , ha $\omega_n^k = 1$. Ebből következik, hogy a

$$H_0, H_1, \dots, H_{n-1}$$

függvények mintavételezésével kapott $h_k: \mathbb{Z}_n \rightarrow \mathbb{C}$ vektorok páronként ortogonálisak és mindegyiknek az önmagával vett belső szorzata n , hiszen

$$\langle h_{k'}, h_{k''} \rangle = \sum_{j=0}^{n-1} h_{k'}(j) \overline{h_{k''}(j)} = \sum_{j=0}^{n-1} \omega_n^{jk'} \overline{\omega_n^{jk''}} = \sum_{j=0}^{n-1} \omega_n^{j(k'-k'')}.$$

Innen a

$$t \mapsto \frac{1}{n} \sum_{k=0}^{n-1} \hat{f}_k H_k(t)$$

függvény a mintavételezés $t = j\tau$ pontjaiban megegyezik a kiindulási F függvénnyel, azaz az F periodikus függvényt közelítettük a H_k periodikus függvények segítségével. (Egyébként ugyanez igaz, ha a k indexek bármely modulo n vett teljes maradékrendszert futnak be.) Speciálisan, a DFT invertálható, és „majdnem” (az $1/n$ szorzótól és az origóra való tükrözéstől eltekintve) saját maga az inverze: $t = j\tau$ helyettesítéssel

$$f_j = \frac{1}{n} \sum_{k=0}^{n-1} \hat{f}_k \omega_n^{jk} = \frac{1}{n} \sum_{k=0}^{n-1} \hat{f}_k \omega_n^{-(-j)k} = \frac{1}{n} \hat{f}_{-j}.$$

A DFT inverzét *inverz diszkrét Fourier-transzformációnak*, *IDFT*-nek nevezzük.

További hasznos észrevétel, hogy

$$\hat{\hat{f}}_k = \sum_{j=0}^{n-1} \bar{f}_j \omega_n^{-jk} = \overline{\sum_{j=0}^{n-1} f_j \omega_n^{jk}} = \overline{\hat{f}_{-k}}.$$

Így, ha az f_j sorozat valós, akkor $\hat{f}_k = \hat{\hat{f}}_k = \overline{\hat{f}_{-k}}$. Ennek az észrevételnek a segítségével megvizsgálhatjuk a

$$\frac{1}{n} \sum_{k=0}^{n-1} \hat{f}_k H_k(t)$$

összegben az egyes tagok jelentését. Az $f_0 H_0(t)$ tag konstans, az átlag n -szerese. Valós f_j sorozat esetén, ha $0 < k \leq n/2$, $f_k = r_k(\cos \varphi_k + i \sin \varphi_k)$, akkor

$$\begin{aligned} \hat{f}_k H_k(t) + \hat{f}_{-k} H_{-k}(t) &= r_k(\cos \varphi_k + i \sin \varphi_k)(\cos(2\pi kt/T) + i \sin(2\pi kt/T)) \\ &\quad + r_k(\cos \varphi_k - i \sin \varphi_k)(\cos(2\pi kt/T) - i \sin(2\pi kt/T)) \\ &= 2r_k \cos(2\pi kt/T + \varphi_k), \end{aligned}$$

azaz $2r_k$ -szor egy koszinuszos jel φ_k fáziseltolással, tehát az eredeti jelet lényegében koszinuszos („harmonikus”) jelek összegére bontottuk, amelyek frekvenciája az $1/T$ alaphfrekvencia k -szorosa, $0 \leq k \leq n/2$. A $2r_k/n = 2|\hat{f}_k|/n = 2|\hat{f}_{-k}|/n$ mennyiség úgy tekinthető, mint a $\cos(2\pi kt/T + \varphi_k)$ harmonikus jelnek az amplitúdója az F jelben, ha $0 < k < n/2$; ha $k = n/2$, akkor $\hat{f}_k = \hat{f}_{-k}$ valós és $H_k = \overline{H_{-k}}$, így $k = n/2$ esetén a $\cos(2\pi kt/T + \varphi_k)$ harmonikus jel amplitúdója az eredeti F jelben $r_k/n = |\hat{f}_k|/n = |\hat{f}_{-k}|/n$. A φ_k eltolási érték a „fáziseltolás”.

Végül vegyük még észre, hogy ha az f_j ($j \in \mathbb{Z}$) sorozat páros, akkor

$$f_j = f_{-j} = \frac{1}{n} \hat{f}_{-(-j)} = \frac{1}{n} \hat{f}_j,$$

ahonnan

$$\hat{f}_k = \frac{1}{n} \hat{\hat{f}}_k = \hat{f}_{-k},$$

azaz az $\hat{f}_k$ sorozat is páros. Ha az f_j sorozat valós és páros, akkor a $\hat{f}_k$ sorozat páros és $\overline{\hat{f}_k} = \overline{\hat{\hat{f}}_k} = \hat{f}_{-k} = \hat{f}_k$, azaz valós is. Hasonlóan, ha az f_j sorozat páratlan, akkor

$$-f_j = f_{-j} = \frac{1}{n} \hat{\hat{f}}_j,$$

ahonnan

$$-\hat{f}_k = \frac{1}{n} \hat{\hat{f}}_k = \hat{f}_{-k},$$

azaz $\hat{f}$ is páratlan. Ha az f_j sorozat valós és páratlan, akkor a $\hat{f}_k$ sorozat páratlan és $\overline{\hat{f}_k} = \overline{\hat{\hat{f}}_k} = \hat{f}_{-k} = -\hat{f}_k$, azaz képzetes.

*** 9.2.43. FFT.** A gyors Fourier-transzformáció (Fast Fourier Transform, *FFT*) a diszkrét Fourier-transzformált gyors kiszámítására szolgál. Legyen $n \in \mathbb{N}^+$ rögzített, és az egyszerűség kedvéért vezessük be az $\omega = \overline{\omega}_n = \omega_n^{-1}$ jelölést. Vegyük észre, hogy az előző pontban használt jelölésekkel $\hat{f}_k$ nem más, mint az $f^{(0)}(x) = \sum_{j=0}^{n-1} f_j x^j$ polinom $x_k = \omega^k$ helyen felvett értéke:

$$f^{(0)}(\omega^k) = \sum_{j=0}^{n-1} f_j (\omega^k)^j = \sum_{j=0}^{n-1} f_j \omega_n^{-kj} = \hat{f}_k.$$

Az $\hat{f}_k$ értékek gyors kiszámításához vezető trükk: ha $n = n_1 n_2$, akkor $y = x^{n_1}$ jelöléssel

$$f^{(0)}(x^{n_1 j_2 + k_1}) = \sum_{k_1=0}^{n_1-1} x^{k_1} f_{k_1}^{(1)}(y),$$

ahol

$$f_{k_1}^{(1)}(y) = \sum_{j_2=0}^{n_2-1} f_{n_1 j_2 + k_1} y^{j_2}, \quad k_1 = 0, 1, \dots, n_1 - 1.$$

Ha $x = \omega^{k_1}, \omega^{k_1+n_2}, \dots, \omega^{k_1+(n_1-1)n_2}$, akkor a hozzá tartozó y ugyanaz, így minden kiszámított $f_{k_1}^{(1)}(y)$ érték többször is felhasználható. Például, ha $n_1 = 2$, $n = 2n_2$, akkor az $f^{(0)}$ polinom ω^k és $\omega^{k+n/2}$ helyen felvett értékeit egyszerre számolhatjuk ki (azt is felhasználva, hogy $\omega^{n/2} = -1$) az alábbi „pillangó művelettel”:

$$\begin{aligned} f^{(0)}(\omega^j) &= f_0^{(1)}(\omega^{2k}) + \omega^k f_1^{(1)}(\omega^{2k}), \\ f^{(0)}(\omega^{k+n/2}) &= f_0^{(1)}(\omega^{2k}) - \omega^k f_1^{(1)}(\omega^{2k}). \end{aligned}$$

Például, ha $n = 8$, $n_1 = 2$, akkor $x = \omega^k$ és $x = \omega^{k+4}$ esetén y értéke ω^{2k} , így az

$$f_0 + f_2 y + f_4 y^2 + f_6 y^3$$

és

$$f_1 + f_3 y + f_5 y^2 + f_7 y^3$$

értékeket kétszer is tudjuk használni, így a munkát nagyjából megfeleztük. Természetesen rekurzívan is alkalmazhatjuk ezt a trükköt. Az alábbi, együtthatóikkal adott polinomok értékeit kell kiszámolnunk a megadott helyeken (a zárójelben a felső sorban az együttható, alsó sorban a helyek szerepelnek; minden sor kiszámítását az alatta lévő sor kiszámítására vezetjük vissza):

$$\begin{array}{cccccccc} \left(\begin{array}{c} f_0, \\ \omega^0 \end{array}, \begin{array}{c} f_1, \\ \omega^1 \end{array}, \begin{array}{c} f_2, \\ \omega^2 \end{array}, \begin{array}{c} f_3, \\ \omega^3 \end{array}, \begin{array}{c} f_4, \\ \omega^4 \end{array}, \begin{array}{c} f_5, \\ \omega^5 \end{array}, \begin{array}{c} f_6, \\ \omega^6 \end{array}, \begin{array}{c} f_7, \\ \omega^7 \end{array} \right) \\ \\ \left(\begin{array}{c} f_0, \\ \omega^0 \end{array}, \begin{array}{c} f_2, \\ \omega^2 \end{array}, \begin{array}{c} f_4, \\ \omega^4 \end{array}, \begin{array}{c} f_6, \\ \omega^6 \end{array} \right) & \left(\begin{array}{c} f_1, \\ \omega^0 \end{array}, \begin{array}{c} f_3, \\ \omega^2 \end{array}, \begin{array}{c} f_5, \\ \omega^4 \end{array}, \begin{array}{c} f_7, \\ \omega^6 \end{array} \right) \\ \\ \left(\begin{array}{c} f_0, \\ \omega^0 \end{array}, \begin{array}{c} f_4, \\ \omega^4 \end{array} \right) & \left(\begin{array}{c} f_2, \\ \omega^0 \end{array}, \begin{array}{c} f_6, \\ \omega^4 \end{array} \right) & \left(\begin{array}{c} f_1, \\ \omega^0 \end{array}, \begin{array}{c} f_5, \\ \omega^4 \end{array} \right) & \left(\begin{array}{c} f_3, \\ \omega^0 \end{array}, \begin{array}{c} f_7, \\ \omega^4 \end{array} \right) \\ \\ \left(\begin{array}{c} f_0, \\ \omega^0 \end{array} \right) & \left(\begin{array}{c} f_4, \\ \omega^0 \end{array} \right) & \left(\begin{array}{c} f_2, \\ \omega^0 \end{array} \right) & \left(\begin{array}{c} f_6, \\ \omega^0 \end{array} \right) & \left(\begin{array}{c} f_1, \\ \omega^0 \end{array} \right) & \left(\begin{array}{c} f_5, \\ \omega^0 \end{array} \right) & \left(\begin{array}{c} f_3, \\ \omega^0 \end{array} \right) & \left(\begin{array}{c} f_7, \\ \omega^0 \end{array} \right) \end{array}$$

A fentiek alapján rekurzív programot írhatunk a diszkrét Fourier-transzformáció elvégzésére, ha n „kis tényezők szorzatára” bontható. A gyakorlatban legtöbbször használt $n = 2^m$ esetben célszerűbb azonban a rekurziót ciklussá átalakítani. Vezessük be a $[d_s d_{s-1} \dots d_2 d_1] = \sum_{j=1}^s d_j 2^{j-1}$ jelölést. Defináljuk az

$$f_{j_1, j_2, \dots, j_s}^{(s)} = \sum_{j=0}^{2^{m-s}-1} f_{[jj_s j_{s-1} \dots j_2 j_1]} x^j, \quad \text{ha } 0 \leq s \leq m, \quad j_1, \dots, j_s \in \{0, 1\}$$

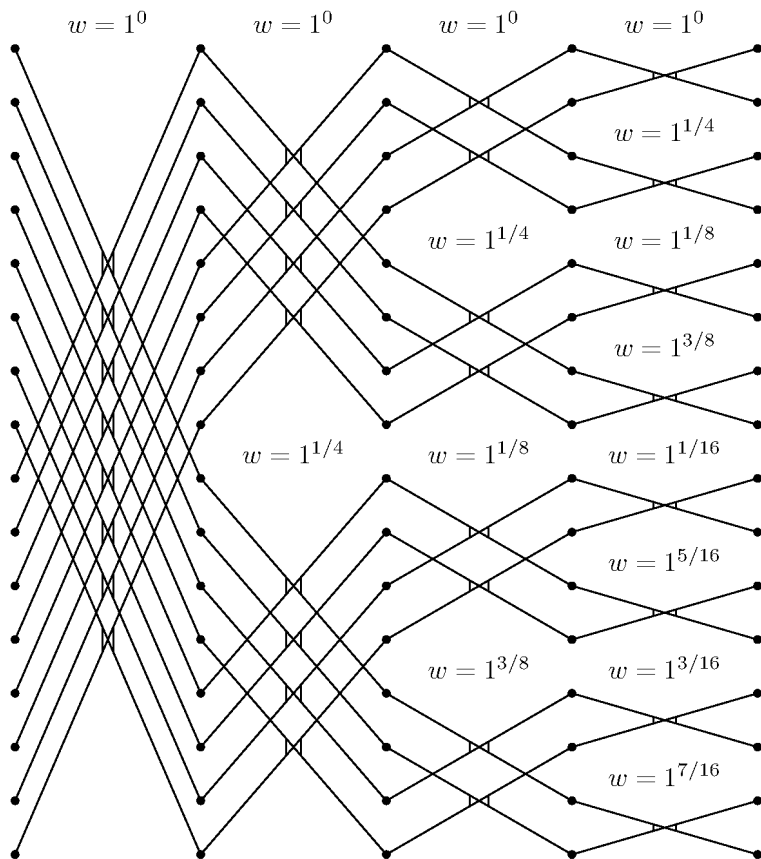
„közbulső polinomokat”. Az $f_{j_1, j_2, \dots, j_m}^{(m)}$ polinomok konstansok, értékük $f_{[j_m j_{m-1} \dots j_2 j_1]}$. Az

$$\begin{aligned} f_{j_1, j_2, \dots, j_s}^{(s)}(\omega^{k2^s}) &= f_{j_1, j_2, \dots, j_s, 0}^{(s+1)}(\omega^{k2^{s+1}}) + \omega^{k2^s} f_{j_1, j_2, \dots, j_s, 1}^{(s+1)}(\omega^{k2^{s+1}}) \\ f_{j_1, j_2, \dots, j_s}^{(s)}(\omega^{k2^s+n/2}) &= f_{j_1, j_2, \dots, j_s, 0}^{(s+1)}(\omega^{k2^{s+1}}) - \omega^{k2^s} f_{j_1, j_2, \dots, j_s, 1}^{(s+1)}(\omega^{k2^{s+1}}) \end{aligned}$$

pillangóművelet segítségével rendre az $s = m-1, m-2, \dots, 1, 0$ értékekre számítjuk ki a függvényértékeket. Egyetlen n elemű A tömböt használunk,

$$f_{j_1, j_2, \dots, j_s}^{(s)}(\omega^{[k_{m-s} k_{m-s-1} \dots k_2 k_1] 2^s})$$

értéke $A[k_1 k_2 \dots k_{m-s} j_1 j_2 \dots j_s]$ -be kerül, ahol $k_1, k_2, \dots, k_{m-s}, j_1, \dots, j_s \in \{0, 1\}$. Így az alábbi algoritmust kapjuk (lásd a 9.2.14 ábrát is):



9.2.14 ábra: FFT; itt $1^{p/q} = \cos(2\pi p/q) - i\sin(2\pi p/q)$.

* **9.2.44. FFT algoritmus.** Az előző pont jelöléseivel az algoritmus az A tömbben lévő

$$A[j_m j_{m-1} \dots j_2 j_1] = f_{[j_m j_{m-1} \dots j_2 j_1]}, \quad j_1, \dots, j_m \in \{0, 1\}$$

sorozat Fourier-transzformáltját számolja ki. Az egész számítás „helyben”, az A tömbben zajlik, a részeredmények és végeredmény is az A tömbben keletkezik, de $\hat{f}_{[k_m k_{m-1} \dots k_2 k_1]}$ nem az A tömb $[k_m k_{m-1} \dots k_2 k_1]$ indexű elemében foglal helyet, hanem az ebből a bit-sorozatból „bitfordítással” kapott indexű helyen:

$$\hat{f}_{[k_m k_{m-1} \dots k_2 k_1]} = A[k_1 k_2 \dots k_{m-1} k_m], \quad \text{ha } k_1, \dots, k_m \in \{0, 1\}.$$

A számítás használ egy T segéd táblázatot, amely az ω hatványait tartalmazza, „bitfordított” sorrendben:

$$T[j_{m-1} \dots j_2 j_1] \leftarrow \omega^{[j_1 j_2 \dots j_{m-1}]}, \quad \text{ha } j_1, \dots, j_m \in \{0, 1\}.$$

Az algoritmus:

- (1) [Inicializálás.] Legyen $l \leftarrow 2^{m-1}$.
- (2) [Menet kezdete.] Legyen $j \leftarrow 0$ és $t \leftarrow 0$.
- (3) [Pillangósorozat kezdete.] Legyen $k \leftarrow j + l$ és $w \leftarrow T[t]$.
- (4) [Pillangó művelet.] Legyen $x \leftarrow A[j]$ és $y \leftarrow wA[j + l]$, majd legyen $A[j] \leftarrow x + y$ és $A[j + l] \leftarrow x - y$, végül legyen $j \leftarrow j + 1$.
- (5) [Pillangósorozat vége?] Ha $j < k$, menjünk vissza (4)-re.
- (6) [Menet vége?] Ha $k + l < n$, legyen $j \leftarrow k + l$, $t \leftarrow t + 1$, és menjünk vissza (3)-ra. (Most $A[k_1 k_2 \dots k_{m-s} j_1 j_2 \dots j_s] = f_{j_1, j_2, \dots, j_s}^{(s)}(\omega^{[k_{m-s} k_{m-s-1} \dots k_2 k_1] 2^s})$, lásd az előző pontot.)
- (7) [Vége?] Legyen $l \leftarrow \lfloor l/2 \rfloor$. Ha $l > 0$, menjünk vissza (2)-re, egyébként az algoritmus véget ért.

Az eredmény kiolvasásához, illetve a T tábla feltöltéséhez szükséges „bitfordítás” eltolásokkal történhet: a számot balra tolva, egyenként megkapjuk bitjeit, és azokat jobbra tolással összerakjuk fordított sorrendben. Még egyszerűbb a következő természetes szám bitfordítottját az előző természetes szám bitfordítottjából számítani, a legnagyobb helyiértékű bithez 1-et hozzáadva, és az átvitelt az alacsonyabb helyiértékek (sic!) felé végezve.

Vegyük észre, hogy ugyanaz a T táblázat különböző m értékekre is megfelel, ha a maximális m értékre számoljuk ki, és csak egy kezdőselejtét használjuk.

Könnyű összeszámolni, hogy az algoritmus $5n \log n$ valós lebegőpontos műveletet használ, míg a polinomértékek Horner-elrendezéssel való kiszámítása $\approx 2n^2$ lebegőpontos műveletet használna.

*** 9.2.45. IFFT algoritmus.** Az előző pontban megadott algoritmus megfordítható, és megfordításával a DFT inverzére kapunk gyors algoritmust: ha a menetek fordított sorrendben hajtjuk végre, $l = 1, 2, \dots, 2^{m-1}$ -re, és a (4) pillangóműveletet invertáljuk, akkor a transzformáció inverzét kapjuk:

- (4') [Inverz pillangó.] Legyen $x \leftarrow A[j]$, $y \leftarrow A[j + l]$, majd $A[j] \leftarrow (x + y)/2$, $A[j + l] \leftarrow (x - y)/(2w)$, végül $j \leftarrow j + 1$.

A felhasznált T táblázat ugyanaz. (4')-ben a kettővel való osztásokat elhagyhatjuk, ha az egész algoritmus elején vagy végén az A tömb minden elemét osztjuk 2^m -mel. Vegyük észre azt is, hogy $1/w = \bar{w}$, így itt sincs szükség osztásra, szorzással is dolgozhatunk.

* **9.2.46. Gyors szorzás FFT-vel.** Legyen $f = \sum_{j=0}^{n-1} f_j x^j$, $g = \sum_{j=0}^{n-1} g_j x^j$, és h az f és g polinomok szorzata. Tegyük fel, hogy $\deg(h) = \deg(f) + \deg(g) < n$. Mivel $\hat{f}_k = f(\omega_n^{-k})$, $\hat{g}_k = g(\omega_n^{-k})$, azt kapjuk, hogy $h(\omega_n^{-k}) = \hat{f}_k \hat{g}_k$, vagyis ha h fokszáma kisebb, mint n , azaz $h = \sum_{j=0}^{n-1} h_j x^j$, akkor $\hat{h}_k = \hat{f}_k \hat{g}_k$ ($0 \leq k < n$). Innen h meghatározható IFFT-vel. Így gyors algoritmust kaptunk polinomszorzásra, amely $\approx 15n \log n$ valós lebegőpontos műveletet használ.

A q alapú számrendszerben felírt $f(q) = \sum_{j=0}^{n-1} f_j q^j$ és $g(q) = \sum_{j=0}^{n-1} g_j q^j$ számok szorzata $h(q) = \sum_{j=0}^{n-1} h_j q^j$, ha a megfelelő f és g polinomok szorzata az n -nél alacsonyabb fokú $h = \sum_{j=0}^{n-1} h_j x^j$ polinom. (A q nem lehet túl nagy, mert kerekítési hibák lépnek fel.) Így számok szorzására kapunk gyors algoritmust. Más gyors algoritmusok is vannak.

* **9.2.47. DCT és IDCT.** A mérnöki gyakorlatban jobban szeretnek valós számsorozathoz valós transzformált sorozatot rendelni. Tekintsünk egy valós változós valós értékű $2T$ szerint periodikus páros F függvényt (most célszerűbb lesz T helyett $2T$ -t használni). Legyen a mintavételi frekvencia az $1/(2T)$ „alapfrekvencia” $2n$ -szerese, ahol $n > 2$ egy természetes szám, azaz legyen $\tau = T/n$, és legyen $\tau_0 = \tau/2$. A mintavételezéssel kapott $f_j = F(\tau_0 + j\tau)$, $j \in \mathbb{Z}$ sorozatot az $f_0, f_1, \dots, f_{n-1}$ értékek egyértelműen jellemzik, mert a sorozat $2n$ szerint periodikus, azaz $f_{j+2n} = f_j$ ($j \in \mathbb{Z}$), és a párosság valamint $\tau_0 = \tau/2$ miatt $f_{-j-1} = f_j$, ha $0 \leq j < n$. A F függvényt szeretnénk „koszinuszos” jelek lineáris kombinációjaként előállítani. Tekintsük a $H_k(t) = \cos(\pi k t / T)$, $k \in \mathbb{Z}$ ugyancsak $2T$ szerint periodikus páros függvényeket. A H_k függvény mintavételezésével a

$$\cos \frac{\pi k(j+1/2)}{n}, \quad j \in \mathbb{Z}$$

sorozatot kapjuk. Legyen

$$c_k = \sum_{j=0}^{n-1} f_j \cos \frac{\pi k(j+1/2)}{n}, \quad \text{ha } k \in \mathbb{Z},$$

azaz c_k az $(f_0, f_1, \dots, f_{n-1})$ és a

$$\left(\cos \frac{\pi k}{2n}, \cos \frac{3\pi k}{2n}, \dots, \cos \frac{(2n-1)\pi k}{2n} \right)$$

$\mathbb{R}^n$ -beli vektorok belső szorzata. Az

$$(f_0, f_1, \dots, f_{n-1}) \mapsto (c_0, c_1, \dots, c_{n-1})$$

leképezés $\mathbb{R}^n$ -et önmagába képezi le. Ezt a leképezést nevezzük *diszkrét koszinusz transzformációnak*, *DCT*-nek. A DCT nyilván lineáris.

Vegyük észre, hogy

$$\sum_{j=0}^{2n-1} (\omega_{4n}^k)^{2j+1} = \omega_{4n}^k \frac{(\omega_{4n}^{2k})^{2n} - 1}{\omega_{4n}^{2k} - 1} = 0,$$

ha $-2n < k < 2n$, $k \neq 0$. Mivel a koszinusz páros és periodikus,

$$(1) \quad \sum_{j=0}^{n-1} \cos \frac{\pi k(j+1/2)}{n} = \frac{1}{2} \sum_{j=-n}^{n-1} \cos \frac{\pi k(j+1/2)}{n} = \frac{1}{2} \sum_{j=0}^{2n-1} \cos \frac{\pi k(j+1/2)}{n} \\ = \sum_{j=0}^{2n-1} \left(\omega_{4n}^{k(2j+1)} + \omega_{4n}^{-k(2j+1)} \right) = 0,$$

ha $-2n < k < 2n$ és $k \neq 0$. Ebből következik, hogy a H_k , $0 \leq k < n$ függvények mintavételezésével kapott $h_k \in \mathbb{R}^n$ vektorok belső szorzata

$$\langle h_{k_1}, h_{k_2} \rangle = \sum_{j=0}^{n-1} \cos \frac{\pi k_1(j+1/2)}{n} \cos \frac{\pi k_2(j+1/2)}{n} \\ = \frac{1}{2} \sum_{j=0}^{n-1} \left(\cos \frac{\pi(k_1+k_2)(j+1/2)}{n} + \cos \frac{\pi(k_1-k_2)(j+1/2)}{n} \right),$$

azaz (1) szerint ha $0 \leq k_1, k_2 < n$, $k_1 \neq k_2$, akkor 0, ha $0 = k_1 = k_2$, akkor n , ha pedig $0 \neq k_1 = k_2 < n$, akkor $n/2$. Innen a

$$t \mapsto \frac{c_0}{n} + \frac{2}{n} \sum_{k=0}^{n-1} c_k H_k(t)$$

függvény a mintavételezés $t = \tau/2 + j\tau$ pontjaiban megegyezik a kiindulási F függvénnyel. Speciálisan, a DCT invertálható: $t = \tau/2 + j\tau$ helyettesítéssel

$$f_j = \frac{c_0}{n} + \frac{2}{n} \sum_{k=0}^{n-1} c_k \cos \frac{\pi k(j+1/2)}{n}.$$

A DCT inverzét *inverz diszkrét koszinusztranszformációnak*, *IDCT*-nak nevezzük.

További hasznos észrevétel, hogy kapcsolat van a diszkrét koszinusz transzformáció és a diszkrét Fourier-transzformáció között, a DCT kifejezhető a DFT-vel: legyen $g_{2j+1} = f_j$ és $g_{2j} = 0$, ha $j \in \mathbb{Z}$. Ekkor a g sorozat valós, páros, és $4n$ szerint periodikus. A diszkrét Fourier-transzformáltja így valós és páros, tehát

$$\hat{g}_k = \frac{\hat{g}_k + \hat{g}_{-k}}{2} = \frac{1}{2} \sum_{j=0}^{4n-1} g_j (\omega_{4n}^{-jk} + \omega_{4n}^{jk}) \\ = \sum_{j=0}^{2n-1} f_j \frac{\omega_{4n}^{-(2j+1)k} + \omega_{4n}^{(2j+1)k}}{2} \\ = \sum_{j=0}^{2n-1} f_j \cos \frac{\pi k(j+1/2)}{n} = \sum_{j=-n}^{n-1} f_j \cos \frac{\pi k(j+1/2)}{n} \\ = 2 \sum_{j=0}^{n-1} f_j \cos \frac{\pi k(j+1/2)}{n} = 2c_k.$$

* **9.2.48. Kétdimenziós DFT és DCT.** A kétdimenziós DFT egy $(f_{j_1, j_2})_{j_1=0}^{n_1-1}{}_{j_2=0}^{n_2-1}$ mátrixhoz $(\hat{f}_{k_1, k_2})_{k_1=0}^{n_1-1}{}_{k_2=0}^{n_2-1}$ mátrixot rendel. Definíciója:

$$\hat{f}_{k_1, k_2} = \sum_{j_1=0}^{n_1-1} \sum_{j_2=0}^{n_2-1} \omega_{n_1}^{-j_1 k_1} \omega_{n_2}^{-j_2 k_2} f_{j_1, j_2}, \quad \text{ha } 0 \leq k_1 < n_1, \quad 0 \leq k_2 < n_2.$$

A definícióból

$$\hat{f}_{k_1, k_2} = \sum_{j_1=0}^{n_1-1} \omega_{n_1}^{-j_1 k_1} \left(\sum_{j_2=0}^{n_2-1} \omega_{n_2}^{-j_2 k_2} f_{j_1, j_2} \right) = \sum_{j_2=0}^{n_2-1} \omega_{n_2}^{-j_2 k_2} \left(\sum_{j_1=0}^{n_1-1} \omega_{n_1}^{-j_1 k_1} f_{j_1, j_2} \right),$$

azaz a kétdimenziós DFT kiszámolható úgy, hogy előbb a mátrix soraira, majd az oszlopaira (vagy fordítva) alkalmazunk egydimenziós DFT-t.

A kétdimenziós DCT definíciója

$$c_{k_1, k_2} = \sum_{j_1=0}^{n_1-1} \sum_{j_2=0}^{n_2-1} \cos \frac{\pi k_1 (j_1 + 1/2)}{n_1} \cos \frac{\pi k_2 (j_2 + 1/2)}{n_2} f_{j_1, j_2},$$

ha $0 \leq k_1 < n_1, \quad 0 \leq k_2 < n_2.$

Ez is kiszámolható úgy, hogy előbb a mátrix soraira, majd az oszlopaira (vagy fordítva) alkalmazunk egydimenziós DCT-t.

Természetesen mindkét transzformáció általánosítható magasabb dimenziós tömbökre is.

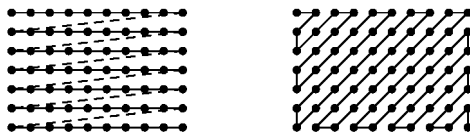
* **9.2.49. Hangtömörítés.** A digitalizált hangjel tömörítésére általában veszteséges eljárásokat használnak. Az alap gondolat: diszkrét Fourier-transzformáció felhasználása a hangjel transzformálására az „*időtartományból*” a „*frekvenci tartományba*”, azaz a jel felbontása eltolt szinuszos jelek összegére. Mivel egy zenei hang csak néhány szinuszos jel összege, a transzformáció után nagyon jól tömöríthető. Mivel a fülünk nem érzékeny a szinuszos jelek eltolására, ez az információ is eldobható. További tömörítést tesz lehetővé, hogy egy erősebb hang mellett megszólaló közeli frekvenciájú, de gyengébb hangot nem érzékelünk, így a közeli frekvenciájú hangokat elég durvábban kvantálni, mert a kvantálási zajt nem halljuk. Hasonlóan, a röviddel az erősebb hang előtt vagy után megszólaló hasonló frekvenciájú gyengébb hangot sem halljuk. Mindezek jelentős tömörítést tesznek lehetővé. Durván a tömörítést úgy képzelhetjük, hogy a hangot DFT-vel „folyamatosan” analizáljuk, a kapott frekvenciaspektrumból kihagyjuk, amit úgysem hallanánk, majd prefix kód és más kódolási eljárások segítségével a maradékot tömörítjük. Visszajátszásnál a dekódolt jelet folyamatosan visszatranszformáljuk: ez nagyjából annak felel meg, mintha egy nagyon jó szintetizátoron játszanánk vissza a jelet. A vázolt eljárás természetesen korántsem ilyen egyszerű a gyakorlatban. A szabványok általában csak a kódot adják meg pontosan. A kódoló és dekódoló szoftver, illetve hardver tervezése nagyon nehéz hangmérnöki feladat.

A jelenlegi egyik legkorszerűbb eljárás az AAC (Advanced Audio Coding). Ennek különböző változatai képezik többek közt a mozgókép-tömörítésre (lásd ott) kifejlesztett MPEG-2, illetve MPEG-4 kódolás hangrészét. Az eljárás az MPEG-1 Audio Layer III

eljárás (elterjedt nevén *MP3*) továbbfejlesztésének tekinthető. DFT helyett a DCT egy módosított változatát használja 2048 alappontos, vagy gyorsan változó hangokat tartalmazó jel (általában beszéd) esetén 256 alappontos „ablakkal”. A mintavételi frekvencia 8 kHz és 96 kHz között változhat, a jel 1-48 csatornás lehet (1 csatorna: mono, 2 csatorna: sztereo, 4 csatorna: kvadro, stb.), és beállítható a kódolt jelfolyam sebessége 2 kbit/s-tól (beszéd) 64 kbit/s-ig vagy feljebb csatornánként, ami már jó minőségű zeneátvitelt tesz lehetővé. Ha csak kis sebességet használunk, a elvesztesség természetesen megnő, a minőség romlik. A kódolás általában nagyon processzorigényes, a dekódolás egyszerűbb, mert a kódolás folyton változó paramétereket határoz meg, a dekódoló ezeket készen kapja.

Elsősorban beszéd valós idejű („majdnem szinkron”) átvitelére kifejlesztett eljárás az *iLBC* (Internet Low Bit Rate Codec). A mintavételi frekvencia 8 kHz, a kvantálás 16 bites. A sebesség rögzített, a kódolás és a dekódolás is gyors. Az alapelv itt más: az átvitt jelfolyam lényegében egy beszédsszintetizátor működtetéséhez szükséges jel. Az eljárás jól tűri a kieső adatacsomagokat. A pontos dokumentáció: RFC 3951. Az iLBC-t használja a Googletalk.

* **9.2.50. Képtömörítés.** Állóképek tömörítésénél is azt használjuk fel, hogy a közeli képelemek között erős a függőség. Ezt bármilyen szokásos tömörítő eljárással jobban kihasználhatjuk, ha az egyszerű sorfolytonos bejárás helyett a még mindig nagyon egyszerű cikcakk bejárást alkalmazzuk: lásd a 9.2.15 ábrát.

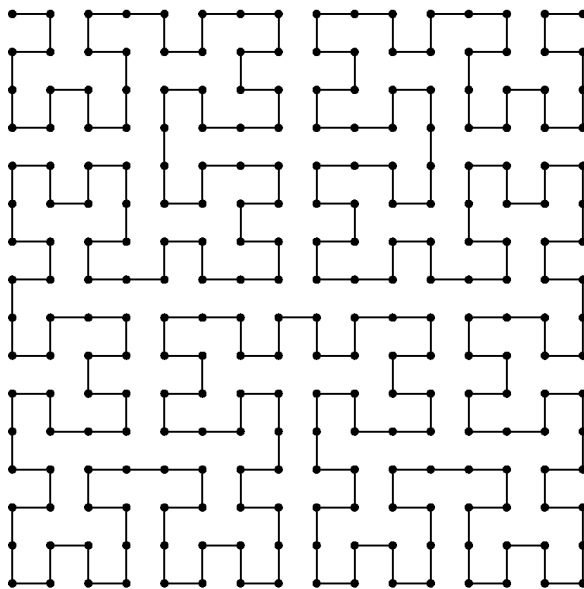


9.2.15 ábra: Sorfolytonos és cikcakk bejárás.

További javulás érhető el, ha sokkal speciálisabb bejárást választunk, például a *Hilbert-görbén* alapuló, a 9.2.16 ábrán látható bejárást, amely „sokáig totyog egy helyben”.

Igazán hatékony tömörítést azonban csak a speciálisan képtömörítésre kifejlesztett eljárások adnak. Három elterjedt képtömörítéssel fogunk megismerkedni.

* **9.2.51. PNG.** A *PNG* (ejtsd: ping; Portable Network Graphics) fájlformátumot digitalizált képek veszteségmentes átvitelére tervezték. Csak a tömörítéssel kapcsolatos részletekkel foglalkozunk (a specifikáció 1.0 verziója alapján), de annyit megjegyzünk, hogy a fájl olyan, elengedhetetlenül szükséges információkon kívül, mint például a sorok és oszlopok hossza és a kép típusa, nagyon sok további, az eredeti képpel kapcsolatos információt tartalmaz, például hogy mennyi a kontrasztvisszaadást jellemző „gamma” érték, a fehérpont és az alapszínek kromacitásai, fizikai képelem (pixel) dimenziók stb.; a részleteket lásd a specifikációban. Nem színes képek esetén az egyes képelemek kódja 1, 2, 4, 8 vagy 16 bit lehet. Színes képek *RGB*-formátumban adhatók meg (Red, Green, Blue, azaz a vörös, zöld, kék alapszínek intenzitását megadva), 8–8–8, illetve 16–16–16 biten. Mindkét esetben megadhatunk pixelenként egy opacitás értéket is, ugyanannyi biten. Ha ez maximális, a kép nem átlátszó, egyébként átlátszik a háttér, nullánál már csak a háttér látszik. Az egy képelemhez tartozó összes érték közvetlenül egymás után jön. A kép „palettával” is megadható: ez egy előre megadott színtáblázat, amely a palettaszínek



9.2.16 ábra: Hilbert-bejárás.

RGB-koordinátáit és opacitását tartalmazza, ekkor a képelemek helyén a táblaindexek vannak.

A sorfolytonosan olvasott kép minden sorát külön-külön egy „jóslás” segítségével jobban tömöríthetővé konvertáljuk. A *jósláshoz* a képelem feletti képelem megfelelő bájtját, valamint az előző megfelelő bájtot és az a feletti bájtot használhatjuk. Úgy kell tekinteni, hogy az első oszlop előtt és az első sor felett csupa nulla van. A fájlba mindig a valódi bájt és a jósolt bájt különbsége kerül. Ha a – soronként megadható – jóslási mód kódja 0, a jósolt érték nulla, nincs jóslás; ha 1, akkor a jóslás az előző megfelelő bájt értéke, jelölje ezt a ; ha 2, akkor a képelem feletti képelem megfelelő bájtja, b a jóslás; ha 3, akkor $\lfloor (a + b)/2 \rfloor$ a jóslás; végül, ha 4, akkor a *Paeth-jóslást* használjuk: legyen a képelem feletti képelem előtti megfelelő bájt c ; a jóslás a , b és c közül az, amelyik legközelebb van $a + b - c$ -hez, egyenlő távolság esetén a , b és c közül az ábécében előbb állót részesítve előnyben. A jóslás segítségével konvertált sorokat egymás után írjuk és a gzip-ben is használt „deflate” tömörítéssel tömörítjük.

Lehetőség van „*előhívódó*” tömörítésre is: a képet a bal felső sarokból kiindulva (maximum) 8×8 képelemes részekre osztjuk, majd a

1	6	4	6	2	6	4	6
7	7	7	7	7	7	7	7
5	6	5	6	5	6	5	6
7	7	7	7	7	7	7	7
3	6	4	6	3	6	4	6
7	7	7	7	7	7	7	7
5	6	5	6	5	6	5	6
7	7	7	7	7	7	7	7

táblázattal megadott sorrend szerint olvassuk: először az egész képből az 1-esek helyén álló képelemek, majd a 2-esek helyén álló képelemeket stb. Dekódolásnál, amikor az 1-es helyén álló képelem megérkezik, az egész (maximum) 8×8 -as blokkot ennek megfelelő színűre festjük. Amikor a 2-es helyén álló képelem megérkezik, a blokk jobb felét átfestjük a megfelelő színre, ezzel megduplázva a vízszintes felbontást. Amikor a 3-asok helyén álló képelemek is megérkeznek, újra átfestjük a blokk alsó felét, ezzel megduplázva a függőleges felbontást stb.

A PNG formátum a GIF (Graphics Interchange Format) fájlformátum továbbfejlesztésének tekinthető; ez utóbbi csak szürkeárnyalatos és „paletta”-színes képeket kezel, nem használ jóslást, és a compress parancshoz nagyon hasonló LZW-típusú tömörítést használ.

*** 9.2.52. JPEG.** A Joint Photographic Experts Group által kidolgozott szabványból csak a digitalizált képek veszteséges tömörítésére kidolgozott változat, annak is az alapverziója terjedt el. (A veszteségmentes változat a PNG-hez hasonló.) Csak az egyik (vesztéséges) alapváltozatot ismertetjük vázlatosan, a sokféle paraméterezési lehetőséget nem. Jó minőségű képeknél akár 10–20-szoros tömörítés is elérhető.

A tömörítés első lépése – csak színes képeknél – az RGB koordináták transzformációja egy másik koordináta-rendszerbe az

$$\begin{aligned} Y &= 77R/256 + 150G/256 + 29B/256, \\ C_b &= -44R/256 - 87G/256 + 131B/256 + 128, \\ C_r &= 131R/256 - 110G/256 - 21B/256 + 128 \end{aligned}$$

transzformációval. A transzformáció a megjelenítő eszközökhöz igazodó RGB-koordinátákat egy másik, látásunkhoz jobban igazodó koordináta-hármasba viszi át. Ez a koordináta-rendszer azért előnyösebb, mert az Y fizikai jelentése a képpont világossága, C_b , illetve C_r jelentése pedig, hogy a szín a fehértől mennyire tér el a kék, illetve vörös felé. A szemünk sokkal érzékenyebb a világosság változásaira, mint a színárnyalatok változásaira, így az Y „világosság” koordinátát nagyobb pontossággal fogjuk átvinni, mint a C_b és C_r „színesség” koordinátákat.

Második lépésként színes képnél – csak vízszintesen vagy erősebb tömörítés esetén függőlegesen is – felére csökkentjük a C_b és C_r képek felbontását, ezzel a színesség leírására szolgáló adatokat felezve vagy negyedelve. A továbbiakban a három képet egymás után, függetlenül kezeljük. (Persze, ha a kép nem színes, csak az Y kép van.) Mindegyiket 8×8 képelem méretű blokkokra bontjuk, szükség szerint kiegészítve az utolsó ismétlésével további oszlopokkal, illetve sorokkal.

Minden blokkra kétdimenziós diszkrét koszinusztranszformációt alkalmazunk. A kapott transzformáltakat lineárisan kvantáljuk, de a kvantálás a koszinusz-transzformált $c_{j,k}$ együtthatóira (nagyjából) $j + k$, azaz a frekvencia növekedésével egyre durvul. A kvantálás finomságát az Y képre, illetve a C_b és C_r képekre táblázat adja meg. Általánosságban azt mondhatjuk, hogy a kvantálás finomabb az Y , mint a C_b és C_r képre. A kvantálás után az együtthatók mátrixában általában csak néhány nem nulla elem marad.

Először a blokkokat sorfolytonosan olvasva a blokkonkénti $c_{0,0}$ együtthatókat visszük át. Ez az együttható az adott blokk átlagát reprezentálja. Mivel általában a szomszédos blokkok átlaga nem nagyon tér el, az első blokk együtthatója után a többi blokkra csak

az együttható előzőtől való eltérését visszküldi át. Ezután a többi együttható átvitele következik: az együtthatók mátrixát cikcakkban járjuk be (lásd a 9.2.15 ábrát), majd a következő blokkra térünk át, sorfolytonosan. Az átvitel előtt futamkódolást, majd prefix kódot alkalmazunk.

A dekódolás a kódolás fordítottja. Nyilván alkalmazható „előhívódó” dekódolás: már az Y kép $c_{0,0}$ együtthatói adnak egy durva és nem színes képet.

* **9.2.53. DjVu.** Az $AT\&T$ terméke a $DjVu$ (ejtsd: dézsá vü) képtömörítő módszer. Igen nagy, szkennelt képek esetében akár 1000-szeres tömörítést lehet vele elérni. Az alapgondolat, hogy a képet három képre bontjuk fel: „háttér”, „előtér” és „maszk”. A háttér és az előtér árnyalatos és általában színes képek, a maszk pedig egy bináris kép, bitjei azt mondják meg, hogy az adott pont a háttérhez vagy az előtérhez tartozik. Mindhárom kép külön-külön jól tömöríthető: a háttér és az előtér felbontását vízszintesen és függőlegesen is általában harmadára csökkenthetjük a minőség romlása nélkül, és mindkettő nagy homogén területeket tartalmaz, míg a maszk bináris, ezért tömöríthető jól. A háttér és az előtér tömörítésére más eljárást használunk, mint a maszk tömörítésére. Az algoritmus, amely a képet háttérre, előtérre és maszkra bontja, az alábbi:

Kezdetben tekintsük az egész képet egy blokknak, a háttér színe legyen kezdetben fehér, az előtéré fekete, majd minden képpontot soroljunk be annak megfelelően, hogy a színe a háttéréhez vagy az előtéréhez áll-e közelebb, a kettő közül az egyikhez: ez adja a maszkot. Az új háttérszín a háttérhez tartozó összes képpont színének átlaga, míg az előtér színe az előtérhez tartozó képpontok színének átlaga. Addig ismételjük az eljárást, amíg a háttér, illetve az előtér színe stabilizálódik (azaz már elegendően keveset változik). Ez az első lépés. Már ez a lépés felbontja a képet, ha csak két szín van, de általában nem ez a helyzet.

Osszuk fel a nagy blokkot kisebb blokkokra, majd minden blokkra ismételjük meg a fenti eljárást, de most a nagyobb blokk háttér- és előtérszínével indulva, és a kisebb blokk háttér-, illetve előtérszínét úgy számolva, hogy 0,2 súllyal a nagyobb blokk, 0,8 súllyal pedig az oda újonnan besorolt képelemek színét vesszük figyelembe. Ismételjük ezt a lépést is, amíg a háttér és az előtér színe stabilizálódik. Ez a második lépés.

Minden blokkot kisebb blokkokra osztva, ismételjük meg minden kisebb blokkra a második lépést. Ezt addig folytatjuk, amíg elég finom nem lesz a felosztás, azaz a képelemek színe már elég keveset tér el az előtér, illetve a háttér színétől.

Az, hogy a második lépésben mindig figyelembe vesszük a nagyobb blokk háttér-, illetve előtérszínét is, akkor válik fontossá, ha egy kisebb blokk csak előtér- vagy csak háttérpontokat tartalmaz. Ekkor a súlyozás nem engedi, hogy az előtér, illetve a háttér színe „elmásszon” a nagyobb blokk előtér, illetve háttér színétől.

A pontos algoritmus további „szűrőket” tartalmaz, amelyek a fenti alapalgoritmus hibáit küszöbölik ki. A dekódolás nyilvánvaló.

* **9.2.54. Mozgóképtömörítés: MPEG.** Mozgóképtömörítésre általánosan elterjedt az $MPEG$ (Moving Pictures Experts Group) eljárás 1-es változata, és terjed a 2-es és 4-es változat is. Csak az $MPEG$ -1-ben használt alapelveket ismertetjük vázlatosan.

Nyilván egy filmnél vagy videófelvételnél két egymás utáni kép („*frame*”) általában nagyon hasonlít egymásra, legtöbbször csak elmozdulnak egy kicsit a képrészletek. Az első képet mint állóképet visszküldi át. A további képek átviteléhez az előző képet használjuk „jósásra”: a képet kis részekre bontjuk, majd minden kis részhez megkeressük a leginkább

hasonló képrészletet az előző képen, átvisszük az elmozdulásvektort és a képrészletek különbségét.

Ha minden további képre ezt az eljárást használnánk, a felhalmozódó hibák miatt a képek hamar használhatatlanná válnának. Ezért néhány megjósolt (predicted, P) kép után újra egy teljes bemenő (intra, I) képet kell átvinnünk. További tömörítés érhető el, ha észrevesszük, hogy bizonyos képrészletek csak egy későbbi képből jósolhatók, például egy mozgó tárgy mögött felbukkanó háttér. Az I, illetve P képek közé tehát kétirányú (bidirectional, B) képeket célszerű beiktatni, amelyek részleteit egy-egy előttük vagy mögöttük lévő I, illetve P kép segítségével jósoljuk. Természetesen ezeket csak akkor lehet kódolni, illetve dekódolni, ha már rendelkezésre áll nemcsak az előttük, hanem a mögöttük lévő P vagy I kép is. Tehát a képek sorozata például a következő lehet: IBBBPBBBPBBBPBBBIBBBPB. ...

Konkrétabban, az MPEG-1 szabvány szerint a hang és kép továbbítása lényegében függetlenül, bár szinkronizálva történik. A hangátvitellel már foglalkoztunk. A képátvitel legkisebb egysége a makroblokk. Ez 16×16 képelem világosság adatait tartalmazza négy 8×8 -as blokkra bontva, valamint mindkét irányban fele akkora felbontással, mint a világosságot a kétféle színességi adatot, két 8×8 -as blokként. Az I képek átvitele a JPEG-nél megismerthez nagyon hasonlóan történik, ezt nem részletezzük.

A P képek átvitelénél néhány makroblokk lehet I típusú, ezeket úgy kódoljuk, mint az I képeknél. A makroblokkok nagy része azonban P típusú: tartozik hozzá egy elmozdulásvektor, és csak az előző I vagy P kép így megadott részétől való eltérést kódoljuk. A kódolás egyébként hasonló, mint az I típusú makroblokknál, de a kvantálási tábla más. Mivel az elmozdulásvektorok nagyon hasonlóak, csak a különbségüket tároljuk, azaz a jóslás mindig az előző makroblokk elmozdulásvektora. A kép sorfolytonosan olvasott makroblokkjainak folyamat szeletnek nevezett részekre bontjuk. A szelet elején és még néhány más esetben, például I típusú makroblokk esetén, a jósolt elmozdulásvektor nullázódik. Mivel a makroblokkok nagy része nulla lesz, ezért minden makroblokk tartalmaz egy „ugrás” kódot, amely megadja, hogy utána hány nulla makroblokk következik. Még a nem nulla makroblokkoknál is az egyes blokkok gyakran nullák, ezért a makroblokk tartalmaz egy hat bites maszkot, amely megmondja, melyek az érdemi blokkok a négy világosság és a két színesség blokkból, a többi nulla.

A B képek átvitele nagyon hasonló a P képek átviteléhez, de itt minden blokkhoz a P képnél szereplő „előre” elmozdulásvektoron kívül egy „hátra” típusú elmozdulásvektor is tartozhat. Ha csak „előre” vektor szerepel, a blokkhoz a jóslást az előző I vagy P kép adja, ha csak „hátra” vektor szerepel, akkor a következő I vagy P kép, ha mindkettő, akkor az előző és a következő I, illetve P képből adódó jóslás számtani közepének alsó egész része.

Az összes fent említett paraméter (elmozdulásvektor, hat bites maszk, ugráskód stb.) egyenként vagy csoportosan külön az adott célra optimalizált prefix kóddal van kódolva. A dekódolás elég gyors, a kódolás viszont meglehetősen időigényes: az ideális elmozdulásvektorok megkeresése minden makroblokkra nem egyszerű. Léteznek más eljárások gyorsabb kódolással, de rosszabb minőséggel, például videótelefonhoz.

9.2.55. További feladatok megoldásokkal. [28], [29]: 4.4–4.8, 4.10, 4.12–4.13, 4.34–4.42, 4.44–4.59.

9.2.56. További feladatok. [25]: V.3.1–V.3.5, V.3.7–V.3.11, V.3.13–V.3.31.

9.3 Hibakorlátozó kódolás

A *hibakorlátozó kódokat* két csoportba sorolhatjuk: hibajelző kódok és hibajavító kódok. Mindkét típussal foglalkozunk. Mindkét esetben az üzenethalmaz elemeihez kódszavakat rendelünk, és a kódszavak segítségével próbáljuk a hibákat jelezni, illetve javítani. Ha az üzenet könnyen megismételhető, akkor a hangsúly általában a hibajelzésen van, ha azonban az ismétlés nehéz vagy lehetetlen, akkor a hibajavításra tolódik át. A hibakorlátozó kódokkal kapcsolatban mindig feltesszük, hogy az egyes kódszavak hossza azonos, a kódszó betűi egy adott véges ábécé, a *kódábécé* elemei, és az átvitel során nincs *szinkronhiba*, vagyis a vétel helyére a kódábécének ugyanannyi betűje érkezik meg, mint amennyit elküldtünk.

9.3.1. Hibajelző kódok feladata. A hibajelző kódok feladata, hogy a vétel helyén észrevegyük, ha az átvitel során az adat megváltozott. Minden hibát természetesen nem lehet felderíteni, hiszen abban az esetben, ha egy elküldött kódszó úgy változik, hogy a vétel helyére egy másik kódszó érkezik, akkor a vevőnek semmi oka nincs kételkedni abban, hogy az elküldött kódszó az volt, mint ami megérkezett. Minden olyan esetben azonban, amikor az érkező jelsorozat különbözik valamennyi lehetséges kódszótól, a vevő biztos lehet benne, hogy az átvitel során sérült a jelsorozat.

9.3.2. Példa. Legyen $d_1, d_2, \dots, d_n$ decimális számjegyek egy sorozata, $n \leq 10$. Egészítsük ki a sorozatot egy $n + 1$ -edik „számjeggyel”, amelynek értéke

$$d_{n+1} = \sum_{j=1}^n j d_j \bmod 11;$$

ha $b_{n+1} = 10$, akkor az X „római számjegy”. Ha valamelyik számjegyet elírjuk, akkor az összefüggés nyilván nem teljesülhet: ha d_j helyett d'_j -t írunk, akkor az összeg $j(d'_j - d_j)$ -vel nőtt, ami nem lehet 11-gyel osztható. Ugyanez a helyzet, ha $1 \leq j < n$ -re d_j -t és d_{j+1} -et felcseréljük: az összeg $j d_{j+1} + (j+1) d_j - j d_j - (j+1) d_{j+1} = d_j - d_{j+1}$ -gyel változik, ami csak akkor lehet osztható 11-gyel, ha $d_j = d_{j+1}$. Ez az ellenőrző „számjegy” tehát véd az egyszeres tévesztések és a felcserélések ellen. Ezt használják könyvek ISBN-számának és a magyar személyi számoknak gépelési hibák elleni védelmére.

9.3.3. Példa: paritásbites kód. A legegyszerűbb hibajelző kód a *paritásbites kód*. Legyen például az üzenethalmaz az n -bites bináris jelsorozatok halmaza, és egészítsük ki ezeket a jelsorozatokat egy $n + 1$ -edik bittel, az úgynevezett *paritásbittel*: amennyiben egy üzenetben az 1-esek száma páratlan, akkor írjunk a bitsorozat végére egy 0-t, míg az ellenkező esetben egy 1-et (vagy fordítva, de egy adott kódban mindig ugyanazon szabály szerint). Az így kiegészített, $n + 1$ -bites szavak mindegyikében páratlan sok 1-es van. Ha most egy ilyen kódszót elküldünk, és a vevőhöz olyan szó érkezik, amelyben az egyesek száma páros, akkor biztos, hogy hiba történt az átvitel során. Ha viszont az egyesek száma páratlan, akkor úgy kell tekintenünk (de nem állíthatjuk), hogy nem történt hiba. Könnyen beláthatjuk, hogy az előbbi eset akkor következik be, ha az átvitel során páratlan sok helyen sérül a kódszó, míg az utóbbi akkor, ha páros sok helyen történik változás. Ez azt jelenti, hogy minden olyan esetben észrevevessük a hibát, ha egy hiba történik, de van olyan eset, amikor két hiba történik, és ezt nem vesszük észre (sőt a konkrét esetben páros sok hiba esetén mindig ez a helyzet). Ez indokolja az alábbi definíciót.

9.3.4. Hibajelző kód. Egy kód t -hibajelző, ha minden olyan esetben jelez, amikor egy elküldött kódszó legfeljebb t helyen változik meg. A kód pontosan t -hibajelző, ha t -hibajelző, de nem $t + 1$ -hibajelző, azaz van olyan $t + 1$ hiba, amelyet a kód nem jelez. Könnyű olyan feltételt adni, amely jellemzi a t -hibajelző, illetve a pontosan t -hibajelző kódokat:

9.3.5. Kódok távolsága és súlya. A kódábécé két egyforma hosszú szavának, u -nak és v -nek a Hamming-távolsága, $d(u, v)$, az azonos pozícióban lévő különböző jegyek száma, és a kód távolsága, $d(C)$, a különböző kódszópárok távolságainak minimuma, ahol C a kódszavak halmaza, röviden a kód. A kód sebességén $\log_q(\#(C))/n$ -et értjük, ahol q a kódábécé elemeinek száma. Nyilván a kódsebesség soha nem nagyobb 1-nél.

A Hamming-távolság rendelkezik a távolság szokásos tulajdonságaival, vagyis bármely u, v, z -re

- (1) $d(u, v) \geq 0$;
- (2) $d(u, v) = 0$ akkor és csak akkor, ha $u = v$;
- (3) $d(u, v) = d(v, u)$ (szimmetria);
- (4) $d(u, z) \leq d(u, v) + d(v, z)$ (háromszög-egyenlőtlenség).

Nyilvánvaló, hogy ha egy kód minden kódszavának betűit ugyanazzal a permutációval permutáljuk, a kódszavak távolsága nem változik. Ugyancsak nem változik a kódszavak távolsága, ha tekintjük a kódábécé betűinek egy permutációját, és minden kódszóban egy adott helyen az ott lévő betű helyére a permutáció általi képét írjuk; azon kódokat, amelyeket egy adott kódból ezen távolságtartó leképezések véges sokszori alkalmazásával kapunk, az adott kóddal *ekvivalens* kódoknak nevezzük.

Ha a kódábécé egy A additív Abel-csoport, akkor a kódábécé egy u szavának a $w(u)$ Hamming-súlya a nullától különböző jegyeinek száma, míg a kód $w(C)$ súlya a nem nulla kódszavak súlyainak minimuma (ha van nem nulla kódszó, azaz a csoport nem egyelemű). Könnyű belátni, hogy $d(u, v) = w(u - v)$, és $w(u) = d(u, 0)$, ahol 0 az azonosan nulla kódszó; speciálisan $w(u + v) = w(u) + w(v)$. Ha még az is igaz, hogy a kódszavak maguk is Abel-csoportot alkotnak a koordinátánkénti művelettel, azaz a kódszavak C halmaza az A^n egy részcsoportha, akkor csoportkódról beszélünk. Ekkor $d(C) = w(C)$. Például páros paritásra való kiegészítéskor a paritáskód csoportkód, míg páratlan paritásra való kiegészítéskor nem.

A továbbiakban egy kód távolságát d és a súlyát w jelöli. (A megadott jelölések kissé pontatlanok, hiszen ugyanaz a betű jelöli a függvényt, mint két kódszó, valamint a kód távolságát, és hasonló igaz a súlyra is, de a környezet alapján mindig világos lesz, hogy éppen minek a jelöléséről van szó.) Mivel két kódszó legalább d helyen különbözik, így, ha egy elküldött kódszó az átvitel során legalább egy, de d -nél kevesebb helyen sérül, akkor az így kapott szó biztosan nem kódszó. Ugyanakkor van a kódban két olyan kódszó, amelyek pontosan d helyen különböznek, és ha az egyiket küldik, és ez úgy változik, hogy éppen a másik érkezik meg, akkor d hiba történt, de ezt a vétel helyén nem vesszük észre, nem tudunk jelezni. Ebből következik, hogy a bevezetett távolságfogalommal egy kód akkor és csak akkor t -hibajelző, ha $t < d$, és akkor és csak akkor pontosan t -hibajelző, ha $t = d - 1$, tehát nagyobb távolság nagyobb hibajelző képességet jelent.

A paritásbites kód esetén a kód távolsága 2. Az eredeti üzenethalmaz elemei közötti távolság ugyanis legalább 1, és vannak olyan n -bit-es sorozatok, amelyek éppen egy helyen különböznek. Ekkor az egyik üzenetben az 1-esek száma páros, a másikon páratlan,

vagyis a kiegészítő bit különbözni fog a két kódszóban, és a két kódszó éppen 2 helyen különbözik egymástól, ezen kódszavak távolsága 2. Ugyanakkor azok a kiegészített bit-sorozatok, amelyek eredetileg legalább két helyen tértek el egymástól, a kiegészítés után is legalább két helyen fognak különbözni, vagyis ezek távolsága ismét minimum 2, és így a kód távolsága valóban pontosan 2. Ez azt jelenti, hogy ez a kód pontosan 1-hibajelző, ahogy azt fentebb már megállapítottuk.

A paritásbitessel a hibát csak érzékelni, jelezni tudjuk, de a hibás jelsorozatot nem tudjuk kijavítani. A hiba javításához tudni kellene, hogy a beérkezett jelsorozat melyik pozíción sérült (és ha a kód nem lenne bináris, akkor azt is, hogy a sérült helyen mi volt eredetileg). Abból, hogy az egyesek száma nem megfelelő párosságú, tehát tudjuk, hogy történt hiba, de nem tudjuk megállapítani, hogy melyik bit hibásodott meg, ugyanis bármelyik (egyetlen vagy páratlan számú) bit meghibásodása ugyanezt eredményezi.

9.3.6. Minimális távolságú dekódolás. Említettük, hogy csupán a vett adatból nem mindig tudjuk megállapítani, történt-e hiba, hiszen bármely elküldött kódszó megváltozhat úgy az átvitel során, hogy bármely másik szó, például akármelyik kódszó érkezzen meg a vétel helyére. A hibajavításhoz meg kell adni egy úgynevezett *döntési függvényt*, amely bármely lehetséges jelsorozathoz hozzárendel egy és csak egy kódszót. (Az is lehetséges, hogy nem minden szó esetén akarunk dönteni.) Ezt a döntési függvényt kell úgy meghatározni, hogy a *döntési hiba*, tehát az a hiba, hogy egy beérkezett jelsorozathoz nem a ténylegesen elküldött kódot rendeljük, a lehető legkisebb legyen. Az előbbi feltételnek megfelelő legjobb függvény nem csupán az átviteli csatornától függ, hanem az üzenetek eloszlásától is, ezért helyette általában egy másik döntési függvényt alkalmazunk. Elég természetesnek tűnik azt feltenni (bár ez nem mindig teljesül), hogy egy vett szóban előforduló kevesebb hiba valószínűbb, mint a több hiba, vagyis nagyobb valószínűséggel volt az üzenet egy olyan kódszó, amely a vett szótól kevesebb helyen tér el, mint amely több helyen különbözik tőle. Másként szólva, egy vett szó esetén azt a kódszót választjuk, amely tőle a lehető legkevesebb helyen tér el, azaz a távolsága a vett szótól minimális. Az ilyen döntési függvény által meghatározott dekódolást *minimális távolságú dekódolás*nak mondjuk. Ilyenkor előfordulhat, hogy egy adott szóhoz egynél több minimális távolságra lévő kódszó van. Ekkor vagy kiválasztunk ezek közül egyet, és az lesz a döntés eredménye (de egy adott döntési függvény esetén az ilyen vett szó esetén mindig ugyanazon kiválasztott, minimális távolságra lévő kódszó mellett döntünk!), vagy az ilyen szó esetén nem döntünk, csupán jelezzük a hibát.

Legyen például $\{0010, 0100, 1111\}$ egy bináris kód. Ekkor az egyes négy bites szavaktól minimális távolságra lévő kódszavakat a 9.3.1 táblázat mutatja. Látható, hogy négy esetben nem egyértelmű a helyzet. Egy lehetőség, hogy ezekben az esetekben is dekódolunk, és például az elől álló kódszavakra döntünk. A másik lehetőség, hogy amennyiben a vett szó az előbbi négy szó valamelyike, akkor nem döntünk, csak jelezzük a hibát. Ha például a három kódszó három színt, mondjuk a fehérét, feketét és pirosat kódolja a példában megadott sorrendben, és mondjuk a kódolt üzenet a fekete volt, míg a vétel helyén a 0000 szót kell dekódolni, akkor a táblázat alkalmazásával a fehérre dekódolunk, ami adott esetben igen rossz döntés lehet. Ebben az esetben célszerűbb nem dönteni, hanem jelezni a hibát, és ha lehet, akkor megismételtetni ezt az üzenetet, vagy valamilyen más módon, például a környező pontok színe alapján dönteni. Azt azért megismétljük, hogy a döntési függvényt a rendszer tervezésekor rögzítettük, és a továbbiakban mindig

0000 $\mapsto$ 0010 0100
 0001 $\mapsto$ 0010 0100
 0010 $\mapsto$ 0010
 0011 $\mapsto$ 0010
 0100 $\mapsto$ 0100
 0101 $\mapsto$ 0100
 0110 $\mapsto$ 0100 0010
 0111 $\mapsto$ 1111
 1000 $\mapsto$ 0100 0010
 1001 $\mapsto$ 1111
 1010 $\mapsto$ 0010
 1011 $\mapsto$ 1111
 1100 $\mapsto$ 0100
 1101 $\mapsto$ 1111
 1110 $\mapsto$ 1111
 1111 $\mapsto$ 1111

9.3.1 táblázat: Egy döntési függvény.

ugyanúgy kell eljárunk az adott rendszer keretein belül. A döntési függvény táblázattal való megadása egyszerű, de rendkívül helyigényes, ezért jobb módszereket fogunk keresni.

Megfigyelhetjük, hogy a dekódolás két részre bontható: a hibajavításnál megpróbáljuk meghatározni, hogy mi volt az elküldött kódszó (ez a nehezebb), majd visszaállítjuk az üzenetet. Mivel az utóbbi egyértelmű, ezért hibajavító kódok dekódolásán legtöbbször csak a hibajavítást értjük.

9.3.7. Hibajavító kód. Egy kód t -hibajavító, ha minden olyan esetben helyesen javít, amikor egy elküldött kódszó legfeljebb t helyen változik meg. A kód *pontosan* t -hibajavító, ha t -hibajavító, de nem $t+1$ -hibajavító, azaz van olyan $t+1$ hibával érkező üzenet, amelyet a kód helytelenül javít, vagy nem javít.

Egy d távolságú kód esetén minimális távolságú dekódolással $t < d/2$ hiba esetén biztosan jól döntünk, hiszen a háromszög-egyenlőtlenség következtében az eredetileg elküldött kódszótól különböző bármely más kódszó biztosan $d/2$ -nél több helyen tér el a vett szótól. Viszont $t \geq d/2$ esetén nincs olyan döntési függvény, amely t -hibajavító, mert a kódban van két olyan kódszó, mondjuk u és w , amelyek pontosan d helyen különböznek. Írjunk u -ban ebből a d számú pozícióból t (de legalább d) helyre a w megfelelő pozícióján található betűt, és jelöljük az így kapott szót v -vel. A v az u -tól t helyen különbözik, míg w -tól $\max\{0, d - t\} \leq d/2 \leq t$ helyen. Ha a dekódolás t -hibajavító lenne, akkor v -t egyrészt u -ra, de másrészt w -re kellene javítania. Tehát egy d -távolságú kód minimális távolságú dekódolással minden $t < d/2$ -re t -hibajavító, és pontosan $\lfloor (d-1)/2 \rfloor$ -hibajavító.

Általánosabban, legyenek $s \geq t$ természetes számok. Egy kód t -hibajavító és s -hibajelző, ha minden legfeljebb t -hibát kijavít és minden legfeljebb s -hibát jelez (ideértve a kijavított legfeljebb t -hibákat is). Megmutatjuk, hogy ha $t + s < d$, akkor minimális távolságú dekódolással minden t -hiba kijavítható és minden s -hiba jelezhető. (Szabadon dönthetünk tehát: ha kevesebb hibát akarunk kijavítani, akkor több hibát jelezhetünk.) Valóban, ha legfeljebb t -hibát javítunk a minimális távolságú dekódolással, akkor $0 < r \leq s$ hiba esetén, ha u volt az eredeti kódszó és v a vett

üzenet, akkor bármely u -tól különböző w kódszóra $d(v, w) \leq t$ lehetetlen, mert ebből $d(u, w) \leq d(u, v) + d(v, w) \leq r + t \leq s + t < d$ következne, így r hibát biztosan jelezni tudunk akkor is, ha minimális távolságú dekódolással minden t -hibát kijavítunk. Másrészt, ha egy kód t -hibajavító és s -hibajelző, akkor $t + s < d$: valóban, ha u és w két kódszó, amelyek távolsága d , és $t + s \geq d$, akkor az u kódszót t (de legfeljebb d) helyen megváltoztatva úgy, hogy ott különbözzön u -tól és megegyezzen w -vel, ha az így kapott v szót vesszük, azt u -ra kell javítanunk, pedig lehet, hogy w -ból keletkezett legfeljebb s hibával.

*** 9.3.8. Hibajavítás ismert hibahelyekkel.** Legyen egy kód távolsága d , és tegyük fel, hogy az átvitel során $t + r$ hiba lépett fel, amelyekből r hibának ismerjük a helyét (például, mert a kódbetűket egyenkénti paritásellenőrzéssel vesszük át). Ha a kódábécé kételemű, akkor az ismert helyű hibákat nyilván ki tudjuk javítani. Egyébként, ha $2t + r < d$, akkor a hibákat ki tudjuk javítani: Legyen u az eredeti kódszó, v a vett szó, w egy tetszőleges kódszó. Jelölje $\tilde{u}$, $\tilde{v}$ és $\tilde{w}$ azokat a szavakat, amelyeket úgy kapunk, hogy az adott r helyen álló betűket elhagytuk. Válasszuk ki ezen „rövidített” $\tilde{u}$, $\tilde{w}$ kódszavak közül azt, amelyik legfeljebb t helyen tér el $\tilde{v}$ -től; ilyen egyetlenegy van, $\tilde{u}$, mert $u \neq w$ esetén $d \leq d(u, w) \leq d(\tilde{u}, \tilde{w}) + r \leq d(\tilde{u}, \tilde{v}) + d(\tilde{v}, \tilde{w}) + r \leq t + r + d(\tilde{v}, \tilde{w})$, ahonnan $d(\tilde{v}, \tilde{w}) > t$. Az $\tilde{u}$ ismeretében u egyértelműen adódik, mert $u \neq w$ esetén $\tilde{u} \neq \tilde{w}$, hiszen $r < d$. Másrészt, ha egy kód bármely ismert r helyen és ismeretlen t helyen fellépő hibáját ki tudjuk javítani, akkor $2t + r < d$. Valóban, ha u és w két kódszó, amelyek távolsága d , és $2t + r \geq d$, akkor az u kódszót t (de legfeljebb d) helyen megváltoztatva úgy, hogy ott megegyezzen w -vel és r (de legfeljebb $d - t$) helyen megváltoztatva úgy, hogy ott egyikkel se egyezzen meg, ha az így kapott v szót vesszük, és ismerjük az r helyet, azt u -ra kell javítanunk, de lehet, hogy w -ból keletkezett legfeljebb t ismeretlen helyű és legfeljebb r ismert helyű hibával.

9.3.9. Ismétléses kód. Legyen egy binárisan kódolt üzenethalmazunk, és küldjük el az üzenetet úgy, hogy minden egyes bitet megháromszorozunk, azaz ugyanazt a bitet háromszor egymás után küldjük. A vétel helyén a három összetartozó bit közül legalább kettő azonos lesz, így a minimális távolságú dekódolás esetén a vett három bithez a többségi döntés alapján rendelünk egy bitet. A döntési hiba még jelentősen csökkenthető, ha az eredeti egy bit helyett nem három, hanem $5, 7, 9, \dots, 2n + 1$ stb., az eredeti bittel azonos jegyet küldünk. Meghatározott feltételek esetén igazolható, hogy n növekedésével a döntési hiba valószínűsége a 0-hoz tart. Ebből azonban hiba lenne arra következtetni, hogy megtaláltuk a szinte biztosan hibátlan adatátvitel módját. Egyrészt, mint említettük, az előbbi eredmény csak bizonyos feltételek esetén teljesül. Másrészt nézzük meg, hogy mi ennek az ára. Az egyes bitek átviteléhez adott, 0-nál hosszabb időre van szükség, így n növekedésével az üzenet egy-egy bitjének átviteléhez szükséges idő is nő, és tart a végtelenhez, vagyis az 1 valószínűséggel hibátlan átvitel esetén egyetlen bitnyi üzenetet sem tudunk továbbítani. Az átviteli idő növekedése egyben az átvitel költségét is növeli, az is tart a végtelenhez. Szerencsére a helyzet nem ennyire rossz. Shannon egy tétele szerint bizonyos feltételek teljesülése esetén lehet az üzeneteket úgy kódolni, hogy az átvitel sebessége egy – csak a csatornától függő – értéket, a *csatorna kapacitást* tetszőlegesen megközelítsen, miközben a dekódolás hibája tetszőlegesen kis érték alá szorítható. A tétel elméleti jelentőségű, ugyanis ilyen kódot nem sikerült konstruálni, és még ha sikerülne is, akkor is használhatatlan lenne a gyakorlatban, olyan nagy lenne a kódszavak hossza, és

olyan nagy lenne a kódszavak száma. A tétel fontossága mégis felbecsülhetetlen, ugyanis azt igazolja, hogy lehetséges olyan kódot konstruálni, amelynél mind a sebesség, mind a döntési hiba kielégít egy reális elvárást. (Az újabb, úgynevezett kód *turbó kódok*nál egyes speciális esetekben az átvitel sebessége megközelíti a csatornapacitást, de a dekódolás nehéz; egyelőre ezeket főleg az úrtávközlésben használják.)

9.3.10. Kétdimenziós paritásellenőrzés. A korábban tárgyalt paritáselemes kód segítségével könnyen tudunk egy minimális távolságú dekódolással 1-hibajavító kódot konstruálni. Legyenek az üzenetek n -bit-es szavak, és tegyük fel, hogy m üzenetünk van. Egészítsünk ki minden kódszót egy paritásbittel például páratlan paritásúvá, majd m ilyen kódszóból alkossunk egy blokkot. Írjuk egymás alá a blokk $n + 1$ -bit-es kódszavait, és most az egy-egy oszlopban álló m -bit-es sorozatokat egészítsük ki egy-egy paritásbittel, például páros paritásúvá. Az így kapott $n + 1$ -bit-es szóval kiegészítve a blokkot kapjuk az eredeti m üzenet kódját, amelyet a 9.3.2 táblázat mutat. A gyakorlatban ezt a kódolási sémát például mágnesszalagokon alkalmazzák, és ott az egyes szavak nyolc bitből álló bájtok, vagyis $n = 8$. Ilyenkor szokás az egyes bájtok ellenőrzésére szolgáló paritásbiteket *VRC*-nek nevezni, ami a *Vertical Redundancy Check* (keresztirányú ellenőrzés) kezdőbetűiből álló rövidítés, míg az ellenőrző bájt az *LRC*, azaz *Longitudinal Redundancy Check* (hosszirányú ellenőrzés).

$b_{0,0}$	$\dots$	$b_{0,j}$	$\dots$	$b_{0,n-1}$	$b_{0,n}$
$\vdots$		$\vdots$		$\vdots$	$\vdots$
$b_{i,0}$	$\dots$	$b_{i,j}$	$\dots$	$b_{i,n-1}$	$b_{i,n}$
$\vdots$		$\vdots$		$\vdots$	$\vdots$
$b_{m-1,0}$	$\dots$	$b_{m-1,j}$	$\dots$	$b_{m-1,n-1}$	$b_{m-1,n}$
$b_{m,0}$	$\dots$	$b_{m,j}$	$\dots$	$b_{m,n-1}$	$b_{m,n}$

9.3.2 táblázat: Kétdimenziós paritásellenőrzés.

Ez a rendszer bárhol fellépő egyetlen hiba esetén képes azt javítani. Ha ugyanis $b_{i,j}$, és csak ez a bit hibás, akkor pontosan egy hiba van az i -edik szóban, tehát ennek ellenőrzése során hibajelzést kapunk. Az összes többi szó ellenőrzése azt adja, hogy azokban nincs hiba, és hasonlóan, a j -edik és csak a j -edik oszlop ellenőrzésénél hibajelzésre kerül sor, vagyis a két eredményből azt kapjuk, hogy az i -edik szó j -edik bitje és csak ez a bit hibás, amit ennek a bitnek a komplementálásával kijavíthatunk. Eszerint azonban minden olyan esetben, amikor az i -edik és csak az i -edik szóban, valamint a j -edik és csak a j -edik oszlopban kapunk hibajelzést, azt gondoljuk, hogy ez a bit hibásodott meg, és ezt „javítjuk”, vagyis az ellenkezőjére változtatjuk. Pedig könnyen beláthatjuk, hogy ellenőrzéskor ugyanerre az eredményre jutunk akkor is, ha minden oszlopban és minden szóban, kivéve a j -edik oszlopot és i -edik szót, páros számú hiba lép fel (ebbe beleértve a hibátlan esetet is 0 hibával), míg a kitüntetett i -edik szóban és j -edik oszlopban is a hibák száma páratlan. Ilyen például, ha az i -edik szóban a $j + 1$ -edik bit, valamint az $i + 1$ -edik szó j -edik és $j + 1$ -edik bitje, tehát összesen három bit hibásodik meg. A vétel helyén semmilyen módszerrel nem tudjuk eldönteni, hogy valóban egy hiba történt-e,

és így helyesen javítunk, vagy a megfigyelt hibajelzés több hiba együttes hatása, aminek következtében vagy egy addig helyes bitet „javítunk” helytelenre, vagy egy tényleg hibás bitet javítunk, de még további, felderítetlen hiba is van a vett üzenetben. Hasonlóan előfordulhat, hogy volt hiba, de észre sem vesszük, nevezetesen, ha minden szóban és minden oszlopban a hibák száma páros. Ennek tipikus példája, amikor négy hiba egy téglalap négy sarkában lép fel, ahol a téglalap két éle egy-egy szóban van. Végül előfordulhat, hogy egynél több szóban, illetve egynél több oszlopban kapunk hibajelzést, amikor biztosan tudjuk, hogy volt hiba, de a hibák száma egynél nagyobb, így javításra ebben a rendszerben nincs lehetőségünk. Ennek legegyszerűbb példája, amikor pontosan két hiba lép fel. A most ismertetett rendszert nevezhetjük *kétdimenziós paritásellenőrzésnek*. Mint említettük, ilyen használnak nagy mágnesszalagos tárolóknál (egy bizonyos rögzítési mód esetén, mert többféle is létezik), ahol egymás mellé írják ki egy kiegészített bájt 9 bitjét, és az adatokat mindig blokkosan tárolják. Ebben az esetben keresztirányban páratlanra, míg hosszirányban párosra egészítenek ki.

9.3.11. Hamming-korlát. Ha egy q elemű ábécé bizonyos n hosszú szavaiból álló C kód t -hibajavító, akkor bármely két kódszóra a tőlük legfeljebb t távolságra lévő szavak halmazai diszjunktak. Mivel egy kódszótól j távolságra pontosan $\binom{n}{j}(q-1)^j$ szó van, azt kapjuk, hogy

$$\sharp(C) \sum_{j=0}^t \binom{n}{j} (q-1)^j \leq q^n.$$

Ez a *Hamming-korlát* a kódszavak számára adott t -nél. Ha egyenlőség teljesül, akkor a kódot *tökéletesnek* nevezzük. (Nyilván t egyértelműen meghatározott.) Mivel kevés tökéletes kód van, a gyakorlatban az alábbi korlát fontosabb.

9.3.12. Singleton-korlát. Ha egy q elemű ábécé n hosszú szavaiból álló C kód távolsága d , akkor minden kódszóból elhagyva $d-1$ betűt (ugyanarról a $d-1$ helyről), még mindig különböznek a kódszavak, de csak $n-d+1$ hosszúak. Innen a kódszavak számára azt kapjuk, hogy $\sharp(C) \leq q^{n-d+1}$, másként $d \leq (n+1)/\log_q(\sharp(C))$; ez a *Singleton-korlát*. Ha egyenlőség áll, a kódot *maximális távolságú szeparálható kód*nak, *MDS-kódnak* nevezzük. Ekkor $\sharp(C) = q^k$, ahol $k = n-d+1$. A *szeparálható (elválasztható)* kód elnevezést az indokolja, hogy (bármely) rögzített $d-1 = n-k$ helyen álló betűket elhagyva a kódszavakból, q^k különböző szó marad, ezért a kódolást végezhetjük úgy, hogy az üzeneteket leképezzük ezekre a szavakra, majd az adott $d-1 = n-k$ helyen kiegészítjük ellenőrző betűkkel, így az ellenőrző betűk elválaszthatók a kódoló betűktől.

9.3.13. Lineáris kód. Ahhoz, hogy a kódolás és a dekódolás minél egyszerűbb legyen, a kódoláshoz olyan rendszereket célszerű alkalmazni, amelyek rendelkeznek valamilyen belső struktúrával. Jó kódok konstruálhatóak algebrai rendszerek segítségével. A gyakorlatban alkalmazott kódok jelentős része lineáris kód: Ha K véges test, akkor a K elemeiből alkotott rendezett n -esek a komponensenkénti összeadással, valamint az n -es minden elemének ugyanazzal az elemmel való szorzásával egy K feletti n -dimenziós K^n lineáris teret alkotnak. Ennek a térnek bármely altere egy *lineáris kód*. Ha az alter k -dimenziós, a kód távolsága d , és a test elemeinek száma q , akkor az ilyen kódot $[n, k, d]_q$ *kódnak* nevezzük. Ha nem lényeges a d , illetve q megadása, akkor elhagyható a jelölésből. Itt a Singleton-korlát alakja $k \leq n-d+1$. Lineáris kódnál mindig feltesszük, hogy a

kódolandó üzenetek K^k elemei, azaz a kódábécé elemeiből képzett k -asok. A lineáris kód sebessége k/n .

A paritásbites kód páratlan sok egyesre való kiegészítésnél nem lineáris, de ha páros sok egyesre egészítünk ki, akkor már lineáris F_2 felett.

9.3.14. Generátormátrix, ellenőrző mátrix, szindróma. A K véges test feletti $[n, k]$ lineáris kódnál célszerű a kódolást egy K^k -t $C \subset K^n$ -re képező G (kölsönösen egyértelmű) lineáris leképezésnek választani, ahol C a kódszavak k -dimenziós altere. Ezt a leképezést mátrixával jellemezhetjük, ez a kódolás *generátormátrixa*. Egy, a szokásos bázisban vett mátrix pontosan akkor generátormátrix, ha az oszlopai bázist alkotnak a kódszavak terében. A hibajavításra használható egy (tetszőleges) $H: K^n \rightarrow K^{n-k}$ szűrjektív lineáris leképezés, amelynek a magja C ; egy ilyen leképezést *ellenőrző leképezésnek*, mátrixát a kód egy *ellenőrző mátrixának* nevezzük. Ha $v \in K^n$, akkor a v -hez tartozó $s = Hv$ vektor, a *szindróma* (magyarul *hibajellemző*) pontosan akkor nulla, ha v kódszó, azaz $v \in C$. A két leképezést csak az köti össze, hogy G képtere H magja: mindkettő a kódszavak halmaza. Ezért a kódszavak halmazát akár a G , akár a H leképezés megadja. A hibajavítás általában nem függ G -től, azaz a kódolástól, csak a kódszavak halmazától. Az ellenőrző mátrix segítségével is meghatározható a kód súlya: az ellenőrző mátrixnak pontosan akkor van m oszlopa, amelyeknek megfelelő vektorok lineárisan függőek, ha van olyan kódszó, amelynek súlya legfeljebb m , hiszen a H mátrixával szorozva a kódszó oszlopmátrixát, H mátrixa oszlopainak lineáris kombinációját kapjuk.

A G kódoló leképezést célszerű úgy megválasztani, hogy a kódszavak meghatározott helyein az üzenet betűi álljanak, mert ekkor a hibajavítás után nincs más dolgunk, mint az „ellenőrző” betűket elhagyni. Ilyenkor *szisztematikus kódolásról* beszélünk. Lineáris kódolásnál ez elérhető például úgy, hogy elemi oszlopműveletek használatával, hasonlóan, mint a Gauss–Jordan-eliminációnál, átalakítjuk a generátormátrixot (lásd a Fano-kód példáját): az elemi oszlopműveletek nem változtatják meg a transzformáció értékékesztét. A kódszavak betűit alkalmasan permutálva azt is elérhetjük, hogy az üzenet betűi a kódszónak az előre megadott k helyén álljanak: a permutáció nem változtatja meg a linearitást és a súlyt.

A szindróma felhasználható a hiba javítására:

9.3.15. Szindrómadekódolás. Ez lineáris kód esetén a minimális távolságú dekódolás egy megvalósítása. Az előző pont jelöléseivel, ha $s \in K^{n-k}$, tekintsük a $H^{-1}(s)$ halmaz egy olyan $e(s)$ rögzített vektorát, amelynek súlya az adott mellékosztályban minimális. Ezeket az $e(s)$ vektorokat *mellékosztály-vezetőnek* fogjuk nevezni. Ha $c \in K^n$ egy kódszó, $v \in K^n$ a vett szó, $e = v - c$ a hiba, és ha $w(e) < d/2$, tehát ha a hiba minimális távolságú dekódolással javítható, akkor $He(s) = s = Hv = Hv - Hc = He - 0 = He$, így e és $e(s)$ ugyanabban a mellékosztályban vannak. A mellékosztályvezető választása miatt $w(e(s)) \leq w(e)$, ahonnan $w(e - e(s)) \leq w(e) + w(-e(s)) = w(e) + w(e(s)) < d$. De $H(e - e(s)) = 0$, így a különbség kódszó, tehát $e = e(s)$, így $c = v - e(s)$, a hibát kijavítottuk. A szindrómadekódolás tárgyánya sokkal kisebb, mint a táblázattal való dekódolása, mert itt csak a mellékosztályvezetőket kell tárolni, de még mindig nagyon nagy lehet.

9.3.16. Példa: Fano-kód. A 3.4.4 ábrán látható *Fano-sík* felhasználható hibajavító kód konstruálására. Megszámozva a pontokat 1-től 7-ig, a kódszavak az egyenesekhez tartoznak: olyan bitsorozatok, amelyekben az adott egyenesre illeszkedő pontoknak megfelelő

bitek egyesek, a többi nulla, illetve ezek egyesekre komplementesei. Kódszó még a csupa nulla illetve csupa egy bitsorozat. Mint könnyen ellenőrizhető, így egy $[7, 4, 3]_2$ lineáris kódot kapunk, melynek a kódszavai: 1110000, 1001100, 0101010, 0011001, 1000011, 0100101, 0100110, 0000000, 0001111, 0110011, 1010101, 1100110, 0111100, 1011010, 1011001, 1111111. A Fano-kód súlya, tehát távolsága is 3. Könnyen ellenőrizhető, hogy 1-hibajavító tökéletes kód (és így 1-hibajelző), de nem MDS-kód. Egy generátormátrixa (a szokásos bázisban) például az

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

mátrix, amiből oszlopműveletekkel (az első oszlopot hozzáadva minden továbbihoz, majd a kapott második oszlopot hozzáadva az elsőhöz és a harmadikhoz, ezután a kapott harmadik oszlopot hozzáadva a másodikhoz, végül a negyedik oszlopot hozzáadva a másodikhoz és a harmadikhoz) az

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

generátormátrixot kapjuk, amely már szisztematikus kódot ad, a kódolandó szó a kódszó elejére, az első négy helyre kerül. Jelölje b_1, b_2, b_3 és b_4 az $\mathbb{F}_2^7$ ezen mátrix oszlopainak megfelelő vektorait, $e_1, e_2, \dots, e_7$, illetve f_1, f_2, f_3 az $\mathbb{F}_2^7$, illetve $\mathbb{F}_2^3$ szokásos bázisát. A H leképezést definiáljuk azzal, hogy a $b_1, b_2, b_3, b_4, e_5, e_6, e_7$ bázis első négy vektorát nullába, az utolsó hármat pedig rendre f_1, f_2, f_3 -ba viszi. Mivel $e_1 = b_1 - e_6 - e_7$, $e_2 = b_2 - e_5 - e_7$, $e_3 = b_3 - e_5 - e_6$ és $e_4 = b_4 - e_5 - e_6 - e_7$, a szokásos bázisban a

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

ellenőrző mátrixot kapjuk. A 000, 100, 010, 001, 110, 101, 011, 111 szindrómákhoz tartozó mellékosztályvezetők rendre 0000000, 0000100, 0000010, 0000001, 0010000, 0100000, 1000000, 0001000. Legyen például az üzenet $c = 0100101$; ellenőrizhető, hogy $Hc = 0$, vagyis c kódszó. Ha a hibavektor $e = 0000100$, vagyis az 5. bit és csak ez a bit az üzenet átvitele során megsérül, akkor a vétel helyén a $v = 0100001$ bitsorozatot kapjuk, és a szindróma, $s = Hv = 100$, amihez mellékosztályvezetőként az e hibavektor tartozik. Megváltoztatva a vett üzenetben az 5. bitet, a 0100101 bitsorozatot kapjuk, egyezésként az elküldött bitsorozattal. Amennyiben két hiba van, például $e = 0000101$, akkor $s = Hv = 101$, és „javítás” után a 0110001 bitsorozatot kapjuk, ami nem egyezik az eredeti sorozattal, vagyis rosszul javítottunk. Ha a hibavektor $e = 1110000$ – maga is kódszó – akkor már észre sem vesszük a hibát.

* **9.3.17. Példa: Reed–Müller-kódok.** $\mathbb{F}_2^t$ pontjait számozzuk meg 1-től 2^t -ig, és legyen $0 < r < t$ rögzített. A kódszavakat úgy kapjuk, hogy minden egyes r -dimenziós affin sokasághoz hozzárendelünk egy nulla-egy sorozatot: az adott affin sokaságra illeszkedő pontoknak megfelelő helyre egyest, a többi helyre nullát írunk, valamint tekintjük még a csupa nulla és a csupa egyes bitsorozatot. Megmutatható, hogy az így kapott kód egy bináris $[n, k, d]_2$ kód, ahol $n = 2^t$, $d = 2^r$, és $k = \sum_{j=0}^r \binom{t}{j}$. A $t = 5$, $r = 4$ paraméterekkel adódó $[32, 6, 16]_2$ kódot használták a Mariner-9 Mars-szonda képeinek Földre küldésére: egy pixel 64 lehetséges szürke árnyalatot tartalmazott, és pixelenként küldték el a képet. (Ez a kód az úgynevezett *Hadamard-kódnak* is speciális esete.)

* **9.3.18. Hamming-kódok.** Az úgynevezett *Hamming-kódok* egyetlen hiba javítására alkalmas lineáris kódok. Legyen $m > 1$. A H ellenőrző leképezés mátrixának, az ellenőrző mátrixnak az oszlopai (a szokásos bázisban) azok az $\mathbb{F}_q^m$ vektorok, amelyeknek az első nem nulla komponense 1. A mátrix oszloprangja nyilván m , így a megfelelő lineáris leképezés képtere $\mathbb{F}_q^m$. Az oszlopok száma $n = 1 + q + q^2 + \dots + q^{m-1} = (q^m - 1)/(q - 1)$, és a kódszavak $k = n - m$ dimenziós alteret alkotnak $\mathbb{F}_q^n$ -ben. Mivel az ellenőrző mátrix bármely két oszlopa lineárisan független, a kód távolsága legalább 3. Több nem lehet, mivel a kód tökéletes 1-hibajavító: $q^k(1 + n(q - 1)) = q^k(1 + q^m - 1) = q^m + k = q^n$. A hibajavítás a vett szó szindrómája segítségével könnyen elvégezhető: ha csak egy hiba van, akkor az e hibavektornak egyetlen nem nulla koordinátája van, legyen ez α . Az $s = He$ szindróma a H mátrixa valamelyik oszlopának az α -szorosa. Mivel minden oszlop legelső nem nulla eleme 1, a szindróma legelső nem nulla eleme α . Ennek ismeretében, a szindrómát osztva α -val, megkereshető (vagy kiszámolható), hogy melyik oszlopot kapjuk; az annyiadik koordinátája volt hibás az üzenetnek. A Fano-kód speciális esete a Hamming-kódnak.

* **9.3.19. Feladat [7].** Készítsünk egy olyan Hamming-kódot a háromelemű test felett, amelynek hossza 13, dimenziója pedig 10. Mutassuk meg ennek segítségével, hogy a TOTÓ-n elegendő $3^{11} = 59049$ hasábot megjátszani, hogy biztosan legyen legalább 12 találatunk.

9.3.20. Polinomkódok. Lineáris kódnál a k hosszú kódolandó szavak tekinthetők $\mathbb{F}_q$ feletti, k -nál alacsonyabb fokú polinomnak is, a betűket nullától indexelve. Ha a kódolást úgy végezzük, hogy ezt a $p(x)$ polinomot beszorozzuk egy rögzített m -ed fokú $g(x)$ polinommal ($m \in \mathbb{N}^+$), akkor lineáris kódot és kódolást kapunk, $n = m + k$ hosszú kódszavakkal, mivel a $p \mapsto pg$ leképezés kölcsönösen egyértelmű. Az ilyen típusú lineáris kódolást *polinomkódolásnak* nevezzük, $g(x)$ a kód *generátorpolinomja*, a kódszavak a többszörösei. A generátorpolinomról feltehetjük (és a továbbiakban fel is tesszük), hogy főpolinom, hiszen osztva a főegyütthatóval, a kódszavak halmaza nem változik. A generátorpolinomot nem célszerű úgy választani, hogy konstans tagja nulla legyen, hiszen ekkor minden kódpolinom konstans tagja is nulla, így a kódszavak nulla indexű betűje nem hordoz információt. A továbbiakban ezért mindig feltesszük, hogy a generátorpolinom konstans tagja nem nulla. Mivel a generátorpolinom is kódszó, a kód súlya nem lehet nagyobb, mint a generátorpolinom súlya, és mivel a k (és így n) növelésével a kódszavak halmaza bővül, a kód súlya csak csökkenhet. A 8.3.59 tétel szerint valamely j -re $g(x)|x^{q^j} - x$, így $g(x)|x^{q^j-1} - 1$, azaz $n \geq q^j$ esetén a kód súlya már csak kettő mert $x^{q^j-1} - 1$ is kódszó, tehát nem célszerű n -et nagyon nagyra választani. Egyébként ha $g(x)|x^\ell - 1$, akkor $n = \ell$ esetén a kód *ciklikus kód*: ha $a_0a_1 \dots a_{n-2}a_{n-1}$ egy kódszó, akkor $a_{n-1}a_0a_1 \dots a_{n-2}$ is

kódszó:

$$\begin{aligned} & a_{n-1} + a_0x + a_1x^2 + \cdots a_{n-2}x^{n-1} \\ & = x(a_0 + a_1x + \cdots + a_{n-2}x^{n-2} + a_{n-1}x^{n-1}) - a_{n-1}(x^n - 1), \end{aligned}$$

így osztható $g(x)$ -szel.

Polinomkódolás egy változatával könnyen készíthetünk szisztematikus kódot is: ha p az üzenetpolinom, akkor $p(x)x^m$ -et maradékosan osztva $g(x)$ -szel $p(x)x^m = q(x)g(x) + r(x)$; a kódszó legyen $p(x)x^m - r(x)$: így a kódszó végén az eredeti üzenet betűi állnak. Mivel az x^m -mel való szorzás és a maradékképzés lineáris, ez lineáris kódolás. A vett szó ellenőrzése is egyszerű: megnézzük, hogy osztható-e $g(x)$ -szel. Ha igen, az eredeti üzenet ott van a vett szóban.

9.3.21. CRC-kódok. Egyszerű, csak hibajelzésre használatos, $\mathbb{F}_2$ feletti polinomkódok az úgynevezett *CRC*, vagyis *Cyclic Redundancy Check*, „ciklikus ellenőrzés” kódok. A kódolás a fent leírt. Megjegyezzük, hogy $\mathbb{F}_2$ felett (sőt, minden $\mathbb{F}_q$ felett, amelyre $\text{char}(\mathbb{F}_q) = 2$, azaz amelyre q kettőhatvány) $r(x) = -r(x)$. Néhány gyakran használt CRC-generátorpolinom:

Név	Generátorpolinom	Távolság	Maximális kódhossz
CRC-1 (paritásbit)	$x + 1$	2	—
CRC-5-USB	$x^5 + x^2 + 1$	3	$2^5 - 1$
CRC-8	$x^8 + x^2 + x + 1$	4	$2^7 - 1$
CRC-16-IBM	$x^{16} + x^{15} + x^2 + 1$	4	$2^{15} - 1$
CRC-16-CCITT	$x^{16} + x^{12} + x^5 + 1$	4	$2^{15} - 1$
CRC-32 (Ethernet, FDDI, gzip, PNG)	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$	3	$2^{32} - 1$
CRC-64-ISO	$x^{64} + x^4 + x^3 + x + 1$	3	$2^{64} - 1$

*** 9.3.22. A CRC-kódok hibajelző képessége.** A paritásbites ellenőrzéssel már foglalkoztunk. A többi CRC-polinom a fenti táblában mind vagy irreducibilis, vagy $x+1 = x-1$ -szeresei egy irreducibilis polinomnak. Mindegyik esetben a kód súlya legalább 2, mert x -hatvány nem lehet kódpolinom. A kód súlya mindaddig nagyobb, mint kettő, ameddig meg nem jelenik a kódpolinomok között egy $x^{j+\ell} + x^j = x^j(x^\ell - 1)$ alakú polinom. Mivel a konstans tag nem nulla, ez csak akkor lehet, ha $g(x)|x^\ell - 1$. Nyilván $x^{i\ell} - 1 = (x^\ell - 1)(x^{(i-1)\ell} + x^{(i-2)\ell} + \cdots + 1)$ is osztható g -vel, és így $x^{i\ell+j} - x^j$ is többszöröse g -nek; ha g egy m -ed fokú ($m > 1$) irreducibilis polinom, akkor a 8.3.59 tétel szerint $g(x)|x^{2^m} - x$, azaz $g(x)|x^{2^m-1} - 1$. Legyen most ℓ a legkisebb olyan érték, amelyre $g(x)|x^\ell - 1$. Maradékosan osztva $2^m - 1$ -et ℓ -lel, $2^m - 1 = i\ell + j$ esetén $x^j - 1 = x^{2^m-1} - 1 - (x^{i\ell+j} - x^j)$ is osztható $g(x)$ -szel, tehát $j = 0$, azaz $\ell|2^m - 1$. Ellenőrizve a lehetséges értékeket, ℓ meghatározható. Ha a kódhossz nem nagyobb, mint ℓ , a kód súlya legalább 3. Ha a CRC-polinom $x-1$ -szer egy m -ed fokú $g(x)$ irreducibilis polinom, akkor minden kódszó is $x-1$ többszöröse, így csak páros lehet a súlya. A fenti gondolatmenet itt is érvényes, a legkisebb ℓ kitevőre, amelyre $x^\ell - 1$ többszöröse a kódpolinomnak, $\ell|2^m - 1$, aminek alapján ℓ meghatározható. Itt a kód súlya legalább 4, hiszen nagyobb, mint 2, és páros. Megjegyezzük, hogy a kód súlya nem lehet túl nagy, ha n nagy: például 32 bites CRC-polinomnál, ha $n = 84$, akkor a kód nem lehet 7-hibajavító, mert $\binom{84}{7} > 2^{32}$, ami ellentmond a Hamming-korlátnak, így távolsága kisebb, mint 15; ha $n = 124$, akkor a

kód nem lehet 6-hibajavító, mert $\binom{124}{6} > 2^{32}$, ami ellentmond a Hamming-korlátnak, így távolsága kisebb, mint 13; stb.

Végül megjegyezzük, hogy minden CRC-kód jelez minden olyan hibát, amelynél a hibás bitek egyetlen olyan intervallumba, „hibacsomóba” esnek, amelynek hossza legfeljebb a CRC-polinom foka: ekkor ugyanis a hibapolinom $e(x)x^j$ alakú, ahol $e(x)$ foka kisebb, mint a CRC-polinom foka, így nem lehet osztható az utóbbival, tehát nem lehet kódszó.

*** 9.3.23. A négy Golay-kód.** A $[23, 12, 7]_2$ Golay-kódot az $x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$ polinom generálja, és tökéletes kód. Ezzel a kóddal védik a műholdas műsorszórás szolgáltatásazonosítását. A $[24, 12, 8]_2$ Golay-kódot ebből úgy kapjuk, hogy minden kódszót kiegészítünk páros paritásúra. Ezt a kódot használták a Voyager űrszondák színes képek továbbítására. A $[11, 6, 5]_3$ Golay-kódot az $x^5 + x^4 + 2x^3 + x^2 + 2$ polinom generálja, és ez is tökéletes kód. A $[12, 6, 6]_3$ Golay-kódot úgy kapjuk, hogy minden kódszót kiegészítünk úgy, hogy a jegyek összege $\mathbb{F}_3$ -ban nulla legyen. Megmutatható, hogy ezek a kódok szoros kapcsolatban állnak egyszerű csoportokkal: például S_{23} illetve S_{24} azon permutációi, amelyek a $[23, 12, 7]_2$ illetve $[24, 12, 8]_2$ bináris Golay-kódot önmagába viszik, egy 10200960, illetve 244823040 elemű egyszerű csoportot alkotnak.

9.3.24. Vandermonde-determináns. Ha $x_1, x_2, \dots, x_m$ egy K test elemei, akkor az

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ x_1 & x_2 & x_3 & \dots & x_m \\ x_1^2 & x_2^2 & x_3^2 & \dots & x_m^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1^{m-1} & x_2^{m-1} & x_3^{m-1} & \dots & x_m^{m-1} \end{pmatrix}$$

mátrix determinánsa

$$\prod_{1 \leq i < j \leq m} (x_j - x_i).$$

Bizonyítás. Az m szerinti indukcióval: vonjuk ki a másodiktól kezdve minden sorból a felette álló x_1 -szeresét. $\square$

9.3.25. Reed–Solomon-kódok. Legyen most K egy tetszőleges véges test, alkossák az ábécét ennek elemei, a K elemszámát jelölje q . Legyen $0 \neq \alpha \in K$ multiplikatív rendje n . (Nyilván $n|q-1$; általában α -t úgy választjuk, hogy $n = q-1$ legyen.) Ekkor az α^i , $0 \leq i < n$ elemek páronként különböznek, és mindegyik gyöke a $z^n - 1 \in K[z]$ polinomnak, ezért megadják ezen polinom összes gyökét. Így $z^n - 1 = \prod_{i=0}^{n-1} (z - \alpha^i)$.

Legyen $0 < k < n$, $m = n - k$ és $g = \prod_{i=1}^m (z - \alpha^i)$. Ez a polinom egy K fölötti, m -edfokú főpolinom, és nyilván osztója a $z^n - 1$ polinomnak. A g mint generátorpolinom által megadott $[n, k]_q$ polinomkód a g (vagy az α) által generált Reed–Solomon-kód. Meghatározzuk a kódtávolságot és egy ellenőrző mátrixot.

Tekintsük a kódpolinomok C halmazának egy c elemét. Mivel g osztója c -nek, g minden gyöke c -nek is, vagyis $c(\alpha^i) = 0$, ha $1 \leq i \leq m$. Fordítva, ha $u \in K^n$, és minden $1 \leq i \leq m$ -re $u(\alpha^i) = 0$, akkor valamennyi i -re $z - \alpha^i$ osztója u -nak, de akkor ezek legkisebb közös többszöröse, azaz a szorzatuk, tehát g is osztója u -nak, vagyis ez esetben u a kódhoz tartozik. Ez azt jelenti, hogy $u \in K^n$ akkor és csak akkor eleme a kódnak, ha g valamennyi gyöke egyben u -nak is gyöke, vagyis ha minden $1 \leq i \leq m$ -re

$\sum_{j=0}^{n-1} (\alpha^i)^j u_j = 0$. Így a $h_{i,j} = \alpha^{ij}$ ($1 \leq i \leq m$, $0 \leq j < n$) mátrix egy ellenőrző mátrix: a hozzá tartozó H lineáris leképezésre $Hu = 0$ akkor és csak akkor, ha $u \in C$. A kód súlyának meghatározásához megmutatjuk, hogy H mátrixának bármely m oszlopa lineárisan független. Legyen $0 \leq j_1 < \dots < j_m < n$, és tekintsük a mátrix j_ℓ ($\ell = 1, 2, \dots, m$) indexű oszlopait. Ezek a mátrix egy m -edrendű négyzetes részmátrixát adják, amelynek ℓ -edik oszlopában az i -edik elem $h_{i,j_\ell} = (\alpha^i)^{j_\ell} = (\alpha^{j_\ell})^i$. Megmutatjuk, hogy ezen részmátrix determinánsa nem nulla. A determináns ℓ -edik oszlopában minden elemből kiemelhető α^{j_ℓ} . Mivel a kiemelt elem nem nulla, ezért az eredeti determináns akkor és csak akkor 0, ha a kiemelés után kapott determináns értéke 0. A kapott determináns ℓ -edik oszlopában α^{j_ℓ} egymás után következő hatványai állnak, a 0 kitevős hatvánnyal kezdve, vagyis ez egy Vandermonde-determináns. Így az előző állítás szerint a determináns értéke $\prod_{0 \leq s < t < m} (\alpha^{j_s} - \alpha^{j_t}) \neq 0$, ami azt jelenti, hogy a mátrix bármely m oszlopa lineárisan független. Ebből a kód d távolsága nagyobb, mint m , és így (mivel nagyobb nem lehet) $d = n - k + 1 = m + 1$, azaz a kód MDS-kód, tehát elég nagy m esetén egynél több hiba is javítható.

9.3.26. A Reed–Solomon-kód dekódolása. A Reed–Solomon-kód lineáris, tehát a hiba javítható például a szindrómadekódolással, de a Reed–Solomon-kódra mutatunk egy ennél lényegesen praktikusabb hibajavítást.

Legyen adott egy $[n, k, d]_q$ Reed–Solomon-kód, $m = n - k$, $d = n - k + 1 = m + 1$, $g = \prod_{i=1}^m (z - \alpha^i)$ a kód generátorpolinomja, e a hibavektor, és $L(z) = \prod_{\{j: e_j \neq 0\}} (1 - \alpha^j z)$ az úgynevezett *hibahelypolinom*. Ennek ismeretében a hibák helye meghatározható: megkeressük, hogy mely α^{-j} -k gyökei $L(z)$ -nek, és ezen j -k megadják a hibák helyét. Legyen $E(z) = \sum_{\{j: e_j \neq 0\}} \alpha^j e_j L_j(z)$ az úgynevezett *hibaérték-polinom*, ahol $L_j(z) = L(z)/(1 - \alpha^j z)$, ha $e_j \neq 0$. Ha még $E(z)$ -t is ismerjük, akkor a hiba javítható is, mert rögzített j esetén $L_i(\alpha^{-j})$ akkor és csak akkor nem nulla, ha $i = j$, ezért $E(\alpha^{-j}) = \alpha^j e_j L_j(\alpha^{-j})$, így

$$e_j = \frac{E(\alpha^{-j})}{\alpha^j L_j(\alpha^{-j})}.$$

A következő tétel lehetővé teszi a két polinom gyors és igen kis tárigényű kiszámítását a könnyen kiszámolható szindróma segítségével.

9.3.27. Tétel. Legyen $s(z)$ a szindrómához tartozó polinom. Az előző pont jelölésével tegyük fel, hogy a hibahelyek száma, azaz $L(z)$ fokszáma legfeljebb $m/2$ (ami azzal ekvivalens, hogy kisebb, mint $d/2$, azaz hibajavítás egyáltalán végezhető). Alkalmazzuk a bővített euklideszi algoritmust az $a(z) = z^m$ és $b(z) = s(z)$ polinomokra. Az ottani jelölésekkel legyen ℓ a legkisebb index, amelyre $\deg(r_\ell) < m/2$, és legyen $r_\ell = ax_\ell + by_\ell$. Ekkor $y_\ell(0) \neq 0$, és $L(z) = y_\ell(z)/y_\ell(0)$, $E(z) = r_\ell(z)/y_\ell(0)$.

A tétel rávilágít a matematika szépségére és egységére. Egy olyan régi algoritmusnak, mint az euklideszi algoritmus, egy igen fontos és hasznos alkalmazását láthatjuk, amelyre Euklidész még csak nem is gondolhatott.

* **Bizonyítás.** Először megmutatjuk, hogy z^m osztja az $E(z) - L(z)s(z)$ polinomot, ahol $s(z) = s_0 + s_1z + \dots + s_{m-1}z^{m-1}$ a szindrómához tartozó polinom. Valóban,

$$\begin{aligned}
E(z) - L(z)s(z) &= \sum_{\{j:e_j \neq 0\}} \alpha^j e_j L_j(z) - L(z) \sum_{i=0}^{m-1} s_i z^i \\
&= \sum_{\{j:e_j \neq 0\}} \alpha^j e_j L_j(z) - L(z) \sum_{i=0}^{m-1} \left(\sum_{j=0}^{n-1} (\alpha^{i+1})^j e_j \right) z^i \\
&= \sum_{\{j:e_j \neq 0\}} \alpha^j e_j L_j(z) L(z) - \sum_{j=0}^{n-1} e_j \sum_{i=0}^{m-1} (\alpha^{i+1})^j z^i \\
&= \sum_{\{j:e_j \neq 0\}} \left(\alpha^j e_j L_j(z) - \alpha^j e_j L(z) \sum_{i=0}^{m-1} (\alpha^j)^i z^i \right) \\
&= \sum_{\{j:e_j \neq 0\}} \left(\alpha^j e_j L_j(z) - \alpha^j e_j L(z) \frac{1 - (\alpha^j z)^m}{1 - \alpha^j z} \right) \\
&= \sum_{\{j:e_j \neq 0\}} \left(\alpha^j e_j L_j(z) - \alpha^j e_j L_j(z) (1 - (\alpha^j z)^m) \right) \\
&= z^m \sum_{\{j:e_j \neq 0\}} \alpha^{j(m+1)} e_j L_j(z);
\end{aligned}$$

itt felhasználtuk s és H definícióját. Ez azt jelenti, hogy alkalmas $f(z)$ polinommal $E(z) = f(z)z^m + L(z)s(z)$. Így z^m és $s(z)$ legnagyobb közös osztója osztója $E(z)$ -nek, és emiatt a fokszáma legfeljebb annyi, mint $E(z)$ fokszáma, ami kisebb, mint $m/2$. Így van olyan maradék az euklideszi algoritmus alkalmazása során, amelynek fokszáma kisebb, mint $m/2$. Az $E(z) = f(z)z^m + L(z)s(z)$ egyenlet $y_\ell(z)$ -szerezéséből kivonva az

$$r_\ell(z) = a(z)x_\ell(z) + b(z)y_\ell(z) = z^m x_\ell(z) + s(z)y_\ell(z)$$

egyenlet $L(z)$ -szerezését, azt kapjuk, hogy

$$(1) \quad E(z)y_\ell(z) - L(z)r_\ell(z) = (f(z)y_\ell(z) - L(z)x_\ell(z))z^m.$$

Megmutatjuk, hogy a zárójelben álló polinom nulla.

A bővített euklideszi algoritmus az $r_0 = a$, $r_1 = b$, $x_0 = 1$, $x_1 = 0$, $y_0 = 0$, $y_1 = 1$ kezdőértékkel indul, q_j az r_{j-1} -nek r_j -vel való osztásakor a hányados, r_{j+1} pedig a maradék. Megmutatjuk, hogy

$$(2) \quad \deg(y_j) = \deg(a) - \deg(r_{j-1})$$

és

$$(3) \quad x_{j-1}y_j - x_jy_{j-1} = (-1)^{j-1},$$

ha $j > 0$. Mindkét állítás teljesül $j = 1$ -re. Indukcióval, mivel $y_{j+1} = y_{j-1} - q_j y_j$, felhasználva (2)-t,

$$\begin{aligned}
\deg(y_{j+1}) &= \deg(y_{j-1} - q_j y_j) = \deg(q_j y_j) = \deg(q_j) + \deg(y_j) \\
&= \deg(r_{j-1}) - \deg(r_j) + \deg(a) - \deg(r_{j-1}) \\
&= \deg(a) - \deg(r_j)
\end{aligned}$$

és mivel $x_{j+1} = x_{j-1} - q_j x_j$, felhasználva (3)-at,

$$x_j y_{j+1} - x_{j+1} y_j = x_j (y_{j-1} - q_j y_j) - (x_{j-1} - q_j x_j) y_j = (-1)^j.$$

Térjünk vissza (1)-hez. Mivel ℓ választása és (2) miatt

$$\deg(y_\ell) = \deg(a) - \deg(r_{l-1}) \leq m - m/2 = m/2,$$

$\deg(E) < m/2$, $\deg(r_\ell) < m/2$, $\deg(L) \leq m/2$, a bal oldal foka (1)-ben kisebb, mint m , így a zárójelben csak nulla állhat. Innen $E y_\ell = L r_\ell$ és $f y_\ell = L x_\ell$. Az E és L relatív prímek, hiszen L minden gyöktényezője az E -t definiáló összeg minden tagját osztja, egy kivételével, valamint (3) szerint x_ℓ és y_ℓ is relatív prímek, innen az következik, hogy L osztója y_ℓ -nek és y_ℓ osztója L -nek, tehát asszociáltak, azaz $L = c y_\ell$ valamely nem nulla konstanssal. Innen $E = c r_\ell$ ugyanazzal a konstanssal. Mivel L konstans tagja 1, kapjuk az állítást.

*** 9.3.28. Példa.** Legyen $K = \mathbb{Z}_{11}$, $n = 10$, $k = 6$, tehát $m = n - k = 4$. A $\mathbb{Z}_{11}$ test elemei helyett a legkisebb nem negatív reprezentánsukat fogjuk használni, 10 helyett A-t írunk hexadecimális jegyként. $\mathbb{Z}_{11}$ -ben $2^2 = 4 \neq 1$, és $2^5 = (2^2)^2 2 = 4^2 2 = A \neq 1$, ezért 2 rendje 10. Legyen $\alpha = 2$. Mivel $m = n - k = 4$, a kód generátorpolinomja $g(z) = \prod_{i=1}^4 (z - \alpha^i) = \prod_{i=1}^4 (z - 2^i) = 1 + 8z + 5z^2 + 3z^3 + z^4$. A kód elemeit úgy kapjuk, hogy a generátorpolinomot megszorozzuk a $\mathbb{Z}_{11}$ feletti legfeljebb ötödfokú polinomokkal. Legyen egy ilyen polinom $4 + 5z + 2z^4$, ekkor a megfelelő kódpolinom

$$u(z) = 4 + 4z + 5z^2 + 4z^3 + Az^4 + Az^5 + Az^6 + 6z^7 + 2z^8,$$

vagyis a kódszó $u = 4454AAA620$. A kód távolsága $d = 5$, tehát a kód képes 2 hibát helyesen javítani. Legyen például $e = 0030200000$ a hibavektor, ekkor a vett szó $v = u + e = 44841AA620$.

Az ellenőrző mátrix most

$$\begin{pmatrix} 1 & 2 & 4 & 8 & 5 & A & 9 & 7 & 3 & 6 \\ 1 & 4 & 5 & 9 & 3 & 1 & 4 & 5 & 9 & 3 \\ 1 & 8 & 9 & 6 & 4 & A & 3 & 2 & 5 & 7 \\ 1 & 5 & 3 & 4 & 9 & 1 & 5 & 3 & 4 & 9 \end{pmatrix},$$

és a szindróma

$$Hv = 0A25,$$

nem nulla, így az átvitel során hiba keletkezett. Hajtsuk végre az euklideszi algoritmust a $z^m = z^4$, valamint a szindrómához tartozó $s(z) = Az + 2z^2 + 5z^3$ polinomra addig, amíg a maradékpolinom foka először lesz kisebb, mint $m/2$, és közben számítsuk ki sorban az $y_j(z)$ polinomokat, ahol $y_j(z)$ a kiterjesztett euklideszi algoritmusban meghatározott együtthatója az $s(z)$ polinomnak, vagyis amivel $r_j(z) = z^m x_j(z) + s(z) y_j(z)$. Mint ismert, ha $y_0 = 0$ és $y_1 = 1$, akkor $y_{j+1} = y_{j-1} - q_j y_j$, ahol q_j a j -edik osztás hányadosa.

A konkrét esetben

$$\begin{aligned} z^4 + 0z^3 + 0z^2 + 0z + 0 : 5z^3 + 2z^2 + Az + 0 &= 9z + 3 \\ 3z^2 + 0z + 3 & \end{aligned}$$

így

$$y_1(z) = 0 - (9z + 3) \cdot 1 = 2z + 8,$$

majd újra osztva maradékosan

$$\begin{aligned} 5z^3 + 2z^2 + Az + 0: 3z^2 + 0z + 3 &= 8z + 7 \\ 2z + 0 \end{aligned}$$

így

$$y_2(z) = 1 - (8z + 7)(2z + 8) = 4z^2 + 7z + 9,$$

vagyis $r_2(z) = 2z$ és $y_2(z) = 4z^2 + 7z + 9$. Szorozzuk meg $y_2(z)$ -t $y_2(0) = 9$ inverzével, 5-tel: $L(z) = 9z^2 + 2z + 1$. Mivel $L(z) = (1 - 4z)(1 - 5z)$, a hiba a vett szó 2 és 4 indexű pozíciójában van, ugyanis $4 = 2^2$, és $5 = 2^4$. Meg kell még határozni a hibák értékét: $E(z) = 5r_2(z) = Az$, $L_2(z) = 1 - 5z$, és $L_4(z) = 1 - 4z$, így

$$e_2 = \frac{E(4^{-1})}{2^2 L_2(4^{-1})} = \frac{8}{4 \cdot 8} = 3,$$

és

$$e_4 = \frac{E(5^{-1})}{2^4 L_4(5^{-1})} = \frac{2}{5 \cdot 9} = 2,$$

vagyis a kiszámolt hibavektor $e = 0030200000$, azaz $u = v - e = 4454AAA620$.

* **9.3.29. Kódrövidítés.** Néhány kód, például a Reed–Solomon-kód csak meghatározott hosszakban konstruálható: például 256 elemű test felett csak 255 és az osztói jöhetnek szóba. Ilyenkor segít a *kódrövidítés*. Tetszőleges kódra gyűjtsük össze mindazokat a kódszavakat, amelyekben egy adott helyen egy adott betű áll. Csak ezeket fogjuk használni, és a kódolás után az adott helyen álló adott betűt kihagyjuk, a dekódolás előtt pedig újra beírjuk. Nyilvánvaló, hogy a kódrövidítés nem csökkenti a távolságot.

Lineáris kódnál azokat a kódszavakat érdemes felhasználni a rövidített kódban, amelyekben az adott helyen nulla áll, mert ekkor a rövidített kód is lineáris lesz. Ha egy $[n, k, d]_q$ lineáris kódot így rövidítünk, akkor azon kódszavak C' altere, amelyekben az adott helyen nulla áll, az eredeti kódszavak C alterének egy alterét, így a C Abel-csoportnak egy részcsoportját alkotja, továbbá bármely két C -beli kódszó különbsége, amelyekben az adott helyen ugyanaz a betű áll, a C' -ben van, így C' indexe C -ben legfeljebb q , ahonnan C' -nek legalább q^{k-1} eleme van. Így k vagy nem változik, vagy eggyel csökken. Ha az eredeti kód MDS-kód volt, és $k > 1$, akkor a rövidített is az marad, mert a $d = n - k + 1$ egyenlőségben a bal oldalon d csak nőhet, a jobb oldalon n eggyel csökken, k viszont legfeljebb eggyel csökkenhet, így a Singleton-korlát miatt egyik oldal sem változhat.

* **9.3.30. Kódok direkt szorzata.** Úgy, mint a kétdimenziós paritásellenőrzésnél, tetszőleges két (azonos ábécéjű) kód felhasználásával készíthetünk egy harmadik, jóval nagyobb távolságú kódot: előbb keresztirányban kódolunk az első kóddal, majd hosszirányban a másodikkal, vagy fordítva. Az így kapott kód a kiindulási *kódok direkt szorzata*. Ha az egyes kódok távolsága d_1 , illetve d_2 , akkor a direkt szorzatuk távolsága legalább $d_1 d_2$; valóban, ha két különböző kódszó valamely sorban különbözik, akkor ott legalább

d_1 helyen különbözik, és legalább d_2 ilyen sornak kell lennie, mert egyébként nem lehetne olyan oszlop, amelyben a két kódszó legalább d_2 helyen különbözik. Megmutatható, hogy lineáris kódok esetén a szorzatkód távolsága $d_1 d_2$,

Például a DVD-n az adatokat (egyebek közt) egy $[208, 192]_{256}$ és egy $[182, 172]_{256}$ rövidített Reed–Solomon-kód direkt szorzata védi, ennek távolsága $17 \cdot 11 = 187$, így nagyjából kétszer annyi munkával sokkal nagyobb távolságot kaptunk.

* **9.3.31. Kaszkád kódok.** Egy további kódótvöző eljárás a *kaszkád kód*. Tegyük fel, hogy egy kód betűi megfeleltethetők egy másik kód adott hosszúságú szavainak. Kódoljunk először az első kóddal, majd a kapott kódszó betűit kódoljuk a második kóddal. Ha az első kód távolsága d_1 , a másodiké d_2 , akkor a kaszkád kód távolsága legalább $d_1 d_2$, hiszen két különböző kódszó az első kódolás után legalább d_1 betűben, és ezek mindegyikének a kódja a második kódolás után legalább d_2 helyen különbözik.

A legegyszerűbb példa kaszkád kódra, amikor egy $[n, k]_{256}$ Reed–Solomon-kód után bájtontként paritásbitet képzünk, így k darab bájtól n darab bájtot, majd ezekből $9n$ bitet kapunk; itt $d_1 = n - k + 1$, $d_2 = 2$.

* **9.3.32. Adatátészövés.** Az átvitel során a hibák gyakran *hibacsomók*ban, idegen szóval *burstök*ben jelentkeznek. Bár például a Reed–Solomon-kódok, valamint a szorzatkódok és a kaszkád kódok is alkalmasak rövidebb hibacsomók javítására, a hosszabb hibacsomók „túlterhelik” a kódot, egyes részekben olyan sok a hiba, hogy nem tudjuk javítani. Ez ellen úgy védekezhünk, hogy a kódolás után az egyes blokkok adatait szétszórjuk: ez az *adatátészövés*. A legegyszerűbb esetben valahány adott hosszúságú blokkot sorfolytonosan helyezünk el egy mátrixban, majd az adatokat oszlopfolytonosan olvassuk ki onnan, de kódolás előtt pedig fordítva végrehajtva ezt, visszaállítjuk az eredeti sorrendet, ezzel az esetleges hibacsomókat szétszórjuk, és csak ez után végezzük a hibajavítást.

→ **9.3.33. Feladat [1].** Igaz-e, hogy egy t hibát javító kód

- (1) legalább $2t + 1$ hibát jelez;
- (2) legalább $2t$ hibát jelez;
- (3) legfeljebb $2t$ hibát jelez.

9.3.34. Feladat [7]. Legyen $a, b, c \in \mathbb{N}$ és $u, v \in \mathbb{F}_2^n$ úgy, hogy a $d(u, v)$ Hamming-távolságuk a . Hány olyan $w \in \mathbb{F}_2^n$ van, amelyre $d(u, w) = b$ és $d(v, w) = c$?

9.3.35. Feladat [7]. Tegyük fel, hogy $u, v, w \in \mathbb{F}_2^n$ Hamming-távolsága páronként c . Mutassuk meg, hogy c páros, és pontosan egy $z \in \mathbb{F}_2^n$ létezik, amelynek távolsága mindháromtól $c/2$.

→ **9.3.36. Feladat [5].** Tekintsük az alábbi bináris kódolást:

$$00 \mapsto 00000, \quad 01 \mapsto 01110, \quad 10 \mapsto 10101, \quad 11 \mapsto 11011.$$

- (1) Mekkora a 01110 és az 10101 kódszavak távolsága?
- (2) Mekkora a kód távolsága?
- (3) Mutassuk meg, hogy a kód csoportkód $\mathbb{Z}_2^5$ -ben.
- (4) Mennyi az 11011 kódszó súlya?
- (5) Mennyi a kód súlya?

(6) Adjuk meg a 00000 kódszótól legfeljebb 1 távolságra lévő $\mathbb{Z}_2^5$ -beli szavak halmazát.

(7) A 01000 szót mire dekódoljuk minimális távolságú dekódolással?

→ **9.3.37. Feladat [5].** Bináris blokk-kódot készítünk 3 hosszú üzenetekhez. Legalább mekkora legyen a kódszavak hossza, ha azt akarjuk, hogy a kód minimális távolságú dekódolással pontosan 1-hiba javító legyen?

→ **9.3.38. Feladat [5].** Létezik-e 3 távolságú tökéletes kód $\mathbb{F}_2^{147}$ -ben?

→ **9.3.39. Feladat [5].** Létezik-e pontosan 1-hibajavító kód $\mathbb{F}_2^{12}$ -ben?

→ **9.3.40. Feladat [5].** Az alábbi, $\mathbb{F}_2$ feletti kódok esetén állapítsuk meg a kód távolságát, hibajelző és hibajavító képességét, hogy lineáris-e, és a lineárisaknál adjunk meg a szokásos bázisban egy generátormátrixot és egy ellenőrző mátrixot:

(1) $(b_1, b_2, b_3) \mapsto (b_1, b_2, b_3, b_1, b_2, b_3);$

(2) $(b_1, b_2, b_3) \mapsto (b_1, b_2, b_3, b_1, b_2, b_3, b_1, b_2, b_3);$

(3) $(b_1, b_2, b_3) \mapsto (b_1, b_2, b_3, b_1 + b_2 + b_3);$

(4) $(b_1, b_2, b_3) \mapsto (b_1, b_2, b_3, b_1 + b_2 + b_3 + 1);$

(5) $(b_1, b_2, b_3) \mapsto (b_1, b_2, b_3, b_1, b_2 + b_3);$

(6) $(b_1, b_2, b_3) \mapsto (b_1, b_2, b_3, b_1, b_1 b_2 + (1 - b_1) b_3);$

(7) $(b_1, b_2, b_3) \mapsto (b_1, b_2, b_3, b_1 + b_2, b + 1 + b_3, b_2 + b_3);$

(8) $(b_1, b_2, b_3) \mapsto (b_1, b_2, b_3, b_1, b_1 + b_2, b_1 + b_2 + b_3);$

(9) $(b_1, b_2, b_3) \mapsto (b_1, b_2, b_3, b_1, 1 - b_2 b_3);$

(10) $(b_1, b_2, b_3) \mapsto (b_1, b_2, b_3, b_1, b_1 b_2, b_1 b_2 b_3).$

→ **9.3.41. Feladat [6].** Egy $[n, k]$ lineáris kód generátormátrixa a szokásos bázisban

(1)
$$\begin{pmatrix} \mathbb{E}_k \\ P \end{pmatrix}$$

blokkmátrix alakú, ahol $\mathbb{E}_k$ a $k \times k$ -as egységmátrix. Mutassuk meg, hogy a $(-P \ \mathbb{E}_{n-k})$ blokkmátrix (a szokásos bázisban) egy ellenőrző mátrixa a kódnak. Megfordítva, ha a $(-P \ \mathbb{E}_{n-k})$ blokkmátrix egy ellenőrző mátrixa a kódnak, akkor mutassuk meg, hogy az (1) blokkmátrix egy lehetséges generátormátrix.

→ **9.3.42. Feladat [4].** Legyen egy $\mathbb{F}_2$ feletti lineáris kód generátormátrixa

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

Adja meg a kód egy ellenőrző mátrixát. Mennyi a kódtávolság?

→ **9.3.43. Feladat [4].** Legyen egy $\mathbb{F}_2$ feletti lineáris kód generátormátrixa

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

Adjon meg egy olyan generátormátrixot, amelyhez ugyanez a kódtér tartozik, de a mátrixának első három sora egységmátrix. Adja meg a kód egy ellenőrző mátrixát. Milyen kódszó felel meg az 110 üzenetnek?

9.3.44. Feladat [4]. Legyen egy bináris kód generátormátrixa

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

Mennyi a kód elemeinek száma és a kódtávolság?

→ **9.3.45. Feladat [4].** Egy bináris kód ellenőrző mátrixa

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

Adja meg a kód egy generátormátrixát. Mi lesz az 10100011011 üzenet kódja? Mi volt a kódolt üzenet, ha a vett szó 111010010000011, és az átvitel során egy hiba lépett fel? Mi volt az eredeti üzenet, ha az adott generátormátrixszal történt a kódolás?

→ **9.3.46. Feladat [6].** Konstruáljon egy $[15, 6]_{16}$ Reed–Solomon-kódot.

* **9.3.47. Feladat [3].** Adja meg az 10010000101 bináris üzenet Hamming-kódját.

* **9.3.48. Feladat [4].** Az előző feladat kódszavában meghibásodik a megadott bit. Végezze el mindegyik esetben a hibajavítást és a dekódolást.

- (1) a 3. bit;
- (2) a 4. bit;
- (3) a 3. és 7. bit;
- (4) a 3., 5., és 6. bit;
- (5) a 4., 6. és 8. bit.

9.3.49. Feladat [5]. Mutassuk meg, hogy az $\mathbb{F}_q^n$ -beli bázisok száma

$$\frac{1}{n!} \prod_{k=0}^{n-1} (q^n - q^k).$$

9.3.50. Feladat [5]. Mutassuk meg, hogy a különböző $[n, k]_q$ lineáris kódok száma

$$\prod_{j=0}^k \frac{q^n - q^j}{q^k - q^j}.$$

9.3.51. További feladatok megoldásokkal. [29], [28]: 4.14–4.23, 4.26, 4.28–4.30, 4.60, 4.62–4.72, 4.75, 78–4.80, 4.4.82–4.86, 4.88–4.106.

9.3.52. További feladatok. [25]: V.1.3–V.1.28, V.2.1–V.2.25; 4.[57]: 4.0-5–4.0-6, 4.0-8, 4.0-16–4.0-18, 4.0-21, 0-25, 4.0-28; 4.[64]: 14.3.1–14.3.4, 14.4.1–14.4.5, 14.5.1–14.5.7, 4.14.6.1–14.6.11.

10

Algoritmusok

Ebben a fejezetben az algoritmuselmélet alapjaival foglalkozunk. Először a különböző gépmodelleket és azok ekvivalenciáit tárgyaljuk részletesen. Azután a kiszámíthatósággal kapcsolatos alapfogalmakkal foglalkozunk, és mutatunk néhány algoritmikusan megoldhatatlan problémát. Végül a nemdeterminisztikus modelleket tárgyaljuk nagyon röviden, de azért bebizonyítva az azok létjogosultságát igazoló tanú-tételt.

10.1 Számítási modellek

10.1.1. Számítási eljárás. Egy *számítási eljárás* alatt egy $C = (Q, Q_b, Q_k, f)$ négyest értünk, ahol Q az állapotok (tetszőleges) halmaza, a $Q_b \subset Q$ és $Q_k \subset Q$ részhalmazai a *bemeneti állapotok*, illetve *kimeneti állapotok* halmazai, az $f: Q \rightarrow Q$ *átmeneti függvény* pedig Q_k elemeit pontonként fixen hagyja, azaz $f(q) = q$, ha $q \in Q_k$. Minden $x \in Q_b$ bemeneti állapot definiál egy $q_0, q_1, q_2, \dots$ *számítási sorozatot* a

$$q_0 = x \quad \text{és} \quad q_{n+1} = f(q_n), \quad \text{ha} \quad n \geq 0$$

rekurzióval. Azt mondjuk, hogy az x bemenetre a számítás n lépésben *véget ér*, ha n a legkisebb olyan egész, amelyre $q_n \in Q_k$; ekkor $q_n = q_{n+1} = q_{n+2} = \dots$ a számítás *eredménye*. Előfordulhat, hogy egy számítás nem ér véget. A számítási eljárás fogalmát azért vezettük be, hogy a szimulálás fogalmát kellő általánosságban definiálhassuk.

10.1.2. Példa. Az euklideszi algoritmust a következőképpen formalizálhatjuk számítási eljárásként. Legyen $Q_k = \mathbb{Z}^1$, $Q_b = \mathbb{Z}^2$, $Q = (\mathbb{Z}^2 \times \{2, 3\}) \cup Q_b \cup Q_k$, és legyen

$$\begin{aligned} f(a, b) &= (a, b, 2), & f(a) &= a, \\ f(a, b, 2) &= a, & \text{ha } b = 0, & \text{és } f(a, b, 2) = (a, b, 3) \text{ egyébként,} \\ f(a, b, 3) &= (b, a \bmod b, 2); \end{aligned}$$

a kapcsolat az algoritmus leírásában használt jelölésekkel nyilvánvaló: a harmadik koordináta azt mutatja, hogy melyik lépésben vagyunk, a és b aktuális értéke pedig r_n , illetve r_{n+1} .

Ha a és b tetszőleges valós számok lehetnek, akkor számos bemenetre a számítás nem ér véget.

10.1.3. Szimulálás. Azt mondjuk, hogy a $C' = (Q', Q'_b, Q'_k, f')$ számítási eljárás a $C = (Q, Q_b, Q_k, f)$ számítási eljárást *szimulálja*, ha van olyan $g: Q_b \rightarrow Q'_b$ függvény, a *bemeneti kódolás*, olyan $h: Q' \rightarrow Q$ függvény, az *állapotdekódolás* és olyan $k: Q' \rightarrow \mathbb{N}^+$ függvény, hogy

- (1) ha $x \in Q_b$, akkor a C számítási eljárás pontosan akkor adja az y eredményt, ha van olyan $y' \in Q'_k$, hogy $g(x)$ bemenettel a C' számítási eljárás az y' eredményt adja, és $h(y') = y$;

- (2) ha $q' \in Q'$, akkor $f(h(q')) = h(f'^{k(q')}(q'))$, ahol $f'^{k(q')}$ azt jelenti, hogy az f' leképezést $k(q')$ -ször ismétljük, azaz a $q' \in Q'$ -nek megfelelő $h(q') \in Q$ állapotból ha egy lépést teszünk C -ben, az megfelel annak, hogy q' -ből $k(q')$ lépést teszünk C' -ben.

Nyilván bármely számítási eljárás szimulálja saját magát. Ha a C' számítási eljárás szimulálja a C számítási eljárást, a C'' számítási eljárás pedig szimulálja C' -t, akkor C'' szimulálja C -t.

10.1.4. Példa. A bővített euklideszi algoritmust a következőképpen formalizálhatjuk számítási eljárásaként: Legyen $Q_k = \mathbb{Z}^3$, $Q_b = \mathbb{Z}^2$, $Q = (\mathbb{Z}^7 \times \{2, 3.1, 3.2\}) \cup Q_b \cup Q_k$; a nyolcadik koordináta azt mutatja, hogy az algoritmus melyik lépésében vagyunk, és a harmadik lépés a 3.1 és 3.2 részlépésekre van felosztva. Legyen a leképezés

$$\begin{aligned} f(a, b) &= (a, 1, 0, b, 0, 1, 0, 2), & f(a, x, y) &= (a, x, y), \\ f(a, x, y, b, u, v, q, 2) &= (a, x, y), & \text{ha } b &= 0 \quad \text{és} \\ f(a, x, y, b, u, v, q, 2) &= (a, x, y, b, u, v, q, 3.1), & \text{ha } b &\neq 0, \\ f(a, x, y, b, u, v, q, 3.1) &= (a, x, y, b, u, v, \lfloor a/b \rfloor, 3.2), \\ f(a, x, y, b, u, v, q, 3.2) &= (b, u, v, a - qb, x - qu, y - qv, q, 2); \end{aligned}$$

az a, x, y, b, u, v, q mennyiségek rendre $r_n, x_n, y_n, r_{n+1}, x_{n+1}, y_{n+1}, q_{n+1}$ -nek felelnek meg.

Nyilván ez a számítási eljárás szimulálja az előző példában adott számítási eljárást, de megfordítva nem, hiszen vannak olyan bemenetek, amelyekre az előző eljárás ugyanazt az eredményt adja, de a most leírt eljárás nem, hiszen az előző eljárás csak a legnagyobb közös osztót adja vissza, ez az eljárás viszont x és y értékét is.

10.1.5. Szimulációk sebességének összehasonlítása. A szimuláció definíciójában szereplő k függvény megadja, hogy a szimulált eljárás egy lépését (a q' állapottól függően) a szimuláló eljárás hány lépésben szimulálja. Ha k azonosan 1, akkor azt mondjuk, hogy a szimuláció *valós idejű* (*real time*). Ha a k függvény korlátos, akkor úgy tekintjük, hogy a sebességkülönbség nem lényeges. Az alábbi definíció, amelybe a „konstans elhanyagolása” be van építve, az ilyen típusú lépésszám-összehasonlításokat teszi egyszerűen leírhatóvá.

10.1.6. Ordó. Legyen $f: \mathbb{N} \rightarrow \mathbb{R}$ egy számsorozat. Jelölje $O(f)$ (nagy ordó f , vagy $O(f(n))$, nagy ordó $f(n)$) mindazon $g: \mathbb{N} \rightarrow \mathbb{R}$ számsorozatok halmazát, amelyekre van olyan (g -től függő) $C \in \mathbb{R}^+$ konstans és $N \in \mathbb{N}$ index, hogy $|g(n)| \leq C|f(n)|$, ha $n \geq N$. Ha f és f^* , illetve g és g^* véges sok tag kivételével megegyeznek, akkor nyilván $g \in O(f)$ pontosan akkor teljesül, ha $g^* \in O(f^*)$ teljesül. Ezért a jelölést akkor is használni fogjuk, ha f vagy g (vagy mindkettő) véges sok indexre nincs értelmezve. (Ugyanezt a kapcsolatot úgy is szokás jelölni, hogy $g \preceq f$ vagy $f \succcurlyeq g$, illetve hogy $f \in \Omega(g)$, azaz $\Omega(g)$ mindazon $f: \mathbb{N} \rightarrow \mathbb{R}$ számsorozatok halmaza, amelyekhez van olyan $C \in \mathbb{R}^+$ és N , hogy ha $n \geq N$, akkor $C|f(n)| \geq |g(n)|$. Az $O(g)$ és $\Omega(g)$ halmazok metszetét $\Theta(g)$ jelöli; $f \in \Theta(g)$ helyett azt is szokás írni, hogy $f \asymp g$.) Gyakran pontatlanul $g \in O(f)$ helyett azt írják, hogy $g = O(f)$. Ha g egy legfeljebb k -ad fokú polinom, akkor $g(n) \in O(n^k)$, vagy pontatlanabban $g(n) = O(n^k)$.

→ **10.1.7. Feladat [3].** Mutassuk meg, hogy bármely számítási eljáráshoz végtelen sok olyan számítási eljárás létezik, amely őt szimulálni képes.

→ **10.1.8. Feladat [6].** Adjunk meg számítási eljárást a valós számokon végzett négy alapművelet és összehasonlítás segítségével az alábbi függvények értékének 2^{-n} -nél ($n \in \mathbb{N}$ rögzített) kisebb hibával való kiszámítására:

- (1) $x \mapsto \sqrt{x}$;
- (2) $(m, x) \mapsto \sqrt[m]{x}$, ahol $m \in \mathbb{N}^+$;
- (3) $x \mapsto \log x$;
- (4) $x \mapsto 2^x$.

° **10.1.9. Feladat [6].** Adjunk meg számítási eljárást e és π értékének 2^{-n} -nél ($n \in \mathbb{N}$ rögzített) kisebb hibával való kiszámítására.

10.1.10. Algoritmus. Több példát láttunk már algoritmusra, de az algoritmus fogalmát nem definiáltuk. Ez nem okoz problémát mindaddig, amíg olyan problémákkal nem kerülünk szembe, amelyeknek a megoldására nem találunk algoritmust. Ha ilyen problémára akadunk, felmerül, hogy van-e egyáltalán algoritmus az adott problémára. Ha meg akarjuk mutatni, hogy nincs, akkor definiálnunk kell, mit is értünk algoritmuson. Mivel több gyakorlati problémára nincs algoritmus, az ilyen „negatív” eredmények nagyon fontosak.

Olyan számítási eljárások érdekelnek bennünket, amelyek számítógépen szimulálhatók. Bizonyos számítási eljárások biztosan nem szimulálhatók számítógépen. Például valós számok lánctörtközelítéseinek meghatározására az euklideszi algoritmushoz nagyon hasonló számítási eljárás adható (lásd a 6.4.1 fejezetet), azonban számítógépen nem tudjuk szimulálni, hiszen valós számokat kellene ábrázolnunk, ami teljes pontossággal számítógépben nem lehetséges, mert kontinuum sok valós szám van. Már két valós szám összehasonlítása is gondot okozna: hiába olvassuk sorban a számok tizedes (vagy bináris stb.) jegyeit, bár az előbb-utóbb kiderül, ha a két szám nem egyenlő, az egyetlen lépésben sem derül ki, hogy a számok egyenlők.

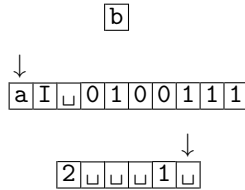
Ha átgondoljuk, hogy mit is kell algoritmus alatt értenünk, amit gépiesen végre tudunk hajtani, például arra juthatunk, hogy papírokra ceruzával jeleket írhatunk, azok közül egyeseket kiradírozva felülírhatunk, vagy a jelsorozat elejére vagy végére újabb jeleket írhatunk. Mivel a jeleket sorfolytonosan olvassuk és írjuk, feltehetjük, hogy adott számú papírszalaggal dolgozunk, amelyek azonban akármennyire meghosszabbíthatók mindkét végükön, de mindig csak egy véges rész az, amin jelek vannak. Eközben véges sok (korlátos számú) dolgot fejben tarthatunk, így nem lényeges megszorítás, ha feltesszük, hogy egyszerre csak egy jelet olvasunk és írunk minden szalagon. Látszólag szükségünk lenne még beszúrásokra is, ez azonban radírozás és arrébb írás segítségével megoldható. Úgy tűnhet, hogy növelné lehetőségeinket, ha „két dimenzióban” használnánk a papírt; ez megfelelné annak, hogy végtelen sok papírszalagunk van, de persze minden időpontban csak véges sok szalagra van írva valami. Azonban egy „kockás” papírlapot egy pontból kiindulva és csigavonalban haladva egy (csak egyik irányban végtelen!) szalaggá vághatunk fel. Természetesen igyekszünk hatékony, de mégis minél egyszerűbb modellt választani, ugyanúgy mint ahogy axiómarendszerek választásánál is erre törekedtünk. Így arra a következtetésre juthatunk, hogy „algoritmus” formájában azok a számítási eljárások adhatók meg, amelyek úgynevezett Turing-gépen szimulálhatók:

10.1.11. Turing-gépek. Egy Turing-gép $k \geq 1$ számú szalagból és egy vezérlőegységből áll. A szalagok mindkét irányban végtelen sok mezőre vannak osztva. Minden mezőn

egy-egy betű van egy véges ábécéből, úgy, hogy véges sok mező kivételével minden mezőn a $\sqcup$ *szóköz* (vagy *üres*) jel áll:

$$\dots \boxed{\sqcup} \boxed{\sqcup} \boxed{a} \boxed{I} \boxed{\sqcup} \boxed{0} \boxed{1} \boxed{0} \boxed{\sqcup} \boxed{\sqcup} \dots$$

Az egyszerűség kedvéért a továbbiakban a szalag jobb és bal szélén álló végtelen sok üres mezőt nem jelezzük. A vezérlőegység véges sok, úgynevezett „belső állapot” egyikében lehet. A belső állapotok között van egy s kezdő („start”) állapot és egy h befejező („halt”) állapot. Minden szalaghoz tartozik egy író-olvasó fej. Az alábbi példában két szalag van, és a vezérlőegység a b belső állapotban van:



Ugyanez egyszerűbb jelöléssel:

$$\begin{array}{c} b \\ \downarrow \\ aI_{\sqcup}0100111 \\ \downarrow \\ 2_{\sqcup\sqcup\sqcup}1_{\sqcup} \end{array}$$

Kezdetben a vezérlőegység az s kezdő állapotban van. Minden lépésben minden fej elolvassa azt a jelet, amely éppen a fej alatt van, majd három dolog történik az éppen leolvasott jelektől és a vezérlőegység belső állapotától függően: minden fej felülírja az olvasott jelet (lehet, hogy ugyanarra, ami volt), minden fej egymástól függetlenül elmozdul egy mezővel jobbra vagy balra, vagy helyben marad, és a vezérlőegység átmegy egy másik belső állapotba (lehet, hogy ugyanabba, amelyben volt). Ha a gép a h befejező állapotba jut, a gép megáll (anélkül hogy bármit is tenne a szalagokkal).

Matematikailag egy T Turing-gép egy $T = (B, A, \varphi)$ hármas, ahol az A , B véges halmazok a *szalagábécé* illetve a *belső állapotok* halmaza, $\sqcup \in A$, $s, h \in B$ és

$$\varphi: B \times A^k \rightarrow B \times A^k \times \{<, =, >\}^k$$

egy tetszőleges leképezés. A $<$, $>$, illetve $=$ jelek az „*irányjelek*”: azt jelentik, hogy az adott szalagon a fej balra lép, jobbra lép, illetve helyben marad. Ha nagyon precízez akarunk lenni, akkor a $k \in \mathbb{N}^+$ számot (a szalagok számát), a $\sqcup$ szóköz jelet és az s, h kezdő és befejező állapotokat is feltüntethetjük a jelölésben: $T = (k, B, A, \sqcup, s, h, \varphi)$. Az, hogy

$$\varphi: (b, a_1, \dots, a_k) \mapsto (b', a'_1, \dots, a'_k, c_1, \dots, c_k),$$

ahol $b, b' \in B$, és ha $1 \leq i \leq k$, akkor $a_i, a'_i \in A$, $c_i \in \{<, =, >\}$, azt jelenti, hogy a gép egy *lépése* a következő: ha a t időpontban b a belső állapota és az egyes szalagokról az $a_1, \dots, a_k$ betűket olvassa, akkor a $t + 1$ időpontra a b' belső állapotba megy át, az olvasott betűk helyére az $a'_1, \dots, a'_k$ betűket írja, és az i -edik szalagon a fej balra lép,

jobbba lép, illetve helyben marad, attól függően, hogy c_i a $<$, a $>$ vagy az $=$ jel. Mivel a Turing-gép a h végállapotban úgysem csinál semmit, megállapodhatunk abban, hogy

$$\varphi: (h, a_1, \dots, a_k) \mapsto (h, a_1, \dots, a_k, =, \dots, =).$$

10.1.12. Turing-gép mint számítási eljárás; bemenet és kimenet. Az előző definíció jelöléseivel egy Turing-gép aktuális állapotát egy

$$q = (b, \alpha_1, \beta_1, \alpha_2, \beta_2, \dots, \alpha_k, \beta_k) \in B \times (A^*)^{2k}$$

sorozat írja le, ahol $\alpha_i \in A^*$ szó az i -edik szalagon szereplő betűk balról jobbra felsorolva az első nem üres jellel kezdve és a fej alatti betűvel végezve, a $\beta_i \in A^*$ szó pedig az i -edik szalagon jobbról balra olvasott betűk az első nem üres jellel kezdve és a fejtől jobbra álló betűvel végezve; mindkettő lehet üres. A számítási eljárás bemeneti állapotai azok az állapotok, amelyekre $b = s$, a kimeneti állapotai pedig azok az állapotok, amelyekre $b = h$. (Ezek a speciális belső állapotok pontosan azért kellenek, hogy a bemenet és a kimenet ne függjön a belső állapottól.) Könnyű megadni az állapotok halmazán a Turing-gép működésének megfelelő leképezést három függvény segítségével: az egyik egy szó utolsó betűjét adja vissza, a másik a szó többi részét, a harmadik pedig a szó végére ír egy adott betűt. Mindig feltesszük, hogy az induláskor minden β_i az üres szó, tehát az α_i -k a bemeneti szavak, a fejek a bemenet jobb szélén állnak. Ha azonban semmit sem tudunk a bemeneti szavakról, akkor például még azt a egyszerű feladatot sem tudjuk Turing-géppel megoldani, hogy töröljük le a szalagokat, hiszen akármeddig lépkedünk balra, nem tudjuk, van-e még valami ettől is balra, így soha nem állhatunk meg. Valamit tehát még tudnunk kell a *bemenetről*. Legegyszerűbb feltenni, hogy $\alpha_i \in A_0^*$, ahol $A_0 = A \setminus \{\sqcup\}$, azaz, hogy a bemeneti szavak nem tartalmaznak üres jelet. Ha mást nem mondunk, ezzel a feltevéssel élünk, bár kevesebb is elég, például hogy legfeljebb adott számú $\sqcup$ jel van a bemenetben egymás mellett, vagy a bemenet bal szélét valamely speciális sorozat jelzi stb. Fontos, hogy csak a bemenetnél élünk ilyen erős megszorítással, a számítás közben nem. A kimenetre hasonló megállapodások érvényesek, mint a bemenetre: a megálláskor az α_i szavakat, azaz a fejektől balra lévő részt tekintjük *kimenetnek*, a β_i szavakat pedig „szemétnek”, sőt, ha mást nem mondunk, csak az α_i szavak végét, az utolsó üres jel utáni betűket (azaz α_i leghosszabb szuffixét, amely nem tartalmaz üres jelet) tekintjük kimenetnek, a többi része α_i -nek „szemét”. Ha Turing-gépeket össze akarunk kapcsolni, a „szemét” zavaró lehet. Meg fogjuk mutatni, hogyan lehet tőle megszabadulni.

Ha csak $m < k$ bemeneti szóról beszélünk, akkor feltesszük, hogy az első m szalagra vannak felírva, a többi szalag az induláskor üres. Speciálisan, ha csak egy szó a bemenet, az az első szalagon van, ez a *szabványos bemenet* (*standard input*). A *bemenet hosszán* a bemeneti szavak hosszának összegét értjük. Hasonlóan, ha $n < k$ kimeneti szóról beszélünk, akkor feltesszük, hogy az utolsó n szalagra vannak felírva a kimenetkor, a többi szalag tartalma „szemét”. Speciálisan, ha csak egy kimeneti szóról beszélünk, akkor az az utolsó szalagon van, ez a *szabványos kimenet* (*standard output*). Néha az utolsó előtti szalagot másik kimeneti szalagként, mint *szabványos hiba* (*standard error*) szalagot használjuk. A *kimenet hosszán* a kimeneti szavak hosszának összegét értjük.

A Turing-gépeket A_0 elemeinek száma szerint szokás elnevezni: ha A_0 egyelemű, akkor *unáris*, ha kételemű, akkor *bináris* stb. gépről beszélünk.

10.1.13. Megjegyzés. A Turing-gépeknek nagyon sok, minden lényeges szempontból ekvivalens definíciója található a könyvekben. Gyakran a bemenet bal széléről indulnak (a mi megállapodásunkkal egyszerűbb az összekapcsolás: két Turing-gépet minden további nélkül „egymás után” működtethetünk, a második bemenete az első kimenete, és a második kezdő állapota az első végállapota); a szalagok csak egyik irányban végtelenek; két, sőt csak egy szalag van; csak unáris a gép; bizonyos szalagokról csak olvasni lehet, másokra csak írni lehet (de legalább egy szalag írható-olvasható); több fej van egy szalagon, és „érzékelik”, ha ugyanott állnak; stb. Nyilván, ha „többet tud” az egyik gép, például több szalag van, bővebb az ábécé stb., akkor triviálisan szimulálható rajta a másik. A másik irány az érdekes. Néhány fontos esetet részletesen tárgyalunk.

10.1.14. Példák. (1) Az a Turing-gép, amelynek csak az $s = h$ belső állapota van, nem csinál semmit, kimenete a bemenet.

(2) Az a Turing-gép, amelynek csak az $s \neq h$ belső állapotai vannak, mindig üres jelet ír és balra lép minden szalagon, és mindig az s állapotban marad, törli a szalagokat, de soha nem áll meg.

(3) Az az egyszalagos Turing-gép, amelynek csak az $s \neq h$ belső állapotai vannak, ha nem üres jelet olvas, akkor balra lép, ha pedig üres jelet olvas, akkor jobbra lép és megáll, továbbá mindig azt írja vissza, amit olvasott, megkeresi a bemenet bal szélső betűjét. Hasonlóan kereshetjük meg egy adott betű balról legelső előfordulását.

(4) Egy egyszalagos gépen azt, hogy **abrakadabra**, kiírathatjuk a szalagra 12 állapottal (üres bemenettel, balról jobbra).

(5) Könnyű megadni olyan kétszalagos gépet, amely $a_1 a_2 \dots a_n$ bemenetre kimenetként az $a_n a_{n-1} \dots a_1$ szót adja: elmegyünk a bemenet bal széléig, majd visszafelé haladva a betűket egyenként a második szalagra másoljuk. Hasonlóan könnyű megadni olyan kétszalagos gépet, amely $a_1 a_2 \dots a_n$ bemenetre $a_1 a_2 \dots a_n a_n a_{n-1} \dots a_1$, $a_1 a_2 \dots a_n a_1 a_2 \dots a_n$, illetve $a_1 a_1 a_2 a_2 \dots a_n a_n$ kimenetet ad.

(6) Bináris gépen $\{\square, 0, 1\}$ jelkészlettel, három szalaggal könnyen megadható olyan gép, amely kettes számrendszerben felírt számokat összead. Jelentse az s kezdő állapot azt, hogy nincs átvitel, a c „carry” állapot pedig, hogy van átvitel. Leolvasva a két utolsó számjegyet, az összeg megfelelő számjegyét kiírjuk a harmadik szalagra, balra lépünk, és az átvitelnek megfelelő állapotba megyünk át. Ha valamelyik szalagon elfogyott a szám, akkor úgy viselkedünk, mintha onnan nullát olvasnánk. Ha mindkét szalagon elfogyott a szám, akkor átvitel esetén 1-et írunk, egyébként üres jelet. Ezután az eredmény jobb szélére megyünk: egy r „vissza” állapotba megyünk át, és jobbra lépünk. Mindaddig ebben az állapotban maradunk és jobbra lépünk, amíg az eredmény szalagon nem üres jelet olvasunk. Üres jelnél balra lépünk, és h állapotba megyünk át. Hasonlóan adható meg három vagy négy szalaggal olyan gép, amely kettes számrendszerben felírt számokat összehasonlít, kivon (ha az eredmény negatív lenne, nullát ad vissza), szoroz, maradékosan oszt, euklideszi algoritmust hajt végre stb.

→ **10.1.15. Feladat [3].** Melyek azok a függvények, amelyek kételemű ábécével, két belső állapottal Turing-gépen kiszámíthatóak?

→ **10.1.16. Feladat [6].** Konstruáljunk az alábbi $f \in \mathbb{N} \rightarrow \mathbb{N}$, illetve $f \in \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ (parciális) függvényeket kiszámító Turing-gépet. Ha a függvény nincs értelmezve, például azért, mert az eredmény nem lenne a megadott halmazban, hibajelzést adhatunk, vagy a gép „elszáll”.

- (1) $f(n) = \text{sgn}(n)$;
- (2) $f(n) = \lfloor 1/n \rfloor$;
- (3) $f(n) = \lfloor n/2 \rfloor$;
- (4) $f(m, n) = m - n$;
- (5) $f(m, n) = m/n$;
- (6) $f(m, n) = (4 - m)/n^2$.

→ **10.1.17. Feladat [7].** Konstruáljunk az alábbi $f \in \mathbb{N} \rightarrow \mathbb{N}$, illetve $f \in \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ (parciális) függvényeket kiszámító Turing-gépet. Ha a függvény nincs értelmezve, például azért, mert az eredmény nem lenne a megadott halmazban, hibajelzést adhatunk, vagy a gép „elszáll”.

- (1) $f(n) = \max\{0, n - 1\}$;
- (2) $f(n) = 1 - \text{sgn}(n)$;
- (3) $f(n) = 1/(n - 2)$;
- (4) f véges sok helyen definiált függvény;
- (5) $f(m, n) = m/(2 - n)$.

10.1.18. Feladat [7]. Konstruáljunk az alábbi $f: \mathbb{N} \rightarrow \mathbb{N}$, illetve $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ függvényeket kiszámító Turing-gépet:

- (1) $f(m, n) = |m - n|$;
- (2) $f(m, n) = \max\{m, n\}$;
- (3) $f(m, n) = \min\{m, n\}$;
- (4) $f(m, n) = \max\{0, m - n\}$;
- (5) $f(m, n) = m^n$;
- (6) $f(n) = n!$.

10.1.19. Feladat [9]. Konstruáljunk az alábbi $f \in \mathbb{N} \rightarrow \mathbb{N}$, illetve $f \in \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ (parciális) függvényeket kiszámító Turing-gépet. Ha a függvény nincs értelmezve, például azért, mert az eredmény nem lenne a megadott halmazban, hibajelzést adhatunk, vagy a gép „elszáll”.

- (1) $f(m, n) = \lfloor m/n \rfloor$;
- (2) $f(m, n) = m \bmod n$;
- (3) $f(n)$ az n -edik Fibonacci-szám;
- (4) $f(n)$ az n osztóinak száma;
- (5) $f(n)$ az n osztóinak összege;
- (6) $f(n)$ az n prímosztóinak száma;
- (7) $f(n)$ az n -nél nem nagyobb prímek száma;
- (8) $f(m, n)$ az m és n legnagyobb közös osztója;
- (9) $f(m, n)$ az m és n legkisebb közös többszöröse;
- (10) $f(n)$ az n -edik prímszám;
- (11) $f(n)$ az n legnagyobb prímosztója;

(12) $f(m, n)$ az m -edik prímszám kitevője n prímtényezős felbontásában;

(13) $f(n) = \lfloor n\sqrt{2} \rfloor$;

(14) $f(m, n) = \lfloor \sqrt[n]{n} \rfloor$;

(15) $f(m, n) = \sqrt[n]{n}$;

(16) $f(m, n) = \binom{n}{m}$.

◦ **10.1.20. Feladat** [9]. Konstruáljunk az alábbi $f: \mathbb{N} \rightarrow \mathbb{N}$ függvényeket kiszámító Turing-gépet (e a természetes alapú logaritmus alapszáma):

(1) $f(n) = \lfloor en \rfloor$;

(2) $f(n) = \lfloor e^n \rfloor$;

(3) $f(n)$ a $\sqrt{2}$ tizedestört előállításában az n -edik jegy;

(4) $f(n)$ az e tizedestört előállításában az n -edik jegy;

(5) $f(n)$ a π tizedestört előállításában az n -edik jegy.

10.1.21. Turing-gép szimulálása csökkentett jelkészlettel. Legyen $T = (B, A, \varphi)$ egy Turing-gép, és A' egy tetszőleges véges ábécé, amelynek legalább két eleme van. Ekkor T szimulálható olyan T' Turing-géppel, amelynek ábécéje A' . Ha egy számítás során a T gép t lépést tesz, akkor a T' gép $O(t)$ lépést tesz.

A konstrukció azt is megmutatja majd, hogyan emlékezhet egy Turing-gép belső állapotai segítségével arra, hogy véges sok esetből melyik állt fenn.

Bizonyítás. Az A elemeit alkalmas n -re A' elemeiből alkotott n -esekkel kódoljuk úgy, hogy A üres jelének kódja az A' üres jeléből alkotott n -es legyen. Ha A' -nek legalább három eleme van, akkor a kódolást lehet úgy is választani, hogy más A -beli jel kódja ne tartalmazza az üres jelet, csak az üres jelé.

A T' konstrukcióját az $A = \{0, 1, 2, 3\}$ és $A' = \{\sqcup, \sqcup, \sqcup, \sqcup\}$ esetben fogjuk részletesen bemutatni, de ebből világos lesz az általános eset is. Feltéve, hogy A -ban a 0 az üres jel, legyen $n = 2$, és válasszuk a $0 \mapsto \sqcup\sqcup$, $1 \mapsto \sqcup\sqcup$, $2 \mapsto \sqcup\sqcup$, $3 \mapsto \sqcup\sqcup$ kódolást. Minden $h \neq b \in B$ belső állapotához T -nek a T' gépnek a $b, b_{\sqcup}, b_{\sqcup}$, a b_i , $i \in A$, valamint a $b_{i,c}$, $i \in A$ és $c \in \{<, >\}$ belső állapotai tartoznak; azért többszöröztük meg minden $b \neq h$ esetén a belső állapotokat, hogy ezek segítségével „emlékezzünk” dolgokra. Ha a T' gép a b belső állapotban van, akkor mindig egy kódszó jobb szélén áll. Elolvasva a kódszó jobb oldali betűjét, attól függően, hogy mit olvasott, a $b_{\sqcup}$ vagy a $b_{\sqcup}$ állapotba megy át (ezzel megjegyezve, hogy mit olvasott), és balra lép. Most attól függően, hogy itt mit olvasott, a b_i állapotok valamelyikébe megy át, ezzel megjegyezve, hogy milyen betű kódját olvasta a két lépésben, a szalagra i^* kódjának bal oldali betűjét írja, és jobbra lép; itt nyilván $i = 0$, ha a $b_{\sqcup}$ állapotban voltunk, és $\sqcup$ betűt olvastunk, $i = 1$, ha $b_{\sqcup}$ állapotban voltunk, és $\sqcup$ -t olvastunk stb., és $\varphi(b, i) = (b^*, i^*, c)$. A b_i állapotban, ha c az $=$ jel, akkor a szalagra i^* kódjának második betűjét írjuk, átmegyünk a b^* állapotba, és helyben maradunk. Egyébként a szalagra i^* kódjának második betűjét írjuk, az i és c értékének megfelelő $b_{i,c}$ állapotba megyünk át, és c értékének megfelelően balra vagy jobbra mozgunk. A $b_{i,c}$ állapotban azt írjuk a szalagra, amit olvastunk, a c értékének megfelelően balra vagy jobbra mozgunk, és a b^* állapotba megyünk át. A T gép bármely lépését T' legfeljebb 4 lépésben szimulálja. Az általános esetben, amikor A betűit A' betűiből képzett n hosszú szavaknak feleltetjük meg, minden lépést legfeljebb $3n - 2$ lépésben tudunk szimulálni. $\square$

10.1.22. Feladat [7]. Legyen $A = \{a_1, a_2, \dots, a_n\}$ egy legalább két betűből álló ábécé. Kódoljuk A betűit a $\{\sqcup, \text{I}\}$ ábécé betűivel úgy, hogy a_i kódja egy i hosszú $\sqcup$ sorozat, amely előtt és után egy-egy I áll. Szimuláljunk egy A szalagábécével működő egyszalagos Turing-gépet ezzel a kódolással.

10.1.23. Példák. Egyszalagos gépen jóval nehezebbnek tűnik dolgozni, mint többszalagos gépen. Nézzünk néhány példát.

(1) Tetszőleges $a_1 a_2 \dots a_n$ bemenetből előállítjuk az $a_1 a_1 a_2 a_2 \dots a_n a_n$ kimenetet. A jobb szélről indulva, az $a_1 a_2 \dots a_{n-1}$ részt balra toljuk: $\sqcup$ jellel felülírjuk a_{n-1} -et, majd a_{n-1} -gyel felülírjuk a_{n-2} -t stb., egészen addig, míg a felülírt jel $\sqcup$ nem lesz, tehát amíg a bal szélét el nem érjük. Eközben mindig csak egy betűre kell „emlékeznünk”. Most visszamegyünk (az első $\sqcup$ jeltől jobbra álló) a_n -ig, balra lépünk, és felülírjuk a_n -nel a $\sqcup$ jelet. Ugyanígy folytatjuk tovább: a_{n-2} -t felülírjuk $\sqcup$ -zel, a_{n-2} -vel felülírjuk a_{n-3} -at, stb.; Ha már nincs mit megduplázni, akkor a jobb szélre megyünk. Hasonlóan állíthatunk elő $a_1 a_1 a_1 a_2 a_2 a_2 \dots a_n a_n a_n$, $a_1 \sqcup a_2 \sqcup \dots a_n \sqcup$, $a_1 \sqcup \sqcup a_2 \sqcup \sqcup \dots a_n \sqcup \sqcup$ stb. kimenetet.

(2) Tetszőleges $a_1 a_2 \dots a_n$ bemenetből előállítjuk az $a_1 a_2 \dots a_n a_n a_{n-1} \dots a_1$ kimenetet. A program lényege, hogy amikor már a szalagon $a_1 a_2 \dots a_n a_n a_{n-1} \dots a_{k+1}$ van, és az a_k jelen állunk, azt felülírjuk $\sqcup$ -zel, jobbra lépünk, amíg $\sqcup$ jelhez nem érünk, azt felülírjuk a_k -val, majd balra lépünk, amíg szóköz jelhez nem érünk, azt visszaírjuk a_k -ra, végül egyet balra lépünk, és a_{k-1} -gyel folytatjuk, ha az nem $\sqcup$, mert akkor végeztünk, csak a jobb szélre kell menni.

(3) Tetszőleges $a_1 a_2 \dots a_n$ bemenetből hasonlóan állíthatjuk elő az $a_n a_{n-1} \dots a_1$ kimenetet, csak nem állítjuk vissza, amit lemásoltunk, és a mindenkor a_k leolvasása előtt balra lépünk, és megjegyezzük, hogy van-e még valami, mert akkor folytatni kell a_{k-1} -gyel, visszatéréskor pedig a $\sqcup$ jelek utáni első nem $\sqcup$ jelet keressük.

(4) A $\{\sqcup, 0, 1\}$ ábécével egy n számú 1 jelet tartalmazó sorozatból állítsuk elő n bináris alakját. Ha $n = 0$, a bemenet üres, a kimenet is üres, készen vagyunk. Egyébként az általános lépés a következő: egy $\sqcup$ jelen állunk, ettől balra vannak a maradék – még át nem alakított – egyesek, jobbra a keresett bináris szám már előállított vége. Az egyesek közül a jobb szélsőt töröljük (hogy helyet csináljunk a következő számjegynek), végiglépünk az egyeseken, meghatározva, hogy páros sok volt-e. Ha igen, egy egyest visszaírunk a bal szélre, ha páratlan volt, akkor nem: ezzel a páratlan esetben tulajdonképpen levonunk egyet. Most páros sok egyes van. Visszalépünk az egyesek jobb szélére: ha $\sqcup$ jelhez érünk, azt átlépve, leírjuk a konvertált alak következő számjegyét: ez természetesen attól függően 0 vagy 1 , hogy páros vagy páratlan sok egyes volt. Megnézzük, hogy van-e még egyes: ha nincs, készen vagyunk. Ha van, megfelezzük a számukat: balra lépve mindig egyet törölünk, egyet meghagyunk, majd visszafelé jövet a „kiritkített” sorozatot „tömörítjük”: a már „tömörített” rész bal szélső egyesén állva azt töröljük, ellépünk a „tömörített” rész jobb szélé mellett álló $\sqcup$ jelig, és felülírjuk egy egyessel. Ha ettől jobbra $\sqcup$ áll, készen vagyunk, egyébként visszamegyünk a „tömörített” rész bal szélére, és és folytatjuk.

(5) Az előző konverzió fordítottját lényegében az egész eljárás megfordításával végezhetjük. Az egyesek számát duplázhatjuk például (1) szerint, de most a másik szélről indulva és ellenkező irányba dolgozva, hogy ne tegyük tönkre a konverzió részeredményét.

(6) Négyzetre emelés: a $\{\sqcup, \text{I}\}$ ábécével egy n darab I jelet tartalmazó sorozathoz állítsunk elő egy n^2 darab I jelet tartalmazó sorozatot. Ha $n = 0$, készen vagyunk. Egyébként először megduplázuk a sorozatot, a két példányt egy $\sqcup$ jel fogja elválasztani: Írjunk

a jobb szélső I jel jobb oldalán lévő $\sqcup$ jeltől jobbra egy I-t, ez lesz az „őrszem”. A sorozatot alkotó I-eket a jobb szélről egyesével töröljük, és átírjuk a sorozat bal szélé melletti $\sqcup$ jeltől jobbra. Ezután visszaállítjuk az eredeti sorozatot, tudva, hogy mindkét szélén egy-egy $\sqcup$ jel van. Most már törölhető az őrszem, a duplázást befejeztük. A továbbiakban nem lényeges, hogy a két sorozatunk egyforma hosszú. Nevezzük a bal oldalt szorzandónak, a jobb oldalt szorzónak. A szorzatot a szorzandótól balra fogjuk előállítani, a kettőt egy $\sqcup$ jel választja el. Minden lépésben, a szorzandó jobb széléről törölve egy I-t, azt átvisszük a szorzat bal szélére. Ha a szorzandó elfogyott, visszaállítjuk, most a szorzó szolgál őrszemként. Ezután a szorzó jobb széléről törölünk egy I-t. Ha a szorzó elfogyott, töröljük a szorzandót, és készen vagyunk.

(7) Négyzetgyökvonás: a $\{\sqcup, I\}$ ábécével, egy n darab I jelet tartalmazó sorozathoz állítsunk elő egy $\lfloor \sqrt{n} \rfloor$ számú I jelet tartalmazó sorozatot. Ha $n = 0$, készen vagyunk. Egyébként az n számú I-től balra, egy $\sqcup$ jellel elválasztva, írunk egy I-t. Ez lesz a kezdő konfiguráció, az általános esetben itt k darab I áll, ahol $k^2 \leq n$. Egy ciklusban kipróbáljuk, ez k helyett $k + 1$ -re is teljesül-e? Először – balról hozzáírva egy I-t – eggyel növeljük k -t, majd a (6)-ban leírtak szerint eljárva, a k darab I mellé, egy $\sqcup$ jellel elválasztva, újabb k darab I-t írunk. Ezután, úgy mint (6)-ban, „ k -t négyzetre emeljük”, és k^2 -et összehasonlítjuk n -el: mindkét sorozat bal széléről egyenként töröljük az I-eket. Ha n fogyna el előbb, akkor k már túl nagy, és készen vagyunk, k^2 maradékát töröljük, k -t eggyel csökkentjük, és megállunk. Egyébként n -et visszaállítjuk, és k növelésétől folytatjuk az eljárást.

10.1.24. Szavak kódolása számmá és vissza. Sokszor szükség van arra, hogy egy Turing-gép bemeneti szavait számnak tekintsük. Ilyenkor mindig feltesszük, hogy a gép A ábécéje a $\{0, 1, \dots, r - 1\}$ számjegyekből áll, és 0 az üres jel. Egy A^* -beli $\alpha = a_n a_{n-1} \dots a_0$ bemeneti szó vagy az üres szó, vagy nem 0-val kezdődik, és r alapú számrendszerben az $|\alpha|_r = \sum_{i=0}^n a_i r^i$ számot reprezentálja. Az $\alpha \mapsto |\alpha|_r$ leképezés kölcsönösen egyértelműen képezi le A^* nem 0-val kezdődő szavait $\mathbb{N}$ -re. Ha csak A_0^* -beli szavakat akarunk számmá kódolni, akkor az $\alpha \mapsto |\alpha|_{r-1}$ leképezést használhatjuk, ahol természetesen $\alpha = a_n a_{n-1} \dots a_0$ esetén $|\alpha|_{r-1} = \sum_{i=0}^n a_i (r - 1)^i$, de itt a jegyek között már $r - 1$ is szerepel, annak ellenére, hogy $r - 1$ alapú számrendszert használunk. Az $\alpha \mapsto |\alpha|_{r-1}$ leképezés kölcsönösen egyértelműen képezi le A_0^* -ot $\mathbb{N}$ -re, ami indukcióval könnyen belátható. Például $r = 3$ esetén $\mathbb{N}^+$ elemeinek ebben az ábrázolásban rendre az 1, 2, 11, 12, 21, 22, 111, 112 stb. szavak felelnek meg. Ennek a számábrázolásnak az az előnye, hogy nincs benne 0, ami az üres jel is. Például egy n darab egyesből álló α szóra $|\alpha|_1 = |\alpha| = n$, ezért egy ilyen szót az n szám *unáris kódjának* nevezzük. Egy unáris kódban felírt n szám Turing-gép általi konvertálása egy $\alpha \in A_0^*$ szóvá, amire $|\alpha|_{r-1} = n$ vagy fordítva, hasonlóan végezhető, mint a példák között leírt unáris-bináris konverzió. Ugyancsak hasonlóan végezhető egy unáris kódban felírt szám konvertálása egy $\alpha \in A^*$ szóvá, ha tudunk annyit a szóról, hogy nem okoz gondot a bal illetve jobb szélének a megtalálása, például ismerünk valamilyen korlátot az α -ban egymás mellett lévő nullák számára.

10.1.25. Turing-gép szimulálása egy szalaggal. Legyen $T = (B, A, \varphi)$ egy Turing-gép k szalaggal. Ekkor T szimulálható olyan egyszalagos S Turing-géppel, amelynek ábécéje szintén A . Ha egy számítás során a T gép t lépést tesz, akkor az S gép $2kt(2t+3) = O(t^2)$ lépést tesz.

Bizonyítás. Az S gép mezőit $2k$ darab szomszédos mezőből álló csoportokra osztjuk. Az induláskor a fej egy ilyen mezőcsoport jobb szélén áll. Ezen mezőcsoportba írt

$$a_1 a_2 \dots a_k f_1 f_2 \dots f_k$$

betűkből $a_1, a_2, \dots, a_k$ rendre azon mezők tartalma, amelyeken induláskor a T gép első, második stb. szalagján a fejek állnak. Az ettől balra álló mezőcsoport első k betűje a T gép szalagjain a fejtől balra, közvetlenül mellette álló betűket tartalmazza stb. Szükség van annak jelzésére is, hogy a szimuláció során hol állnak T szalagjain a fejek. Az S szalagján egy-egy mezőcsoport $f_1, f_2, \dots, f_k$ betűi ezt adják meg: ha a T gép i -edik szalagján a mezőcsoportban szereplő a_i betűn áll a fej, akkor f_i nem az üres jel, egyébként az üres jel. Kezdetben tehát az S gép szalagján azon mezőcsoport $f_1, f_2, \dots, f_k$ mezői, amelyeknek a bal szélén a fej áll, mind nem üresek, az összes többi mezőcsoport $f_1, f_2, \dots, f_k$ mezői pedig mind üresek. A T gép egy lépésének szimulálása annak a $2k$ hosszú mezőcsoportnak a jobb széléről indul, amelyben a leginkább jobbra lévő fej van. A szimuláció során S „emlékszik” arra, hogy T milyen állapotban van, és arra is, hogy egy mezőcsoport melyik mezőjén áll. Balra lépkedve megkeresi minden szalaghoz a fejet, és „megjegyzi” a megfelelő szalagjelet is. Mikor minden fejet megtalált, tudja, mit kell tenni: mit írjon a megfelelő mezőkbe, merre mozgítsa a fejeket, és melyik állapotba menjen át. Jobbra visszafelé haladva a megfelelő helyeken ír a szalagra, és megfelelően mozgatja a fejeket. Hogy eközben ne kelljen balra visszalépni, célszerűen, miközben balra mozog, minden fejnek „megelőlegezi”, hogy balra fog lépni, és balra mozgítja el. Ha mégsem balra mozdul a fej, jobbra haladva korrigál.

Ha eddig a T gép n lépését szimuláltuk, akkor a fejek legfeljebb n mezőcsoporttal mozduktak el balra vagy jobbra. Így a következő lépés szimulálása során legfeljebb $2n + 1$ mezőcsoportot kell balra haladva végigolvasnunk, hogy „begyűjtsük” a jelenlegi helyzetre vonatkozó információkat. Ezután legfeljebb még egy mezőcsoportnyit haladunk balra, majd visszafelé legfeljebb $2n + 3$ mezőcsoporton kell végiglépegetnünk. Így az $n + 1$ -edik lépés szimulálása legfeljebb $2k(4n + 5)$ lépést igényel. Innen a szimuláció teljes lépésszáma legfeljebb $\sum_{n=0}^{t-1} 2k(4n + 5) = 2kt(2t + 3)$. □

10.1.26. Megjegyzés. Ha az előző tételben szereplő S gép kétszalagos, akkor már $O(t \log t)$ lépésben is elvégezhető a szimulálás. Ennek az állításnak a bizonyítása bonyolultabb.

10.1.27. Feladat [6]. Konstruáljunk az alábbi $f \in \mathbb{N} \rightarrow \mathbb{N}$, illetve $f \in \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ (parciális) függvényeket kiszámító egyszalagos Turing-gépet úgy, hogy a megadott k számú mezőt fogjuk össze egy mezővé (hasonlóan, mint többszalagos gép szimulálásánál egyszalagoson). Ha a függvény nincs értelmezve, például azért, mert az eredmény nem lenne a megadott halmazban, hibajelzést adhatunk, vagy a gép „elszáll”.

- (1) $f(n) = \lfloor n/2 \rfloor$, $k = 4$;
- (2) $f(m, n) = \text{sgn}(m)/n$, $k = 3$;
- (3) $f(m, n) = m + n$, $k = 3$.

10.1.28. Szemétgyűjtés. Legyen $T = (B, A, \varphi)$ egy Turing-gép. Ekkor T módosítható egy azonos szalagszámú S Turing-géppé, amely szimulálja T működését, és ugyanazokkal az A_0^* -beli bemeneti szavakkal indítva, mint T -t, ugyanazokat az A_0^* -beli kimeneti szavakat

produkálja, de nem hagy „szemetet”, azaz a kimeneti szavakon kívül a szalagok minden mezője üres. Ha egy számítás során a T gép t lépést tesz, és elolvassa a bemenetét (azaz a számítás során a bemenet minden mezőjén járt fej), akkor az S gép $O(t^2)$ lépést tesz.

A „szemétgyűjtéssel” működő Turing-gépek összekapcsolása egyszerű: egy gép kimeneti szalagjait a következő gép bemeneti szalagként használhatja.

Bizonyítás. Az S konstrukciója könnyű, ha az ábécéje tartalmaz egy olyan jelet is, amelyet A nem. Ha például $\star \notin A$, akkor a $\star$ jelet „második üres jelként” használhatjuk: ha T üres jelet írna, akkor ezt a jelet írjuk, ha pedig ezt a jelet olvassuk, akkor úgy viselkedünk, mint T , ha ugyanezen a szalagon az üres jelet olvassa. Mielőtt megállnánk, végezzünk minden szalagon szemétgyűjtést: minden szalagon először jobbra lépve írjunk egy $\star$ jelet, majd jobbra haladva töröljünk mindent az első $\sqcup$ jelig. Ezután balra haladva keressük meg a $\star$ jelet, töröljük, és lépünk balra, majd balra lépkedve, keressük meg az első $\star$ jelet (ha $\sqcup$ jelet találunk, írjuk át $\star$ -ra), és ettől balra töröljünk mindent az első $\sqcup$ jelig. Ezután jobbra haladva keressük meg a $\star$ jelet, töröljük, és menjünk a kimeneti szó jobb szélére. Eközben legfeljebb kétszer járjuk be azt a részt, ahol már ezelőtt is jártunk, így $O(t)$ lépést teszünk.

Ha ugyanazt az ábécét akarjuk használni, akkor kódolást kell alkalmaznunk. Ha $a \in A$, akkor kódja legyen $\sqcup a$, míg a fenti $\star$ kódja legyen egy olyan pár, amelynek első betűje nem $\sqcup$. A szimuláció azzal kezdődik, hogy a bemeneti szavakat „széthúzzuk”, $\sqcup$ jeleket írva betűik közé. Mivel Telolvassa a bemenet, a bemeneti szavak hossza legfeljebb $t + 1$, így ez $O(t^2)$ lépésben megtehető (lásd a fentebbi példákat). A szemétgyűjtés után a kimeneti szavakat „összenyomjuk”, törölve a betűik közé írt $\sqcup$ jeleket; ez szintén legfeljebb $O(t^2)$ lépést igényel. $\square$

Eddig minden feladatra új Turing-gépet készítettünk. A valódi számítógépeknél viszont minden új feladathoz programot írunk, és ugyanazt a gépet használjuk. Ez megtehető Turing-gépeknél is.

10.1.29. Univerzális Turing-gépek. Legyen A egy (legalább kételemű) ábécé, $k \geq 1$. Van olyan $k + 1$ szalagos U Turing-gép A ábécével, hogy bármely k szalagos $T = (B, A, \varphi)$ Turing-gépre a T bemenetét felírva az U első k szalagjára, a $k + 1$ -edik szalagra pedig egy, csak a φ -től függő $\omega \in A^*$ „programot” írva (amelynek utolsó betűje nem üres jel, és legfeljebb $6k + 4$ üres jelet tartalmaz egymás mellett), U szimulálja T működését (az első k szalagján). Ha A -nak legalább három eleme van, akkor U -t úgy is választhatjuk, hogy a programok ne tartsanak üres jelet. Ha T egy bemeneten t lépést tesz, akkor U a szimulálást $O(t)$ lépésben végzi.

Bizonyítás. Az egyszerűség kedvéért először feltesszük, hogy A -nak legalább három eleme van, és a szimulációt $k + 2$ szalagos gépen végezzük. Később megmutatjuk, hogyan lehet ezeket a megszorításokat kiküszöbölni.

Az első k szalag megfelel a szimulált gép szalagjainak, a $(k + 1)$ -edik szalagon lesz a program, a $k + 2$ -edik szalagon az „utasításregiszter”. A

$$\varphi: B \times A^k \rightarrow B \times A^k \times \{<, =, >\}^k$$

függvény koordinátafüggvényei legyenek β , α és γ ; ezek tehát rendre a B , A^k , illetve $\{<, =, >\}^k$ halmazban vesznek fel értékeket. Feltehetjük, hogy a $\sqcup$ üres jel mellett A

tartalmazza a 0 és 1 jeleket. Minden B -beli belső állapotot kódoljunk valahogy (azonos hosszúságú) 0–1 sorozattá. Az $=$, $<$, illetve $>$ jelek kódja legyen $\sqcup$, 0, illetve 1. A $(k+1)$ -edik szalagra a φ függvény kódját írjuk, az alábbi módon: írjuk a szalagra a

$$(1) \quad \gamma(a_1, \dots, a_k, b) \alpha(a_1, \dots, a_k, b) \beta(a_1, \dots, a_k, b) a_1 \dots a_k b$$

szavakat tetszőleges sorrendben, ahol $a_1, \dots, a_k \in A$ az egyes szalagokról olvasott betűk (ezeket nem kódoljuk), és $b \in B \setminus \{h\}$. A $k+2$ -edik szalagra a kezdőállapot kódja kerül. Az U univerzális gép konstrukciójának alapgondolata, hogy az aktuális belső állapot $(k+2)$ -edik szalagon lévő kódját balról jobbra haladva összehasonlítjuk a φ kódjában szereplő, (1) által leírt szavak b kódjával, ami egy fix hosszúságú 0-1-sorozat. Ha egyezést találunk, akkor az első k szalagon található betűket hasonlítjuk össze a programban található $a_1 \dots a_k$ betűkkel. Ha itt is egyezést találunk, akkor tudjuk, mit kell tenni: az aktuális állapotot a $k+2$ -edik szalagon felülírjuk $\beta(a_1, \dots, a_k, b)$ -vel, az első k szalagra az $\alpha(a_1, \dots, a_k, b)$ által megadott betűket írjuk, és az első k szalagon a $\gamma(a_1, \dots, a_k, b)$ által megadott elmozdulásokat hajtjuk végre, majd visszamegyünk a program elejére, és az értelmezés következő lépésére térünk át. Ha viszont nem találunk teljes egyezést, akkor elmegyünk az (1)-ben megadott szó bal széléig, és a következő szóval próbálkozunk. Megállunk akkor kell, ha nem találjuk az aktuális belső állapot kódját a programban, mert a „halt” állapot kódja az egyetlen, amely nem szerepel a programban. A lépkedés közben az aktuális állapot kódja mint „mérőléc” is szerepel: minden belső állapot kódja ugyanolyan hosszú, így a kódokat a „mérőléc” segít átlépni és másolni.

Induláskor a program, illetve a belső állapot kódjának bal szélén állunk. Az U univerzális gép működését pontosan az alábbi algoritmus adja meg:

- (1) [Start: belső állapot keresése.] Balra lépkedve, hasonlításuk össze a $(k+2)$ -edik szalagon szereplő belsőállapot-kódot azzal a kóddal, amelyet a $(k+1)$ -edik szalagról olvasunk. Ha a $(k+1)$ -edik szalagról üres jelet olvasunk, a $(k+2)$ -edikről pedig nem, akkor már nincs több belső állapot kód a programszalagon, meg kell állnunk: írjunk $\sqcup$ jelet a $(k+1)$ -edik és $(k+2)$ -edik szalagra, és menjünk (15)-re. Egyébként, ha eltérés van, menjünk (3)-ra. Ha a $(k+2)$ -edik szalagon üres mezőre értünk, a két belső állapot kód ugyanaz.
- (2) [Start: betűk keresése.] A $k+1$ -edik szalagon balra haladva, az ott szereplő $a_1, \dots, a_k$ betűket hasonlításuk össze az első k szalagról olvasható betűkkel. Ha nincs eltérés, lépünk a $(k+2)$ -edik szalagon jobbra egyet, a bal szélső nem üres mezőre, és menjünk (6)-ra. Ha eltérés van, jegyezzük meg, hogy hány betűt kell még balra átlépni a $(k+1)$ -edik szalagon.
- (3) [Tovább: keresés.] Amíg a $(k+2)$ -edik szalagról nem üres jelet olvasunk, lépkedjünk balra a $(k+2)$ -edik és $(k+1)$ -edik szalagon is, mindkét szalagon átlépve a kódszót. Egyébként balra haladva lépünk át a szükséges számú, maximum k betűt a $(k+1)$ -edik szalagon, és az utolsó lépésnél lépünk vissza jobbra egyet a bal szélső nem üres mezőre a $(k+2)$ -edik szalagon.
- (4) [Tovább: β és α .] Amíg a $(k+2)$ -edik szalagról nem üres jelet olvasunk, lépkedjünk jobbra a $(k+2)$ -edik és balra a $(k+1)$ -edik szalagon, mindkettőn átlépve a kódszót; utána lépünk vissza balra egyet a jobb szélső nem üres mezőre a $(k+2)$ -edik szalagon, és balra haladva lépünk át a k darab betűt is a $k+1$ -edik szalagon.

- (5) [Tovább: γ .] Balra haladva lépjük át a k darab „irányjelet” is a $(k+1)$ -edik szalagon, majd menjünk (1)-re.
- (6) [Vissza: megtaláltuk az utasítást.] Menjünk vissza a kódszó elejére a $(k+2)$ -edik szalagon: lépünk jobbra, amíg üres jelet nem olvasunk, majd lépünk egyet balra.
- (7) [Értelmezés: β , a belső állapot.] Másoljuk át a következő belső állapotot a $(k+1)$ -edik szalagról a $(k+2)$ -edik szalagra: balra lépkedve, ha a $(k+2)$ -edik szalagról nem üres jelet olvasunk, írjuk felül a $(k+1)$ -edik szalagról olvasott jellel.
- (8) [Értelmezés: α , a betűk.] A $(k+1)$ -edik szalagon k lépést balra lépve, írjuk a leolvasott betűket az első k szalagra.
- (9) [Értelmezés: γ , az irányjelek.] A $(k+1)$ -edik szalagon k lépést balra lépve, hajtsuk végre a γ által megadott, a $(k+1)$ -edik szalagról leolvasott betűknek megfelelő elmozdulásokat az első k szalagon, majd lépünk jobbra k lépést a $(k+1)$ -edik szalagon és egy lépést a $(k+2)$ -edik szalagon.
- (10) [Vissza: α .] Lépünk jobbra k lépést a $(k+1)$ -edik szalagon.
- (11) [Vissza: β és betűk.] Ha a $(k+1)$ -edik szalagon üres jel áll, akkor már túlmentünk a program elején, de ezt csak itt lehet észlelni: lépünk ezen a szalagon egyet balra, majd menjünk (13)-ra. Egyébként menjünk vissza a kódszó elejére a $(k+2)$ -edik és a $(k+1)$ -edik szalagon: lépünk jobbra, amíg üres jelet nem olvasunk a $(k+2)$ -edik szalagon. Ezután menjünk a $(k+1)$ -edik szalagon k lépést jobbra, a $(k+2)$ -edik szalagon pedig lépünk egyet balra.
- (12) [Vissza: belső állapot és következő γ .] Menjünk vissza a kódszó elejére a $(k+1)$ -edik és a végére a $(k+2)$ -edik szalagon: lépünk jobbra a $(k+1)$ -edik és balra a $(k+2)$ -edik szalagon, amíg a $(k+2)$ -edik szalagon üres jelet nem olvasunk. Ezután lépünk a $(k+1)$ -edik szalagon k lépést jobbra, a $(k+2)$ -edik szalagon pedig lépünk egyet jobbra, és menjünk (10)-re.
- (13) [Vissza: $(k+1)$ -edik szalag eleje.] Amíg a $(k+1)$ -edik szalagról üres jelet olvasunk, lépünk rajta balra.
- (14) [Vissza: $(k+2)$ -edik szalag eleje.] Menjünk vissza a kódszó elejére a $(k+2)$ -edik szalagon: lépünk jobbra, amíg üres jelet nem olvasunk, majd lépünk egyet balra, és menjünk (1)-re.
- (15) [Vége.] Álljunk meg. (A kimenet az első k szalagon van.)

Az alábbiakban állapotokkal is megadjuk a fenti algoritmust végrehajtó Turing-gépet, de csak a számunkra legfontosabb $k=1$ esetben. Ekkor 15 belső állapot is elegendő, nem kell semmit „megjegyezni”. A fenti (1)–(15) pontoknak rendre az $s, s_1, t_0, t_1, t_2, v_0, e_0, e_1, e_2, v_1, v_2, v_3, v_4, v_5, h$ állapotok felelnek meg. A most következő leírásban ha nem mondjuk, hogy írunk, akkor ugyanazt a jelet írjuk vissza a szalagra, amit olvastunk, és ha nem mondjuk, hogy melyik állapotba menjünk, akkor maradunk ugyanabban az állapotban. Az első, második és harmadik szalagról olvasott betűt rendre a_1, a_2, a_3 jelöli.

s: Ha $a_3 \neq \sqcup$ és $a_2 = \sqcup$, akkor menjünk a h állapotba. Ha $a_3 \neq \sqcup$ és $a_2 = a_3$, akkor a második és harmadik szalagon lépünk balra. Ha $a_3 \neq \sqcup$ és $a_2 \neq a_3$, akkor a második és harmadik szalagon lépünk balra, és menjünk a t_0 állapotba. Ha $a_3 = \sqcup$, akkor menjünk át az s_1 állapotba.

- s_1 : Ha $a_1 = a_2$, akkor a második szalagon lépünk balra, a harmadik szalagon lépünk jobbra a bal szélső nem üres mezőre, és menjünk a v_0 állapotba. Ha $a_1 \neq a_2$, akkor a második szalagon lépünk balra, a harmadikon jobbra, és menjünk a t_1 állapotba.
- t_0 : Ha $a_3 \neq \sqcup$, akkor a második és harmadik szalagon lépünk balra. Ha $a_3 = \sqcup$, akkor a harmadik szalagon lépünk jobbra, és menjünk a t_1 állapotba.
- t_1 : Ha $a_3 \neq \sqcup$, akkor a második szalagon balra, a harmadik szalagon jobbra lépünk. Ha $a_3 = \sqcup$, akkor a második és harmadik szalagon is lépünk balra, és menjünk a t_2 állapotba.
- t_2 : A második szalagon lépünk balra, és menjünk az s állapotba.
- v_0 : Ha $a_3 \neq \sqcup$, akkor a harmadik szalagon lépünk jobbra; egyébként a harmadik szalagon lépünk balra, és menjünk az e_0 állapotba.
- e_0 : Ha $a_3 \neq \sqcup$, akkor írjuk a_2 -t a harmadik szalagra, és a második és harmadik szalagon lépünk balra; egyébként menjünk az e_1 állapotba.
- e_1 : Írjuk a_2 -t az első szalagra, a második szalagon lépünk balra, és menjünk az e_2 állapotba.
- e_2 : Az első szalagon lépünk az a_2 által kódolt módon, a második és harmadik szalagon pedig lépünk jobbra, és menjünk a v_1 állapotba.
- v_1 : A második szalagon lépünk jobbra, és menjünk a v_2 állapotba.
- v_2 : Ha $a_2 = \sqcup$, de $a_3 \neq \sqcup$, akkor a második szalagon lépünk balra, és menjünk a v_4 állapotba. Egyébként ha $a_3 \neq \sqcup$, akkor a második és harmadik szalagon lépünk jobbra, ha pedig $a_3 = \sqcup$, akkor a második szalagon lépünk jobbra, a harmadik szalagon lépünk balra, és menjünk a v_3 állapotba.
- v_3 : Ha $a_3 \neq \sqcup$, akkor a második szalagon lépünk jobbra, a harmadik szalagon lépünk balra, ha pedig $a_3 = \sqcup$, akkor a második és harmadik szalagon is lépünk jobbra, és menjünk a v_1 állapotba.
- v_4 : Ha $a_2 = \sqcup$, akkor a második szalagon lépünk balra, egyébként menjünk a v_5 állapotba.
- v_5 : Ha $a_3 \neq \sqcup$, akkor a harmadik szalagon lépünk jobbra, ha pedig $a_3 = \sqcup$, akkor a harmadik szalagon lépünk balra, és menjünk az s állapotba.
- h : Álljunk meg.

Térjünk vissza az általános eset tárgyalására. Még meg kell szabadulnunk a $(k+2)$ -edik szalagtól. Észrevehetjük, hogy a $(k+1)$ -edik szalagon azt használtuk ki, hogy φ kódjától jobbra $2k+1$ üres jel áll. Írjuk ezektől jobbra a $(k+2)$ -edik szalagon álló kódszót, és hagyjuk el a $(k+2)$ -edik szalagot. Még mindig két fejre van azonban szükségünk a $(k+1)$ -edik szalagon. A megoldás ötlete ugyanaz, mint a 10.1.25 pontban. „Húzzuk szét” a mezőket, és minden mező mellé, tőle jobbra tegyünk egy újabb mezőt: ha itt nem $\sqcup$ van, hanem mondjuk 0, az azt jelzi, hogy itt a fej. Kezdsénnél most is a két fej a kezdőállapot kódjának jobb szélén, illetve φ kódjának jobb szélén áll. A φ kódja és a kezdőállapot kódja között most $4k+2$ üres jel van. Nem nehéz az algoritmust úgy megváltoztatni, hogy az eredeti $k+2$ szalagos változat működését szimulálja.

Ha T unáris, akkor nincs az üres jelen kívül két további jelünk, de a három jelet az unáris gép jeleiből alkotott párokkal kódolhatjuk (az üres jel kódja legyen $\sqcup\sqcup$). A fej kódokat is számolva, most φ kódja és a kezdőállapot kódja között $6k+3$ üres jel van, de a kezdőállapot kódjának jobb szélén is állhat üres jel, így legfeljebb $6k+4$ üres jel áll egymás mellett a teljes programkódban.

Végül vegyük észre, hogy ha A -nak legalább három eleme van, akkor a programot úgy is kódolhatjuk, hogy a kódban ne szerepeljen $\sqcup$ jel. Például, ha $0, 1 \in A$, akkor $\sqcup \neq a \in A$ kódolására a $0a$ párt, $\sqcup$ kódolására az 10 párt, míg elválasztó jelként az 11 párt használhatjuk. A fej jelzésére 1 -et, míg hiányának jelzésére 0 -t használunk. Persze U -t ennek megfelelően értelemszerűen módosítani kell.

Nyilván egy lépés szimulálása konstans idő alatt történik (persze a konstans függ a program hosszától). $\square$

A konstrukció némi változtatásával megoldható, hogy egyáltalán ne legyen szükség új szalagra:

*** 10.1.30. Egyszalagos univerzális Turing-gép.** Legyen A egy (legalább kételemű) ábécé. Van olyan egyszalagos U Turing-gép A ábécével, hogy bármely egyszalagos $T = (B, A, \varphi)$ Turing-gépre a T bemenetét és egy, csak a φ -től függő $\omega \in A^*$ „programot” (amelynek jobbszélső betűje nem üres jel, és legfeljebb 11 üres jelet tartalmaz egymás mellett) felírva az U szalagjára, U szimulálja T működését. Ha A -nak legalább három eleme van, akkor U -t úgy is választhatjuk, hogy az ω programok ne tartalmazzanak üres jelet. Ha T szemégyűjtéssel dolgozott, akkor U is. Ha T egy bemeneten t lépést tesz, akkor U a szimulálást $O(t)$ lépésben végzi.

Megjegyezzük, hogy további ügyeskedéssel egy univerzális Turing-gép betűinek, illetve belső állapotainak száma eléggé lecsökkenthető. Például megadható univerzális Turing-gép 6 elemű ábécével és 6 belső állapottal (amely egyszalagos, de bármely k -szalagos gépet tud szimulálni.)

Bizonyítás. Az előző bizonyítás konstrukcióját kell egy kicsit módosítani. Írjunk az ott szereplő program mindkét szélére egy-egy kétbetűs $\sqcup 0$ jelet, amelynek jelentése „üres mező rajta álló fejjel”. Most négy „fej” jelzés van a szalagon, a két szélső között van a program, azokon kívül van a tényleges szalagtartalom; módosítsuk ennek megfelelően a szimulációt: a programban való „keresgélés” során a két szélső „fej” helyzete nem változik, a mozgás a szalagon pedig úgy történik, hogy az egész programot a négy „fej”-jel együtt mozgatjuk. Megállás előtt a jobb szélső „fej”-től indulva, a bal szélső „fej”-jel bezárólag töröljük a programot. $\square$

10.1.31. Feladat [7]. Egyszalagos, háromelemű szalagábécével rendelkező Turing-gépek szimulálását végző háromszalagos univerzális Turing-gép második és harmadik szalagjára legfeljebb négy-négy betűs „programot” írunk. Vizsgáljuk meg, hogy az egyes „programok” esetén milyen gépet szimulál az univerzális gép. (A legtöbb eset triviális.)

10.1.32. Félszalagos Turing-gépek. Néha a Turing-gépet úgy szokás definiálni, hogy a szalagjai csak az egyik irányban végtelenek:

$\boxed{\sqcup} \boxed{a} \boxed{I} \boxed{\sqcup} \boxed{0} \boxed{1} \boxed{0} \boxed{\sqcup} \boxed{\sqcup} \dots$

Ha a gép balra haladva bármelyik szalagján „lelép” a szalagról, akkor úgy tekintjük, hogy „elszállt”: soha nem jut el a halt állapotba (még akkor sem, ha éppen abba ment volna át).

10.1.33. Félszalagos Turing-gép szimulálása Turing-gépen. *Bármely félszalagos Turing-géphez létezik Turing-gép ugyanazzal a szalagszámmal és ábécével, amely a félszalagos Turing-gépet szimulálja, és ha az n lépést tett, akkor legfeljebb $O(n)$ lépést tesz.*

Bizonyítás. Írjuk a félszalagos Turing-gép szalagjainak tartalmát a Turing-gép megfelelő szalagjának „nemnegatív páros sorszámú” mezőibe (nulla sorszámúnak a félszalagos gép szalagjának bal szélső mezőjét tekintjük). A Turing-gépen a páratlan mezőket hagyjuk végig szabadon, kivéve a -1 sorszámú mezőt, amelybe írunk az ürestől különböző jelet. Ha valamelyik szalagon erre a mezőre érünk, menjünk egy olyan állapotba, amelyben a gép minden szalagon állandóan balra lép és ugyanabban az állapotban marad, azaz „elszáll”. Egyébként a szimulálás nyilvánvaló és költsége is nyilvánvaló: lényegében ugyanazt tesszük, mint a félszalagos gép, a páratlan mezőket átlépve. $\square$

10.1.34. Turing-gép szimulálása félszalagos gépen. *Bármely Turing-géphez létezik félszalagos Turing-gép ugyanazzal a szalagszámmal és ábécével, amely a Turing-gépet szimulálja, és ha az n lépést tett, akkor legfeljebb $O(n)$ lépést tesz.*

Természetesen így van univerzális Turing-gép egyetlen félszalaggal és kételemű ábécével is.

Bizonyítás. Az alapgondolat, hogy a félszalagos gép minden szalagján a mezőket három végtelen részre osztjuk: az egyikbe kerülnek a „jobb oldali”, a másikba a „bal oldali” mezők, a harmadikba pedig egy „szalagvégjel”. Nullától számozva a félszalagos Turing-gép szalagjainak mezőit, írunk a hárommal osztható sorszámú mezőkbe üres jelet, kivéve a 0 sorszámú mezőt, ahova egy, az üres jeltől különböző jelet írunk; ez lesz a „szalagvégjel”. Minden szalagon a fej alatt és tőle balra elhelyezkedő mezőket írjuk a hárommal osztva maradékul egyet adó sorszámú mezőkbe, de fordított sorrendben, mint ahogy a Turing-gép szalagján voltak. Minden szalagon a fejtől jobbra álló mezőket írjuk a hárommal osztva maradékul kettőt adó sorszámú mezőkbe. A szimulálás nyilvánvaló: minden szalagon „hármásával” mozgunk, de figyeljük a szalagvégjelet is, és ha ráléptünk, irányt és maradékot váltunk. Nyilván az eredeti gép bármely lépését korlátos számú lépéssel tudjuk szimulálni. $\square$

10.1.35. Post-gép. Ez a számítási modell adattárolóként sort (*first in first out* vagy *FIFO* adattárat) használ. Ez egy, a gép véges, legalább két elemű A ábécéjéből képzett $\gamma \in A^*$ szó. Szemben a Turing-géppel, most csak ezen szó végére tudunk írni, és csak az elejéről tudunk olvasni, de az elolvasott betű törlődik is. A gép képes érzékelni, ha $\gamma = \emptyset$, azaz γ az üres szó. Ha $\gamma \in A^+$, akkor legyen $\text{head}(\gamma)$ a γ első betűje, $\text{tail}(\gamma)$ pedig a γ maradék részéből álló szó; legyen $\text{tail}(\emptyset) = \emptyset$. Az A ábécének itt is van egy kitüntetett betűje, amelyet most $\sharp$ fog jelölni, a maradék ábécé $A_0 = A \setminus \{\sharp\}$. Maga a gép egy véges irányított címkézett gráf, a „programgráf”, amely négy különböző típusú csúcsot tartalmaz: van pontosan egy „start” címkéjű csúcs, ennek befoka nulla, kifoka egy, innen indul a gép. Vannak „halt” címkéjű csúcsok, ezek kifoka nulla, ha a gép ilyenbe jut, akkor megáll. A gép bemenete, illetve kimenete γ értéke a számítás kezdetén, illetve végén. A „ $\gamma \leftarrow \gamma a$ ” címkéjű csúcsok értékadást írnak le, egy a kifokuk; ezeknél a az A ábécé bármely konkrét betűje lehet, amelyet a γ végére írunk. Végül a „ $\gamma \leftarrow \text{tail}(\gamma)$ ” címkéjű „vizsgáló” csúcsok kifoka $\sharp(A) + 1$, és a kimenő élek címkéje $\emptyset$, illetve az A ábécé

betűi; ezekből a csúcsokból a gép a $\emptyset$ címkéjű élen megy tovább, ha a γ üres szó volt, és a $\text{head}(\gamma)$ címkéjű élen egyébként; az elolvasott betű törlődik a γ elejéről.

10.1.36. Tétel: Post-gép szimulálása Turing-gépen. *Bármely Post-gép szimulálható egyszalagos Turing-gépen ugyanazzal az ábécével.*

Bizonyítás. Először feltesszük, hogy a Turing-gép ábécéje $A \cup \{\sqcup\}$, ahol A a Post-gép ábécéje és $\sqcup \notin A$. A Turing-gép belső állapotai alapvetően a Post-gép csúcsainak felelnek meg, a szalagra pedig a mindenkor γ szó van írva. A „ $\gamma \leftarrow \gamma a$ ” típusú csúcsoknál a Turing-gép az γ szótól jobbra lévő első $\sqcup$ jelen áll, ide az $a \in A$ betűt írja, és ha a következő csúcs is ilyen típusú, akkor az annak megfelelő b' belső állapotba megy át, és eggyel jobbra lép; ha a csúcs „ $\gamma \leftarrow \text{tail}(\gamma)$ ” típusú, akkor a Turing-gép a γ szó bal szélső betűjén áll, azt $\sqcup$ üres jellel írja felül, az olvasott betűnek megfelelően megy tovább ($\sqcup$ olvasása üres γ szót jelent), és ha a következő csúcs is ilyen típusú, akkor az annak megfelelő b' belső állapotba megy át, és eggyel jobbra lép; különböző típusú csúcsok esetén egy $b'_<$ illetve $b'_>$ belső állapotot iktatunk közbe, amelyben a szimuláló Turing-gép megkeresi a γ szó megfelelő végét. A „halt” állapotba lépés előtt az γ jobb szélső betűjére állunk. Végül vegyük észre, hogy az új $\sqcup$ betű bevezetését nyilván elkerülhetjük betűpárok használatával.

10.1.37. Tétel: Turing-gép szimulálása Post-gépen. *Bármely egyszalagos Turing-gép szimulálható Post-gépen ugyanazzal az ábécével.*

Bizonyítás. Először feltesszük, hogy a Post-gép ábécéje $A \cup \{\#\}$, ahol A a Turing-gép ábécéje és $\sqcup$ üres jellel és $\# \notin A$. A Turing-gép belső állapotainak a Post-gép bizonyos „ $\gamma \leftarrow \text{tail}(\gamma)$ ” típusú csúcsai felelnek meg, és a Post-gép a $\gamma \in (A \cup \{\#\})^*$ szóval dolgozik, amely $\beta\#\alpha$ alakú, ahol β a Turing gép feje alatt és attól jobbra álló betűkből álló szó, α pedig a fejtől balra álló betűkből álló szó, természetesen mindkettő az utána illetve előtte álló végtelen $\sqcup$ -sorozat nélkül, a $\#$ jel pedig a „töréspontot” jelzi.

A Turing-gép egy lépésének szimulálása úgy kezdődik, hogy a Post-gép „elolvassa a fej alatt álló betűt”, β első betűjét. Ha a Turing-gépnek jobbra kell lépnie, akkor látszólag egyszerű dolga van: a szalagra írandó betűt hozzáírja γ végéhez. Ha azonban β egyetlen betűből állt, akkor a következő lépésben $\sqcup$ jelet kellene olvasnia. Ezért mindig egyszer „körbeléptetjük” a γ szót: először elolvassuk a következő betűt: ha ez $\#$, akkor előbb egy $\#$, majd egy $\sqcup$, aztán még egy $\#$ jelet írunk γ végére, ha pedig ez nem $\#$, akkor egy $\#$ jelet, majd az olvasott betűt írjuk γ végére, és folytatjuk, amíg végül egy $\#$ jelet olvasunk és írunk. A „körbeléptetés” befejezéséhez egy újabb $\#$ jel olvasásáig folytatjuk az olvasást és írást, de ezt a $\#$ jelet már nem írjuk ki.

Ha az aktuális betű elolvasása után a Turing-gépnek helyben kell maradnia, akkor az eljárás valamivel egyszerűbb: először egy $\#$ jelet írunk γ végére, majd az írandó betűt, és „körbeléptetjük” a γ szót.

Végül, ha az aktuális betű elolvasása után a Turing-gépnek balra kell lépnie, akkor két „körbeléptetést” alkalmazunk: Először egy $\#$ jelet írunk γ végére, majd az írandó betűt, és körbeléptetünk, de az első $\#$ jel elérése után „késleltetéssel”, azaz csak két betű kiolvasása után írjuk vissza az elsőt, majd egy újabb betű kiolvasása után a másodikat stb. Mikor $\#$ jelet olvasunk, akkor egy $\#$ jelet írunk ki, és csak aztán írjuk ki az előzőleg olvasott betűt, ami eredetileg α utolsó betűje volt. (Azt az esetet is kezelni tudjuk, amikor α üres volt.) Újabb körbeléptetéssel előállíthatjuk az új $\gamma' = \beta'\#\alpha'$ szót, és ezután a b' belső állapotnak megfelelő csúcsba mehetünk.

10.1.38. Korlátozott gépmodellek. Ha egy Turing-gépre különböző megszorításokat teszünk, *korlátozott gépmodelleket* kapunk. Például feltehetjük, hogy vannak „*csak bemenet*” szalagok, amelyeken a gép nem írhat, és csak balra léphet, vannak „*csak kimenet*” szalagok, amelyeket a gép írhat, de csak jobbra léphet rajtuk, és vannak *veremtárak* vagy *vermek*, amelyeken a gép írhat és olvashat, valamint balra is, jobbra is léphet, de ha balra lép, akkor törölnie kell, amit olvasott (azaz üres jelet kell a helyére írni); ezek a szalagok szolgálhatnak bemenetként és kimenetként is. A fenti megszorításnál a csak bemeneti szalagok „*online*” használatáról beszélünk; az „*offline*” használatnál megengedjük, hogy a csak bemeneti szalagokon akármerre lépjen a fej, de ezekre a szalagokra a gép nem írhat (azaz azt kell visszaírnia, amit olvasott). Egyéb megszorításokat is tehetünk, például egyes szalagokra kiköthetjük, hogy félszalagok legyenek, azaz csak jobbra legyenek végtelenek. Természetesen a különböző megszorítások kevesebbet „tudó” gépeket eredményezhetnek, amelyeken már nem lehet Turing-gépet szimulálni. (Nyilvánvaló, hogy ha van olyan szalag, amelyen a gép írhat is, olvashat is, és mindkét irányba szabadon mozoghat, akkor tud szimulálni Turing-gépet.)

Például egy *véges automata* lényegében egy olyan Turing-gép, amelynek egy online bemeneti szalagja van, és egy kimeneti szalagja, amelyre azonban csak egyszer írhat, közvetlenül azelőtt, hogy átmegy a végállapotba, és nem léphet rajta semerre. Így csak két dolgot tehet: a bemenetet elfogadja (ha nem üres jelet ír) vagy elutasítja (ha üres jelet ír). A *Rabin-Scott-automata* ennek a nemdeterminisztikus változata (a nemdeterminisztikus Turing-gépeket lásd később); mindig szimulálható determinisztikus véges automatával, bár az állapotok száma exponenciálisan megnő (a szimulációhoz a nemdeterminisztikus gép „halt” állapottól különböző belső állapotainak nem üres részhalmazait kell választani a determinisztikus gép belső állapotainak). A *Mealy-automata* hasonló, de a bemenet szalagokat online olvasva, minden lépésben ír a „csak kimenet” szalagokra. A *Moore-automata* abban különbözik a Mealy-automatától, hogy a kimenet csak a belső állapotától függ; a Mealy- és a Moore-automata nyilván ekvivalensek. Ezeknél többet tud az *egyveremtáras gép*, amelynek egy bemeneti szalagja van és egy veremtára, amely egyúttal a kimenet is. A különböző korlátozott gépmodellek fontos szerepet játszanak az informatikában, más tárgyakban lesz róluk szó. Itt egyetlen eredmény bizonyítására szorítkoznak.

10.1.39. Tétel. *Bármely egyetlen félszalaggal rendelkező T Turing-géphez létezik olyan V kétveremtáras gép, amelynek mindkét veremtára félszalag, a Turing-gépet szimulálja ugyanazzal az ábécével, és ha az n lépést tett, akkor legfeljebb $O(n)$ lépést tesz.*

Bizonyítás. A V első veremtára lesz a bemenet és a kimenet is, kezdetben a másik veremtárban üres jelek vannak, és a fej a bal szélső mezőn áll. A szimulálás alapgondolata, hogy a T szalagján a fej alatti és attól balra lévő jeleket az első veremtár tartalmazza, míg a másik veremtárban a T szalagján a fejtől jobbra lévő jelek vannak, de fordított sorrendben. Ha balra mozdul el T feje, akkor az első vermen balra mozdulunk és így itt törölnünk kell, a második verembe viszont írunk és itt jobbra mozdulunk, valamint megjegyezzük, hogy az első veremből kell majd olvasni. Ha T feje jobbra mozogna, akkor az első verembe írunk és itt jobbra lépünk, a második vermen pedig balra lépünk, és így ott törölni kell, valamint megjegyezzük, hogy a második veremből kell majd olvasni. Ha nem mozdulunk el, akkor egyik vermen sem mozdulunk, de ahonnan olvasnunk kell majd, oda írunk, és „nem felejtjük el”, hogy honnan kell majd olvasni. Egyetlen probléma van: ha T szalagján

a kezdeti pozíciótól jobbra álló mezőre lépünk, a szimuláló gép második vermén a fej balra „lelép” a szalagról, és így V „elszáll”. Ezt megelőzendő, legelső lépésként a második verembe „őrszemként” (*sentinel*) írunk egy üres jelet, és minden, a második verembe írt betű mellé, tőle jobbra írunk egy nem üres jelet, ami jelzi, hogy a második verem még nem üres. Ha a második veremtárban balra kellene lépünk, először mindig ellenőrizzük, hogy a verem üres-e. Ha nem, akkor kettőt is léphetünk balra. Ha viszont elértük az „őrszemet”, akkor ténylegesen nem lépünk balra, de üres jel olvasásának megfelelően működünk.

10.1.40. RAM-gép. A *RAM-gép* (*RAM*: Random Access Memory, tetszőleges elérési memória) a valódi számítógépekhez közelebb álló gépmoddell. (Egy „valódi számítógép” például a [46], Vol. 1 Fas. 1 könyvben leírt MMIX gép, amely ugyan csak szimulátorként és metaszimulátorként létezik, de kiválóan összefoglalja a létező gépek legfontosabb tulajdonságait.) Az M memória minden $M[k]$ ($k \in \mathbb{Z}$) rekesze tetszőleges egész számot tárolhat, de egyszerre mindig csak véges sok nem nulla értéket tárol. A gépnek három regisztere van: az A *akkumulátor*, a B *regiszter* és az I *indexregiszter*; ezek tartalma is egész szám. Van még egy *programmemória*, ennek rekeszei természetes számokkal vannak indexelve, és *utasításokat* tartalmaznak. Az *utasításkészlet* az alábbi (a % jel után, megjegyzésként leírtuk, hogy az utasítás mit csinál):

CLR	% $A \leftarrow 0$; clear A , azaz A törlése
INC	% $A \leftarrow A+1$; increment A , azaz A növelése
DEC	% $A \leftarrow A-1$; decrement A , azaz A csökkentése
GET B	% $A \leftarrow B$; get B , azaz A -ban a B értékét kapjuk meg
GET I	% $A \leftarrow I$; get I , azaz A -ban a I értékét kapjuk meg
PUT B	% $B \leftarrow A$; put B , azaz A értékét B -be tesszük
PUT I	% $I \leftarrow A$; put I , azaz A értékét I -be tesszük
ADD	% $A \leftarrow A+B$; add, azaz összeadás
LD	% $A \leftarrow M[I]$; load, azaz töltés a memóriából
ST	% $M[I] \leftarrow A$; store, azaz tárolás a memóriába
JNP p	% jump non positive, azaz ugrás, ha nem pozitív: % $A \leq 0$ esetén a programvégrehajtás a p -edik soron folytatódik.

Mint látható, minden adat csak az akkumulátoron keresztül érhető el, a B és I regiszterek csak az akkumulátorból kaphatnak értéket. A programvégrehajtás a nulla sorszámú sorral indul, és minden sor sorban végrehajtódik, ha nincs ugrás. A gép akkor áll meg, ha a vezérlés olyan sorra kerül, amely nem tartalmaz utasítást. Minden RAM-gép tekinthető számítási eljárásnak, az állapotot a regiszterek tartalma, a memória tartalma, és az aktuális programsor sorszáma adja meg. A memória és a regiszterek, csak a memória, csak a regiszterek, vagy azok egyike, például az akkumulátor is tekinthető bemenetnek illetve kimenetnek; hogy ez nem lényeges, azt az alább részletezendő példa mutatja.

10.1.41. RAM-gép végrehajtási ideje. Egy RAM-gép lépésszáma nem a legjobb mérőszáma annak, hogy „mennyi munkát végez”, mert tetszőleges hosszúságú egész számokkal végzett műveletekkel szimulálhatunk vektorműveleteket. (Turing-gépnél nincs ilyen lehetőség, mert a szalagábécé véges.) Ezért célszerűbb RAM-gépek lépésszáma helyett a *futásidejükről* beszélni. Ezt úgy kapjuk, hogy egy lépés idejét nem egységnyiinek vesszük, hanem annyinak, amennyi az adott lépésben (operandusként, illetve eredmény-

ként) szereplő összes egész szám bitjei számának összege, ahol minden számnál egy bitet számolunk az előjelre. Így a 0 egybites, a $0 \neq n \in \mathbb{Z}$ szám bitjeinek száma pedig $2 + \lfloor \log |n| \rfloor$. Emiatt szokás *logaritmikus költségű* RAM-gépről is beszélni. Például a LD utasítás futásideje, ha I tartalma 11, az M[11] tartalma pedig -20, akkor $5 + 6 = 11$.

10.1.42. Példák. (1) Kiszámítjuk egy, a A akkumulátorban lévő a természetes szám kettes számrendszerbeli alakját úgy, hogy ha a szám m bites, akkor csak $O(m)$ lépést teszünk, és $O(m)$ bites számokkal számolunk, így a futásidő $O(m^2)$. A 2^k tag együtthatója a $-k$ indexű rekeszben fog megjelenni. A szegényes utasításkészlet miatt érdemes bevezetni az

```
LDI n    % I←n, A←M[n]
```

és

```
STI n    % B←A, I←n, M[n]←A
```

„makrókat”, ahol $n \in \mathbb{N}$ adott, konkrét természetes szám, bár most csak az $n = 1$ és $n = 2$ eseteket fogjuk használni. (Az LDI illetve STI névben az I betű az angol „*immediate*”, azaz „*közvetlen*” szóra utal.) Az első definíciója

```
CLR      % A←0
INC      % A←A+1, tehát A←1
INC      % A←2
⋮
INC      % A←n
PUT I    % I←n
LD       % A←M[n]
```

a másodiké pedig

```
PUT B    % B←A, azaz A mentése
CLR      % A←0
INC      % A←1
INC      % A←2
⋮
INC      % A←n
PUT I    % I←n
GET B    % A←B, azaz A visszaállítása
ST       % M[n]←A
```

ahol mindkét definícióban n darab INC utasítás szerepel (másként nem tudunk konkrét számokat megadni a gépnek). A második makró – a B regiszter módosításától eltekintve – az első „fordítottja”. A program maga két részből áll. Az első megkeresi a legkisebb olyan m természetes számot, amelyre $a < 2^m$, és ezt $M[2]$ -be teszi, valamint $0 \leq k \leq m$ esetén

a -2^k számot beírja $M[-k]$ -ba. Az $a < 2^m$ feltétel ekvivalens az $a + 1 \leq 2^m$ feltétellel, ez pedig az $a + 1 - 2^m \leq 0$ feltétellel, ez utóbbit ellenőrizzük. Az $a + 1$ értéket $M[1]$ -ben tároljuk. A program második része számolja ki a jegyeket. Mindkét részben az egyszerűség kedvéért nem abszolút címeket, hanem $0:, 1:, \dots, 9:$ alakú (felüldefiniálható) *szimbolikus címkéket* használunk, azaz a címke egy d decimális számjegy. Az ugró utasításban **dF** (d forward) vagy **dB** (d backward) szerepel, attól függően, hogy az adott ugró utasításban előre vagy vissza kell ugrani a megadott címkehez. A „valódi programba” egy „assembler” teszi be az abszolút sorszámkokat. (Természetesen tetszőleges címkéket is használhatnánk, de a tíz lehetséges „*lokális címke*” bőven elég lesz számunkra, és az ilyen típusú címkék a valódi assemblerek esetén is rendkívül hasznosak.) Mindkét programrészben a ciklusmag m -szer kerül végrehajtásra, ezért $O(m)$ lépést teszünk. Az első programrészt a 10.1.1 táblázat, a másodikat pedig a 10.1.2 táblázat tartalmazza.

	INC	% $A \leftarrow a + 1$
	STI 1	% $M[1] \leftarrow a + 1$
	CLR	% $A \leftarrow 0$
	STI 2	% $M[2] \leftarrow 0$
	DEC	% $A \leftarrow -2^0$
	STI 0	% $M[0] \leftarrow -2^0$
1:	LDI 1	% $A \leftarrow a + 1$; a ciklusmag kezdete
	PUT B	% $B \leftarrow a + 1$
	LDI 2	% $A \leftarrow -m$
	PUT I	% $I \leftarrow -m$
	LD	% $A \leftarrow -2^m$
	ADD	% $A \leftarrow a + 1 - 2^m$
	JNP 2F	% ha $a < 2^m$, akkor kész az első rész
	LD	% $A \leftarrow -2^m$
	PUT B	% $B \leftarrow -2^m$
	ADD	% $A \leftarrow -2^{m+1}$
	PUT B	% $B \leftarrow -2^{m+1}$
	GET I	% $A \leftarrow -m$
	DEC	% $A \leftarrow -(m + 1)$
	PUT I	% $I \leftarrow -(m + 1)$
	GET B	% $A \leftarrow -2^{m+1}$
	ST	% $M[-(m+1)] \leftarrow -2^{m+1}$
	GET I	% $A \leftarrow -(m + 1)$
	STI 2	% $M[2] \leftarrow -(m + 1)$
	CLR	% $A \leftarrow 0$
	JNP 1B	% ciklusmag vége, ugrás vissza

10.1.1 táblázat: Első programrész.

(2) Hasonló program írható más alapú számrendszerbe való konverzióra. A másik irányú konverzió egyszerűbb.

2:	LDI 2	% A ← −m
	PUT I	% I ← −m
	CLR	% A ← 0
	ST	% M[−m] ← 0, 2^m együtthatója 0
	GET I	% A ← −m
	INC	% A ← −(m − 1)
	STI 2	% M[2] ← −(m − 1), a ciklusszámláló inicializálása
3:	LDI 1	% A ← a + 1, a ciklusmag kezdete
	PUT B	% B ← a + 1
	LDI 2	% A ← −k, a ciklusszámláló
	PUT I	% I ← −k
	LD	% A ← −2 ^k
	ADD	% A ← a + 1 − 2 ^k
	JNP 5F	% ha $a < 2^k$, akkor a jegy 0, előre ugrunk; egyébként 1 a jegy
	STI 1	% M[1]-be $a + 1 - 2^k$ kerül, ez az új $a + 1$
	LDI 2	% A ← −k, ciklusszámláló
	PUT I	% I ← −k
	CLR	% A ← 0
	INC	% A ← 1, ez a k -adik jegy
4:	ST	% M[−k]-ba beírjuk a k -adik jegyet
	GET I	% A ← −k
	INC	% A ← −(k − 1), k csökkentése
	STI 2	% M[2] ← −(k − 1)
	JNP 3B	% ugrás vissza, ha nincs vége a ciklusnak
		% üres utasítás, megállunk
5:	CLR	% A ← 0, a jegy nulla
	JNP 4B	% ugrás vissza beírni a k -adik jegyet

10.1.2 táblázat: Második programrész.

10.1.43. Feladat [8]. Írjunk szorzó programot RAM-gépre.

10.1.44. Turing-gép szimulálása RAM-gépen. Bármely egyszalagos Turing-gép szimulálható RAM-gépen. Ha a Turing-gép lépésszáma n , akkor a RAM-gép $O(n)$ lépést tesz $O(\log n)$ jegyű számokkal, tehát a RAM-gép végrehajtási ideje $O(n \log n)$.

Bizonyítás. Feltehetjük, hogy a $T = (B, A, \varphi)$ Turing-gép üres jele 0, ábécéje $A = \{0, 1, \dots, r\}$, a belső állapotai pedig $B = \{0, 1, \dots, m\}$, ahol 0 a start, m pedig a halt. Legyenek φ koordinátái β , α és γ , azaz $\alpha(j, i) \in A$, $\beta(j, i) \in B$ és $\gamma(j, i) \in \{<, =, >\}$, ha $i \in A$ és $j \in B$. A szimuláció során a memóriarekeszek tartalma megfelel a szalagon álló betűknek, I pedig a fej helyzetét tartalmazza. A program a P_j , $0 \leq j \leq m$ és $Q_{j,i}$, $0 \leq i \leq r$, $0 \leq j < m$ részekből áll (a programrészek sorrendje érdektelen). A P_j programrész azt utánozza, hogy a Turing-gép a j állapotban van, kiolvassa, hogy mi áll a szalagon, majd ettől függően más-más $Q_{j,i}$ -re ugrik:

```

LD                % A ← M[I]
JNP <Qj,0 címe>  % ide ugrunk, ha nullát olvastunk
DEC
JNP <Qj,1 címe>  % ide ugrunk, ha egyet olvastunk
DEC
⋮
JNP <Qj,r címe>  % ide ugrunk, ha r-et olvastunk

```

A P_m programrész álljon egyszerűen egyetlen üres programsorból. A $Q_{j,i}$ programrész átírja a „szalag” tartalmát, módosítja I -t a fej mozgásának megfelelően, majd az új j' állapotnak megfelelő $P_{j'}$ programrészre ugrik. A $Q_{j,i}$ -hez tartozó $\gamma(j,i)$ -nek megfelelő módosítást egy DEC utasítás, illetve egy INC utasítás hajtja végre, vagy pedig teljesen kimarad ez a sor, attól függően, hogy $\gamma(j,i)$ értéke $<$, $>$ vagy $=$:

```

CLR                % A ← 0
INC                % A ← 1
⋮
INC                % A ← α(j,i)
ST                % M[I] ← α(j,i) írás a szalagra
GET I             % A ← I
<A módosítása γ(j,i)-nek megfelelően>
PUT I             % I ← A
CLR                % A ← 0
JNP <Pβ(j,i) címe> % ugrás a megfelelő belső állapothoz
                  % tartozó részre

```

Maga a program így épülhet fel a fent definiált részekből:

```

CLR    % A ← 0
PUT I  % I ← A
P0
⋮
Pm
Q0,0
⋮
Qm-1,r

```

A végrehajtási időre vonatkozó becslés onnan következik, hogy a Turing-gép egy lépése a RAM-gép korlátos számú lépésének felel meg, és hogy a Turing-gép n lépésben legfeljebb n rekeszbe ír bármit is, így ezek címe legfeljebb $O(\log n)$ hosszú. $\square$

10.1.45. Megjegyzés. Az előző szimulációnál a kimenetbe beleszámít az I regiszter tartalma is a megálláskor, hisz ez adja meg, hol áll a fej. Ha ezt el akarjuk kerülni, akkor

az eredményt arrébb kell másolni úgy, hogy $M[I]$ tartalma $M[0]$ -ba kerüljön, $M[I - 1]$ tartalma $M[-1]$ -be kerüljön stb., mielőtt megállunk. Ez nem nehéz, ha I tartalma nem pozitív: $M[1], M[2], \dots, M[k]$ használható „segédregiszterként” egy alkalmas k -ra. Ha I tartalma pozitív, akkor némi trükközésre van szükségünk: írjunk $M[I + 1]$ -be egy olyan nagy számot, amely már nem szerepel az ábécében, és másoljuk

$$M[1], M[2], \dots, M[I], M[I + 1]$$

tartalmát k hellyel jobbra, hogy $M[1], M[2], \dots, M[k]$ felszabaduljon „segédregiszternek”. Ezután a másolás már könnyen megoldható.

Észrevehetjük, hogy a szimulációban az ADD utasítást nem használtuk. Erre csak akkor van szükség, ha az A regisztert kívánjuk bemenetként és kimenetként is használni (a 10.1.42 példában leírt konverzióval), és nem akarunk nagyon nagy futási időt. Míg az ADD utasítással az a és b számok összeadásának futási ideje definíció szerint $O(\log |a| + \log |b|)$, nélküle az összeadáshoz legalább $\min\{|a|, |b|\}$ idő kell, mert minden lépés legfeljebb eggyel növeli a legnagyobb tárolt szám abszolút értékét, ezért még a lépésszám is $\min\{|a|, |b|\}$.

10.1.46. RAM-gép szimulálása Turing-gépen. Egy RAM-gépre írt programhoz van olyan négyszalagos Turing-gép, amely szimulálja a program működését, és ha a RAM-gép elolvassa bemenetét és futásideje n , akkor a Turing-gép lépésszáma $O(n^2)$.

Bizonyítás. A Turing-gép ábécéje legyen $\{\square, 0, 1, -, ;\}$. Az első, második és harmadik szalagon rendre A , B és I aktuális tartalma szerepel kettes számrendszerben, előjellel. Ha a negyedik szalagon minden rekesz tartalmát sorra feltüntetnénk, akkor gondot jelentene, hogy a RAM-gép képes akár a 2^m sorszámú rekeszbe is írni $O(m)$ idő alatt, így a szalag teleírt része nagyon hosszú lesz, tehát nagyon hosszú időbe telik, amíg a fej végiglépeget rajta. Ezért ST utasításkor a negyedik szalagra lényegében egy párt írunk fel: az eddig felírtaktól jobbra egy $;M[I];I$ sorozatot írunk, ahol $M[I]$ és I tartalmát kettes számrendszerben adjuk meg előjellel. A RAM-gép bemenetét ugyanezzel a kódolással írjuk erre a szalagra. Erről a szalagról sohasem törölünk semmit. Ha LD utasítást kell végrehajtani, jobbról balra végiglépegetünk ezen a szalagon, és megkeressük adott I -vel a legkésőbbi feljegyzést; ha nincs feljegyzés, az olvasás eredménye 0. Az ugyanarra a címre való újabb írások mintegy „eltakarják” a régieket. A többi utasítást könnyű szimulálni Turing-géppel.

Turing-gépünk egy olyan „szupergép” lesz, amelyben a RAM-gép minden program-sorának megfelel belső állapotok egy halmaza; ezek egy olyan Turing-gépet alkotnak, amely végrehajtja az adott utasítást, majd a fejeket mind a négy szalagon a feljegyzések jobb szélére viszi. Minden ilyen Turing-gép halt állapota megegyezik a következő utasításhoz tartozó Turing-gép start állapotával; feltételes ugrás esetén, ha a feltétel teljesül, az adott sornak megfelelő gép start állapotába megy át a „szupergép”. A nulladik programsornak megfelelő Turing-gép start állapota lesz a „szupergép” start állapota, míg az üres soroknak a „szupergép” halt állapota felel meg.

A legtöbb utasítás szimulálása a RAM-gép végrehajtási idejével arányos számú lépéssel történik. Kivétel az olvasás, de ha a RAM-gép futásideje n , akkor ehhez sem kell $O(n)$ -nél több lépés, így a teljes lépésszám $O(n^2)$. $\square$

10.1.47. Megjegyzés. Az előző tétel bizonyításából világos, hogy ha jelentősen kibővítjük a RAM-gép utasításkészletét (például kivonás, „immediate” konstansok, „imme-

diate” írás és olvasás, szorzás, osztás stb.), a fenti tétel akkor is érvényes marad. Ha a regiszterek számát megnöveljük, akkor is csak a szalagok számát kell megnövelni.

10.1.48. Tárolt programú gép. Egy másik, a valódi számítógépekhez közel álló számítógépmoddell a *tárolt programú gép*. A memória ugyanolyan, mint a RAM-gépnél, de most a program is a memóriában van. A gépnek csak egy regisztere van, az *A akkumulátor*. Az *utasításkészlet* lehet például az alábbi:

LD <i>n</i>	% $A \leftarrow M[n]$
LDI <i>n</i>	% $A \leftarrow n$
ST <i>n</i>	% $M[n] \leftarrow A$
ADD <i>n</i>	% $A \leftarrow A + M[n]$
ADDI <i>n</i>	% $A \leftarrow A + n$
SUB <i>n</i>	% $A \leftarrow A - M[n]$
JNP <i>p</i>	% $A \leq 0$ esetén a programvégrehajtás % a <i>p</i> címen folytatódik.

Minden utasítás két szomszédos rekeszt foglal el a memóriában: a kisebb című rekeszben van az utasítás kódja, ami egy nem nulla egész szám, a nagyobb című pedig az *n* szám. A programvégrehajtás a 0 címen lévő utasítással indul, és megáll, ha érvénytelen utasításkódot olvas. Mivel az utasításban *n* felülírható, indexregiszterre (és *B* regiszterre) nincs szükség, és a gép igen „szerény” utasításkészlet esetén is nagyon rugalmas. A tárolt program elve Neumann Jánostól származik, és nagyon fontos újítás volt az első számítógépeknél, hiszen bonyolult hardver építése nemcsak nagyon drága lett volna, hanem jelentősen nőtt volna a hardvermeghibásodások száma is (az első gépeket kb. óránként kellett javítani).

Természetesen ez a gép is még tovább bővíthető további utasításokkal és regiszterekkel. Durván szólva azt lehet mondani, hogy egy tárolt programú gép ekvivalens egy „hasznos” utasításkészletű RAM-géppel, abban az értelemben, hogy az egyik minden utasítása konstans számú utasítással szimulálható a másikon.

*** 10.1.49. Markov-automaták.** Egy *Markov-automata* egy olyan speciális $f: Q \rightarrow Q$ számítási eljárás, amelyben az állapotok Q halmazát (σ, i) párok alkotják, ahol $\sigma \in A^*$ valamely A véges ábécére és valamely adott $N \in \mathbb{N}$ természetes számra $0 \leq i \leq N$. A bemeneti állapotok a $(\sigma, 0)$ párok, a kimeneti állapotok pedig a (σ, N) párok. Az átmeneti függvényt a $0 \leq i < N$ -re megadott $\alpha_i, \beta_i \in A^*$ szavak és $0 \leq a_i, b_i \leq N$ számok segítségével adjuk meg: ha α az a legrövidebb szó, amelyre $\sigma = \alpha\alpha_i\beta$ valamely $\beta \in A^*$ -ra, akkor $f(\sigma, i) = (\alpha\beta_i\beta, b_i)$, ha pedig nincs ilyen szó, akkor $f(\sigma, i) = (\sigma, a_i)$ minden $0 \leq i < N$ esetén és természetesen $f(\sigma, N) = (\sigma, N)$.

*** 10.1.50. Turing-gép szimulálása Markov-automatán.** *Egyszalagos Turing-gép szimulálható Markov-automatán.*

Bizonyítás. Az ötlet az, hogy – az előző definíció jelöléseivel – σ az aktuális szalagtartalom lesz, a fej pedig beágyazzuk a szalagba, az éppen olvasott betű mellé, attól balra. Feltehetjük, hogy a $T = (B, A, \varphi)$ Turing-gép belső állapotai és ábécéjének elemei számok, $B = \{0, 1, \dots, n\}$, ahol 0 a start, n pedig a halt állapot és $A = \{0, 1, \dots, r\}$, a 0 az üres jel. A Turing-gép szalagábécéjét egyetlen betűvel kell bővíteni. Legyen $A \cup \{\downarrow\}$

a Markov-automata ábécéje, ahol $\downarrow$ a fej jele. A szimuláció során σ mindig tartalmazza a fej jelet. A Turing-gép egy $0 \leq j < n$ állapotának a Markov-automata $j(r+2)^2 \leq i < (j+1)(r+2)^2$ állapotai fognak megfelelni, az n állapotnak pedig a $N = n(r+2)^2$ állapot. A Turing-gép egy lépését a Markov-automata legfeljebb $2r+4$ lépése fogja szimulálni. Legyen $\varphi(j, k) = (j', k', c)$, ahol $c \in \{<, =, >\}$, azaz tegyük fel, hogy a Turing-gép a j belső állapotban a k számot olvasva a j' belső állapotba megy át, a k' számot írja ki, és a c irányba lép. Az alapgondolat, hogy a Turing-gép j belső állapotának megfelelő $i = j(r+2)^2 + k$ ($0 \leq k \leq r$) Markov-automata állapotokban sorra ellenőrizzük, hogy a fej alatt k van-e, azaz legyen $\alpha_i = k\downarrow$. Ha nem, a következő i -re lépünk, azaz mindegyik esetben $\alpha_i = i+1$. Ha c az = jel, akkor legyen $\beta_i = k'\downarrow$, $b_i = j'(r+2)^2$, azaz ha megtaláltuk, hogy a Turing-gép mit olvasna és helyben kell maradnunk, akkor írjuk ki a megfelelő k' betűt és a fej jelet, és menjünk a Markov-automata j' -nek megfelelő állapotai közül az elsőre. Ha c a < jel, akkor hasonlóan legyen $\beta_i = \downarrow k'$, $b_i = j'(r+2)^2$, azaz ha megtaláltuk, hogy a Turing-gép mit olvasna és balra kell lépünk, akkor írjuk ki a fej jelet, majd k' -t, majd menjünk a Markov-automata j' -nek megfelelő állapotai közül az elsőre. Ha nem találtuk a fejjet, akkor így végül az $i = j(r+2)^2 + r+1$ állapotba jutunk. Ekkor a szalag (teleírt) részének az elején áll a fej, tehát legyen $\alpha_i = \downarrow$, és ha c az = jel, akkor legyen $\beta_i = k'\downarrow$, ha pedig c a < jel, akkor legyen $\beta_i = \downarrow k'$. Maradt a jobbra lépés kezelése. Ha c a > jel, akkor legyen $\beta_i = \alpha_i = k\downarrow$, és legyen $b_i = j(r+2)^2 + (k+1)(r+2)$. A Markov-automata ezen állapota azt jelenti, hogy a j állapotban a k betűt olvastuk. Ez az állapot az utána következő $r+1$ állapottal együtt – hasonlóan az eddig leírtakhoz – elolvassa a fejtől jobbra álló jelet, és megcseréli a fejjel, majd a Markov-automata $j'(r+2)^2$ állapotába megy. $\square$

*** 10.1.51. Markov-automata szimulálása Turing-gépen.** *Markov-automata szimulálható Turing-géppel.*

Bizonyítás. A Markov-automata definíciójánál használt jelöléseket fogjuk használni. Feltehetjük, hogy a Markov-automata ábécéje nem tartalmazza a $\square$ jelet. A szimulálást $N+1$ szalagos Turing-gépen végezzük. Az első szalagra kerül a σ szó, az $i+2$ -edik szalagra pedig az α_i és β_i szavak egy $\square$ jellel elválasztva. Minden i -re a szimulálást belső állapotok egy halmaza végzi ($i = N$ -re a halt állapot): a szó bal széléről indulva megkeressük az α_i szót σ -ban, és felülírjuk $\square$ jelekkel. (Ha nem találjuk, készen vagyunk, áttérhetünk az α_i -nek megfelelő lépésekre.) Most összehasonlítjuk β_i hosszát az üres helyek számával, és megfelelő irányba addig mozgatjuk az α vagy a β szót, amíg az üres helyek száma egyenlő nem lesz β_i hosszával. Végül bemásoljuk az üres helyekre a β_i szót, és a b_i -nek megfelelő lépésekre térünk át. Azok az esetek, amikor α , β , α_i vagy β_i üres szó, némi elővigyázatosságot igényelnek. $\square$

*** 10.1.52. Sejtautomaták.** A sejtautomaták egy „nagyon erősen párhuzamos” számítási modellt írnak le. Szokás „nem Neumann elvű” számítógépekről is beszélni, ami óriási tévedés, mert a sejtautomatákat Neumann János használta először önreprodukáló automaták létezésének bizonyítására. Az alapgondolat, hogy a d -dimenziós tér minden $\mathbb{Z}^d$ -beli *rácspont*jába teszünk egy-egy ugyanolyan (véges) automatát. Ennek állapotait valamely véges halmaz, az A állapot-ábécé elemei adják meg. Itt is feltesszük, hogy a $\square$ *üres állapot* szerepel az állapotok között. A triviális eset kizárására feltesszük, hogy $A_0 = A \setminus \{\square\}$ nem üres, azaz legalább két állapot van. Az $i \in \mathbb{Z}^d$ pontban lévő automata adott t időpontbeli állapotát jelölje a_i . A következő, $t+1$ időpontban ez az automata

valamely a'_i állapotban lesz. Ez az állapot csak az adott automata valamely adott korlátos (véges sok rácpontból álló) környezetében lévő automaták állapotától függ, és ez a környezet minden automataira ugyanúgy néz ki. Az összes automata állapotváltozása egyszerre, szinkronizáltan történik. Pontosabban, adott egy $K = (k_1, k_2, \dots, k_n)$ véges sorozat, a *környezet*, amely $\mathbb{Z}^d$ -beli vektorokból áll, és egy $\varphi: A^n \rightarrow A$ *átmeneti függvény*. Minden $i \in \mathbb{Z}^d$ -re $a'_i = \varphi(a_{i+k_1}, a_{i+k_2}, \dots, a_{i+k_n})$. Feltesszük továbbá, hogy a $t = 0$ kezdeti időpontban csak véges sok automata van nem üres állapotban, és hogy $\varphi(\sqcup, \sqcup, \dots, \sqcup) = \sqcup$, azaz a nem üres állapotok „nem generálódnak maguktól”. Indukcióval adódik, hogy minden $t \in \mathbb{N}$ időpontban csak véges sok automata van nem üres állapotban.

Formálisan, a *sejtautomata* az (A, K, φ) hármas. Világos, hogy egy sejtautomatát számítási eljárásnak tekinthetünk, ha állapotnak az összes olyan $\mathbb{Z}^d$ -t A -ba képező $i \mapsto a_i$ függvényt tekintjük, amely csak véges sok helyen vesz fel az üres jeltől különböző értéket, kimeneti állapotnak pedig azon állapotok halmazát, amelyek „stabilak”, azaz amelyekre $a_i = a'_i$ minden $i \in \mathbb{Z}^d$ -re.

*** 10.1.53. Példák.** (1) Ha a K környezetben pontosan azok a $k \in \mathbb{Z}^d$ vektorok vannak, amelyeknek minden koordinátája 0, kivéve legfeljebb egyet, amely lehet 1 vagy -1 is, akkor *Neumann-szomszédságról* beszélünk. (A $d = 2$ esetben ilyen szomszédsággal, 29 állapottal adott meg Neumann János önreprodukáló sejtautomatát; lásd [15], 11–56. o.)

(2) Ha a K környezetben pontosan azok a $k \in \mathbb{Z}^d$ vektorok vannak, amelyeknek minden koordinátája 0, 1 vagy -1 , akkor *Moore-szomszédságról* beszélünk. Jól ismert példa sejtautomatára a $d = 2$ esetben $A = \{\sqcup, \text{I}\}$ ábécével és Moore-szomszédsággal a *Conway-féle életjáték*; ennél φ értéke I, ha pontosan három változója I, az előző érték, ha pontosan négy változója I, és $\sqcup$ egyébként.

(3) Természetesen további szomszédságok is elképzelhetők. A masszív parallel gépek meglehetősen hasonlóak ehhez a gépmodellhez, de $\mathbb{Z}^d$ helyett annak egy véges részhalmaza szerepel.

*** 10.1.54. Sejtautomata szimulálása Turing-gépen.** Bármely sejtautomata szimulálható Turing-gépen.

Bizonyítás. A szimulálást háromszalagos gépen fogjuk végezni. Legyen A a sejtautomata állapotábécéje. Az egyszerűség kedvéért tegyük fel, hogy a sejtautomata ábécéje tartalmaz az üres jelen kívül még legalább három jelet, és ezek 0, 1 és $-$; legyen a Turing-gép ábécéje is A . Írjuk fel az első szalagra tetszőleges sorrendben mindazokat az (a_i, i) , $i \in \mathbb{Z}^d$ párokat, amelyekre $a_i \neq \sqcup$

$$a_i a_i \dot{i}_1 \dot{i}_2 \dots \sqcup \dot{i}_d$$

alakban, ahol az i vektor $i_1, \dots, i_d$ koordinátáit a 0, 1, $-$ jelekkel adjuk meg kettes számrendszerben.

Az alapgondolat, hogy az első szalagon szereplő „állapotleírásból” (amelyben az üres állapotban lévő rácpontok nem szerepelnek) a harmadik szalagra kiszámítjuk az új állapotleírást, a második szalagot használva segédszalagnak. A $K = (k_1, \dots, k_n)$ környezetet „emlékezetünkben tartva” tekintünk egy, az első szalagon szereplő i vektort, és minden $k_1, \dots, k_n$ vektorra írjuk fel a $j = i - k_\ell$ vektor koordinátáit az üres jellel elválasztva a második szalagra. A j egy olyan vektor, amelyben az állapot változhat. (Az első szalagon azt az i -t, amellyel éppen dolgozunk, úgy jelöljük meg, hogy a kétszer szereplő a_i

állapotbetűből a jobb oldalit ideiglenesen $\square$ -re cseréljük.) Ha ez a vektor már szerepel a harmadik szalagon, töröljük, és a következővel folytatjuk. Egyébként számítsuk ki a $j + k_1$ vektor koordinátáit, és írjuk a második szalagra j koordinátáitól balra (elválasztó jelnek $\square$ jelet használunk). Újra végigolvasva az első szalagot, keressük meg a $j + k_1$ vektorhoz tartozó állapotot, és írjuk a második szalagon a $j + k_1$ -től balra eső $\square$ jeltől balra (ha a vektor nem szerepel az első szalagon, az állapot $\square$), majd számítsuk ki, és írjuk a második szalagra a $j + k_2$ vektor koordinátáit, és keressük meg az ehhez a vektorhoz tartozó állapotot stb. Ha a j környezetéhez tartozó összes állapot megvan, „emlékezetből” tudhatjuk, hogy milyen állapotba megy át a j vektorhoz tartozó automata. Ha az új állapot nem az üres, a j vektort és a hozzá tartozó új állapotot írjuk a harmadik szalagra, ugyanabban a formátumban, ahogy az első szalagon volt.

Végül, ha minden új állapot megvan, ellenőrizzük, hogy az új állapotleírás (sorrendtől eltekintve) megegyezik-e a régivel. Először megnézzük, hogy ugyanolyan hosszú-e. Ha igen, az első szalagon szereplő minden (a_i, i) párt megkeressük a harmadik szalagon. Ha mindet megtaláltuk, az új állapotleírás ugyanaz, és megállhatunk. Egyébként töröljük az első szalagot, átmásoljuk rá a harmadik szalag tartalmát, és folytatjuk a szimulálást. $\square$

*** 10.1.55. Turing-gép szimulálása sejtautomatán.** Minden egyszalagos Turing-gép A ábécével és B belsőállapot-halmazzal szimulálható egydimenziós sejtautomatán Neumann-szomszédsággal $\natural(A) + 4\natural(B)$ elemű állapotábécével.

Bizonyítás. Az alapgondolat, hogy a fejet beágyazzuk a szalagba. Feltehetjük, hogy A és B diszjunktak. Legyen az állapotábécé $A \cup B \cup (B \times \{<, =, >\})$. Minden sejt valamely $a \in A$ állapotban van, kivéve egyet, amely a $B \cup (B \times \{<, =, >\})$ állapotok valamelyikében van, ez a „fej”, a többi alkotja a „szalagot”. A fej által éppen olvasott betűt a tőle balra álló sejt reprezentálja. A Turing-gép egy lépését két fázisban szimuláljuk. Az első fázisban a fej a Turing-gép aktuális b belső állapotának megfelelő állapotban van. Észelve a tőle balra álló „szalagjelet”, átmegy a megfelelő (b', x) állapotba ($x \in \{<, =, >\}$), míg a tőle balra álló „szalagjel” a megfelelő a' -re változik. Minden más „szalagjel” változatlan marad. A második fázisban történik a fej mozgása: ha x az = jel, akkor a fej a (b', x) állapotból a b' állapotba megy át, míg a „szalagjelek” nem változnak. Ha x a > jel, akkor a fej jobbra mozog: a tőle jobbra álló automata a b' állapotba megy át, míg ő maga abba a „szalagállapotba”, amelyben a tőle jobbra álló automata volt. A többi automata állapota nem változik. Hasonlóan mozog balra a fej, ha x a < jel. Nyilván csak a Neumann-szomszédságot használtuk. $\square$

*** 10.1.56. Church-féle λ -kalkulus.** A Turing-gépekkel egyidős Alonzo Church 1936-ban bevezetett úgynevezett λ -kalkulusa. Ebben az alapfogalom a függvény. A függvényekkel különböző műveletek végezhetők, például egymásba lehet helyettesíteni őket. A legfontosabb művelet az absztrakció művelete, a λ -művelet. Például

$$s = \lambda x.[x - x^3/6 + x^5/120]$$

az s -et egy függvénynek (adott esetben egy ötödfokú polinomfüggvénynek, a sin függvény egy közelítésének) definiálja, amelyre $s(x) = x - x^3/6 + x^5/120$. A λ -kalkulus ismertetése magyar nyelven Csörnyei [11] könyvében található meg. A λ -kalkulus is ekvivalens egyéb algoritmusfogalmakkal. Alapgondolatai szerepelnek az egyik legrégebbi programozási nyelvben, az 1959-ben bevezetett és ma is használatos LISP nyelvben (például az

EMACS szövegszerkesztő ezen a nyelven programozható). Több komputeralgebra-rendszer is tartalmaz függvényabsztrakciót műveletként.

→ **10.1.57. Feladat** [9]. Hogyan írhatunk bárhonnán hívható „szubrutint” tárolt programú gépre? Oldjuk meg ugyanezt RAM-gépre, illetve Turing-gépre.

10.1.58. További feladatok. [25]: VII.1.1–VII.1.6, VII.1.9–VII.1.13, VII.1.17, VII.1.19, VII.1.24–VII.1.26; [59]: III.2.1–III.2.25.

10.2 Kiszámíthatóság

10.2.1. Kiszámítható függvények. Legyen A egy legalább kételemű ábécé, amely tartalmazza a $\sqcup$ jelet, és legyen $A_0 = A \setminus \{\sqcup\}$. Egy $f: A_0^{*m} \rightarrow A_0^{*n}$ függvényt *Turing-kiszámíthatónak* vagy röviden csak *kiszámíthatónak* nevezünk, ha van olyan Turing-gép (akárhány, de legalább $\max\{m, n\}$ szalaggal, A ábécével), amely bármely $(\alpha_1, \alpha_2, \dots, \alpha_m) \in A_0^{*m}$ bemenettel (vagyis az első m szalagjára rendre az $\alpha_1, \alpha_2, \dots, \alpha_m$ szavakat írva) megáll, és az utolsó n szalagjára rendre $f(\alpha_1, \alpha_2, \dots, \alpha_m)$ koordinátái vannak írva.

Általánosabban, egy $f \in A_0^{*m} \rightarrow A_0^{*n}$ parciális függvényt *parciálisan Turing-kiszámíthatónak* vagy röviden csak *parciálisan kiszámíthatónak* nevezünk, ha van olyan Turing-gép (akárhány, de legalább $\max\{m, n\}$ szalaggal, A ábécével), amely egy

$$(\alpha_1, \alpha_2, \dots, \alpha_m) \in A_0^{*m}$$

bemenettel (vagyis az első m szalagjára rendre az $\alpha_1, \alpha_2, \dots, \alpha_m$ szavakat írva) pontosan akkor áll meg, ha $(\alpha_1, \alpha_2, \dots, \alpha_m) \in \text{dmn}(f)$, és ekkor az utolsó n szalagjára rendre $f(\alpha_1, \alpha_2, \dots, \alpha_m)$ koordinátái vannak írva.

Ha egy Turing-gépet egy függvény kiszámítására akarunk felhasználni, akkor általában kényelmesebb néhány „írásjellel” kibővíteni az ábécét, és egyetlen szalagon adni meg a bemenetet. Ugyanez érvényes a kimenetre is. Például, ha egy egyváltozós egész együtthatós polinom a bemenet, akkor választhatjuk az $A = \{\sqcup, 0, 1, -\}$ ábécét, minden együtthatót más szalagra írva fel kettes számrendszerben, de kényelmesebb az ábécéhez hozzávenni a $;$ pontosvessző jelet is, és az együtthatókat (mondjuk a kitevők növekvő sorrendjében) egy szalagra felírni, pontosvesszővel választva el azokat. Ha egy többváltozós, egész együtthatós $\sum a_{i_1, \dots, i_\ell} x_1^{i_1} x_2^{i_2} \cdots x_\ell^{i_\ell}$ polinom a bemenet, akkor az ábécéhez még a $,$ vessző jelet is hozzávéve, az $a_{i_1, \dots, i_\ell}, i_1, \dots, i_\ell$; szavakat, ahol $a_{i_1, \dots, i_\ell} \neq 0$, tetszés szerint egymás után írva adhatjuk meg a polinomot. Ezen megfontolások alapján elsősorban az $f: A_0^* \rightarrow A_0^*$ kiszámítható függvények és az $f \in A_0^* \rightarrow A_0^*$ parciálisan kiszámítható függvények érdekelnek bennünket.

10.2.2. Nyelvek. Gyakran csak igen-nem problémák érdekelnek bennünket, és a Turing-gépet ilyen problémák megoldására használjuk. Például, ha csak az érdekel bennünket, hogy egy

$$p(x_1, \dots, x_\ell) = \sum a_{i_1, \dots, i_\ell} x_1^{i_1} x_2^{i_2} \cdots x_\ell^{i_\ell}$$

egész együtthatós polinomra a $p(x_1, \dots, x_\ell) = 0$ egyenletnek van-e egész számokból álló megoldása, akkor olyan Turing-gépet szeretnénk készíteni, amely ezt megmondja. Azok a bemenetek, amelyekre van megoldás, az összes lehetséges bemenetek egy részhalmazát alkotják, és ami érdekel bennünket, az úgy fogalmazható, hogy egy adott bemenet

benne van-e ebben a részhalmazban. Nem világos, hogy van-e olyan Turing-gép, amely ezt megmondja, bár olyan Turing-gépet tudunk készíteni, amely (valamilyen sorrendben kipróbálva az összes $(x_1, \dots, x_\ell) \in \mathbb{Z}^\ell$ lehetőséget) megáll, ha van megoldás, és azt ki is írja.

A fenti megfontolások alapján, az előző definíció jelöléseivel, egy $\mathcal{L} \subset A_0^*$ halmazt *nyelvnek* fogunk nevezni. Bár az előző pont megfontolásai szerint elsősorban a nyelvek érdekelnek bennünket, az alábbi két fogalmat mégis célszerű lesz általánosabban definiálni.

10.2.3. Eldönthető nyelvek. Az előző pont jelöléseivel, egy $\mathcal{L} \subset A_0^*$ nyelvet, vagy általánosabban egy $\mathcal{L} \subset A_0^{*m}$ halmazt *Turing-eldönthetőnek* vagy röviden csak *eldönthetőnek* nevezünk, ha van olyan Turing-gép (legalább m szalaggal, A ábécével), amely bármely A_0^{*m} -beli bemenetre megáll, és jelzi, hogy a bemenet benne van-e $\mathcal{L}$ -ben: ha benne van, akkor az A_0^* -beli kimeneti szó nem üres, ha pedig nincs benne, akkor üres. Az $\mathcal{L} \subset A_0^{*m}$ halmaz nyilván pontosan akkor eldönthető, ha az $A_0^{*m} \setminus \mathcal{L}$ komplementere eldönthető. Minden véges halmaz eldönthető, mivel megadható olyan Turing-gép, amely „emlékszik” a halmazra. Mivel kontinuum sok nyelv van – hiszen egy megszámlálható végtelen halmaznak kontinuum sok részhalmaza van –, de csak megszámlálható sok Turing-gép – hiszen egy Turing-gépet teljesen jellemez a (B, A, φ) hármas, amelyek mindegyike megszámlálható sokféle lehet, mert feltehetjük, hogy $A, B \subset \mathbb{N}$ –, kell lennie nem eldönthető nyelvnek (sőt, ezek vannak többségben).

10.2.4. Felsorolható nyelvek. Az előző pont jelöléseivel, egy $\mathcal{L} \subset A_0^*$ nyelvet, vagy általánosabban egy $\mathcal{L} \subset A_0^{*n}$ halmazt *Turing-felsorolhatónak* vagy röviden csak *felsorolhatónak* nevezünk, ha vagy üres, vagy van olyan Turing-gép (legalább n szalaggal, A ábécével), amellyel valamely adott $I \in A_0$ jelre, $\{I\}^*$ szavait írva a bemenetre, $\mathcal{L}$ elemeit kapjuk meg kimenetként (esetleg több bemenetre is ugyanazt). Nyilván lényegtelen, hogy A_0 melyik betűjét választjuk I -nek, hiszen a Turing-gép kezdheti azzal a működését, hogy végigmegy a bemeneten, és annak minden betűjét kicseréli I -re. Mivel kontinuum sok nyelv van, és megszámlálható sok Turing-gép, kell lennie nem felsorolható nyelvnek.

10.2.5. Kiszámítható parciális függvények. Az előző pont jelöléseivel egy $f \in A_0^* \rightarrow A_0^*$ parciális függvényt *Turing-kiszámíthatónak* vagy röviden csak *kiszámíthatónak* nevezünk, ha értelmezési tartománya eldönthető, ő maga pedig parciálisan kiszámítható. Ilyen függvényeknél adott bemenetről előbb el tudjuk dönteni, hogy az értelmezési tartományban van-e, és ha igen, csak akkor kezdjük kiszámítani a függvényt, így gépünk biztos, hogy megáll. Ha jelezni akarjuk, hogy a bemenet nincs az értelmezési tartományban, egyik lehetőségünk, hogy az utolsó előtti szalagot „standard error” szalagnak tekintjük, és ha a bemenet nincs az értelmezési tartományban, ide az üres jelet írjuk, egyébként pedig nem az üres jelet. A másik lehetőség, hogy az eredményt mindig valamilyen (az üres jeltől különböző) „írásjellel” zárjuk le, és a kimenet csak akkor lesz üres, ha a bemenet nincs az értelmezési tartományban. Általánosabban, az $f \in A_0^{*m} \rightarrow A_0^{*n}$ parciális függvényt *Turing-kiszámíthatónak* vagy röviden csak *kiszámíthatónak* nevezünk, ha értelmezési tartománya eldönthető, ő maga pedig parciálisan kiszámítható. A fenti két módszer segítségével itt is jelezhetjük, hogy a bemenet nincs az értelmezési tartományban.

→ **10.2.6. Feladat [3].** Mutassuk meg, hogy ha az ugyanazon ábécé feletti $\mathcal{L}_1$ és $\mathcal{L}_2$ nyelvek eldönthetőek, akkor $\mathcal{L}_1 \cap \mathcal{L}_2$, $\mathcal{L}_1 \cup \mathcal{L}_2$, $\mathcal{L}_1 \setminus \mathcal{L}_2$ és $\mathcal{L}_1 \triangle \mathcal{L}_2$ is az.

→ **10.2.7. Feladat [3].** Mutassuk meg, hogy ha az ugyanazon ábécé feletti $\mathcal{L}_1$ és $\mathcal{L}_2$ nyelvek felsorolhatóak, akkor $\mathcal{L}_1 \cap \mathcal{L}_2$ és $\mathcal{L}_1 \cup \mathcal{L}_2$ is az.

10.2.8. Feladat [7]. Mutassuk meg, hogy ha az ugyanazon ábécé feletti $\mathcal{A}$, $\mathcal{B}$ és $\mathcal{C}$ nyelvekre $\mathcal{A}$ és $\mathcal{B}$ felsorolhatóak és diszjunktak, $\mathcal{C}$ pedig eldönthető, valamint $\mathcal{A} \subset \mathcal{C} \subset \mathcal{A} \cup \mathcal{B}$, akkor $\mathcal{A}$ is eldönthető.

→ **10.2.9. Feladat [6].** Mutassuk meg, hogy ha az ugyanazon ábécé feletti $\mathcal{A}$ és $\mathcal{B}$ nyelvek felsorolhatóak, akkor léteznek olyan diszjunkt felsorolható $\mathcal{A}_1$ és $\mathcal{B}_1$ nyelvek, amelyekre $\mathcal{A}_1 \subset \mathcal{A}$, $\mathcal{B}_1 \subset \mathcal{B}$, és $\mathcal{A}_1 \cup \mathcal{B}_1 = \mathcal{A} \cup \mathcal{B}$.

10.2.10. Tétel. Az előző definíció jelöléseivel egy nem üres $\mathcal{L} \subset A_0^*$ nyelv akkor és csak akkor felsorolható, ha van olyan kiszámítható $f: A_0^* \rightarrow A_0^*$ függvény, amelynek $\mathcal{L}$ az értékkészlete. Általánosabban, rögzített n -re és bármely m -re, egy nem üres $\mathcal{L} \subset A_0^{*n}$ halmaz pontosan akkor felsorolható, ha valamely kiszámítható $f: A_0^{*m} \rightarrow A_0^{*n}$ függvény értékkészlete.

Bizonyítás. Feltehetjük, hogy $A = \{0, 1, \dots, r\}$ és 0 az üres jel. Az első állítás bizonyításához vegyük észre, hogy először egy Turing-géppel az $|\alpha|_r$ szám unáris felírásává konvertálva egy $\alpha \in A_0^*$ bemeneti szót, majd működtetve az $\mathcal{L}$ -et felsoroló Turing-gépet ($I=1$), olyan Turing-gépet kapunk, amely egy $f: A_0^* \rightarrow A_0^*$ függvényt számít ki, melynek értékkészlete $\mathcal{L}$. Megfordítva, $\{1\}^*$ egy ℓ hosszú szavát Turing-géppel előbb olyan $\alpha \in A_0^*$ szóvá konvertálva, amelyre $\ell = |\alpha|_r$, majd működtetve az f -et kiszámító Turing-gépet, $\mathcal{L}$ egy felsorolását kapjuk.

Az általános esetben is hasonlóan járunk el, de miután az $\alpha_i \in A_0^*$, $1 \leq i \leq m$ bemeneti szót minden szalagon átkonvertáltuk $|\alpha_i|_r$ unáris alakjává, ezeket valahogyan egyetlen szám unáris alakjává kell konvertálni. Tanultuk, hogy a $\varphi(u, v) = w(w+1)/2 + u$, $w = u+v$ összefüggésekkel definiált függvény kölcsönösen egyértelműen képezi le $\mathbb{N} \times \mathbb{N}$ -et $\mathbb{N}$ -re (lásd 5.2.7), és nyilván könnyen számítható még unáris Turing-gépen is. Így a

$$(1) \quad (j_1, j_2, \dots, j_m) \mapsto \varphi\left(j_1, \varphi\left(j_2, \varphi\left(j_3, \dots, \varphi(j_{m-1}, j_m) \dots\right)\right)\right)$$

leképezés kölcsönösen egyértelműen képezi le $\mathbb{N}^m$ -et $\mathbb{N}$ -re, és nyilván könnyen számítható még unáris Turing-gépen is.

A megfordításhoz φ inverzét kell kiszámítani. Azon $u, v \in \mathbb{N}$ számok megkereséséhez, amelyekre $\varphi(u, v)$ egy adott $z \in \mathbb{N}$ természetes szám, meg kell keresni azt az (egyetlen) w természetes számot, amelyre $w = u + v$ és $z = w(w+1)/2 + u$. Sorban próbálkozva a $w = 0, 1, \dots$ értékekkel (hasonlóan, mint 10.1.23(7)-ben), keressük meg azt az (egyetlen) w -t, amelyre $0 \leq z - w(w+1)/2 = u \leq w$. □

10.2.11. Megjegyzés. A tanult fogalmak közül a parciálisan kiszámítható parciális függvények fogalma az alapfogalom, mert ennek segítségével az összes többi megfogalmazható: a kiszámítható függvények a mindenütt értelmezett parciálisan kiszámítható függvények, az eldönthető halmazok (lényegében) azok a halmazok, amelyeknek a karakterisztikus függvénye kiszámítható, a kiszámítható parciális függvények az eldönthető értelmezési tartományú parciálisan kiszámítható parciális függvények, a (nem üres) felsorolható halmazok pedig az előző tétel szerint a kiszámítható függvények értékkészletei.

10.2.12. A Church-tézis. Az előző fejezet eredményei alátámasztják az úgynevezett *Church-tézist*, mely szerint „algoritmikusan pontosan az számítható ki, ami Turing-géppel”. Szokás *Church–Turing-tézisről* is beszélni, mert Church eredetileg a λ -kalkulusra fogalmazta meg tézisé. A tézis természetesen nem bizonyítható, hiszen az algoritmus fogalmát nem definiáltuk, de minden eddigi tapasztalat alátámasztja. Egy kicsit pontosabb formában a tézis azt mondja ki, hogy az algoritmikusan parciálisan kiszámítható parciális függvények éppen a parciálisan Turing-kiszámítható parciális függvények.

10.2.13. Tétel. Az előző definíció jelöléseivel egy $\mathcal{L} \subset A_0^*$ nyelv akkor és csak akkor felsorolható, ha van olyan Turing-gép (akárhány szalaggal, A ábécével), amelynek első szalagjára $\alpha \in A_0^*$ -ot írva, akkor és csak akkor áll le, ha $\alpha \in \mathcal{L}$, azaz ha $\mathcal{L}$ egy $f \in A_0^* \rightarrow A_0^*$ parciálisan kiszámítható parciális függvény értelmezési tartománya. Általánosabban, rögzített m -re és bármely n -re, egy nem üres $\mathcal{L} \subset A_0^{*m}$ halmaz pontosan akkor felsorolható, ha valamely $f \in A_0^{*m} \rightarrow A_0^{*n}$ parciálisan kiszámítható parciális függvény értelmezési tartománya.

Vegyük észre, hogy itt az értelmezési tartomány szerepel, míg az előző tételben az értékkészlet.

Bizonyítás. Az egyik irány könnyű: legyen $\mathcal{L} \subset A_0^{*m}$ felsorolható; feltehetjük, hogy nem üres. Vegyünk egy T Turing-gépet, amely felsorolja $\mathcal{L}$ -et, és egészítsük ki egy olyan T' Turing-géppé, amely sorra előállítja T -nek a $0, 1, 2, \dots$ unáris kódját az $m + 1$ -edik szalagra bemenetnek, futtatja T -t, majd megnézi, hogy T kimenete az első m szalagra írt adott $(\alpha_1, \dots, \alpha_m) \in A_0^{*m}$ -e, és megáll, ha igen.

A másik irányt először arra a speciális esetre bizonyítjuk, amikor $\mathcal{L}$ nyelv. Feltehetjük, hogy $A = \{0, 1, \dots, r\}$, ahol 0 az üres jel, és hogy $\mathcal{L}$ nem üres. Legyen $\alpha \in \mathcal{L}$ tetszőleges, de rögzített szó, amelynek csak az a szerepe, hogy ezt fogjuk a kimenetre írni, ha „jobbat nem tudunk”. Legyen T az a Turing-gép, amely pontosan akkor áll meg, ha a bemenete egy $\xi \in \mathcal{L}$ szó. Tekintsünk egy T' Turing-gépet, amelynek első szalagjára (unáris kódban) egy $i \in \mathbb{N}$ természetes számot írva, a T első szalagjára (unáris kódban) a $j = i - \lfloor \sqrt{i} \rfloor^2$ számot írja (mert így minden j természetes szám végtelen sokszor kerül T első szalagjára), azt átkonvertálja azzá a $\xi \in A_0^*$ szóvá, amelyre $|\xi|_r = j$, majd i (azaz egyre több) lépésen keresztül próbálja működtetni (azaz szimulálja) T -t. Így minden ξ bemenettel egyre több lépésen át futtatjuk T -t. Ha ezalatt a T gép leáll, akkor T' az utolsó szalagjára ξ -t ír, és leáll. Ha ezalatt T nem áll le, akkor T' az utolsó szalagjára az α szót írja. A T' gép az $\mathcal{L}$ nyelvet sorolja fel.

Az általános esetben, azaz ha $m > 1$, csak annyit kell módosítanunk, hogy az előző tétel bizonyításában látott módon, az ott szereplő (1) leképezés inverzével a j számot „szétkódoljuk” egy $(j_1, j_2, \dots, j_m) \in \mathbb{N}^m$ szám m -essé, és ezt írjuk T bemenő szalagjaira, ezt szalagonként konvertáljuk egy $(\xi_1, \dots, \xi_m) \in A_0^{*m}$ bemenetté, majd i lépésen keresztül működtetjük T -t. Ha ezalatt a T gép leáll, akkor T' utolsó szalagjaira $(\xi_1, \dots, \xi_m)$ kerül, egyébként egy előre rögzített $(\alpha_1, \dots, \alpha_m) \in \mathcal{L}$. $\square$

10.2.14. Lemma. Eldönthető nyelvek felsorolhatóak. Általánosabban, 10.2.1 jelöléseivel, ha egy $\mathcal{L} \subset A_0^{*m}$ halmaz eldönthető, akkor felsorolható is.

Bizonyítás. Tegyük fel, hogy $\mathcal{L} \subset A_0^{*m}$ eldönthető. Ha $\mathcal{L} = \emptyset$, akkor készen vagyunk, egyébként legyen $(\alpha_1, \dots, \alpha_m) \in \mathcal{L}$ tetszőleges, de rögzített.. Bármely

$$(\xi_1, \dots, \xi_m) \in A_0^{*m}$$

bemenetre, ha az $\mathcal{L}$ -beli, másoljuk a kimenetre, egyébként pedig legyen a kimenet

$$(\alpha_1, \dots, \alpha_m). \quad \square$$

10.2.15. Tétel. *Egy nyelv pontosan akkor eldönthető, ha ő is és a komplementere is felsorolható. Általánosabban, 10.2.1 jelöléseivel, $\mathcal{L} \subset A_0^{*m}$ pontosan akkor eldönthető, ha $\mathcal{L}$ és $A_0^{*m} \setminus \mathcal{L}$ is felsorolható.*

Bizonyítás. Ha $\mathcal{L}$ eldönthető, akkor a komplementere is, így az előző lemma szerint mindkettő felsorolható. Megfordítva, tegyük fel, hogy $\mathcal{L}$ és a komplementere is felsorolható. Készítsünk két Turing-gépet, az egyik $\mathcal{L}$ -et, a másik a komplementerét sorolja fel, és egy harmadik gépet, amely felváltva ellátja őket a felsorolásokhoz szükséges bemenettel, futtatja, és figyel, hogy melyik adja ki $(\alpha_1, \dots, \alpha_m)$ -et. Ez előbb-utóbb bekövetkezik, és akkor eldöntöttük, benne van-e az $(\alpha_1, \dots, \alpha_m)$ bemenet $\mathcal{L}$ -ben. Könnyű a három gépet egyetlen géppé összekapcsolni. $\square$

→ **10.2.16. Feladat [3].** Mutassuk meg, hogy vannak ugyanazon ábécé feletti $\mathcal{L}_1$ és $\mathcal{L}_2$ felsorolhatóak nyelvek, amelyekre $\mathcal{L}_1 \setminus \mathcal{L}_2$ és $\mathcal{L}_1 \triangle \mathcal{L}_2$ nem az.

10.2.17. A megállási feladat. Példát akarunk mutatni arra, hogy van algoritmikusan megoldhatatlan problémásereg. Az úgynevezett megállási feladról (*Halting Problem, HP*) fogjuk megmutatni, hogy Turing-géppel nem megoldható: adott egy Turing-gép és a bemenete. Döntsük el, hogy a Turing-gép az adott bemeneten megáll-e? Többet fogunk belátni, két irányban is élesítve az állítást. Először megmutatjuk, hogy létezik olyan Turing-gép, amelyről nem lehet eldönteni, hogy mely bemeneteken áll meg. Ezután megmutatjuk, hogy egy Turing-gép programja alapján nem lehet eldönteni, hogy egyetlen, például az üres bemeneten megáll-e.

Hogy a megállási probléma nem lehet könnyű, azt a következő példa mutatja. A számelmélet egy híres megoldatlan problémája a *Goldbach-sejtés*, mely szerint minden kettőnél nagyobb páros szám előáll két prímszám összegeként, például $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$ stb. Könnyű olyan Turing-gépet megadni, amely megpróbál ellenpéldát keresni erre a sejtésre: üres bemenettel generáljuk sorra a négyenél nagyobb páros számokat az egyik szalagon. Minden ilyen n páros számhoz generáljuk sorra az $1 < p \leq n/2$ páratlan számokat, és döntsük el (próbaosztással), hogy p prím-e? Ha igen, $n - p$ -t is vizsgáljuk meg, hogy prím-e? Ha ez is prím, menjünk a következő n -re, egyébként a következő p -re. Ha adott n -re minden p -t kipróbáltunk, és egy se jó, találtunk egy ellenpéldát. Egy olyan algoritmus, amely eldöntené, hogy ez az üres bemenettel indított Turing-gép megáll-e, megoldaná a Goldbach-sejtést!

A megállási probléma pontos megfogalmazásához legyen egy $T = (B, A, \varphi)$ Turing-gép $\mathcal{L}_T$ nyelve azon $\alpha \in A_0^*$ szavak halmaza, amelyekre a gép minden szalagjára az α szót írva, ezzel a bemenettel T megáll.

Előbb csak kétszalagos Turing-gépre bizonyítunk.

10.2.18. Tétel. *Bármely T Turing-gépre $\mathcal{L}_T$ felsorolható. Bármely ábécére van olyan kétszalagos T Turing-gép, amelyre $\mathcal{L}_T$ nem eldönthető.*

Bizonyítás. Az $\mathcal{L}_T$ nyelv a 10.2.13 tétel szerint felsorolható, mert az a T' gép, amely saját egyetlen α bemenetét lemásolja minden szalagjára, mindegyiken visszamegy α jobb szélére, majd úgy működik, mint T , pontosan $\mathcal{L}_T$ szavaira áll le.

Figyeljük meg, hogy a másik állítás bizonyításának lényege az átlós eljárás. Lényegében egy U kétszalagos univerzális Turing-gépet fogunk felhasználni, amelynek ábécéje tetszőleges, de a gépet kicsit átalakítjuk, hogy az inputja A_0^* -beli legyen. Nyilván feltehetjük, hogy $A = \{0, 1, \dots, r\}$. A T gép második szalagjára egy egyszalagos gép programját unáris kódban írjuk fel. A T a működését azzal kezdi, hogy a második szalagon az unáris kódot (a már látott módon) konvertálja a szokásos A^* -beli programmá, majd úgy működik, mint U . A 10.2.15 tétel szerint elég azt megmutatnunk, hogy $A_0^* \setminus \mathcal{L}_T$ nem felsorolható.

Tegyük fel indirekt módon, hogy $\mathcal{L}_T$ komplementere felsorolható. Ekkor a 10.2.13 tétel szerint létezik olyan T_k Turing-gép k szalaggal, amely pontosan akkor áll le az $\alpha \in A_0^*$ bemenettel, ha $\alpha \notin \mathcal{L}_T$. Készítsünk egy egyszalagos T^* gépet, amely a következőképpen működik: először széthúzza az α bemeneti szót, hogy szomszédos betűi között $2k - 1$ üres jel álljon, majd visszamegy a jobb szélére, és T_k működését szimulálja egy szalagon. A T^* nyilván pontosan akkor áll le, ha $\alpha \notin \mathcal{L}_T$. Legyen T^* programja (unáris kódban) ω . Írjuk a T mindkét szalagjára az ω szót. A szimuláció miatt T pontosan akkor áll le, ha $\omega \notin \mathcal{L}_T$, ami ellentmond $\mathcal{L}_T$ definíciójának. $\square$

10.2.19. Tétel. *Bármely ábécére van olyan egyszalagos S Turing-gép, amelyre $\mathcal{L}_S$ nem eldönthető, azaz nem eldönthető, hogy adott bemenetre S megáll-e.*

Bizonyítás. Készítsünk olyan S egyszalagos Turing-gépet, amely azzal kezdi működését, hogy az α bemenet minden betűjét megduplázza, majd a kapott szó betűit széthúzza egy-egy $\square$ jelet írva közéjük, visszamegy a jobb szélre, és az előző tételben szereplő T kétszalagos gép működését szimulálja egy szalagon. Ekkor $\mathcal{L}_S = \mathcal{L}_T$. $\square$

10.2.20. Tétel. *Eldönthetetlen, hogy egy (leírásával adott) egyszalagos Turing-gép az üres bemeneten megáll-e. Pontosabban, legyen $A = \{0, 1, \dots, r\}$ az ábécé (ahol 0 az üres jel), és álljon $\mathcal{L} \subset \{1\}^*$ azon A ábécéjű egyszalagos Turing-gépek unáris kódban felírt programjaiból, amelyek az üres bemenettel megállnak. Ekkor $\mathcal{L}$ nem eldönthető.*

Bizonyítás. Az előző tételben megadott S gépet módosítsuk úgy, hogy először egy adott $\alpha \in A_0^*$ szót írjon ki a szalagra, menjen a jobb szélére, majd működjön úgy, mint S . Az így kapott T_α gép persze függ az α szótól. Az α szóból és S programjából ki-számíthatjuk T_α univerzális Turing-gépnek szóló programját egy P Turing-géppel. Ha a Turing-gépek programjainak unáris kódjaiból el tudnánk dönteni, hogy üres bemenettel megállnak-e, akkor ezt a gépet működtetve a P gép után, olyan Turing-gépet kapnánk, amely eldöntené, hogy S az α bemenettel megáll-e, ami az előző tétel szerint lehetetlen. $\square$

További példát ad megoldhatatlan problémaseregbe az alábbi tétel.

10.2.21. Tétel. *Eldönthetetlen, hogy egy (leírásával adott) T Turing-gépre az $\mathcal{L}_T$ nyelv üres-e. Pontosabban, legyen $A = \{0, 1, \dots, r\}$ az ábécé (ahol 0 az üres jel), és álljon $\mathcal{L}' \subset \{1\}^*$ azon T' egyszalagos Turing-gépek unáris kódban felírt programjaiból, amelyekre a $\mathcal{L}_{T'}$ nyelv üres, azaz amelyekre T' semmilyen bemenettel sem áll meg. Ekkor $\mathcal{L}'$ nem eldönthető.*

Bizonyítás. A tételt az előző tételre vezetjük vissza. Adott egyszalagos T Turing-géphez konstruáljunk egy egyszalagos T' gépet, amely a következőt csinálja: először letörli a szalagot, majd úgy működik, mint a T gép. Ha T az üres bemeneten véges sok lépésben

megáll, akkor T' minden bemeneten véges sok lépésben megáll, így $\mathcal{L}_{T'}$ nem üres. Ha T az üres bemeneten nem áll meg, akkor T' semmilyen bemeneten sem áll meg. Ez esetben is T programjából a T' programja Turing-géppel megadható. Ha lenne olyan Turing-gép, amely az $\mathcal{L}'$ nyelvet eldönti, akkor ezt a T programjából T' programját kiszámító gép kimenetével mint bemenettel működtetve olyan gépet kapnánk, amely az előző tételben szereplő $\mathcal{L}$ nyelvet eldönti, ami lehetetlen. $\square$

10.2.22. Matematikai problémák algoritmikus megoldhatatlansága. Az eddig tekintett tételek azon alapulnak, hogy a megállási probléma eldönthetetlen, és azon múlnak, hogy Turing-gépekről akarunk valamit Turing-gépekkel eldönteni. Azt gondolhatnánk, hogy a „valódi” matematikai problémáknál nem ez a helyzet. Ez nem így van, sok fontos matematikai problémáról belátták, hogy algoritmussal megoldhatatlan. Két példát mutatunk. Az első *Hilbert tizedik problémája*, amely 1900-ból származik, és csak 1970-ben oldották meg: azt kérdezi, van-e olyan algoritmus, amely egy (többváltozós) egész együtthatós p polinomra eldönti, hogy a $p = 0$ egyenletnek van-e egészekből álló megoldása? A válasz tagadó:

10.2.23. Diophantoszi egyenletek algoritmikus megoldhatatlansága. Azon p többváltozós, egész együtthatós p polinomok nyelve (a polinomok kódolását lásd a 10.2.1 pontban), amelyekre a $p = 0$ egyenletnek van egészekből álló megoldása, nem eldönthető.

Bizonyítás. A bizonyítás nehéz, lásd például Manyin [66] könyvét. $\square$

10.2.24. Dominó-probléma. Véges sok egyforma méretű, négyzet alakú dominót tartalmazó halmazról algoritmussal eldönthetetlen, hogy ilyen dominókkal lefedhető-e az egész sík (a dominókat nem szabad forgatni, mert akkor már egy dominó is elég). Pontosabban, kódoljuk a dominókészletet úgy, hogy dominók oldalaira természetes számokat írunk, amelyeket kettes számrendszerben kódolunk, az északi, keleti, déli és nyugati oldalon lévő számokat ebben a sorrendben pontosvesszőkkel elválasztva egymás mellé írjuk, majd a dominók kódjait szintén pontosvesszőkkel elválasztva írjuk egymás mellé. Azon dominókészletek kódjaiból álló nyelv, amelyekkel a sík lefedhető, nem eldönthető.

Bizonyítás. A bizonyítás vázlatát lásd a Rónyai–Iványos–Szabó [74] könyvben, 222. o. $\square$

10.2.25. Parciális rekurzív és primitív rekurzív függvények. Az $f \in \mathbb{N}^n \rightarrow \mathbb{N}^m$ típusú függvényeket, annak kifejezésére, hogy nem feltétlenül az egész $\mathbb{N}^n$ -en vannak értelmezve, *parciális függvények*nek szokás nevezni. Az

$$n \mapsto n^+, \quad n \in \mathbb{N},$$

$$0^{(n)}: \mathbb{N}^n \rightarrow \mathbb{N}, \quad 0^{(n)}(x_1, x_2, \dots, x_n) = 0, \quad n \in \mathbb{N}$$

$$p_i^{(n)}: \mathbb{N}^n \rightarrow \mathbb{N}, \quad p_i^{(n)}(x_1, x_2, \dots, x_n) = x_i, \quad 1 \leq i \leq n \quad (i\text{-edik vetítés})$$

függvényeket *alappfüggvények*nek fogjuk nevezni. Tekintsük továbbá az alábbi operációkat:

- (1) *összetétel*, amely az $f \in \mathbb{N}^n \rightarrow \mathbb{N}^m$ és $g \in \mathbb{N}^m \rightarrow \mathbb{N}^k$ parciális függvényekhez a $h = g \circ f \in \mathbb{N}^n \rightarrow \mathbb{N}^k$ összetett parciális függvényt rendeli;
- (2) *egyesítés*, amely az $f_i \in \mathbb{N}^n \rightarrow \mathbb{N}^{m_i}$ parciális függvények $f_1, f_2, \dots, f_k$ sorozatához az értelmezési tartományok metszetén értelmezett

$$(f_1, \dots, f_k): (x_1, x_2, \dots, x_n) \mapsto (f_1(x_1, x_2, \dots, x_n), \dots, f_k(x_1, x_2, \dots, x_n))$$

függvényt rendeli, amely $\mathbb{N}^{m_1+m_2+\dots+m_k}$ -ba képez;

- (3) *rekurzió*, amely az $f \in \mathbb{N}^n \rightarrow \mathbb{N}$ és $g \in \mathbb{N}^{n+2} \rightarrow \mathbb{N}$ parciális függvényekhez a

$$h(x_1, \dots, x_n, 0) = f(x_1, \dots, x_n)$$

kezdeti feltétellel és

$$h(x_1, \dots, x_n, k^+) = g(x_1, \dots, x_n, k, h(x_1, \dots, x_n, k)), \quad \text{ha } k \in \mathbb{N}$$

rekurzív lépéssel definiált függvényt rendeli, amelyre $(x_1, \dots, x_n, 0) \in \text{dmn}(h)$ pontosan akkor, ha $(x_1, \dots, x_n) \in \text{dmn}(f)$, és minden $k \in \mathbb{N}$ -re $(x_1, \dots, x_n, k^+) \in \text{dmn}(h)$ pontosan akkor, ha $(x_1, \dots, x_n, k, h(x_1, \dots, x_n, k)) \in \text{dmn}(g)$;

- (4) a *minimalizáló operáció* vagy μ -*operáció*, amely az $f \in \mathbb{N}^{n+1} \rightarrow \mathbb{N}$ parciális függvényhez a

$$\begin{aligned} h(x_1, \dots, x_n) &= \mu x_{n+1} (f(x_1, \dots, x_n, x_{n+1}) = 0) \\ &:= \min \{x_{n+1} : f(x_1, \dots, x_n, x_{n+1}) = 0\} \end{aligned}$$

összefüggéssel definiált függvényt rendeli, amelyre $(x_1, \dots, x_n) \in \text{dmn}(h)$ pontosan akkor, ha van olyan $x_{n+1} \in \mathbb{N}$, amelyre $(x_1, \dots, x_n, k) \in \text{dmn}(f)$ minden $k \leq x_{n+1}$ esetén és $f(x_1, \dots, x_n, x_{n+1}) = 0$. (A μ -operáció az inverz és implicit függvények definiálására szolgál; ez az egyetlen operáció, amely függvényből is parciális függvényt csinálhat.)

A parciális függvényekből álló $f_1, \dots, f_N$ sorozatot az f parciális függvény *parciális rekurzív megadásának* nevezzük, ha $1 \leq i \leq N$ esetén f_i vagy az alapfüggvények valamelyike, vagy az $f_1, \dots, f_{i-1}$ függvények közül valamelyekre alkalmazott (1)–(4) operációk segítségével áll elő, és $f = f_N$. Az f parciális függvényt *parciálisan rekurzív* függvénynek nevezzük, ha van parciális rekurzív megadása. Az f egy olyan $f_1, \dots, f_N$ parciális rekurzív megadását, amelyben $1 \leq i \leq N$ esetén f_i vagy az alapfüggvények valamelyike, vagy az $f_1, \dots, f_{i-1}$ függvények közül valamelyekre alkalmazott (1)–(3) operációk segítségével áll elő, az f *primitív rekurzív megadásának* nevezzük. Ha f -nek van primitív rekurzív megadása, akkor f -et *primitív rekurzív* függvénynek nevezzük. Vegyük észre, hogy a primitív rekurzív függvények értelmezési tartománya az egész $\mathbb{N}^n$ valamely $n \in \mathbb{N}$ -re, mert az alapfüggvények mindenütt értelmezve vannak, és csak a μ -operáció csökkentheti az értelmezési tartományt.

10.2.26. Példák primitív rekurzív függvényekre. (1) Az 1, 2, stb. konstansok (mint $\mathbb{N}^0$ -n értelmezett függvények) definíciója $1 := 0^+$, $2 := (0^+)^+$, stb., azaz a $0^{(0)}$ függvény és az $n \mapsto n^+$ függvény néhányszori összetételével kapjuk őket.

(2) Az

$$n^- = \begin{cases} n - 1, & \text{ha } n > 0, \\ 0, & \text{ha } n = 0 \end{cases}$$

függvény rekurzív definíciója $0^- := 0$ és $(n^+)^- := n$, azaz az előző definícióban szereplő rekurzió jelöléseivel $f = 0^{(0)}$ és $g = p_1^{(2)}$ választással adódik h függvényként. Az $\mathbb{N}$ identikus leképezése az $n \mapsto n^+$ leképezésnek és ennek a leképezésnek az összetétele.

(3) A természetes számok összeadását és szorzását rekurzióval definiáltuk: Az összeadást az $m + 0 := m$ és $m + (n^+) := (m + n)^+$ összefüggésekkel definiáltuk, azaz az

előző definícióban szereplő rekurzió jelöléseivel f -et az identikus leképezésnek, g -t pedig az $(y_1, y_2, y_3) \mapsto y_3^+$ leképezésnek választva kapjuk. A szorzást az $m \cdot 0 := 0$ és $m \cdot (n^+) := m \cdot n + m$ összefüggésekkel definiáltuk, azaz f -et 0-nak, g -t pedig $(y_1, y_2, y_3) \mapsto y_3 + y_1$ leképezésnek választva kapjuk.

(4) Az

$$n \mp m = \begin{cases} n - m, & \text{ha } n \geq m, \\ 0, & \text{ha } n < m \end{cases}$$

telített kivonás rekurzív definíciója $n \mp 0 := n$, $n \mp (m^+) := (n \mp m)^-$, azaz az előző definícióban szereplő rekurzió jelöléseivel f -et az identikus leképezésnek, g -t pedig az $(y_1, y_2, y_3) \mapsto y_3^-$ leképezésnek választva kapjuk. A sgn függvény rekurzív definíciója $\text{sgn}(0) := 0$, $\text{sgn}(n^+) := 1$.

(5) Az informatikában elterjedt jelöléssel, ha R egy binér reláció, legyen

$$[xRy] = \begin{cases} 1, & \text{ha } (x, y) \in R, \\ 0, & \text{ha } (x, y) \notin R \end{cases}$$

az R karakterisztikus függvénye. Nyilván $[n < m] = \text{sgn}(m \mp n)$ és

$$[n = m] = (1 \mp \text{sgn}(n \mp m)) \cdot (1 \mp \text{sgn}(m \mp n)).$$

Ezen függvények segítségével könnyen adódik, hogy minden $f: \mathbb{N}^n \rightarrow \mathbb{N}^m$ függvény, amely csak véges sok helyen vesz fel egy adott $c \in \mathbb{N}^m$ konstanstól különböző értéket, primitív rekurzív. Például $3 \cdot [n = 0] + 2 \cdot [n = 1]$ az a függvény, amely a 0 helyen 3, az 1 helyen 2, egyébként 0.

(6) Az $n \bmod m$ függvény rekurzív definíciója adott m -re: $0 \bmod m := 0$ és $n^+ \bmod m := (n \bmod m)^+ \cdot [(n \bmod m)^+ < m]$.

(7) A $\text{quo}(n, m) = \lfloor n/m \rfloor$ „hányados” függvény rekurzív definíciója adott m -re: $\text{quo}(0, m) := 0$ és

$$\text{quo}(n^+, m) = \text{quo}(n, m) + [(n \bmod m) = m^-].$$

*** 10.2.27. Tétel.** *Parciálisan rekurzív parciális függvény parciálisan kiszámítható unáris kódolásban: minden $f = (f_1, \dots, f_m) \in \mathbb{N}^n \rightarrow \mathbb{N}^m$ parciálisan rekurzív parciális függvényre az a $g = (g_1, \dots, g_m) \in \{1\}^{*n} \rightarrow \{1\}^{*m}$ függvény, amelyre $(\alpha_1, \dots, \alpha_n) \in \text{dmn } g$ pontosan akkor, ha $(|\alpha_1|, \dots, |\alpha_n|) \in \text{dmn } f$ és*

$$|g_i(\alpha_1, \dots, \alpha_n)| = f_i(|\alpha_1|, \dots, |\alpha_n|),$$

ha $1 \leq i \leq n$ és $(\alpha_1, \dots, \alpha_n) \in \text{dmn } g$, parciálisan kiszámítható olyan Turing-géppel, amelynek ábécéje $A = \{\sqcup, 1\}$.

Bizonyítás. A bizonyítás nem nehéz: az az alapgondolata, hogy ha adott az f egy parciális rekurzív felírása, akkor az alapfüggvények triviális programjaiból, a négy operációt programozva szemégyűjtéssel, lépésenként felépíthetők a parciális rekurzív felírásban szereplő függvények programjai, szubrutinként használva az előző függvényeket kiszámító programokat. A részleteket mellőzzük. $\square$

A tétel megfordítása is igaz:

* **10.2.28. Tétel.** *Parciálisan kiszámítható parciális függvény parciálisan rekurzív: az $A = \{0, 1, \dots, r-1\}$ ábécére, amelyben 0 a szökőz, bármely*

$$f = (f_1, \dots, f_m) \in A_0^{*n} \rightarrow A_0^{*m}$$

parciálisan kiszámítható parciális függvényre az a $g = (g_1, \dots, g_m) \in \mathbb{N}^n \rightarrow \mathbb{N}^m$ függvény, amelyre $(|\alpha_1|_{r-1}, \dots, |\alpha_n|_{r-1}) \in \text{dmn}(g)$ pontosan akkor, ha $(\alpha_1, \dots, \alpha_n) \in \text{dmn}(f)$ és

$$g_i(|\alpha_1|_{r-1}, \dots, |\alpha_n|_{r-1}) = |f_i(\alpha_1, \dots, \alpha_n)|_{r-1},$$

ha $1 \leq i \leq n$ és $(\alpha_1, \dots, \alpha_n) \in \text{dmn}(f)$, parciálisan rekurzív parciális függvény.

Bizonyítás. A bizonyítás lényege, hogy mindent számmá kódolunk, majd felépítjük a Turing-gép működését szimuláló parciálisan rekurzív parciális függvényt. Legyen $T = (B, A, \varphi)$ egy k szalagos Turing-gép, amely parciálisan kiszámítja az f parciális függvényt. Feltehetjük, hogy T szemétyűjtéssel dolgozik. Azt is feltehetjük, hogy a belső állapotok számok, a 0 a „halt” állapot, az 1 pedig a „start” állapot. A $<$, $=$, $>$ jelek helyett írjunk rendre 0-t, 1-et, illetve 2-t. A Turing-gép egy állapotát – felhasználva az arról mondottakat, hogy hogyan tekinthetjük a Turing-gépet számítási eljárásnak – az abban szereplő A^* -beli szavakat r alapú számrendszerben számoknak tekintve egy $q = (b, i_1, j_1, \dots, i_k, j_k) \in \mathbb{N}^{2k+1}$ vektorral adhatjuk meg. Ha $q' = (b', i'_1, j'_1, \dots, i'_k, j'_k)$ a következő állapot, akkor q' nyilván q függvénye; megmutatjuk, hogy ez a függés primitív rekurzív. Az ℓ -edik szalagon éppen olvasott a_ℓ betűre $a_\ell = i_\ell \bmod r$, így ez primitív rekurzív függvénye i_ℓ -nek. A $\varphi(b, a_1, \dots, a_k) = (b', a'_1, \dots, a'_k, c'_1, \dots, c'_k)$ függvényt terjesszük ki az egész $\mathbb{N}^{k+1}$ -re úgy, hogy ahol nem volt definíálva, ott legyen nulla. Az így kiterjesztett függvény véges sok hely kivételével mindenütt nullát vesz fel, így primitív rekurzív. Ha $c'_\ell = 1$, azaz az ℓ -edik szalagon helyben maradunk, akkor $i'_\ell = i_\ell$ és $j'_\ell = j_\ell$. Ha $c'_\ell = 0$, azaz az ℓ -edik szalagon balra lépünk, akkor i'_ℓ az $\lfloor i_\ell/r \rfloor$ hányados és $j'_\ell = j_\ell \cdot r + a'_\ell$. Végül, ha $c'_\ell = 2$, az ℓ -edik szalagon jobbra lépünk, akkor $i'_\ell = i_\ell \cdot r + a'_\ell$ és j'_ℓ a $\lfloor j'_\ell/r \rfloor$ hányados. Ezzel beláttuk, hogy q' a q primitív rekurzív függvénye.

Most már definiálhatjuk a Turing-gépet leíró függvényt. Legyen rekurzív definícióval

$$q^*(b, i_1, j_1, i_2, j_2, \dots, i_k, j_k, 0) = (1, i_1, 0, i_2, 0, \dots, i_n, 0, 0, \dots, 0) \in \mathbb{N}^{2k+1}$$

és

$$q^*(b, i_1, j_1, \dots, i_k, j_k, t^+) = q^*(q'(b, i_1, j_1, \dots, i_k, j_k), t),$$

ha $t \in \mathbb{N}$. A q^* függvény azt írja le, hogy a T Turing-gépet a $t = 0$ -ra adott kódú kezdőállapotból indítva, a t időpontban milyen állapotban van, és nyilván primitív rekurzív. Legyen q_ℓ^* a q^* függvény ℓ -edik koordinátája. Az utolsó koordinátára alkalmazzuk a μ -operációt. Azt kapjuk, hogy a

$$t(b, i_1, j_1, \dots, i_k, j_k) = \min\{t: q_1^*(b, i_1, j_1, \dots, i_k, j_k, t) = 0\}$$

megállási időpont parciálisan rekurzív parciális függvény, és pontosan akkor van értelmezve, ha az adott bemenetre a Turing-gép megállt. Így parciálisan rekurzív függvények a kimenetet leíró „ i ”-koordináták, azaz a

$$q_{2\ell}^*(b, i_1, j_1, \dots, i_k, j_k, t(b, i_1, j_1, \dots, i_k, j_k)),$$

$\ell = 1, 2, \dots, m$ koordináta-függvények. Indukcióval t szerint adódik, hogy q^* csak az $i_1, \dots, i_n$ és t változóktól függ. Innen $t(b, i_1, j_1, \dots, i_k, j_k)$ és a kimenetet leíró függvények is csak az $i_1, \dots, i_n$ változóktól függenek. A $t(b, i_1, j_1, \dots, i_k, j_k)$ függvény, és így a kimenetet leíró függvények is pontosan akkor vannak értelmezve, ha az adott bemenetre a Turing-gép megállt. Ezzel beláttuk, hogy a kimenet a bemenet parciálisan rekurzív parciális függvénye.

Egyetlen probléma maradt: a tételben $r - 1$ alapú számrendszer szerepel, míg itt r alapú számrendszerben dolgoztunk. Meg kell mutatnunk, hogy az

$$n = |\alpha|_{r-1} \quad (\alpha \in A_0^*)$$

számhoz az $m = |\alpha|_r$ számot rendelő függvény mindenütt értelmezett parciálisan rekurzív függvény. Legyen $d = n \bmod (r-1)$. Az α utolsó betűje, a következő jegy $d' = d + (r-1) \cdot [d = 0]$. A konverzió egy lépését leíró $s(n, m)$ függvény első koordinátája $\lfloor (n - d')/(r-1) \rfloor$, második koordinátája pedig $m \cdot r + d'$. Legyen rekurzíóval $s^*(n, m, 0) = (n, 0)$ és $s^*(n, m, h^+) = s^*(s(n, m), h)$, ha $h \in \mathbb{N}$, ahol H a konverzió aktuális lépésének sorszáma. A h konverziós hossz, azaz az a lépésszám, amelyre a maradék először nulla lesz, a μ -operációval mint

$$h(n, m) = \min\{h: s_1^*(n, m, h) = 0\}$$

adódik, ahol s_1^* az s^* első koordinátája, a konvertált érték pedig $s_2^*(n, m, h(n, m))$, az s^* második koordinátája, és nem függ m -től, csak n -től, de minden n -re értelmezve van, és pontosan azokat a számokat veszi fel értékként, amelyeknek r alapú (szokásos) felírásában nem szerepel nulla. A másik irányú konverzió ennek a függvénynek az inverze, és hasonlóan adható meg. $\square$

*** 10.2.29. Rekurzív függvények.** Egy $f \in \mathbb{N}^n \rightarrow \mathbb{N}^m$ parciális függvényt *rekurzív* parciális függvénynek nevezünk, ha értelmezési tartományának karakterisztikus függvénye (mint $\mathbb{N}^n$ -en értelmezett függvény) parciálisan rekurzív és f is parciálisan rekurzív. Mivel az egész $\mathbb{N}^n$ karakterisztikus függvénye nyilván parciálisan rekurzív, az egész $\mathbb{N}^n$ -en értelmezett függvény pontosan akkor rekurzív, ha parciálisan rekurzív. Az előző két tétel szerint a rekurzív karakterisztikus függvényű részhalmazok az eldönthető halmazoknak, a parciálisan rekurzív parciális függvények értékkészletei a felsorolható halmazoknak, a rekurzív függvények pedig a kiszámítható függvényeknek felelnek meg, e tételek bizonyításában használt kódolással. Néha át is viszik a rekurzív függvények elméletében használt elnevezéseket a Turing-gépek elméletébe.

→ **10.2.30. Feladat [5].** Alkalmazzuk a rekurzíó operációját a megadott $f: \mathbb{N} \rightarrow \mathbb{N}$ és $g: \mathbb{N}^3 \rightarrow \mathbb{N}$ függvényekre, és határozzuk meg, hogy milyen h függvényt kapunk:

- (1) $f(x_1) = x_1, g(x_1, x_2, x_3) = x_1 + x_3$;
- (2) $f(x_1) = x_1, g(x_1, x_2, x_3) = x_1 + x_2$;
- (3) $f(x_1) = 2^{x_1}, g(x_1, x_2, x_3) = x_3^{x_1}$;
- (4) $f(x_1) = 1, g(x_1, x_2, x_3) = x_3(1 + \operatorname{sgn}|x - 1 + 2 - 2x_3|)$;
- (5) $f(x_1) = 1, g(x_1, x_2, x_3) = (x_3 + 1) \operatorname{sgn}(1 + x_3/3)$.

→ **10.2.31. Feladat [3].** Mutassuk meg, hogy a megadott h függvények primitív rekurzívak (a változók természetes számok):

- (1) $h(x_1, x_2) = x_1 \div x_2^2$;
- (2) $h(x_1) = 3^{x_1}$;
- (3) $h(x_1, x_2, x_3) = x_1^2 x_2 + (x_3 \bmod 2)$.

→ **10.2.32. Feladat [3].** Mutassuk meg, hogy az

$$f(n) = \begin{cases} n^2, & \text{ha } n \text{ páros,} \\ n + 1, & \text{ha } n \text{ páratlan} \end{cases}$$

összefüggéssel definiált függvény primitív rekurzív.

→ **10.2.33. Feladat [5].** Mutassuk meg, hogy a $\tau(n)$ az n osztóinak száma és $\tau(0) = 0$ összefüggéssel definiált függvény primitív rekurzív.

→ **10.2.34. Feladat [5].** Mutassuk meg, hogy a prímszámok halmazának karakterisztikus függvénye primitív rekurzív.

→ **10.2.35. Feladat [3].** Alkalmazzuk a minimalizáció operációját (a megadott, természetes szám változókra) a megadott sorrendben:

- (1) $f(x_1) = 3, i = 1$;
- (2) $f(x_1) = x_1/2, i = 1$;
- (3) $f(x_1, x_2) = p_1^{(2)}(x_1, x_2), i = 2$;
- (4) $f(x_1, x_2) = x_1 \div x_2, i = 1, 2$;
- (5) $f(x_1, x_2) = x_1 - 1/x_2, i = 1, 2$;
- (6) $f(x_1, x_2) = 2^{x_1}(2x_2 + 1), i = 1, 2$.

→ **10.2.36. Feladat [3].** Az alábbi függvényekről (a változók természetes számok) mutassuk meg, hogy parciálisan rekurzívak:

- (1) $f(x_1) = 2 - x_1$;
- (2) $f(x_1) = x_1/2$;
- (3) $f(x_1, x_2) = x_1 - 2x_2$;
- (4) $f(x_1, x_2) = x_1/(1 - x_1 x_2)$.
- (5) $f(x_1) = \sqrt{x_1}$;
- (6) $f(x_1) = \lfloor \sqrt{x_1} \rfloor$.

10.2.37. További feladatok. [25]: VII.2.3–VII.2.6, VII.2.9–VII.2.29; [59]: III.1.1–III.1.44; III.3.1–III.3.9, III.3.15–III.3.48, III.4.1–III.4.43.

10.3 Idő és tár

10.3.1. Algoritmusok idő- és tárigénye. Egy $T = (B, A, \varphi)$ Turing-gép *időigénye* a gép lépésszámainak $t(n)$ maximuma az összes n hosszú bemenetre véve (ha valamelyikre nem áll meg, akkor $+\infty$). A T *tárigénye* azon mezők számának $s(n)$ maximuma az összes n hosszú bemenetre véve, amelyekre a gép ír (mást, mint ami ott állt, így a bemenet elolvasása nem számít a tárigénybe). Hasonló definíció adható más számítási modellek esetén is. Azt mondjuk, hogy egy $\mathcal{L} \subset A_0^*$ nyelv, vagy általánosabban, egy $\mathcal{L} \subset A_0^{*m}$

halmaz $g(n)$ időben eldönthető, ha eldönthető olyan Turing-géppel, amelynek időigénye legfeljebb $g(n)$. Hasonlóan, azt mondjuk, hogy egy $\mathcal{L} \subset A_0^*$ nyelv, vagy általánosabban, egy $\mathcal{L} \subset A_0^{*m}$ halmaz $g(n)$ tárral eldönthető, ha eldönthető olyan Turing-géppel, amelynek tárigénye legfeljebb $f(n)$. Azt mondjuk, hogy egy $f \in A_0^* \rightarrow A_0^*$ vagy általánosabban egy $f \in A_0^{*m} \rightarrow A_0^{*k}$ kiszámítható parciális függvény $g(n)$ időben kiszámítható, ha kiszámítható (annak eldöntésével együtt, hogy az értelmezési tartományában vagyunk-e) olyan Turing-géppel, amelynek időigénye legfeljebb $g(n)$. Hasonlóan, azt mondjuk, hogy egy $f \in A_0^* \rightarrow A_0^*$ vagy általánosabban egy $f \in A_0^{*m} \rightarrow A_0^{*k}$ kiszámítható parciális függvény $g(n)$ tárral kiszámítható, ha kiszámítható (annak eldöntésével együtt, hogy az értelmezési tartományában vagyunk-e) olyan Turing-géppel, amelynek tárigénye legfeljebb $g(n)$.

Mivel a g függvényben szereplő konstansok egyszerű szimulációsokkal (az ötlet az, hogy több mezőt összefogunk egy mezőbe, sokkal nagyobb szalagábécét és belső állapot halmazt használva) csökkenthetők, nincs értelme (ellentétben a valódi programokkal) a konstansokkal foglalkozni. Ezért csak azzal foglalkozunk, hogy mennyi a tárigény, illetve időigény nagyságrendje. (Ezzel egyúttal eltekintünk a technikai fejlődés hatásától és a gépek egyedi jellegzetességeitől is.) Ha ez $O(n)$, akkor azt mondjuk, hogy *lineáris*, ha $O(n^2)$, akkor azt mondjuk, hogy *négyzetes*, ha $O(n^3)$, akkor azt mondjuk, hogy *köbös*, ha pedig van olyan $p(n)$ polinom, hogy $O(p(n))$, akkor azt mondjuk, hogy *polinomiális*. A polinomiális időben eldönthető nyelvek osztályát P-vel jelöljük, a polinomiális időben kiszámítható $f \in A_0^* \rightarrow A_0^*$ parciális függvények osztályát pedig FP-vel. Az alábbi táblázat illusztrálja az időigény felmérésének fontosságát. A táblázatban az időegység (órajel) 1 ns, és az egyes oszlopok azt mutatják, hogy adott idő alatt mekkora maximális bemeneti méretű probléma oldható meg az első sorban megadott időigény esetén. Az utolsó oszlop azt mutatja, hogy a sebességet tízszeresre növelve, hogyan változik az adott idő alatt megoldható maximális probléma mérete.

Maximális méret

Idő- igény	1 mp.	1 perc	1 óra	1 nap	1 év	·10
n	10^9	$6 \cdot 10^{10}$	$3,6 \cdot 10^{12}$	$8,64 \cdot 10^{13}$	$3,15 \cdot 10^{17}$	·10
$n \log n$	39620077	$1,94 \cdot 10^9$	$9,85 \cdot 10^{10}$	$2,11 \cdot 10^{12}$	$6,41 \cdot 10^{14}$	$\approx \cdot 10$
n^2	31622	244948	1897366	9295160	177642157	$\cdot \sqrt{10} \approx \cdot 3,16$
n^3	1000	3914	15326	44208	316007	$\cdot \sqrt[3]{10} \approx \cdot 2,15$
2^n	29	35	41	46	54	$+ \log 10 \approx +3,32$
$n!$	12	13	15	16	19	$+1/\log_{10} n$

10.3.2. Példák. (1) Bináris többszalagos Turing-gépen bináris alakban adott természetes számok összeadása lineáris időben, szorzása és maradékos osztása pedig négyzetes időben elvégezhető a jól ismert algoritmusokkal. (A jelenleg ismert leggyorsabb algoritmus szorzásra és osztásra $O(n \log n \log \log n)$ időt igényel.) Ugyanez igaz egész számokra.

(2) Az euklideszi algoritmusnál, ha $a \geq b > 0$ vagy $a \leq b < 0$ (egy lépés után ez a helyzet, ha az algoritmus nem ért véget) és a -t osztva b -vel a maradék $r = a \bmod b$, akkor $|a| \geq |b| + |r| > 2|r|$, ahonnan $|r| < |a|/2$, így minden lépésben a számok abszolút értékének szorzata legalább feleződik, tehát $\lceil \log |ab| \rceil$ lépés után a szorzat kisebb lesz, mint 1, így valamelyik tényező nulla. Innen az euklideszi (és a bővített euklideszi) algoritmus futásideje bináris (ternáris, stb.) alakban adott számokra köbös.

(3) Ha az euklideszi algoritmust természetes számokra ismételt kivonással végezzük (a nagyobbik számból kivonjuk a kisebbiket), akkor a lépésszám már $\ln k o(1, n)$ kiszámításánál is n lesz, ami exponenciális a bemenet hosszában. Persze, ha unárisan írjuk fel a bemenetet, akkor az ismételt kivonással működő algoritmus is négyzetes a bemenet hosszában. Ez egyrészt arra hívja fel a figyelmet, hogy nem mindegy, hogy kódoljuk a bemenetet, ha pontosak akarunk lenni, a kódolást is meg kell adni, például gráfalgoritmusoknál, hogy a gráf milyen formában adott. Ha egyszerűbb esetekben, például számoknál, nem adjuk meg a kódolást, feltesszük, hogy valamilyen „ésszerű” kódolást használunk. Másrészt ez a példa azt is mutatja, hogy unáris bemenet (és így unáris gép) nem célszerű a sebesség (időigény) meghatározására.

10.3.3. Nemdeterminisztikus Turing-gépek. Egy N nemdeterminisztikus Turing-gép szintén egy $N = (B, A, \varphi)$ hármas, ahol az A, B véges halmazok a szalagábécé, illetve a belső állapotok halmaza, $\sqcup \in A, s, h \in B$ és $\varphi \subset (B \times A^k) \times (B \times A^k \times \{<, =, >\}^k)$ egy tetszőleges reláció, amely az egész $B \times A^k$ -n van értelmezve, azaz most $B \times A^k$ egy elemének egynél több képe is lehet. Itt is, ha nagyon precízek akarunk lenni, akkor a szalagok $k \in \mathbb{N}^+$ számát, a $\sqcup$ szóköz jelet, és az s, h „start” és „halt” állapotokat is feltüntethetjük a jelölésben: $N = (k, B, A, \sqcup, s, h, \varphi)$. Az, hogy

$$(b, a_1, \dots, a_k, b', a'_1, \dots, a'_k, c_1, \dots, c_k) \in \varphi,$$

ahol $b, b' \in B$ és ha $1 \leq i \leq k$, akkor $a_i, a'_i \in A, c_i \in \{<, =, >\}$, azt jelenti, hogy a gép egy *megengedett lépése* vagy *legális lépése* a következő: ha a t időpontban b a belső állapota és az egyes szalagokról az $a_1, \dots, a_k$ betűket olvassa, akkor a $t + 1$ időpontra a b' belső állapotba megy át, az olvasott betűk helyére az $a'_1, \dots, a'_k$ betűket írja, és az i -edik szalagon a fej balra lép, jobbra lép, illetve helyben marad, attól függően, hogy c_i a $<$, a $>$ vagy az $=$ jel. Egy nemdeterminisztikus Turing-gépnek egy időpontban tehát több megengedett lépése is lehet. A gép egy *megengedett számolása* vagy *legális számolása* egymás utáni megengedett lépések sorozata. Természetesen minden Turing-gép egyben nemdeterminisztikus Turing-gép is. Egy nemdeterminisztikus Turing-gép úgy tekinthető, mint egy olyan Turing-gép, amely minden időpillanatban (faszzerűen) „osztódni” képes. A nemdeterminisztikus Turing-gépek a Turing-gépek olyan általánosításai, amelyek már nem modelleznek semmilyen reális számítástechnológiát, (kivéve talán a *DNS* számításokat), hanem felismerésekre használhatók. Jelentőségükre a tanútétel világít majd rá.

Azt mondjuk, hogy az N nemdeterminisztikus Turing-gép t időben *elfogadja* az $\alpha \in A_0^*$ szót, ha ezzel a szóval mint bemenettel van a gépnek olyan megengedett számolása, amely legfeljebb t lépésben megáll, és megálláskor a kimenet nem üres. (Lehetnek más megengedett számolások, melyek sokkal tovább tartanak, meg sem állnak, vagy a szót elutasítják.) Hasonlóan definiáljuk azt, hogy a gép az α szót s tár felhasználásával fogadja el. Azt mondjuk, hogy N az $\mathcal{L} \subset A_0^*$ nyelvet *felismeri*, ha $\mathcal{L}$ pontosan azokból a szavakból áll, amelyeket N elfogad (akármilyen időben és tárral). Ha a gép minden n hosszúságú $\alpha \in \mathcal{L}$ szót legfeljebb $f(n)$ időben felismer, akkor azt mondjuk, hogy a gép $\mathcal{L}$ -et $f(n)$ időben felismeri. Hasonlóan, ha a gép minden n hosszúságú $\alpha \in \mathcal{L}$ szót legfeljebb $f(n)$ tár felhasználásával felismer, akkor azt mondjuk, hogy a gép $\mathcal{L}$ -et $f(n)$ tárral felismeri. Azon nyelvek osztályát, amelyek nemdeterminisztikus Turing-gépen polinomiális időben felismerhetők, NP-vel jelöljük.

10.3.4. Tétel. A nemdeterminisztikus Turing-géppel felismerhető nyelvek pontosan a felsorolható nyelvek.

* **Bizonyítás.** Tegyük fel, hogy $\mathcal{L}$ felsorolható. Ekkor a 10.2.13 tétel szerint van olyan Turing-gép, amelynek első szalagjára egy α szót írva, akkor és csak akkor áll meg, ha $\alpha \in \mathcal{L}$. Módosítsuk a gépet úgy, hogy ha megáll, írjon előtte az utolsó szalagjára egy, az üres jeltől különböző jelet, jelezve ezzel, hogy a bemenetet felismerte. Ez a gép nyilván $\mathcal{L}$ szavait fogadja el.

Megfordítva, tegyük fel, hogy T felismerhető egy nemdeterminisztikus Turing-géppel. Megmutatjuk, hogy $\mathcal{L}$ felsorolható. Feltehetjük, hogy $\mathcal{L}$ nem üres. Legyen $\alpha \in \mathcal{L}$. Ha a nemdeterminisztikus Turing-gép k szalagos, készítsünk egy olyan determinisztikus Turing-gépet, amely hasonlóan működik, mint egy univerzális Turing-gép (lásd 10.1.29), de a $k + 1$ -edik szalagjára nem csak a nemdeterminisztikus Turing-gép ω programját kell írni (amely, mint tudjuk, legfeljebb $6k + 5$ üres jelet tartalmazhat), hanem attól balra, $6k + 6$ üres hellyel elválasztva a nemdeterminisztikus Turing-gép egy η legális számolását is, hasonlóan kódolva, mint a programot. (Mind a kettőt együtt unáris kódban írjuk fel, és mielőtt indulnánk, dekódoljuk.) A gép először ellenőrizze, hogy az ω program egy legális Turing-program-e, majd ellenőrizze, hogy a felírt η számítás a $\xi \in A_0^*$ szóra legális-e. Ha igen, írja ki a ξ szót. Ha bármilyen problémát talál, írja ki az α szót. $\square$

10.3.5. Tanú. Számos esetben egy „tanú” megkönnyíti egy probléma eldöntését. Ha például egy összetett számhoz mellékelünk tanúként egy nem triviális osztót, egyetlen maradékos osztással könnyű ellenőrizni, hogy a szám összetett, anélkül lényegesen nehezebb. Legyen A egy legalább háromelemű ábécé, amely tartalmazza az üres jelet, és legyen $\mathcal{L} \subset A_0^*$ egy nyelv. Azt mondjuk, hogy $\mathcal{L}_2 \subset A_0^* \times A_0^*$ az $\mathcal{L}$ -nek egy $f(n)$ hosszúságú, $g(m)$ idejű tanúja, ha $\mathcal{L}_2$ (determinisztikus) Turing-gépen A ábécével $g(m)$ idő alatt eldönthető, és $\xi \in \mathcal{L}$ akkor és csak akkor, ha van tanúja: van olyan $\eta \in A_0^*$ szó, amelyre $|\eta| \leq f(|\xi|)$ és $(\xi, \eta) \in \mathcal{L}_2$.

10.3.6. Példák. (1) Egy természetes szám összetett voltának tanúja egy nem triviális osztója. Ez legfeljebb n hosszúságú, ahol n a szám hossza, és a számot az első, a tanút a második szalagra írva, a maradékos osztás (mondjuk egy harmadik szalaggal, ahova az osztó egy „eltoltját” írjuk) $O(m^2)$ időben elvégezhető, ahol $m \leq 2n$, a bemenet hossza.

(2) Egy (akárhány határozatlanú) egész együtthatós polinom reducibilis voltának tanúja a polinom egy valódi osztója.

(3) Egy gráf nem síkba rajzolható voltának tanúja egy olyan részgráf, amely az öt szögpontú teljes gráffal vagy a „három ház, három kút” gráffal topologikusan izomorf.

(4) Hamilton-kör létezésének (irányított vagy irányítatlan gráfban) tanúja a Hamilton-kör.

(5) Két gráf izomorf voltának tanúja az izomorfizmust megadó leképezéspár.

10.3.7. Tanú-tétel. Az előző definíció jelöléseivel

- (1) minden olyan $\mathcal{L}$ nyelvnek, amely nemdeterminisztikus Turing-gépen $f(n)$ időben felismerhető, van $O(f(n))$ hosszúságú, lineáris idejű tanúja;
- (2) ha egy $\mathcal{L}$ nyelvnek van $f(n)$ hosszúságú, $g(m)$ idejű tanúja, akkor nemdeterminisztikus Turing-gépen $2f(n) + g(n + f(n))$ idő alatt felismerhető.

* **Bizonyítás.** Az első állítás bizonyítása nagyon hasonlít az előző tétel bizonyításának második felére: a lineáris idejű tanú a második szalagra írt program és a legális számítás kódja lesz, amelyeket most, kihasználva, hogy nem unáris géppel dolgozunk, üresjel-mentes kódban írunk fel a szalagra egy elválasztó jellel elválasztva, majd hogy

lineáris futásidőt érjünk el, ha a nemdeterminisztikus gép k szalagos volt, akkor a programot a $k + 1$ -edik szalagra, a legális számítás kódját pedig a $k + 2$ -edik szalagra másoljuk.

A második állítás bizonyításához az $\mathcal{L}_2$ nyelvet eldöntő T Turing-gépből az N nemdeterminisztikus gépet a következőképpen konstruáljuk meg: működésének kezdetén N csak a második szalagon mozog, minden lépésben az A ábécé egy-egy betűjét írva ki az összes lehetséges módon, és ha az nem $\sqcup$, akkor balra lépve. Ha a kiírt betű $\sqcup$, akkor a gép „determinisztikussá változik”, és a második szalagon jobbra lépkedve visszamegy a kiírt szó jobb szélére, majd innen kezdve úgy működik, mint T . Ha van tanú, (és csak akkor) az egyik legális számítás éppen szimulálja T működését. A tanú kiírása és a visszalépkedés $2f(n)$ ideig tart, a legrövidebb legális számítás pedig $g(n + f(n))$ ideig. $\square$

10.3.8. Következmény. Egy $\mathcal{L}$ nyelv pontosan akkor NP-beli, ha van polinomiális idejű és hosszúságú tanúja.

Bizonyítás. Ha az $\mathcal{L}$ nyelv NP-ben van, akkor (1) szerint van polinomiális hosszúságú tanúja, amely ugyanolyan nagyságrendű időben fel is ismerhető. Megfordítva, ha a nyelvnek van polinomiális hosszúságú tanúja, amely polinomiális időben felismerhető, akkor (2) szerint van olyan nemdeterminisztikus Turing-gép, amely polinomiális időben felismeri. $\square$

10.3.9. Megjegyzés. Az nyilvánvaló, hogy $P \subseteq NP$. Az elméleti informatika leghíresebb sejtése, hogy a tartalmazás valódi. Vannak úgynevezett *NP-teljes* problémák (pontosabban NP-teljes nyelvek), amelyek az NP-beli problémák közül a legnehezebbek abban az értelemben, hogy tudjuk, hogy ha ezek bármelyikére van polinomiális idejű algoritmust, akkor $P = NP$. Ezek a problémák tehát „egyforma nehezek” abban az értelemben, hogy ha bármelyikre sikerülne polinomiális futásidejű algoritmust adni, akkor a többire is kapnánk ilyen algoritmust. Ma már több száz NP-teljes problémát ismerünk, de egyikre sem ismerünk polinomiális idejű algoritmust, ami alátámasztja a sejtést, hogy $P \neq NP$. (Természetesen vannak olyan problémák is, amelyekről tudjuk, hogy NP-ben vannak, de nem tudjuk, hogy NP-teljesek lennének, sőt, azt sejtjük, hogy nem azok, ilyen volt például nemrégén még az, hogy egy szám összetett-e.) Az NP-teljes problémák létezésének bizonyítása azon múlik, hogy sikerült megmutatni, a „kielégíthetőség” problémája NP-teljes: ez a probléma annak eldöntését kívánja, hogy egy logikai műveletekkel, logikai kifejezésként felírt $f: \{\uparrow, \downarrow\}^n \rightarrow \{\uparrow, \downarrow\}$ logikai függvény *kielégíthető*-e, azaz van-e hozzá a változóknak olyan helyettesítése, amelyre igaz értéket vesz fel. Kiderül, hogy „ugyanolyan nehéz” a probléma, ha csak a $\neg$, $\wedge$, $\vee$ műveleteket engedjük meg, sőt, már akkor is, ha a formula konjunktív normál alakban van, és a konjukciókkal összekapcsolt diszjunkciók mindegyike csak három tagú. Azt már könnyebb megmutatni, hogy az így kapott „3-kielégíthetőség” ugyanolyan nehéz, mint az egyszerű, véges gráfok három színnel való jólszínezhetőségének problémája, és más gráfelméleti problémák, például a Hamilton-kör létezése, Hamilton-út létezése, irányított Hamilton-kör létezése, irányított Hamilton-út létezése stb. (mindezekben a problémákban a gráfot csúcsmátrixával adjuk meg).

Általában, ha egy problémáról nem tudjuk, hogy P-ben van, pláne, ha NP-teljes, az azt jelenti, hogy nem lehet a megoldására hatékony programot készíteni. Előfordulhat azonban, hogy kisebb méretekre tudunk hatékony programot készíteni (például Hamilton-kör keresésére több száz csúcsig), hogy van hatékony valószínűségi algoritmus (a Miller–Rabin-teszt számok összetett voltának bizonyítására), hogy a feladat valamely speciális esetére van hatékony algoritmus (például irányított körtől mentes irányított gráfban a

leghosszabb irányított út megkeresésére), hogy egy, a legrosszabb esetben exponenciális futásidejű algoritmus a gyakorlati esetekben polinomiális futásidejű (például a szimplex módszer általában köbös futásidejű, bár vannak esetek, amikor a futásidő exponenciális), végül, hogy tudunk hatékony algoritmust találni a feladat közelítő megoldására.

→ **10.3.10. Feladat [5].** Vizsgáljuk meg a [10.1.18](#) feladatban konstruált (többszalagos, bináris) Turing-gépek futásidő- és tárigényét.

→ **10.3.11. Feladat [8].** Vizsgáljuk meg a [10.1.19](#) feladatban konstruált (többszalagos, bináris) Turing-gépek futásidő és tárigényét.

→ **10.3.12. Feladat [8].** Az előző feladatban megvizsgált (többszalagos, bináris) Turing-gépekre, ha a futásidő nem polinomiális, próbáljunk polinomiális méretű tanút találni.

10.3.13. Feladat [10]. Adjunk polinomiális méretű és futásidejű tanút egy természetes szám prímfelbontására.

10.3.14. További feladatok. [\[25\]](#): VII.3.16–VII.3.22.

Irodalom

- [1] Aho, A. V.–Hopcroft, J. E.–Ullman, J. D.: *Számítógép-algoritmusok tervezése és analízise*. Műszaki Könyvkiadó, Budapest, 1982.
- [2] Alexandrov, P. Sz.: *Bevezetés a halmazok és függvények általános elméletébe*. Akadémiai Kiadó, Budapest, 1952.
- [3] Bálintné Sz. M.–Czédli G.–Szendrei Á.: *Absztrakt algebrai feladatok*. Tankönyvkiadó, Budapest, 1988.
- [4] Birkhoff, G.–Bartee, T. C.: *A modern algebra a számítógép-tudományban*. Műszaki Könyvkiadó, Budapest, 1974.
- [5] Bruder Gy.: *Feladatok relációkra*. <http://compalg.inf.elte.hu/~zslang/Bruder>, ELTE IK, Budapest, 2005. október 19.
- [6] Bruder Gy.: *Feladatok halmazokra*. <http://compalg.inf.elte.hu/~zslang/Bruder>, ELTE IK, Budapest, 2006. szeptember 1.
- [7] Busacker, R. G.–Saaty, T. L.: *Véges gráfok és hálózatok. Bevezetés alkalmazásokkal*. Műszaki Könyvkiadó, Budapest, 1969.
- [8] Cormen, T. H.–Leiserson, C. E.–Rivest, R. L.: *Algoritmusok*. Műszaki Könyvkiadó, Budapest, 1999.
- [9] Cormen, T. H.–Leiserson, C. E.–Rivest, R. L.–Stein, C.: *Új algoritmusok*. Scholar Kiadó, Budapest, 2003.
- [10] Csákány B.: *Algebra. Kézirat*. Tankönyvkiadó, Budapest, 1980.
- [11] Csörnyei Z.: *Lambda-kalkulus. A funkcionális programozás alapjai*. $\text{TypeT}_{\text{E}}\text{X}$, Budapest, 2007.
- [12] Demetrovics J.–Denev, J.–Pavlov, R.: *A számítástudomány matematikai alapjai*. Tankönyvkiadó, Budapest, 1989.
- [13] Dörfler, W.–Mühlbacher, J.: *Graphentheorie für Informatiker*. Walter de Gruyter, Berlin – New York, 1973.
- [14] Dringó L.–Kátai I.: *Bevezetés a matematikába. Egységes jegyzet*. Nemzeti Tankönyvkiadó, Budapest, 1996.
- [15] Drommerné Takács V. (szerk.): *Sejtautomaták*. Gondolat Kiadó, Budapest, 1978.
- [16] Eukleidész: *Elemek*. Gondolat, Budapest, 1983.
- [17] Fagyejev, D. K.–Szominszkij, I. Sz.: *Felsőfokú algebrai feladatok*. Műszaki Könyvkiadó, Budapest, 1973.
- [18] Feymann, R. P.: *Feynman Lectures on Computation*. Addison-Wesley, 1996.
- [19] Fried E.: *Általános algebra*. Tankönyvkiadó, Budapest, 1981.
- [20] Fried E.: *Algebra I.–II.* Nemzeti Tankönyvkiadó, Budapest, 2000.
- [21] Fuchs L.: *Algebra. Kézirat*. Tankönyvkiadó, Budapest, 1970.

- [22] Fuchs L.: *Bevezetés az algebrába és a számelméletbe. Kézirat.* Tankönyvkiadó, Budapest, 1977.
- [23] Gács P.–Lovász L.: *Algoritmusok.* Tankönyvkiadó, Budapest, 1987.
- [24] Gathen, v. z., J. – Gerhard, J.: *Modern computer algebra.* Cambridge University Press, 1999.
- [25] Gavrilov, G. P.–Szapozsenko, A. A.: *Diszkrét matematikai feladatgyűjtemény.* Műszaki Könyvkiadó, Budapest, 1981.
- [26] Gonda J.: *Bevezető fejezetek a matematikába. Kiegészítés. Egyetemi jegyzet.* ELTE TTK, Budapest, 1998.
- [27] Gonda J.: *Bevezető fejezetek a matematikába III. Egyetemi jegyzet.* ELTE TTK, Budapest, 2000.
- [28] Gonda J.: *Gyakorlatok és feladatok a Bevezetés a matematikába című tárgyhoz. Polinomok, véges testek, kongruenciák, kódolás. Egyetemi jegyzet.* ELTE TTK, Budapest, 2001.
- [29] Gonda J.: *Gyakorlatok és feladatok a Bevezetés a matematikába című tárgyhoz. Polinomok, véges testek, kongruenciák, kódolás. Megoldások. Egyetemi jegyzet.* ELTE TTK, Budapest, 2001.
- [30] Györfi L., Györi S. – Vajda I.: *Információ- és kódelmélet.* Typotex, Budapest, 2005.
- [31] Hainzmann J.–Varga S.–Zoltai J.: *Elektronikus áramkörök.* Nemzeti Tankönyvkiadó, Budapest, 2000.
- [32] Hajnal A.–Hamburger P.: *Halmazelmélet.* Tankönyvkiadó, Budapest, 1983.
- [33] Hajnal P.: *Gráfelmélet.* Polygon, Szeged, 1997.
- [34] Hajós György: *A geometria alapjai.* Nemzeti Tankönyvkiadó, Budapest, 1999.
- [35] Hall, G. G.: *Alkalmazott csoportelmélet.* Műszaki Könyvkiadó, Budapest, 1975.
- [36] Halmos P. R.: *Véges dimenziós vektorterek.* Műszaki Könyvkiadó, Budapest, 1984.
- [37] Halmos P. R.: *Elemi halmazelmélet.* Sigler, L. E.: *Halmazelméleti feladatok.* Műszaki Könyvkiadó, Budapest, 1981.
- [38] Hewitt, E.–Stromberg, K. R.: *Real and abstract analysis.* Springer-Verlag, Berlin–Göttingen–Heidelberg, 1965.
- [39] Jákó P.: *Digitális hangtechnika.* Kossuth Kiadó, Budapest, 2002.
- [40] Kahan, W.: *Lecture Notes on the Status of IEEE Standard 754 Binary Floating-Point Arithmetic. Kézirat.* WWW.
- [41] Kalmár L.: *A matematika alapjai, I./I., I./II., II./I., II./II. Kézirat.* Tankönyvkiadó, Budapest, 1978, 1969, 1969, 1971.
- [42] Kaluzsnynin, L. A.: *Bevezetés az absztrakt algebrába.* Tankönyvkiadó, Budapest, 1979.
- [43] Kelley, J. L.: *General topology.* D. Van Nostrand Company Inc., Princeton, New Jersey, 1955.
- [44] Kiss E.: *Bevezetés az algebrába.* Typotex, Budapest, 2007.
- [45] Kovács F. Ferenc: *Az informatika VLSI áramkörei.* Pázmány Egyetem Elektronikus Kiadó, Budapest, 2004.

- [46] Knuth, D. E.: *The art of computer programming. Vol. 1, 2, 3. Third edition. Vol. 1 Fas. 1, Vol. 4 Fas. 0,1,2,3,4. (Magyarul is.)* Addison–Wesley, 1998.
- [47] Knuth, D. E.: *The Stanford GraphBase.* Addison–Wesley, 1993.
- [48] Kuros, A. G.: *Felsőbb algebra.* Tankönyvkiadó, Budapest, 1967.
- [49] Laczkovich M.: *Sejtés és Bizonyítás.* TypoT_EX, Budapest, 1998.
- [50] Laczkovich M.–T. Sós V.: *Analízis I.–II.* Nemzeti Tankönyvkiadó, Budapest, 2005, 2007.
- [51] Landau, E.: *Grundlagen der Analysis.* Chelsea Publishing Company Inc., New York, 1948.
- [52] Láng Csabáné: *Bevezető fejezetek a matematikába I.–II. Egyetemi jegyzet.* ELTE, Budapest, 2000.
- [53] Láng Csabáné: *Példák és feladatok I. Komplex számok. Egyetemi jegyzet.* ELTE, Budapest, 2003.
- [54] Láng Csabáné: *Számelmélet. Példák és feladatok.* ELTE Eötvös kiadó, Budapest, 2005.
- [55] Láng Csabáné: *Kombinatorika. Példák és megoldások.* ELTE IK, Budapest, 2006. szeptember 7. <http://compalg.inf.elte.hu/~zslang>.
- [56] Láng Csabáné: *Feladatok a bevezető fejezetek a matematikába tárgy I. félévéhez.* ELTE IK, Budapest, 2007. július 25. <http://compalg.inf.elte.hu/~zslang>.
- [57] Láng Csabáné: *Feladatok a bevezető fejezetek a matematikába tárgy III. félévéhez.* ELTE IK, Budapest, 2007. <http://compalg.inf.elte.hu/~zslang>.
- [58] Láng Csabáné–Gonda J.: *Bevezetés a matematikába II. Egyetemi jegyzet.* ELTE, Budapest, 1995.
- [59] Lavrov, I. A.–Makszimova, L. L.: *Halmazelméleti, matematikai logikai és algoritmuselméleti feladatok.* Műszaki Könyvkiadó, 1987.
- [60] Leindler L.–Schipf F.: *Analízis I. Egységes jegyzet. Kézirat.* Tankönyvkiadó, Budapest, 1978.
- [61] van Leeuwen, J. (Ed.): *Algorithms and complexity Vol. A, B.* Elsevier, Amsterdam, 1990.
- [62] Lovász L.: *Algoritmusok bonyolultsága. Kézirat. ELTE TTK* Tankönyvkiadó, Budapest, 1991.
- [63] Lovász L.: *Kombinatorikai problémák és feladatok.* TypoT_EX, Budapest, 2000.
- [64] Lovász L. – Pelikán J. – Vesztergombi K.: *Diszkrét matematika.* Typotex, Budapest, 2006.
- [65] Manna, Z.: *Programozásmélet.* Műszaki Könyvkiadó, Budapest, 1981.
- [66] Manyin, J. I.: *Bevezetés a kiszámíthatóság matematikai elméletébe.* Műszaki Könyvkiadó, Budapest, 1986.
- [67] Marcus, A.: *Algebra.* Kolozsvári Egyetemi Kiadó, 2008.
- [68] Mendelson, E.: *Introduction to mathematical logic.* D. Van Nostrand Company Inc., Princeton, New Jersey, 1964.
- [69] Niven, I.–Zuckerman, H. S.: *Bevezetés a számelméletbe.* Műszaki Könyvkiadó, 1978.

- [70] Penrose, R.: *A császár új elméje. Számítógépek, gondolkodás és a fizika törvényei.* Akadémiai Kiadó, Budapest, 1993.
- [71] Quine, W. V. O.: *A logika módszerei.* Akadémiai Kiadó, Budapest, 1968.
- [72] Recski A.: *Matroid theory and its applications in electric network theory and in statics.* Akadémiai Kiadó, Budapest, 1989.
- [73] Révész Gy.: *Bevezetés a formális nyelvek elméletébe.* Akadémiai Kiadó, Budapest, 1979.
- [74] Rónyai L.–Ivanyos G.–Szabó R.: *Algoritmusok.* TypoTEX, Budapest, 1999.
- [75] Rudin, W.: *A matematikai analízis alapjai.* Műszaki Könyvkiadó, Budapest, 1978.
- [76] Safarevics, I. R.: *Algebra.* Typotex Kiadó, Budapest, 2000.
- [77] Salomon, D.: *Data compression.* Springer Verlag, New York, 2000.
- [78] Sárközy A.: *Számelmélet és alkalmazásai.* Műszaki Könyvkiadó, Budapest, 1978.
- [79] Sárközy A.–Surányi J.: *Számelmélet feladatgyűjtemény. Kézirat.* Tankönyvkiadó, Budapest, 1964.
- [80] Sierpiński, W.: *200 feladat az elemi számelmélet köréből.* Tankönyvkiadó, Budapest, 1964.
- [81] Székelyhidi L.: *Erdős Jenő válogatott előadásai.* Debreceni Egyetem Matematikai Intézet, 2004.
- [82] Szele T.: *Bevezetés az algebrába.* Tankönyvkiadó, Budapest, 1977.
- [83] Szendrei Á.: *Diszkrét matematika; logika, algebra, kombinatorika.* Polygon, Szeged, 2000.
- [84] Totik V.: *Halmazelméleti feladatok és tételek.* Polygon jegyzettár, Szeged, 1997.
- [85] Trahtenbrot, B. A.: *Algoritmusok és absztrakt automaták.* Műszaki Könyvkiadó, Budapest, 1978.
- [86] van der Waerden, B. L.: *Moderne Algebra I.–II.* Springer-Verlag, Berlin–Göttingen–Heidelberg, 1959.
- [87] Vinogradov, I. M.: *A számelmélet alapjai.* Tankönyvkiadó, Budapest, 1968.
- [88] Vollmar, R.: *Sejtautomata algoritmusok.* Műszaki Könyvkiadó, Budapest, 1982.

Mutató

- [75, 192
- AAC 314
- (A) 230
- ábécé 60, 286, 365
- Abel-csoport 56, 74, 204, 220, 224, 227, 321
- Abel, Niels Henrik (1802–1829) 56, 264
- ablak 300
- ábrázolás 204
- abszolút érték 95, 101, 237, 239
- $|p|$ 101
- $|x|$ 85
- $|z|$ 95
- absztrakcióval való definíció 131
- A^* 286
- adaptív Huffman-kód 295
- adat 281
- adatátszövés 336
- adatformátum 301
- adattábla 39
- adattípus 73
- additív 158
 - inverz 56, 90, 94, 101, 105
 - jelölés 56
 - rend 229
 - részcsoport 233
- additivitás 248
- Adleman, Leonard Max 154
- adó 281
- Advanced Encryption Standard 254
 - $(a_1, a_2, \dots, a_n)$ 230
- AES 148, 154, 252
- affin sokaság 329
 - transzformáció 208
- Agnesi-görbe 22
- Agnesi, Maria Gaetana (1718–1799) 22
- Agrawal, Manindra 144
- A halmaz képe 24
- Aho, Alfred V. 386
- akkor és csak akkor 7
- akkumulátor 359, 365
- $a \equiv b \pmod{m}$ 146
- $a \equiv b \pmod{m}$ 146
- aktuális állapot 344
- aláírás 156
- alap 62, 75
- alapfüggvény 375
- alaphalmaz 17
- alapkörrendszer 178
- alaplemez 66
- alappont 306
- alapzaj 306
- alatt 111
- $\aleph_0$ 131
- Alexandrov, Pavel Szergejevics (1896–1982) 386
- algebra 202
 - alaptétele 94, 98
- algebrai 264, 264–266
 - alak 95
 - derivált 248
 - dimenzió 127
 - egyenlet 99
 - elem 265
 - programozási nyelvek 15
 - rendszer 326
 - struktúra 242
 - testbővítés 250
- algebrailag független 277
- algoritmikusan parciálisan kiszámítható 372
- algoritmus 107, 144, 155, 186, 190, 192, 224, 246, 262, 269, 289, 291, 297, 303, 310–311, 342, 368, 372, 375, 381
- állandó 299
- állapot 365
- állapotdekódolás 340
- álprím 156

alsó egész rész *85*
 — határ *31, 291*
 — tulajdonság *31, 93*
 — korlát *30*
 $[x]$ *85*
 általános affin csoport *208*
 — asszociativitás tétele *62*
 — disztributivitás *77*
 — helyzet *17*
 — helyzetű *52*
 — kommutativitás tétele *63*
 — lineáris csoport *208*
 — rekurziótétel *61, 62*
 általánosított Bernoulli-egyenlőtlenség *51*
 — folyamprobléma *197*
 — kontinuumhipotézis *132, 132*
 alternáló *275*
 — csoport *222*
 alternatív *106*
 alulról korlátos *30*
 — nyílt *30*
 — zárt *30*
 amplitúdó *308*
 analóg jel *304*
 $a \not\equiv b \pmod{m}$ *146*
 $a \not\equiv b \pmod{m}$ *146*
 antikommutatív *102*
 antiszimmetria *14*
 antiszimmetrikus *26, 27, 29, 137*
 $\tilde{a}$ *146*
 $\tilde{a} \bmod m$ *146*
 A^+ *286*
 Appel, Kenneth I. *200*
 áramirány *66*
 áramkör *65*
 A-ra való leszűkítés *23*
 A-ra való megszorítás *23*
 argumentum *34, 40, 96*
 Arisztotelész (i.e. 383–322) *10*
 Arkhimédész (i.e. 287–212) *167*
 arkhimédészi spirális *23*
 arkhimédészien rendezett *83, 83–84, 94*
 — — test *89*
 ASCII *70*
 ASCII-kód *283*
 assembler *361*
 assembly *33*
 asszociativitás *18*
 asszociált *137, 137–138, 236–238, 256–257, 264*
 asszociatív *26, 53–55, 69, 102, 161, 205*
 asszociativitás *16, 38, 101, 105*
 asszociátor *106*
 astroid *22*
 AT&T *318*
 átlagos információtartalom *282, 282*
 — szóhosszúság *291, 295, 298*
 átlós eljárás *374*
 átmeneti függvény *340, 365, 367*
 átmérő *174*
 átszállított mennyiség *194*
 attribútumok *39*
 átvitel *71*
 átvivő kapu *68*
 automata *366*
 automorfizmus *203, 203, 216, 228, 230*
 axióma *6, 9–10*
 axiomatikus alapfogalmak *10*
 — módszer *6*
 — tárgyalás *73*
 Babbage [bebidzs], Charles (1792–1871) *55*
 backward *361*
 bájt *70, 252*
 bájtankénti helyettesítés *252*
 bal gyerek *188*
 — kimenő él *188*
 — oldali mellékosztály *214*
 — — nullosztó *77*
 balideál *230*
 Bálintné Szendrei Mária *386*
 balinverz *55*
 bal oldali semleges elem *55*
 Bartee, Thomas C. *386*
 base *66*
 bázis *66*
 BCD *70*
 beágyazás *74, 80, 82*
 beágyazható *242*
 befejezési szám *193*
 befejező állapot *343*
 befok *184, 186–187, 193*

bejárási szám *193*
 belső állapot *343, 344, 382*
 — automorfizmus *216*
 — szorzás *103*
 — tagja *287*
 — tár *189*
 bemenet *344, 359, 382*
 — hossza *344*
 bemeneti állapot *340*
 — kódolás *340*
 bemenő *319*
 Bernays, Paul Isaac (1888–1977) *15*
 Bernoulli lemniszkátája *23*
 Bernoulli [bernuli], Daniel (1700–1782) *51*
 Bernoulli-egyenlőtlenség *51*
 Bernoulli [bernuli], Jacob (1654–1705) *23*
 Bernstein, Felix (1878–1956) *125*
 beszéd *315*
 beszédszintetizátor *315*
 betű *286, 382*
 betűnkénti kód *289, 291*
 — kódolás *283, 285, 287*
 B-fa *190*
 bidirectional *319*
 bijekció *107*
 bijektív *34, 35, 203, 228*
 bináris *344*
 — fa *188*
 — jegy *70*
 — keresés *282*
 — kód *286*
 — kupac *188*
 binárisan kódolt decimális *70*
 binary coded decimal *70*
 — digit *70*
 binér művelet *40, 55, 76, 202, 236*
 — reláció *21, 24, 39, 40, 74*
 binomiális együttható *117*
 — tétel *116, 117–118*
 Birkhoff, Garrett (1911–1996) *386*
 bit *70, 281, 282, 360*
 bitfordítás *311*
 bitsorozat *252*
 bizonyítási módszerek *10*
 bizonyítványok kiállítása *154*
 bizonytalanság *281*
 blokk *252*
 blokkoló folyam *194, 195–196*
 bolha *130*
 Bolyai Farkas (1775–1856) *11*
 Boole-algebra *233, 233*
 Boole-algebrai összeg *17*
 Boole-függvény *65*
 Boole, Georg (1815–1864) *17, 65, 231, 233*
 Boole-gyűrű *231, 233*
 Boruvka, Otakar (1899–1995) *181*
 börtön *286*
 bővebb *14*
 bővítés *230, 264–265*
 — foka *264*
 bővített euklideszi algoritmus *139, 239, 332, 341, 381*
 — komplex szám *95*
 — valós szám *85*
 B_q -fa *190*
 Bruder Györgyi *386*
 burst *336*
 Busacker, Robert G. *386*
 byte *70*
 byteszervezésű gép *70*
 $\mathbb{C}$ *94*
 Cantor tétele *126*
 Cantor-féle átlós eljárás *126*
 Cantor, Georg (1845–1918) *83, 126, 132*
 $\text{card}(A)$ *108*
 Cardano [kardano], Gerolamo (1501–1576) *94, 263*
 Cardano-képlet *94, 263*
 cardinal number *108*
 Carmichael, Robert Daniel (1879–1967) *156*
 Carmichael-szám *156*
 carry *71*
 casus irreducibilis *94*
 Catalan, Eugène Charles (1814–1894) *61*
 Catalan-számok *61*
 Cauchy [kósi], Augustin (1789–1857) *89*
 Cauchy-sorozat *89*
 Cayley tétele *177, 220*
 Cayley [kéli], Arthur (1821–1895) *105, 177, 220*
 Cayley-számok *105*

cél *194*
 centralizátor *216*
 centrum *216*
 c *132*
 char(*R*) *229*
 Church [csó(r)cs], Alonzo (1903–1995) *368, 372*
 Church-tézis *372*
 Church–Turing-tézis *372*
 ciklikus *208, 214, 220, 254*
 — csoport *211–212*
 — — rendje *212*
 — ellenőrzés *330*
 — kód *329*
 — részcsoporthatár *212*
 ciklois *22*
 ciklus *172, 222*
 cím *190*
 címkézett gráf *181*
 ${}^iC_n^k$ *112*
 ciisszois *22*
 CMOS *66*
 C_n *172*
 C nyelv *181*
 $\vec{C}_n$ *184*
 Cohen, Paul Joseph *132*
 complementer MOS *66*
 compress *304, 317*
 Conway-féle életjáték *367*
 Conway, John H. *367*
 Cormen, Thomas H. *107, 181, 386*
 CRC *330*
 csak bemenet *358*
 — kimenet *358*
 Csákány Béla *386*
 család *13*
 csapóajtó függvény *148*
 csatorna *66, 281, 284*
 csatornakapacitás *324*
 csatornakódolás *285*
 csillag *172*
 csonka csúcshatár *287, 292*
 csonkítás *85*
 csoport *56, 202, 204–205, 217, 220*
 — rendje *211, 214*
 — — végtelen *211*
 csoportkód *321*
 csökkentett jelkészlet *347*
 Csörnyei Zoltán *368, 386*
 csúcs *169, 175–176, 178, 181, 183, 185, 190, 195, 200, 356*
 csúcscímke *181*
 csúcscímkézés *181*
 csúcscímkézett gráf *181*
 csúcshalmaz törlésével kapott gráf *174*
 csúcshalmaz törlésével kapott irányított gráf *186*
 csúcsmátrix *200, 384*
 csúcssúlyozás *181*
 csúcssúlyozott gráf *181*
 Czédli Gábor *386*
 Daemen, Joan *252*
 DCT *312*
 De Morgan-szabály *18, 38*
 de Bruijn, Nicolaas Govert *200*
 Dedekind, Julius Wilhelm Richard (1831–1916) *83, 87*
 Dedekind-szelet *87*
 deflate *301, 316*
 deg(*f*) *244*
 deg[−](*v*) *184*
 deg⁺(*v*) *184*
 deg(*v*) *170*
 dekódolás *302*
 Demetrovics János *386*
 demodulátor *285*
 demultiplexer *68*
 Denev, Jordan *386*
 depletion *66*
 derivált *248*
 Descartes-féle levél *22*
 Descartes [dékárt], René (1831–1916) *21–22, 39, 60, 172*
 Descartes-szorzat *21, 39, 60, 122, 172, 220, 236*
 determináns *208–209, 332*
 DFT *307*
 diagonális *21, 61*
 — mátrixú transzformáció *216*
 dichotom *26, 27, 29*
 dichotomia *124*
 diédercsoport *206*

differencia 17
 $\setminus$ 17
 Diffie–Hellmann–Merkle-kulcscsere 148
 Diffie, Whitfield 148
 diffúzió 66
 digitális aláírás 154, 155–156, 285
 — boríték 154
 — szűrés 307
 digitalizálás 304
 Dijkstra módszere 190
 Dijkstra, Edsger Wybe (1925–2002) 190
 dinamika 306
 dinamikus 299
 — programozás 192
 Dinic módszere 195
 Dinic, E. A. 195
 diofantikus probléma 151
 Dirac tétele 181
 Dirac [dirák] Gabriel Andrew
 (1925–1984) 181
 direkt szorzat 21, 220, 220, 236, 242
 Dirichlet [diriklé], Peter Gustav Lejeune
 (1805–1859) 161
 Dirichlet-szorzat 161
 diszjunkció 7
 diszjunkt 16, 60, 109
 diszjunktív normál alak 69
 diszkrét direkt szorzat 220
 — Fourier-transzformáció 307, 313
 — Fourier-transzformált 308
 — koszinusz transzformáció 312, 313
 — logaritmus probléma 148, 148–149
 diszkrimináns 271
 disztributív 54, 75, 102–103, 232
 — háló 232, 233
 disztributivitás 17, 18, 38, 76, 101,
 105–106, 232
 disztributivitási szabályok 17
 DjVu 318
 $d^-(v)$ 184
 dmn 23
 D_n 206
 DNS 382
 domain 23
 dominó 375
 döntési függvény 322
 — hiba 322
 Dörfler, Williband 386
 $d^+(v)$ 184
 DQ-tároló 68
 drain 66
 Dringó László 386
 Drommerné Takács Viola 386
 DSS 156
 duplázási eljárás 100, 105
 dúsitásos 66
 $d(u, v)$ 321
 $d(v)$ 170
 DVD 336
 Edmonds, Jack R. 195
 Edmonds–Karp-heurisztika 195
 egész együtthatos 248
 — szám 73, 75, 90, 137–138, 140, 149
 — számok 74
 egész számok additív csoportja 211
 egy szalag 349
 egybevágóság 206
 egyedi információtartalom 281
 egyenes 6, 10, 104
 — egyenletrendszere 105
 — paraméteres egyenlete 104
 egyenlet 94
 egyenletes kód 287
 = 7, 10
 egyenlőség 10, 21, 165, 282
 egyenlőtlenség 106, 166
 egyértelmű 95, 140, 142, 240, 245, 257,
 274, 276
 — faktorizációs tartomány 236
 egyértelműen dekódolható 283
 — létezik 8
 $\exists!$ 8
 egyértelműség 46, 84, 277
 egy és csak egy létezik 8
 egyesekre komplement 147
 egyesítés 15, 208, 375
 egyhatározatlanú polinom 237, 243
 egység 137, 137–138, 226, 236–239, 245,
 256, 281
 egységcsoport 137
 egységelem 54, 56, 56, 69, 81, 94, 101,
 105, 110, 137, 161, 202, 204, 206,

- 211, 217, 220, 226, 232, 232–233, 236, 243–244, 256, 275
- egységelemes gyűrű 76, 227–228
- integritási tartomány 136–138, 226–227, 236–237, 245, 249, 261, 275–276, 278
- egységgyökök 206, 248, 306
- egységvektor 102, 104
- egyszalagos 374
- univerzális Turing-gép 355
- egyszerű 177
- csoport 224, 331
- görbe 197, 198–199
- gráf 170, 172
- gyűrű 230, 241
- út 174
- egyszerűsítési szabály 53, 54, 59, 205
- együttható 63, 76, 243, 260, 274
- egváltozós művelet 40
- egyveremtáras gép 358
- egzisztenciális kvantor 7
- Eisenstein, Ferdinand Gotthold Max (1823–1852) 260
- ekvivalencia 7
- ekvivalenciaosztály 28, 146, 213, 233
- ekvivalenciareláció 28, 28, 36, 73–74, 79, 137, 146, 187, 213, 234, 241
- ekvivalens 107, 129–130, 172
- kód 321
- él 169, 176–178, 181, 183, 185, 195, 199, 201
- élcímke 181
- élcímkézés 181
- élcímkézett 188
- gráf 181
- eldönthető 370, 370, 372–375, 383
- elektróda 66
- elektromos tér 65
- elektron 66
- elektronhiány 66
- elektronszerkezet 206
- elem rendje 211, 214
- — végtelen 211
- $\in$ 13
- elemei száma 108
- elemi formulák 7
- oszlopművelet 327
- szimmetrikus polinom 276, 276–278
- $\mathfrak{h}(A)$ 108
- elfogadja 382
- élgráf 172
- élhalmaz törlésével kapott gráf 173
- élhalmaz törlésével kapott irányított gráf 186
- ellenőrző leképezés 327, 329
- mátrix 327, 329, 332
- ellentett 56, 147
- ellentettképzés 85
- ellipszis 22
- éllistas ábrázolás 185
- élmátrix 200
- elméleti informatika 384
- elmozdulásvektor 319
- elnyelési tulajdonság 232
- eloszlás 281–282, 282
- előhívódó 316, 318
- előjel 360
- függvény 85
- nélküli 70
- előjeles térfogat 103
- előjelszabály 75, 76, 90
- előtagja 287
- előtér 318
- első 30
- koordináta 21
- elsőbbségi sorok 188
- elsőfajú Stirling-szám 115
- elsőfokú csúcs 176
- élsúly 190
- élsúlyozás 181, 194
- élsúlyozott gráf 181, 193
- irányított gráf 190
- elszáll 355
- élszínezett irányított fa 287
- eltolás 206
- eltolt szinuszos 306
- elvágja 178
- elvágó élhalmaz 194
- halmaz 178
- elválasztható 326
- elvégezhető az osztás 205, 205
- Emacs 369

- $E^-(S)$ 183
 endomorfizmus 203, 228, 229
 endomorfizmusgyűrű 227, 228
 enhancement 66
 Enigma 148
 entrópia 155, 282, 282, 291, 298
 epimorfizmus 203, 228, 245
 $E^+(S)$ 183
 Eratoszthenész (i.e. 276?–194?) 144
 Eratoszthenész szitája 144
 erdő 178
 Erdős és DeBruijn tétele 200
 Erdős Jenő (1931–2004) 200, 389
 eredmény 40, 340
 erős komponens 187, 193
 erősen összefüggő 187
 érték 34, 194
 értékkészlet 23, 198, 371
 értelmezési tartomány 23, 370, 372, 376, 379, 381
 $E(S)$ 170
 és 7
 escape 298, 299
 esély 113
 Eudoxosz ($\approx$ i.e. 408–355) 166
 Eukleidész ($\approx$ i.e. 300) 10–11, 94, 142, 386
 euklideszi algoritmus 139, 340, 342, 381–382
 — gyűrű 237, 238–241, 246, 250, 256, 275
 Euler tétele 198, 236
 Euler-féle φ függvény 149, 159
 Euler–Fermat-tétel 149
 Euler [ajler], Leonhard (1871–1952) 149, 179, 198
 Euler-vonal 179, 179
 $\mathbb{E}_X$ 206
 exponenciális 382, 385
 fa 176, 177–178, 187
 Fagyeev, D. K. 386
 faktoriális 224
 faktorcsoport 217, 218
 faktorgyűrű 234, 240–241
 faktoriális 111
 faktORIZÁCIÓ 227
 faktorstruktúra 217, 242
 Fano, Gino (1871–1952) 10, 327
 Fano-kód 327
 Fano-sík 10, 327
 $f \asymp g$ 341
 Fax 300
 fáziseltolás 308, 308
 felbonthatatlan 136–137, 137, 140, 239
 — elemek szorzata 240
 felbontható 283, 286, 289
 felcserélhető 56, 204
 felcserélhetőség 101
 félcsoport 55, 202, 204–205, 220
 féligrendezés 29
 felismerhető 382–383
 felismeri 382
 feloldható 224
 felsorolható 370, 371–373, 382
 felső becslés 194
 — egész rész 85
 — háromszög mátrix 216
 — határ 31
 — — tulajdonság 31, 83–86, 93
 — korlát 30
 $[x]$ 85
 félszalagos Turing-gép 355
 felülírható 365
 felülről korlátos 30
 — nyílt 30
 — zárt 30
 félvezető 66
 fém 66
 ferdetest 81, 101, 267
 Fermat [ferma], Pierre (1601–1665) 149, 151, 227, 266
 Fermat-prím 266
 Fermat-sejtés 227
 Fermat-szám 145
 Fermat-tétel 149
 Ferrari, Lodovico (1522–1565) 94
 Ferro, Scipione del (?1465–1526) 94
 feszített irányított részgráf 186, 187
 — részgráf 173
 feszítőerdő 178
 feszítőfa 177, 177
 feszültség 66, 68
 FET 65
 Feynman, Richard P. 386

- FFT 308, 310
- Fibonacci, Leonardo Pisano (1170–1250) 61–62
- Fibonacci-szám 62, 166
- $f_{i_1, i_2, \dots, i_n}$ 274
- field effect transistor 65
- FIFO 356
- film 318
- first in first out 356
- fix hosszúságú kód 287
- fixpont 126
- fixpontos ábrázolás 85
- fizika 282
- fizikai képelem 315
- törvény 206
- $f \succ g$ 341
- Floyd, Robert W. (1936–2001) 193
- fok 244, 244, 265–266, 274, 274–275
- foka 264
- fokszám 170, 237, 245, 250, 276
- folyam 194
- folytonos függvény 197
- Fontana, Niccolo „Tartaglia” [tartajja] (?1500–1557) 94
- Ford–Fulkerson-tétel 194
- fordítóprogram 41
- fordított lengyel jelölés 41
- szorzás 209
- Ford Lester Randolph, ifj. 194
- forгатás 104, 206, 209, 216
- formális hatványsor 244, 275
- formalizálás 8
- formalizálható 8
- forrás 66, 184, 194
- forráskódolás 284
- FORTH 41
- forward 361
- Fourier [furié], Jean Baptiste Joseph (1768–1830) 307–308
- Fourier-sor 307
- Fourier-transzformáció 307
- főgyűthető 244, 244–246, 256, 260, 262
- főideál 230, 236, 240, 250
- főpolinom 244, 248, 250, 256, 329
- főváros 200
- FP 381
- $\mathbb{F}_q$ 267
- Fraenkel, Abraham Adolf (1891–1965) 131
- frame 318
- frekvenciartomány 314
- Fried Ervin 386
- Frobenius-endomorfizmus 229–230
- Frobenius, Ferdinand Georg (1849–1917) 229–230
- Fuchs László 386–387
- Fulkerson, Delbert Ray (1924–1976) 194
- futamkódolás 299, 318
- futásidő 107, 359
- függvény 34, 38, 107, 109, 118, 368
- inverze 38
- függvényabsztrakció 369
- függvényösszetétel 57
- $f(x)$ 34
- $f(x_1, x_2, \dots, x_n)$ 273
- f_x 34
- $f: x \rightarrow y$ 34
- $f: X \rightarrow Y$ 34
- $f: x \mapsto y$ 34
- Gács Péter 387
- $G^\times$ 56
- $\mathbb{GA}(F^n)$ 208
- Galois [galoá], Évariste (1811–1832) 224, 264
- gamma 315
- $\gamma \leftarrow \gamma a$ 356
- $\gamma \leftarrow \text{tail}(\gamma)$ 356
- gate 66
- Gathen, von zur, Joachim 387
- Gauss lemmája 256
- tétele 257
- Gauss-egész 227, 239
- Gauss-egészek 138
- Gauss-gyűrű 236, 237, 240, 256–257, 260, 262, 275
- Gauss, Johann Carl Friedrich (1777–1855) 94, 138, 256–257, 266, 327
- Gauss–Jordan-elimináció 327
- Gavrilov, G. P. 387
- gazdaságos kódolás 284, 291
- generált ideál 230

generátor *208, 211–212*
generátormátrix *327*
generátorpolinom *329, 330–332*
generátorrendszer *208*
generátum *208*
geometria *10, 96, 206*
geometriai alakzat *206*
— alkalmazás *104*
— jelentés *97, 103*
gépmodell *359*
Gerhard, Jürgen *387*
Germain, Marie-Sophie (1776–1831) *148*
 $G = (\varphi, E, V)$ *169*
GIF *317*
 $g \preceq f$ *341*
 $\mathbb{GL}(F^n)$ *208*
Golay-kód *331*
Golay, Marcel J. E. (1902–1989) *331*
Goldbach, Christian (1690–1764) *373*
Goldbach-sejtés *373*
Gonda János *387–388*
Google *8*
Googletalk *315*
 $[G: H]$ *214*
Gödel, Kurt (1906–1978) *15, 132*
gömbfelület *198*
görbe *197*
— kezdőpontja *197*
— végpontja *197*
görög ábécé *14*
— matematika *94*
 G/N *217*
 $G = (\psi, E, V)$ *183*
gráf *21, 169, 181, 197, 383–384*
gráfalgoritmus *185*
gráfalgoritmusok *181*
gráfelmélet *169*
grafikon *21, 34*
Gray, Frank *181*
Gray-kód *181*
grupoid *55, 207*
gyakoriság *281, 283*
gyenge reláció *29*
gyerek *187, 188, 190*
gyermeke *9*
gyors Fourier-transzformáció *308*
gyök *89, 244, 245–246, 249–250, 261–262, 331*
gyökér *187, 187–188*
gyökeres fa *187*
gyöktényező leválasztása *245*
gyöktényezős alak *255*
gyökvonás *89, 97*
Györfi László *387*
Győri Sándor *387*
gyűjtemény *13*
gyűrű *76, 202, 226, 229–230, 234, 236, 243, 245–246, 273, 275, 279*
— karakterisztikája *229*
gzip *301, 316*
 $\mathbb{H}$ *42, 100*
ha ... akkor ... *7*
Hadamard [ádámár], Jaques (1865–1963) *329*
Hadamard-kód *329*
Hainzmann János *387*
hajlásszög *105*
Hajnal András *132, 387*
Hajnal Péter *387*
Hajós György (1912–1972) *387*
Haken, Wolfgang *200*
Hall, G. G. *387*
halmaz *6, 13, 131*
— képe *24*
halmazelmélet *14*
halmazművelet *18, 231*
halmaznak lenni *13*
Halmos Pál R. *132, 387*
háló *232, 232–233*
hálózat *194, 195*
halt *343, 356, 382*
Halting Problem *373*
Hamburger Péter *132, 387*
Hamel-bázis *127*
Hamel, Georg Karl Wilhelm (1877–1954) *127, 134*
Hamilton-féle számok *100*
Hamilton-kör *180, 383–384*
Hamilton [hemilt], Sir William Rowan (1805–1865) *100, 180*
Hamilton-út *180, 384*
 $\downarrow$ *6, 6*

Hamming-kód *329*
 Hamming-korlát *326*
 Hamming, Richard Wesley (1915–1998) *321, 326, 329*
 Hamming-súly *321*
 Hamming-távolság *321*
 hang *314*
 hangmérnök *314*
 hangya *130*
 hányados *69, 262*
 hányadoscsoport *217*
 hányadosgyűrű *234*
 hányadostest *241, 242, 256–257, 260, 262, 272*
 hardver *65, 365*
 — alapelem *65*
 — logikai alapelem *65*
 harmadfokú *263*
 — egyenlet *94*
 hármasszámrendszer *70*
 harmonikus *308*
 — szám *145*
 háromdimenziós forgatás *104*
 — tér *102, 104*
 három ház, három kút *173, 199*
 3-kielégíthetőség *384*
 háromlevelű rozetta *23*
 háromszög *174*
 háromszög-egyenlőtlenség *95, 102, 106, 321*
 hash *154, 156*
 hashtábla *185*
 hash-transzformáció *70, 71, 304*
 hasít *268*
 hasonló *37, 130, 133*
 hasonlóság *206*
 Hasse-diagram *30–31, 233, 287*
 Hasse, Helmut (1898–1979) *30*
 határozatlan *243, 274*
 háttér *318*
 hatvány *62, 148*
 $\varnothing$ *19, 19*
 hatványhalmaz-axióma *19*
 hatványozás *75*
 hatványösszeg *276, 278*
 Hausdorff-féle maximumelv *123*
 Hausdorff, Felix (1868–1942) *123*
 hegyesszög *103*
 Hellmann, Martin Edward *148*
 hely *34*
 helyettesítés *252, 384*
 helyettesítési érték *244, 247*
 helyiértékes előállítás *70*
 Hensel, Kurt (1861–1941) *269*
 Hensel-lemma *269*
 Hewitt, Edwin *89, 132, 387*
 hexadecimális *45, 70, 155*
 hibacsomó *331, 336*
 hibaérték-polinom *332*
 hibahelypolinom *332*
 hibajavítás *320, 323, 327*
 hibajavító *323, 323, 326*
 — kód *323*
 hibajellemző *327*
 hibajelzés *320*
 hibajelző *321, 323*
 — kód *320, 321*
 hibakorlátozó kód *320*
 — kódolás *285*
 hibavektor *329*
 high *42*
 Hilbert tizedik problémája *375*
 Hilbert, David (1862–1943) *315, 375*
 Hilbert-görbe *315*
 hiperbola *22*
 hiperbolikus spirális *23*
 hiperkocka *170, 172*
 hitelesítés *285*
 H_n *170, 172*
 homeomorf *198*
 homogén binér reláció *21*
 — polinom *274, 276*
 — reláció *39*
 homomorf invariáns *204*
 — kép *203, 204, 211, 228, 229*
 homomorfizmus *203, 204, 209, 228, 234, 236, 264*
 — magja *218, 218, 234*
 homomorfizmus-tétel *218, 234*
 Hopcroft, John E. *386*
 hossz *174, 186*
 hozzárendelés *34*

- HP 373
- Huffman, David Albert (1925–1999) 293, 295
- Huffman-kód 293, 295, 300
- hurokél 169, 170, 183, 201
- hű reprezentáció 204, 231
- i* 94
- IBM Cell 33, 42
- Stretch 70
- 360 70
- IDCT 313
- ideál 227, 230, 234, 240–241
- idegen 16
- idempotencia 16
- idempotens 232
- identikus leképezés 34, 57, 61
- — skalárszorosai 216
- IDFT 307
- idő 281
- időben eldönthető 381
- kiszámítható 381
- időigény 380
- időszerű 210
- rész 101
- időtartomány 314
- IEEE 754 86, 92, 167
- $(i_1, i_2, \dots, i_n)$ 274
- IFFT 311
- $\uparrow$ 6, 6, 384
- IGFET 66
- iLBC 315
- illeszkedési leképezés 169, 183
- mátrix 200
- reláció 169, 171
- illeszkedik 7, 169
- image 23
- immediate 360
- $\mathfrak{I}(p)$ 101
- implikáció 7
- $\mathfrak{I}(z)$ 95
- index 37, 214, 214–215, 217
- indexelt család 37, 122, 219, 236
- halmaz 37
- halmazcsalád 37
- indexhalmaz 37
- indexregiszter 359, 365
- indirekt 9
- indukció 44, 46, 53–55, 59, 62, 76–77, 90, 90, 109, 118, 158, 163, 197, 245, 249, 276
- elve 44, 90
- inf 31
- infimum 31, 85
- infix 287
- információ 281, 281
- információforrás 281
- informatika 61, 169–170, 377
- injekció 35
- injektív 34, 74, 203, 228, 283
- inkongruens 146
- insulated gate FET 66
- integrálás 272
- integrált áramkör 307
- integritási tartomány 78, 79, 81, 230, 241–242, 272
- intervallum 30, 167
- intervallumaritmetika 85
- intervallum-aritmetikai 167
- intervallumskatulyázás 94
- intervallumskatulyázási tulajdonság 89
- intra 319
- invariáns részcsoport 215, 216
- invertálható 228
- inverter 66, 68
- inverz 24, 37, 55, 110, 137, 202–204, 250
- diszkrét Fourier-transzformáció 307
- — koszinusztranszformáció 313
- kép 24
- inverzképzés 207, 216
- irány 28
- irányítás 103, 183
- irányítatlan gráf 169, 183, 185, 200
- irányított ciklus 184
- címkézett gráf 356
- csillag 184
- él 23
- fa 187, 187–188, 190, 287
- gráf 183, 184, 187, 192–193, 200
- kör 186, 186, 193, 195
- ösvény 184
- részfa 187
- részgráf 186

- séta *186*
- szupergráf *186*
- teljes gráf *184, 186*
- út *186, 187, 194–195*
- vonal *186*
- irányjel *343*
- irányvektor *104*
- irracionalis *166*
 - szám *90, 110*
- irreducibilis *136–137, 138, 237, 240, 250, 252, 256, 260–261, 264–265, 268*
 - elem *227, 250*
 - faktor *262*
 - főpolinom *255, 261*
 - polinom *250, 254–256*
- irreflexív *26, 27, 29*
- ISBN *320*
- ismert hibahely *324*
- ismétléses kód *324*
 - kombináció *112*
 - permutáció *112*
 - variáció *111*
- Ivanyos Gábor *181, 375, 389*
- Iverson, Kenneth Eugene (1920–2004) *52*
- Iverson-konvenció *52*
- izolált csúcs *169, 172*
- izomorf *171, 172–173, 184, 199, 203, 211, 218, 220–221, 228, 233–234, 236, 264, 267*
- izomorfizmus *203, 209, 228*
- j* *94, 101*
- Jacobi, Carl Gustav Jacob (1804–1851) *102*
- Jacobi-identitás *102*
- Jákó Péter *387*
- Jarník, Vojtěch (1897–1970) *182*
- javító hálózat *194, 195*
 - út *194, 195*
- j*-edik koordinátafüggvény *40*
- j*-edik projekció *40*
- jel *65*
- jelanalízis *307*
- jellemzők *39*
- Jensen-egyenlőtlenség *282*
- Jensen, Johan Ludwig William Valdemar (1859–1925) *282*
- jobb gyerek *188*
 - kimenő él *188*
 - oldali mellékosztály *214*
 - — nullosztó *77*
- jobbideál *230*
- jobbinverz *55*
- jobb oldali semleges elem *55*
- jobbsodrású *102*
- jólrendezés *33*
- jólrendezési tétel *123*
- jólrendezett *33, 33, 59, 70, 85, 139, 239–240*
- jólszínezés *200*
- jólszínezhető *200, 384*
- Jordan [zsordā], Camille (1838–1922) *199, 327*
- Jordan-tétel *199*
- jóslás *316, 318*
- JPEG *317*
- k* *101*
- Kahan, William *387*
- Kalmár László (1905–1976) *387*
- Kaluzsnyin, Lev Arkadevics (1914–1990) *387*
- kanonikus alak *142, 144, 158–159*
 - leképezés *36, 73, 218, 234*
- kapacitás *194, 195*
- kapacitásfeltétel *194*
- kapcsolási idő *68*
 - rajz *65*
- kapcsoló *65*
- kapcsolóelem *65*
- κ *158*
- kapu *66*
- karakterisztika *251*
- karakterisztikus egyenlet *263*
 - függvény *47, 379*
- karakterkészlet *283*
- kardiod *23*
- Karp, Richard Manning *195*
- kaszád kód *336*
- Kátai Imre *386*
- Kayal, Neeraj *144*
- Kelley, John L. *15, 132, 387*
- kép *24, 318*
- képelem *300, 315*

képrészlet 319
 képtömörítés 315, 317
 képzetes 94, 95, 308
 — rész 95, 101, 102, 105
 kerekítés 85
 kerekítési hiba 85
 — irány 167
 — szabály 86
 $\ker(\varphi)$ 218, 234
 késleltetés 65
 kétdimenziós DFT 314
 — diszkrét koszinusztranszformáció 317
 — paritásellenőrzés 326
 kételemű test 81
 kétértelmű 319
 kétlap 206
 kétrészes gráf 173
 kétszalagos 373
 kettes komplement 147
 — számrendszer 70, 147–148
 kettőhatvány 70, 266
 kétváltozós művelet 40
 — reláció 21
 kétveremtáras gép 358
 keverés 252
 keveset fogyaszt 68
 kezdeti feltétel 376
 kezdő állapot 343
 kezdőpont 183, 184, 186
 kezdőszó 30, 61, 108
 kiegészítő halmaz 17
 kielégíthető 384
 kifok 184, 193, 292
 kijelentés 6
 kimenet 344, 359
 — hossza 344
 kimeneti állapot 340
 kínai maradéktétel 152, 153, 155, 236, 269
 — postás-probléma 183
 kisebb 29
 Kiss Emil 387
 kiszámítható 369–370, 371
 — függvény 369
 kiterjesztés 23
 kiterjesztett euklideszi algoritmus 334
 kitevő 62, 75
 kiürítéses 66
 kiválasztási axióma 122, 123
 — függvény 39, 122
 kivonás 382
 kizáró vagy 252, 254
 Klein-féle csoport 206
 Klein, Felix Christian (1849–1925) 206
 klikk 172
 K_n 172
 Knuth, Donald E. 69, 107, 388
 $\vec{K}_n$ 184
 kockakettőzés 266
 kód 283, 301, 314, 321
 — átlagos szóhosszúsága 291
 — kiterjesztése 298
 — sebesség 321
 — súlya 321, 327, 329–330, 332
 — távolsága 321
 kódábécé 286, 320
 kódfa 287, 288, 291
 kódhossz 304
 kódok direkt szorzata 335
 kódolandó ábécé 286, 299
 — — kiterjesztése 298
 kódolás 202, 283, 301, 349
 kódoláselmélet 10
 kódoló ábécé 286
 kód Rövidítés 335
 kódszó 286
 kódtábla 301
 kombináció 111
 kombinatorika 107
 kombinatorikus robbanás 180
 kommunikáció 281
 kommutatív 53–54, 56, 81, 103, 161, 204, 211, 220, 226, 236, 243, 267
 — egységelemes gyűrű 116–117, 147, 228, 236, 240–241, 245
 — félcsoport 56
 — gyűrű 76
 kommutativitás 16, 18, 38, 102
 kompatibilis 147, 241
 — az osztályozással 73–74, 215
 — osztályozás 234
 komplement ábrázolás 75, 147

- komplementer *17, 38, 147, 173, 186, 232, 370, 373*
- komplex egységgyök *97, 97*
- gyök *99*
- szám *73, 94, 97, 101*
- számpár *101*
- komplexus *207*
- komplexusművelet *207*
- komplexusszorzás *217, 234*
- komponens *176, 178*
- kompozíció *25, 40*
- komputeralgebra *369*
- rendszer *131*
- kongruencia *153, 269*
- megoldása *150*
- kongruenciarendszer *152–153*
- megoldása *151*
- kongruens *146*
- konjugálás *101, 210, 216*
- konjugált *95, 101, 105, 216*
- elemosztály *216, 216, 267*
- transzponált *209*
- konjuktív normál alak *384*
- konjunkció *7*
- konjuktív normál alak *69*
- konstans polinom *243, 274*
- tag *243, 260, 274*
- konstruktív *269*
- konsztrasztvizsgaadás *315*
- kontinuum számosság *132*
- számosságú *122, 130, 131*
- kontinuumhipotézis *132, 132*
- konvergál *166*
- konvolúció *161, 161–162*
- koordinátánként *220, 236*
- koordinátarendszer *266, 317*
- koordinátázás *202*
- korlátozott gépmodell *358*
- koszinusz *96*
- koszinoszos jel *308*
- $[K:F]$ *264*
- Kovács F. Ferenc *387*
- köbös *381, 381, 385*
- kölcsönösen egyértelmű *34, 37, 74, 80, 82, 84, 94, 101, 107, 109, 203, 228*
- König tétele *197*
- König Dénes (1884–1944) *188, 197*
- König-egyenlőtlenség *133*
- König Gyula (1849–1913) *133*
- König-lemma *188*
- kör *174, 175–178*
- környezet *367*
- körosztási polinom *248*
- kötött előfordulás *7*
- követi *29*
- közé esik *30*
- közös határ *199*
- osztó *142, 146, 237*
- többszörös *142, 237*
- tulajdonság *131*
- központi egység *65*
- tár *65*
- közvetlen *360*
- közvetlenül követi *30*
- megelőzi *30*
- kristály *206*
- kristályrács *66, 206*
- kritikus csúcs *193*
- él *193*
- út *193*
- kromacitás *315*
- kromatikus szám *200*
- Kronecker-eljárás *262*
- Kronecker-féle δ -függvény *61*
- Kronecker, Leopold (1823–1891) *61, 262*
- Kruskal algoritmus *181*
- Kruskal, Joseph Bernard, ifj. *181*
- kulcs *40, 70, 148, 190*
- kulcs-cím transzformáció *70*
- kulcscsere *148, 148*
- kupac *188, 189, 293*
- tulajdonság *188*
- kupacépítés *189*
- kupacrendezés *189*
- Kuratowski tétele *199*
- Kuratowski, Casimir (1896–1980) *199*
- Kuros, Alekszander Gennagyijevics (1908–1971) *388*
- különbség *17*
- külső tár *189*
- kvadrális *70*
- kvantálás *305, 315, 317*

- kvantálási függvény *305*
kvantor *7, 52*
— hatásköre *7*
kvaternió *73, 100, 101, 104–105, 209–210, 246*
kvaterniócsoport *217*
kvaterniók *102*
kvaterniópár *105*
kvaterniószorzás *102*
 $K_{3,3}$ *173*
L *42*
Laczkovich Miklós *266, 388*
Lagrange interpolációs alappolinom *261*
— — eljárás *261*
— tétele *214*
Lagrange-interpoláció *262*
Lagrange [lágr̃̂zs], Jozeph Louis (1736–1813) *214, 261*
 λ -kalkulus *368, 372*
 λ -művelet *368*
lánc *29, 122–123*
láncolt lista *244, 275*
lánc tört *163, 166*
lánc tört közelítés *163, 164, 166*
Landau, Edmund (1877–1938) *388*
Láng Csabáné *388*
Lavrov, I. A. *388*
lebeg *68*
lebegőpontos aritmetika *167*
— számábrázolás *86*
Leeuwen, Jan van *388*
lefogó csúcshalmaz *197*
legális lépés *382*
— számolás *382*
legjobb közelítés *166*
legkisebb *30, 232*
— felső korlát *31*
— közös többszörös *138, 142, 144, 237*
 $\text{lkk}(a_1, a_2, \dots, a_n)$ *138*
 $\text{lnko}(a_1, a_2, \dots, a_n)$ *138*
legnagyobb *30, 232*
— alsó korlát *31*
— közös osztó *138, 138–140, 150, 237, 239, 249, 256, 268, 275*
legsűkebb *208*
Leindler László *89, 388*
Leiserson, Charles E. *107, 181, 386*
leképezés *34, 200*
lekérdező nyelv *8*
lelép *355*
Lempel, Abraham *300–301*
lengyel jelölés *41*
lenyomat *154, 156*
lépés *343*
lépésszám *359, 380*
lerajzolás *197, 198*
leszűkítés *23*
létezés *46, 86, 240, 245, 276, 366, 384*
 $\exists$ *7*
levél *187*
lexikografikus rendezés *33*
lezár *66*
lineáris *215, 381, 381*
— csoport *208*
— kód *326, 327, 330*
— kongruencia *151*
— polinom *244, 274*
— rendezés *29*
— tér *326*
— transzformáció *208*
Lisp *368*
lista *185*
 $\ln$ *115*
log *255, 281*
logaritmikus jelleg *305*
— költségű *360*
— spirális *23*
logaritmus *281*
— naturalis *115*
logika *6*
— axiómái *10*
— tanítása *73*
logikai fogalom *10*
— formula *7, 68*
— függvény *65, 65, 68–69, 279, 384*
— jel *7, 18, 65*
— művelet *41, 65, 69, 231–232*
— szita formula *118*
lokális címke *361*
Lorentz-csoport *210*
Lorentz, Hendrick Anton (1853–1928) *210*
Lovász László *387–388*

low 42
 LRC 325
 $\mathcal{L}_T$ 373
 lyuk 66
 LZW 301, 304, 317
 LZ77 300
 mag 234, 236, 264
 magasság 187
 mágneslemez 71
 mágnesszalag 325
 majorálja 124
 makró 360
 makroblokk 319
 Makszimova, L. L. 388
 Manna, Zohar 388
 Manyin, Jurij Ivanovics 375, 388
 maradék 69, 146, 246, 250
 maradékos osztás 69, 69, 246–247, 381
 — — tétele 245, 246
 maradékosztály 146, 233
 maradékosztály-gyűrű 234
 maradékrendszer 146
 Marcus, Andrei 388
 Mariner-9 329
 Markov, Andrej Andrejevics, ifj. 365
 Markov-automata 365
 Mars 329
 másodfajú Stirling-szám 115
 másodfokú 263
 — pont 199
 második koordináta 21
 masszív paralel 172
 maszk 318
 matematika 375
 matematikai elmélet 6
 — indukció 44, 90
 — — elve 44, 90
 — logika 10
 mátrix 76, 200, 230
 max 30
 maximális 30, 109, 123
 — értékű folyam 194
 — folyam 194–195
 — ideál 240, 240–241, 250
 — kommutatív részcsoport 215
 maximális távolságú szeparábilis kód 326
 McMillan, Brockway 289
 McMillan-egyenlőtlenség 289
 MDS-kód 326, 328, 332, 335
 Mealy-automata 358
 Mealy, George H. 358
 megállási feladat 373
 — probléma 375
 megegyezik 245
 megelőzi 29
 megengedett lépés 382
 — számolás 382
 megfeleltetés 21
 megfordítás 183, 185
 meghatározottság 14, 14
 — axiómája 15
 meghatározottsági axióma 14
 megismételhető 320
 megjósolt 319
 megmaradási feltétel 194
 megoldhatatlan 266
 — problémásereg 373, 374
 megszámlálható 122, 128, 128–129
 megszámlálhatóan végtelen 128, 128
 megszorítás 23
 mellékosztály 215–217, 233, 234
 mellékosztály-vezető 327
 mélységi bejárás 192–193
 memória 68, 359, 365
 Mendelson, Elliott 388
 menet 189
 Menger, Karl (1902–1985) 197
 Menger tétele elvágó csúcshalmazra 197
 Menger tétele elvágó élhalmazra 197
 Merkle, Ralph C. 148
 merőleges 103–104
 metall-oxid-semiconductor 66
 metrikus tér 197
 $\cap$ 16, 38, 38, 60, 208, 215, 230
 metszet tulajdonságai 16
 $\cap_i X_i$ 38
 mező 39
 mezőnév 39
 mikroprocesszor 167
 Miller, Garry Lee 155
 Miller–Rabin-féle teszt 155
 Miller–Rabin-teszt 384

min 30
 $\forall$ 7
 minimális 30, 109, 238
 — befejezési idő 193
 — összsúlyú feszítőerdő 181
 — — feszítőfa 182
 — távolságú dekódolás 322
 minimalizáció 380
 minimalizáló operáció 376
 minimálpolinom 264, 264–265
 mintavételezés 304
 mintavételi frekvencia 304, 315
 $-\infty$ 85
 MMIX 42
 mod 85
 modem 285
 moduláris hatványozás 148
 modulátor 285
 mohó algoritmus 110, 182
 Moivre [moávre], Abraham de
 (1667–1754) 97, 119
 Moivre-azonosság 97
 Moivre-tétel 119
 molekula 206
 mondat 7
 monoid 55
 monom 244, 267, 274, 275–276
 monomorfizmus 203, 228, 242–243, 274
 monoton csökkenő 37
 — növekedő 37, 80, 82, 84
 Monster 225
 Moore-automata 358
 Moore, Edward Forrest (1925–2003) 358, 367
 Moore-szomszédság 367
 Morgan, Augustus de (1806–1871) 18, 38
 Morse-kód 286, 295
 Morse, Samuel Finley Breese (1791–1872) 286
 MOS 66
 MOSFET 66
 $m|n$ 135
 mozgás 210
 Möbius, August Ferdinand (1790–1868) 158, 161–162
 Möbius-féle inverziós formula 162
 Möbius-függvény 158
 Möbius-transzformált 161
 MPEG 314, 318
 MPEG-2 314
 MP3 315
 multifok 274, 275
 multiindex 275
 multiplexer 68
 multiplikatív 148, 158, 159, 161–162, 209
 — csoport 254
 — inverz 57, 90, 94, 101, 147, 149, 252
 — jelölés 56
 mutató 190
 μ 158
 Mühlbacher, Jörg 386
 műholdas műsorszórás 331
 Müller, D. E. 329
 μ -operáció 376
 művelet 10, 40, 44, 73, 207, 250
 — invertálható 205
 műveleti tábla 41
 művelet kompatibilis az
 ekvivalenciarelációval 73
 művelet kompatibilis az osztályozással 73
 művelettartó 42, 73
 — leképezés 202
 művelettel kompatibilis osztályozás 217
 n csatornás MOSFET 66
 nagymester sakk támadás 149
 nagyobb 29
 $O(f)$ 341
 $\binom{n}{k}$ 111
 NaN 86
 NAND 68
 naptár 92
 NBG-axiómarendszer 15
 n-dimenziós hiperkocka 170
 n-ed fokú 221
 negáció 7
 negatív 78
 — logika 42
 négydimenziós 102
 negyedfokú 263
 — egyenlet 94
 négyes 70
 négyszínsejtés 200

négyszög 174
 négyzetes 381, 381–382
 négyzetmentes 249, 267
 Neile-féle parabola 22
 Neile, William (1637–1670) 22
 nem 7
 — kapu 66
 nemdeterminisztikus Turing-gép 382,
 382–383
 nemnegatív elemek halmaza 88
 Network Working Group 301
 Neumann–Bernays–Gödel-féle
 axiómarendszer 15
 Neumann János, Margittai (1903–1957)
 15, 365–367
 Neumann-szomszédság 367
 nevek 39
 nevező 79, 273
 Newton képletei 278
 Newton-féle háromágú szigony 22
 — szerpentin 22
 Newton [njuˈtn], Isaac (1643–1727) 22,
 278
 $n!$ 111
 n határozatlanú formális hatványsor 275
 n -határozatlanú polinom 273
 $\wp(\mathbb{N})$ 130
 Nikomakhosz (≈ 100) 48
 Niven, Ivan Morton (1915–1999) 166, 388
 $[n, k, d]_q$ kód 326
 NOR 67
 normálalak 68–69
 normális lebegőpontos szám 86
 — részcsoport 215
 normállánc 224
 normálosztó 215, 215–218, 224
 normált polinom 244
 normálvektor 104
 not and 68
 NOT kapu 66
 not or 67
 nő 8–9
 növekményes 66
 növelés 196
 NP 382, 384
 NP-teljes 384
 n -reguláris 170
 n -szeres gyök 249
 nulla 44, 137
 — polinom 244, 274, 276–277
 nullelem 53, 56, 56, 94, 101, 105, 202,
 232, 232–233
 nullér művelet 40
 nullgyűrű 76, 147, 241
 nullosztó 147
 nullosztómentes 78, 226, 236, 243–244,
 246, 252, 274
 — gyűrű 229
 nullosztópár 77
 nullváltozós művelet 40
 ν 158
 nybble 70
 nyelv 66, 184
 nyelv 370, 370–372, 374–375, 380, 382,
 384
 nyíldiagrammal 23
 nyílt 30
 — gömb 198
 — irányított 186
 — — vonal 186
 — séta 174
 — vonal 174, 179
 nyilvános kulcs 154
 — kulcsú kódolás 154
 nyitott formula 7
 nyolcas 70
 nyomulás 196
 nyújtás 103
 $\mathbb{O}$ 105
 offline 358
 oktális 70
 oktáv 105, 106
 $\Omega(g)$ 341
 ω 47
 $\mathcal{O}(n)$ 208
 online 358
 opacitás 315
 operáció 34
 operandus 40
 operátor 34
 optimális kód 291
 — prefix kód 291–292

órajel 381
 órajelvezérelt 65
 $O(f)$ 341
 $O(r, s)$ 209
 ország 200
 ortogonális 307
 — csoport 208–209
 oszd meg és uralkodj 190
 oszlopindex 200
 oszlopkeverés 253
 osztály 13, 15, 131
 osztályegyenlet 216
 osztályozás 28, 28, 116, 187
 osztás 90
 osztható 135–136, 136
 oszthatóság 135, 146, 239, 256
 osztó 30, 135–136, 137–138, 142, 146,
 237, 246, 260, 262, 383
 osztók összege 159
 — száma 159
 önreprodukáló automata 366
 önzetű 66
 önzáró 66
 — MOSFET 66
 öröknaptár 92
 őrszem 359
 ősz 125
 őskép 24
 összeadás 52, 74, 79, 81, 85, 90, 94–95,
 101–102, 105, 147, 236, 241, 274, 381
 — monoton 75, 78–79
 — szigorúan monoton 78
 összeadással kompatibilis
 ekvivalenciareláció 233
 összeadástartó 74, 80, 82, 84, 94, 101, 215
 összeférhetetlen vagy 7, 68
 összefésülés 189
 összefüggő 175, 176–180
 összeg 52, 63, 243, 275
 összegzési függvény 161, 162
 — tétel 114
 összehasonlítás 124
 összehasonlítható 26, 29, 29, 124
 összehúzás 103
 összes dolgok halmaza 15
 összesség 13
 összetétel 25, 40, 375
 összetett 383–384
 — szám 142
 ösvény 172
 öt szögpontú teljes gráf 199
 P 381, 384
 p csatornás MOSFET 66
 — típusú 66
 Paeth, Alan W. 316
 Paeth-jóslás 316
 paletta 315
 pálya 116
 pár 15
 parabola 22
 paralelepipedon 103
 paralelogramma területe 103
 paralelogramma-azonosság 96
 paralelogramma-szabály 102
 páratlan 69, 137, 308
 — permutáció 222
 — prím 266
 páraxióma 15
 parciális függvény 34, 372, 375, 377–379
 — művelet 42
 — rekurzív megadás 376
 — rendezés 29
 — törtekre bontás 272
 parciálisan kiszámítható 369, 370, 372,
 377–378
 — — függvény 369
 — rekurzív 376, 377–380
 — Turing-kiszámítható 369, 372
 párhuzamos 366
 — él 195
 — élek 169
 párhuzamossági axióma 10
 paritás 222
 paritásbit 320
 paritásbités kód 320
 páronként diszjunkt 16
 páros 69, 137, 308, 313, 373
 — gráf 173, 197
 — permutáció 222
 párosítás 197
 Pascal [pászkál], Blaise (1623–1662) 117
 Pascal-háromszög 117

Pavlov, Radiszlav 386
 Peano-axiómák 44, 46, 90
 Peano, Giuseppe (1858–1932) 44–46, 90
 Pelikán József 388
 Penrose, Roger 389
 periodikus 313
 — jel 305
 periódusideje 304
 permutáció 35, 57, 110, 116, 220, 264,
 321, 327
 permutációcsoport 221
 PERT 193
 Petersen-gráf 170, 172, 199
 Petersen, Julius Peter Cristian
 (1839–1910) 170
 PGP 154
 π 96
 pillangó művelet 309
 piros-kék algoritmus 183
 pitagoraszai számhármakok 157
 pixel 315
 PLA 69
 $\text{PGL}(F^n)$ 219
 $+\infty$ 85
 P_n 172
 PNG 315
 $P_n^{i_1, i_2, \dots, i_r}$ 112
 $\vec{P}_n$ 184
 Poincaré-csoport 210
 Poincaré [poekäré], Jules Henri
 (1854–1912) 210
 pointer 190, 304
 polinom 119, 202, 238, 244–246, 248, 272,
 273, 275–276, 329
 — maradék sorozat 258
 polinomfaktORIZÁLÁS 267
 polinomfüggvény 245, 245–246, 279
 polinomiális 381, 384–385
 — együttható 117
 — idő 382
 — tétel 117
 polinomkódolás 329
 polinomszorítás 312
 pont 7, 10, 286
 pontonként 226
 pontos alsó korlát 31
 — felső korlát 31
 pontosan akkor 7
 — az egyik 7
 — egy létezik 8
 pontosan t -hibajavító 323
 pontosan t -hibajelző 321
 Post, Emil Leon, (1897–1954) 356
 Post-gép 356
 PostScript 41
 pótlás axiómája 131
 pozitív 78
 — logika 42
 — természetes számok 44
 — töltésű 66
 precedencia 40
 predicted 319
 predikátum 6, 8–10, 65
 — tagadása 13
 prefix 287, 300
 — kód 287, 288–289, 291, 300–301, 318
 prefixmentes halmaz 287
 — kód 287
 prím 70, 144, 148, 154–155, 237, 251,
 261–262
 prímelem 137, 137–138, 140, 227, 237,
 239, 241, 250, 260
 prímszám 136, 137, 140, 142, 147–149,
 168, 206, 229, 245, 248, 250, 260,
 269, 373, 380
 prímszámmrendű 214
 prímszámtétel 142
 prímtényező 144
 prímtényezőkre bontás 144
 prímtest 243
 prímtesztelés 144
 próbaosztás 144
 processzor 92
 $\prod_{k=1}^n x_k$ 62

program 365
 programmable logical array 69
 programmemória 359
 programok 381
 programozási nyelv 73
 programozható logikai sík 69
 projekció 39, 236
 projektív általános lineáris csoport 219
 projektív speciális lineáris csoport 219
 Prolog 10
 protokoll 148
 Prüfer-csoport 206
 Prüfer, Ernst Paul Heinz (1896–1934) 206
 $\mathbb{PSL}(F^n)$ 219
 pszeudohányados 246
 pszeudomaradék 246
 pszeudoosztás 246
 Pythagoras (i.e. VI. sz.) 83
 Q 79, 206
 q -ad rendű B-fa 190
 q -ad rendű fa 188
 q -alapú kupac 188
 Quine, Willard Van Orman 389
 $\mathbb{R}$ 85, 130
 $R(a)$ 24
 $R(A)$ 24
 Rabin, Michael Oser 155, 358
 Rabin–Scott-automata 358
 racionális függvény 272
 — szám 73, 79, 83–84, 90, 90, 110, 241
 rácspont 366
 R^{-1} 24
 $R^{-1}(B)$ 24
 R^X 226
 rajzjel 66
 rajzolható 197, 198
 rákövetkezés 44, 46, 52
 rákövetkezésre zárt 20
 rákövetkezője 44
 RAM 68, 359
 RAM-gép 359, 359
 range 23
 real time 341
 Recski András 389
 redukált maradékosztály 146
 — maradékrendszer 146, 149
 redundancia 283
 Reed, Irving Stoy 329, 331–332
 Reed–Muller-kód 329
 Reed–Solomon-kód 331, 332, 335
 reflexív 14, 26, 27–29, 137
 reflexivitás 107, 124
 regiszter 359, 365
 reguláris gráf 170
 — reprezentáció 204, 231
 regularitás 205
 regularitási axióma 134
 rejtjelezés 135, 154–155, 202
 rejtjelező 154
 rekesz 359
 rekord 39, 70–71, 188
 rekurzió 46, 61, 163, 269, 273, 376, 379
 rekurziótétel 46, 46, 52–53, 61
 rekurzív 379
 — lépés 376
 reláció 39, 184, 186, 382
 — inverze 24
 — irányított gráfja 23
 relációban van 21
 relációk gráfja 27
 reláció kompatibilis az
 ekvivalenciarelációval 74
 reláció kompatibilis az osztályozással 74
 relatív cím 71
 — entrópia 282
 — gyakoriság 281
 — hiba 86, 115
 — prím 138, 138, 140, 146, 149, 152–153,
 158, 165, 236, 248
 relativitáselmélet 210
 rend 211, 212, 214
 rendezés 29, 58, 75, 79, 85, 109, 186
 rendezett 33, 58
 — halmaz 29
 — integritási tartomány 78, 78–79, 81
 — pár 20, 21, 40
 — test 81, 82–86, 88, 90, 94–95
 rendezett n -es 59
 (x, y) 20
 rendszer 13
 reneszánsz 94
 $\Re(p)$ 101

reprezentáció 204, 231
 reprezentáns 74, 146, 250
 részbenrendezés 29, 109, 137, 186
 részbenrendezett 33, 122–123
 — halmaz 29, 232
 részcsoporth 207, 207–208, 212, 214–215, 230, 321
 részfeladat 193
 részfélcsoport 207
 részgráf 173, 177, 383
 részgrupoid 207
 részgyűrű 230
 részhalmaz 14, 128
 $\subset$ 14
 részhalmaz-axióma 14, 15
 részháló 232, 233
 részstruktúra 242
 résztest 230
 Révész György 389
 $\Re(z)$ 95
 RFC 155, 301
 (R, φ) 237
 RGB 315, 317
 Rijmen, Vincent 252
 Rijndael 252
 Rijndael-test 254
 RIPEMD-160 154
 Rivest, Ronald Linn 107, 154, 181, 386
 $R[x]$ 244
 $R[x_1, x_2, \dots, x_n]$ 275
 rng 23
 robotvezérlés 104
 Rónyai Lajos 181, 375, 389
 RPN 41
 RSA 149, 154, 154–156
 Rudin, Walter 89, 99, 389
 Russell, Bertrand (1872–1970) 15, 45
 Russell-paradoxon 15
 $R[x]$ 244
 $R[x_1, x_2, \dots, x_n]$ 273
 Saaty, Thomas L. 386
 $\mathbb{SA}(F^n)$ 208
 Safarevics, I. R. 389
 saját gyökképlet 264
 Salomon, David 389
 Sárközy András 389
 Saxena, Nitin 144
 Schipp Ferenc 89, 388
 Schönnemann–Eisenstein-tétel 260, 261
 Schönnemann, T. 260
 Schröder–Bernstein-tétel 125
 Schröder, Ernst (1841–1902) 125
 Schrödinger, Erwin Rudolf Jozef Alexander (1887–1961) 206
 Scott, Dana Stewart 358
 segédkulcs 252, 254
 — hozzáadása 253
 sejtautomata 367
 sejtés 384
 semleges elem 55
 sem ... sem ... 7
 sem-sem kapu 67
 sentinel 359
 séta 174, 175
 SHA-1 154
 Shamir, Adi 154
 Shannon mintavételi törvénye 305
 Shannon, Claude Elwood (1916–2001) 252, 281, 291, 305, 324
 Shannon-kód 295
 — létezése 291
 Shannon tétele zajmentes csatornára 291
 Sidon Simon (1892–1941) 110
 Sidon-sorozat 110
 Sierpiński, Waclaw (1882–1969) 389
 Sigler, Laurence Edward 132, 387
 sík 95
 — egyenlete 104
 — paraméteres egyenlete 104
 síkba rajzolás 198–199
 — rajzolható 198–199, 383
 síkgeometria 6–7
 síkrács 172
 Singleton, R. C. 326
 Singleton-korlát 326
 skalár rész 101
 skaláris szorzás 103
 skatulya elv 109
 $\mathbb{SL}(F^n)$ 208
 S_n 172, 221
 SNaN 86
 $\vec{S}_n$ 184

sokaság 13
 Solomon, Gustave (1930–1996) 331–332
 $\mathbb{SO}(n)$ 209
 Sophie Germain prím 148
 $\mathbb{SO}^+(1, 3)$ 210
 sor 356
 — vége 300
 sorindex 200
 sorkeverés 253
 sorozat 52, 60, 126, 243
 $\mathbb{SO}(r, s)$ 209
 source 66, 194
 szózás 155
 speciális affin csoport 208
 — — transzformáció 208
 — eset 384
 — lineáris csoport 208
 — Lorentz-csoport 210
 — ortogonális csoport 209
 — unitér csoport 209
 SQL 8
 SSH 148
 SSL 148
 standard error 344, 370
 — input 344
 — output 344
 start 343, 356, 382
 statikus 299
 — CMOS 66
 Stein, Clifford 386
 Stirling-formula 114
 Stirling [sztörling], James (1692–1770)
 114–115
 Stone tétele 233
 Stone [sztoun], Marshall Harvey
 (1903–1989) 233
 Stromberg, Karl R. 89, 132, 387
 súly 181, 276, 276
 súlyozott gráf 181
 $\mathbb{SU}(n)$ 209
 sup 31
 Surányi János 389
 süllyesztés 188
 szabad előfordulás 7
 — változó 7, 7–8
 szabályos kerekítés 85
 — test 170, 172
 Szabó Réka 181, 375, 389
 szabvány 167, 314
 szabványos bemenet 344
 — hiba 344
 — kimenet 344
 szalag 342
 szalagábécé 343
 számelmélet 135, 373
 — alaptétele 140
 számelméleti függvény 158, 158, 162
 számítási eljárás 340, 340–342, 344, 359,
 365, 367
 — modell 380
 — sorozat 340
 számítógép 55, 65, 70, 95, 200, 275, 304,
 342, 351, 359, 366
 számítógépes ábrázolás 70, 75, 80, 85–86,
 147, 201
 — algoritmus 217
 — tárolás 244
 számjegy 320
 számláló 79, 273
 számosság 108, 131, 132
 számrendszer 70, 349
 Szapozsenko, A. A. 387
 szavak 60
 Székelyhidi László 389
 szektor 71, 190
 szélességi bejárás 192, 192, 195
 szelet 87, 166, 319
 Szele Tibor 389
 személyi szám 320
 — törzsállomány 39
 szemét 344
 szemétygyűjtés 351, 355
 Szendrei Ágnes 132, 386, 389
 szeparábilis 326
 szerkeszthető 266, 266
 szigetelő 66
 szigetelt kapu 66
 σ 159
 σ_r 159
 sgn 85, 96
 szigorú pár 29
 — reláció 29

— részbenrendezés *29*
 szigorúan antiszimmetrikus *26, 27, 29, 186*
 — konvex *282*
 — közé esik *30*
 — majorálja *124*
 — monoton *37*
 — — csökkenő *37*
 — — növekedő *37*
 — párhuzamos élek *183*
 szilícium *66*
 szilícium-dioxid *66*
 szimbolikus címke *361*
 szimmetria *14, 107, 321*
 szimmetriacsoport *206*
 szimmetriaelv *206*
 szimmetriatengely *206*
 szimmetrikus *26, 27–28, 137*
 — csoport *57, 221, 221*
 — differencia *17*
 — kulcs *154*
 — polinom *275, 276*
 — polinomok alaptétele *276*
 $\triangle$ *17*
 szimplex módszer *385*
 szimuláció *341*
 szimulál *340, 341, 345, 347, 349–350, 356–359, 362, 364–368*
 szín *287*
 szindróma *327, 329, 332, 334*
 szindrómadekódolás *327*
 színesség *317*
 színezett gráf *181*
 szinkronhiba *320*
 szint *187, 287*
 szinteltolás *305*
 szinusz *96*
 szisztematikus kód *330*
 — kódolás *327*
 szó *60, 120, 252, 286*
 szóköz *287, 343, 382*
 szolgáltatásazonosítás *331*
 Szominszkij, I. Sz. *386*
 szomszédos *169, 172*
 szomszédságtartó *172*
 szorzás *53, 75, 79, 81, 90, 94, 101, 105, 147, 236, 241, 274, 381*
 — monoton *78–79*
 — szigorúan *78*
 szorzástartó *80, 82, 84, 94, 101*
 szorzat *25, 53, 62, 243*
 — differenciálási szabálya *248*
 $\times_{i \in I} X_i$ *39*
 szótár *299, 300, 304*
 szótárkód *299*
 szög *96–97, 103*
 szögharmadolás *266*
 szögpont *169, 183*
 szövegszerkesztő *369*
 szubnormális lebegőpontos szám *86*
 szubrezultáns algoritmus *259*
 szuffix *287*
 $\sum_{k=1}^n x_k$ *63*
 szupergráf *173*
 szuperjektív *34*
 szuprémum *31, 85*
 születésnap-paradoxon *113*
 szülő *125, 187, 188*
 szűrjektív *34, 203, 228*
 $\mathbb{T}$ *206*
 tá *286*
 táblaváltó *299*
 táblázat *200*
 tag i -ed fokú *243*
 takarítás *196*
 tanú *383, 383–384*
 tanú-tétel *383*
 tápfeszültség *68*
 tárigény *327, 380*
 tároló *65*
 tárolt programú gép *365*
 tárral eldönthető *381*
 — kiszámítható *381*
 Tartaglia $\rightarrow$ Fontana, Niccolo *94*
 tartalmazás *21*
 tartomány *198, 198–199*
 τ *159*
 távolság *104, 105, 174*
 Teichmüller, Oswald (1913–1943) *123*
 Teichmüller–Tukey-lemma *123*
 telepfeszültség *66*

telített 195
 — él 194
 — irányított részgráf 186, 187
 — kivonás 377
 — részgráf 173
 teljes csúcs 287
 — gráf 172
 — indukció 61, 70, 276
 — — elve 44, 90
 — inverz kép 218, 234
 — maradékrendszer 146, 149, 307
 — rendezés 29
 teljes diszjunktív normál alak 69
 teljesen additív 158, 158
 — multiplikatív 158, 158
 teljes konjunktív normál alak 69
 tér 281
 térbeli forgatás 210
 téridő 102, 210
 terjengősség 283
 természetes logaritmus 115
 — szám 44, 45, 46, 58, 69–70, 90, 108, 135, 140, 188
 terminal 194
 ternáris 70
 — kód 286
 térrács 172
 térszerű 101
 — rész 101
 tértükrözés 210
 térvezérlésű tranzisztor 65
 test 81, 94, 147–148, 219, 226, 230, 236, 240–241, 246, 250, 264, 267, 272, 275
 testbővítés 250, 265
 testvér 187
 tesztpolinom 268
 tétel 6, 9
 tételbizonyító algoritmus 10
 tetraéder 178
 $\Theta(g)$ 341
 t -hibajavító 323
 t -hibajelző 321
 ti 286
 tisztán képzetes 101
 — — kvaternió 102–103
 titkos kulcs 148, 252
 titkosítás 285
 titokmegosztás 262
 titokrész 262
 tizenhatos 70
 tízes számrendszer 70, 140
 TLS 148
 tompaszög 103
 topologikus rendezés 186, 193
 topologikusan izomorf 199, 199
 tórusz 172
 totálisan additív 158
 — multiplikatív 158
 Totik Vilmos 389
 TOTÓ 329
 többhatározatlanú polinom 273
 többletes kód 75
 többszörös 135–136, 138
 — élek 169
 — gyök 249
 többváltozós függvény 61
 tökéletes 326
 — kód 328–329, 331
 — szám 161, 168
 tömb 42, 244, 275
 tömörítés 283, 304, 319
 törlési szabály 53, 59
 törtrész 85–86
 törzsszám 136, 137, 140
 Trahtenbrot, Borisz Abramovics 389
 transzfinit indukció 61, 62
 — rekurziótétel 61
 transzformáció 34
 transzponált 209
 transzpozíció 222, 222
 tranzisztor 66–67
 tranzitív 14, 26, 27–29, 137, 186
 — halmaz 47
 — lezárt 60
 tranzitivitás 107, 124
 trichotom 26, 27, 29
 trigonometrikus alak 96
 — függvény 55, 94
 triviális ideál 230
 — infix 287
 — normálosztó 215
 — osztó 137

- prefix *287*
- részcsoporth *207, 214*
- szuffix *287*
- Tschirnhaus, Ehrenfried Walter
(1651–1708) *264*
- Tschirnhaus-transzformáció *264*
- T. Sós Vera *388*
- Tukey, John Wilder (1915–2000) *123*
- túlsordul *70*
- túlsordulás *86, 115, 147*
- turbó *325*
- Turing, Alan Mathison (1912–1954)
342–343, 351, 355, 368–370, 372–373, 382
- Turing-eldönthető *370*
- Turing-felsorolható *370*
- Turing-gép *130, 343, 369, 373–374, 379, 381, 383*
- nyelve *373*
- Turing-kiszámítható *369–370*
- tükörözés *96, 206, 216*
- $\cup$ *206*
- Ullman, Jeffrey D. *386*
- $\cup(n)$ *206, 209*
- unáris *344, 382*
- kód *286, 349, 374*
- unér művelet *40, 55*
- $\cup$ *15*
- unió *15, 37, 38, 60*
- tulajdonságai *16*
- unióaxióma *16*
- $\cup_i X_i$ *37*
- unitér csoport *209*
- univerzális *374*
- kvantor *7*
- Turing-gép *351*
- univerzum *15*
- unokája *9*
- unsigned *70*
- út *174, 175–176, 178, 187, 195*
- utasítás *359*
- utasításkészlet *359, 364, 365, 365*
- utazó ügynök problémája *182, 183*
- utód *125*
- utolsó *30*
- utótagja *287*
- üres *343*
- állapot *366*
- gráf *169*
- halmaz *15*
- — axiómája *15*
- összeg *244, 274*
- szó *286*
- szorzat *211*
- $\{\}$ *15*
- úrtávközlés *325*
- ütemezés *193*
- üzenet *154, 281*
- üzenetkódolás *284*
- vágás *178, 178*
- vagy *7, 8*
- vagy ... vagy ... *7*
- Vajda István *387*
- valódi ideál *230*
- infix *287*
- Lorentz-csoport *210*
- normálosztó *215*
- osztó *137, 161*
- prefix *287*
- részcsoporth *207*
- részhalmaz *14, 108, 129*
- szuffix *287*
- tartalmazás *21*
- valós *308, 313*
- idejű *341*
- rész *95, 101, 102, 105*
- szám *73, 84, 85, 86, 88, 90, 166*
- számpár *94*
- valószínűség *155*
- valószínűségi módszer *268*
- prímszámteszt *144*
- teszt *155, 155*
- változó *7, 299, 384*
- Vandermonde, Alexandre Théophile
(1735–1796) *331–332*
- Vandermonde-determináns *331*
- van der Waerden, Bartel Leendert
(1903–1996) *389*
- Varga Sándor *387*
- variáció *111*
- véges *108, 109, 128, 170*
- ábécé *120, 343*

- Abel-csoportok alaptétele *220*
- automata *130, 358*
- bővítés *264, 265*
- ciklikus csoport *212*
- csoport *216*
- geometriák *10*
- gráf *170, 176–181*
- gyűrű *228*
- halmaz *107*
- irányított *186*
- jellegű *122, 122–123*
- összeg *274*
- rendű elem *212*
- sorozat *59, 60, 224*
- test *202, 211, 250–251, 254–255, 267, 331*
- tesztek alaptétele *267*
- tulajdonságú *122*
- végesen generált Abel-csoportok alaptétele *220*
- véget ér *340*
- végpont *169, 183, 184, 186*
- ∞ *95, 108, 122, 128–130, 142, 170, 188, 229, 245*
- végtelen ciklikus csoport *211*
 - sorozat *45, 59, 243*
- végtelenségi axióma *20*
- vegyes szorzás *103*
 - szorzat *103*
- vektor *95–96, 101, 102–104*
 - rész *101*
- vektori szorzat *102*
- vektoriális szorzás *102*
 - szorzat *103*
- vektorkvantálás *306*
- véletlen *155, 262*
- Venn-diagram *17*
- Venn, John (1834–1923) *17*
- verem *358*
- veremtár *358*
- vessző *288, 295*
- vesszőmentes kód *288*
- vesszős kód *288*
- Vesztergombi Katalin *388*
- veszteséges *283*
- veszteségmentes *283*
- vetítés *39*
- vetület *103*
- vevő *281*
- vezérlőegység *342*
- vezet *66*
- vezetés *66*
- videófelvétel *318*
- videótelefon *319*
- Vinogradov, Ivan Matejevics (1891–1983) *389*
- Vollmar, Roland *389*
- vonat *174*
- vonás *286*
- Voyager *331*
- VRC *325*
- Warshall–Floyd-algoritmus *193*
- Warshall, Stephen (1935–2006) *193*
- $w(C)$ *321*
- Wedderburn tétele *267*
- Wedderburn, Jozeph Henry MacLagan (1882–1948) *267*
- Welch, Terry *301*
- Wigner Jenő Pál (1902–1995) *206*
- Wiles, Andrew *151*
- Wilson tétele *248*
- Wilson, John (1741–1793) *248*
- X^I *39*
- $X \preceq Y$ *124*
- $X \prec Y$ *124*
- X -et Y -ra képező függvény *34*
- $\wp(X)$ *126*
- $x \bmod y$ *85*
- $X \rightarrow Y$ *34*
- $Y \succeq X$ *124*
- $Y \succ X$ *124*
- $\mathbb{Z}$ *74*
- zaj *305*
- $\mathbb{Z}[\alpha]$ *227*
- $[\mathcal{F}(x)]$ *52*
- zárt *30*
 - alak *164*
 - formula *7, 8*
 - irányított séta *186*
 - — vonal *186*
 - séta *174*
 - vonal *174, 175, 179*

zene [315](#)

Zermelo, Ernst Friedrich Ferdinand
(1871–1953) [14](#), [45](#), [131](#)

Zermelo–Fraenkel-axiómarendszer [131](#)

zérógyűrű [76](#)

ZF [131](#)

ZFC [131](#), [132](#)

Ziv, Jacob [300–301](#)

zlib [301](#)

$\mathbb{Z}_m$ [147](#)

Zoltai József [387](#)

Zorn-lemma [123](#)

Zorn, Max August (1906–1993) [123–124](#)

$\mathbb{Z}_{p^\infty}$ [206](#)

Zsegalkin, Ivan Ivanovics (1869-1947) [279](#)

Zsegalkin-polinom [279](#)

Zuckerman, Herbert S. (1906–1993) [166](#),
[388](#)