Tartalomjegyzék

Első rész

ALAPOK

1. Matematikai logika

A matematikai logika a gondolkodás és következtetés formális szabályaival foglalkozik. A „formális” szó azt jelenti, hogy a gondolatok, kijelentések szerkezetét és azok igazságát vizsgáljuk. A matematikai logikát a számítástudományban is széleskörűen alkalmazzák, például programozási nyelvekben, szakértői rendszereknél, mesterséges intelligenciában. Mindemellett az emberi gondolkodás törvényszerűségeinek ismerete a mindennapi életben is elengedhetetlen.

1.1. A kijelentéskalkulus

1.1.1. Kijelentések és igazságértékük

A matematikai logika formalizálja azt a nyelvet, amelyben a matematikai állításokat kimondjuk. A beszélt és írott nyelvek sokféleségéből fakadó félreérthetőség miatt a matematikában a lehetséges állításokat, kijelentéseket mesterséges, formális nyelven fejezzük ki, amely a köznapi nyelvnek csak logikai szempontból jelentős elemeit tartalmazza. Először magát a ***kijelentés*** fogalmát kell tisztáznunk. A kijelentés minden szóban vagy írásban kifejezett képződmény, amelyhez valamilyen ***igazságérték*** tartozik. Általában azt követeljük meg, hogy a kijelentések igazságértéke IGAZ vagy HAMIS legyen (***kétértékűség elve***), és a kettő egyidejűleg ne teljesüljön. (Szokás a kijelentéskalkulust ***ítéletkalkulusnak*** is nevezni.) A matematikában léteznek olyan kijelentések, melyek igazságértéke nem ismert, ezekről esetenként feltételezzük, hogy igazak (***sejtések***).

1.1. példa. Tekintsük az alábbi kijelentéseket:

A_1 : A rózsa virág.
A_2 : A Rózsa egy név.
A_3 : A 4 prímszám.
A_4 : Minden 2-nél nagyobb páros szám két prímszám összege.

Ekkor A_1, A_2 IGAZ kijelentések, A_3 HAMIS kijelentés, A_4 igazságértéke pedig ismeretlen, amiről azt gondoljuk, hogy IGAZ (ez a páros GOLDBACH-féle sejtés). Jegyezzük meg, hogy jelek vagy betűk nem minden sorozata kijelentés:

A_5 : A 3 szám nagyobb.
A_6 : Miért szeretjük a gyerekeket?

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
I	I	H	I	I	I	I
I	H	H	H	I	H	H
H	I	I	H	I	I	H
H	H	I	H	H	I	I

1.1. ábra. A logikai műveletek igazságtáblázata.

1.1.2. Predikátumok

A matematikai elméletekben általában olyan fogalmak, kijelentések szerepelnek, amelyek ún. *változókat* tartalmaznak. Ezeket ***predikátumoknak*** nevezzük. A változók meghatározott objektumok lehetnek. Amennyiben a változók értékeit rögzítjük, kijelentéseket kapunk, más szóval a változók helyébe konkrét értékeket írva a predikátumok igazságértéke egyértelműen eldönthető.

1.2. példa. Vizsgáljuk meg az alábbi predikátumokat: $P(\alpha), Q(x, y), S(a, b, c)$. Ha P a „...prímszám" predikátum, akkor $P(3)$ jelentése: a 3 prímszám, a kijelentés tehát IGAZ; amennyiben P a „...páros szám" predikátum, akkor a 3 páros kijelentés igazságértéke HAMIS. $Q(x, y)$ jelentheti például azt, hogy „az x pont illeszkedik az y egyenesre", $S(a, b, c)$ pedig azt, hogy sorrendben az első és a második bemenet összege a harmadikkal egyenlő, vagyis ekkor $S(3, 4, 7)$ igazságértéke IGAZ.

Az 1.2. példa arra is rávilágít, hogy a predikátumok változói közötti sorrendiség lényeges.

1.1.3. Kijelentések összekapcsolása, kijelentésformulák

A kijelentések összekapcsolásával ***kijelentésformulákat*** kaphatunk. Az összekapcsolás jelölésére különleges szimbólumokat, ***logikai összekötőjeleket*** (***logikai műveleti jeleket,*** idegen szóval junktorokat) alkalmazunk. Az alábbi írásmód a szokásos: $\neg A$ a „nem A"-ra, $A \wedge B$ „A és B"-re, $A \vee B$ „A vagy B"-re, $A \Rightarrow B$ „ha A akkor B"-re, $A \Leftrightarrow B$ „A pontosan akkor, ha B"-re. Ezeket a logikai műveleteket sorrendben *tagadásnak* vagy *negációnak, és*-nek vagy *konjunkciónak, vagy*-nak vagy *diszjunkciónak,* továbbá *implikációnak* és *ekvivalenciának* nevezzük. A kijelentéskalkulusban az összekapcsolások igazságértéke az egyes részkifejezések igazságértékeiből ún. ***igazságtáblázatok*** szerint egyértelműen adódik. Az 1.1. ábra a logikai összekötőjelekre vonatkozó szokásos igazságtáblázatot mutatja. Az IGAZ értéket I-vel, a HAMIS értéket H-val rövidítjük.

Vessünk egy pillantást az implikációra. Mivel helytelen állításból logikailag helyes következtetéssel mind IGAZ, mind HAMIS állításhoz eljuthatunk, ha az A kijelentés HAMIS, akkor $A \Rightarrow B$ igazságértékét mindig célszerű IGAZ-nak rögzíteni. Jegyezzük meg, hogy az összekapcsolások igazságértéke független attól, hogy a részkifejezések között tartalmilag van-e logikai összefüggés vagy nincs.

1.3. példa.

A_7 : Ha 7 páros szám, akkor az Euklideszi geometriában a síkbeli háromszögek belső szögeinek összege 180°.

Ekkor A_7 IGAZ kijelentés, mert a 7 páratlan szám.

A mindennapi életben a „vagy" kétféle értelemben is előfordul.

1.4. példa.

A_8 : Süt a nap vagy esik az eső.
A_9 : Ősz van, vagy tavasz van.

A_8 a „megengedő vagy"-ot illusztrálja: ha a kijelentés IGAZ, akkor a két lehetőség közül legalább az egyik (esetleg mindkettő) teljesül. Az A_9 kijelentés pedig a „kizáró vagy"-ra példa, a két lehetőség közül valamelyik teljesülhet, de a kettő egyszerre nem. A továbbiakban a „vagy" mindig a „megengedő vagy"-ot jelenti. Ennek felel meg a diszjunkció oszlopa az iménti táblázatban.

A köznyelvben az „és", „vagy" kötőszavakat nemcsak a konjunkció illetve diszjunkció értelemben használjuk.

1.5. példa.

A_{10} : És mégis mozog a föld.
A_{11} : Vagy huszonötezer szurkoló lehetett a mérkőzésen.

1.1.4. A kijelentéskalkulus tételei és szabályai

Valamely kijelentésformulát ***kielégíthetőnek*** nevezünk, ha alkalmas behelyettesítéssel igazságértéke IGAZ lesz. Nagyon fontosak az ***általános érvényű kijelentésformulák***, amelyek minden behelyettesítés esetén igazak. Ezeket a ***kijelentéskalkulus tételeinek*** vagy ***tautológiáknak*** nevezzük. A kijelentéskalkulus tételeiből ***következtetési szabályok*** adódnak, amelyek segítségével igaz kijelentésekből újabb igaz kijelentéseket kaphatunk. Az alábbiakban felsoroljuk a kijelentéskalkulus fontosabb tételeit. Az írásmódot a zárójelek elhagyásával egyszerűsítettük annak figyelembevételével, hogy a $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$ logikai összekötőjelek közül a sorrendben előbbi erősebben kapcsol, mint az utána következő. Úgy is mondjuk, hogy a sorrendben előbbinek nagyobb a ***precedenciája***.

(1) $A \vee \neg A$ (a harmadik kizárásának tétele)
(2) $\neg(A \wedge \neg A)$ (az ellentmondás tétele)
(3) $\neg(\neg A) \Leftrightarrow A$ (a kettős tagadás tétele)
(4) $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$ (DE MORGAN egyik tétele)
(5) $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$ (DE MORGAN másik tétele)
(6) $A \Rightarrow B \Leftrightarrow \neg B \Rightarrow \neg A$ (a kontrapozíció tétele)
(7) $(A \Rightarrow B) \wedge A \Rightarrow B$
(8) $(A \Rightarrow B) \wedge \neg B \Rightarrow \neg A$
(9) $(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$
(10) $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$ (a disztributivitás egyik tétele)
(11) $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$ (a disztributivitás másik tétele)

(7)–(9)-ből a következtetés alábbi szabályai származtathatók:

- $((A \Rightarrow B) \wedge A) \Rightarrow B$ (*modus ponens*).
- $((A \Rightarrow B) \wedge \neg B) \Rightarrow \neg A$ (*modus tollens*).
- $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$ (*modus barbara* vagy *lánckövetkeztetés szabálya*).

Minden kijelentésformuláról véges számú lépésben eldönthető, hogy általános érvényű-e (hogyan?). Meg lehet tehát adni kijelentésformulák és következtetési szabályok egy rendszerét, amellyel a kijelentéskalkulus újabb tételeihez juthatunk. Ezt az eljárást ***levezetésnek*** nevezzük.

Lényegesen eltérő körülmények adódhatnak akkor, ha feladjuk a kétértékűség elvét, és kettőnél több igazságértéket is megengedünk. Példaként említhetőek a közép- és felsőfokú képzésben a matematika és az informatika oktatásához használt szimbolikus programozási nyelvek (pl. MAPLE, MATHEMATICA, DERIVE) kijelentéseinek igazságértékei, amelyek az IGAZ, HAMIS (TRUE, FALSE) értékeken kívül a NEM TUDOM (FAIL) értéket is felvehetik. Többértékű logika egyéb alkalmazott tudományokban is felbukkan, ilyen például a kvantummechanika.

Gyakorlatok

1.1-1. Fejezzük ki a „kizáró vagy”-ot a negáció, konjunkció és a diszjunkció segítségével.

1.1-2. Igazoljuk, hogy az alábbi kijelentésformulák kielégíthetőek:

a) $\neg(A \Rightarrow \neg A)$

b) $((A \Rightarrow B) \Rightarrow (B \Rightarrow A))$

c) $(A \Rightarrow (B \wedge C)) \wedge \neg((B \vee C) \Rightarrow A)$.

1.1-3. Bizonyítsuk be, hogy az alábbi kijelentésformulák a kijelentéskalkulus tételei:

a) $(A \Rightarrow B) \vee (B \Rightarrow A)$

b) $(A \wedge B) \Rightarrow A$

c) $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$.

1.2. A predikátumkalkulus

A matematikai problémák formalizálására a kijelentéskalkulus még nem elég. A kijelentések további vizsgálatánál olyan kifejezésekbe ütközünk, mint a „minden” és „lézetik”. Ezekre a kifejezésekre ***kvantorokat*** vezetünk be: a $\exists$ („van olyan”, „létezik”) egzisztenciális kvantort és a $\forall$ („minden”) univerzális kvantort.

1.6. példa. Tekintsük az alábbi kijelentést: „Minden veréb madár.” Ha V-vel jelöljük a „veréb” és M-el a „madár” predikátumot, akkor az iménti kijelentést a

$$\forall x\ (V(x) \Rightarrow M(x))$$

alakban írhatjuk.

Legyen Q valamilyen, az x változót tartalmazó kifejezés. A

$$\exists x\ Q(x) \quad \text{és a} \quad \forall x\ Q(x)$$

típusú kijelentések esetén az x változó minden előfordulására azt mondjuk, hogy a kvantor hatáskörében van. Ha egy kijelentésben egy változó minden előfordulása valamilyen kvantor hatáskörében van, akkor azt mondjuk, hogy a változó ***kötött***, egyébként ***szabad*** változó.

1.7. példa. Jelentse az $A(x,y)$ kétbemenetű predikátum azt, hogy „az x ember édesanyja y". Ekkor az a kijelentés, hogy „mindenkinek van édesanyja" az alábbi módon formalizálható:

$$\forall x\ \exists y\ A(x,y).$$

Ha hangsúlyozni akarjuk azt, hogy mindenkinek pontosan egy édesanyja van, akkor ezt az $\exists!$ („egyértelműen létezik" vagy „pontosan egy létezik") szokásos jelölés segítségével tehetjük meg:

$$\forall x\ \exists! y\ A(x,y).$$

A predikátumkalkulus tételeihez hasonló módon juthatunk el, mint a kijelentéskalkulusban. Az alábbiakban felsoroljuk a predikátumkalkulus fontosabb tételeit.

(1) $\neg\forall x\ A(x) \Leftrightarrow \exists x\ \neg A(x)$
(2) $\neg\forall x\ \neg A(x) \Leftrightarrow \exists x\ A(x)$
(3) $\neg\exists x\ A(x) \Leftrightarrow \forall x\ \neg A(x)$
(4) $\neg\exists x\ \neg A(x) \Leftrightarrow \forall x\ A(x)$
(5) $\forall x\ \forall y\ A(x,y) \Leftrightarrow \forall y\ \forall x\ A(x,y)$
(6) $\exists x\ \exists y\ A(x,y) \Leftrightarrow \exists y\ \exists x\ A(x,y)$
(7) $\exists x\ \forall y\ A(x,y) \Rightarrow \forall y\ \exists x\ A(x,y)$

Az első négy tételt szokás a tagadás, a következő hármat a felcserélhetőség tételeinek nevezni. Figyeljük meg, hogy a (7) tételben implikáció, és nem ekvivalencia fordul elő.

1.8. példa. Formalizáljuk azt a kijelentést, hogy „mindenki szeret valakit". Legyen $L(x,y)$ kétbemenetű predikátum jelentése „x szereti y-t". Ekkor az iménti kijelentés a $\forall x\ \exists y\ L(x,y)$ alakban írható, ami nem ugyanaz, mint a $\exists y\ \forall x\ L(x,y)$, hiszen ezen utóbbi jelentése „van valaki, akit mindenki szeret". Márpedig ha van valaki, akit mindenki szeret, akkor valóban mindenki szeret valakit, de fordítva nem feltétlenül.

Nincs mechanikus eljárás a kijelentések formalizálására, minden esetben alaposan és pontosan értelmezni kell a kijelentéseket, szükség esetén átfogalmazva őket a kvantorok segítségével. A kvantorok a köznyelvben és a matematikai nyelvben többféle szószerkezettel is kifejezhetők. A „minden", „az összes", „tetszőleges", „bármely" szavak az univerzásis kvantort jelzik, a „létezik", „van olyan", „található", „néhány", „valamely", „alkalmas", „bizonyos", stb. szavak az egzisztenciális kvantorra utalnak.

1.9. példa. Formalizáljuk az alábbi kijelentéseket: az ELTE-n
a) „az összes szak tetszőleges évfolyamán tanul lány hallgató";
b) „van olyan szak, ahol valamelyik évfolyam összes hallgatója lány".
Jelentse a $G(x)$ predikátum azt, hogy x lány, az $S(x,y)$ predikátum azt, hogy x az y szak hallgatója, $E(x,y)$ pedig azt, hogy x az y évfolyamra beiratkozott. Ekkor a a kijelentések az alábbi alakban írhatók:

a) $\forall x\ \forall y\ \exists z\ (G(z) \wedge S(z,x) \wedge E(z,y))$
b) $\exists x\ \exists y\ \forall z\ (G(z) \wedge S(z,x) \wedge E(z,y))$.

A predikátumkalkulus alkalmazhatósága céljából általában még néhány kiegészítést szokás tenni. Ezek közül mi az *azonosság* jelölésére szolgáló „=" *egyenlőségjelet* említjük (*predikátumkalkulus azonossággal*). Az egyenlőségjelet a logikai műveleti jelek közé célszerű sorolni.

Figyeljük meg, hogy a kvantifikálás mindig csak változókra vonatkozott, ami a matematika széles területének leírásához elegendő. Az ilyen tulajdonsággal bíró predikátumkalkulust ***elsőrendű predikátumkalkulusnak*** nevezzük. Esetenként azonban felléphet a predikátumok kvantifikálásának szükségessége, amivel magasabb rendű predikátumkalkukusokhoz juthatunk. Ezekkel mi nem foglalkozunk.

Gyakorlatok

1.2-1. Jelölje $L(x,y)$ azt a predikátumot, hogy „x szereti y-t". Formalizáljuk az alábbi kijelentéseket:
a) Mindenki szeret mindenkit.
b) Van valaki, akit szeret valakit.

1.2-2. Jelölje a $\Gamma(x,y)$ predikátum azt, hogy „x gyermeke y-nak", a $\Theta(x,y)$ predikátum azt, hogy „x házastársa y-nak", továbbá jelölje $\Phi(x)$ azt, hogy „x férfi". Formalizáljuk az alábbi kijelentéseket:
a) x fia y-nak,
b) x unokája y-nak,
c) x testvére y-nak,
d) x apósa y-nak,
e) x unokatestvére y-nak,
f) x veje y-nak.

1.2-3. Formalizáljuk az alábbi kijelentéseket:
a) Nem mind arany, ami fénylik.
b) Ki korán kel, aranyat lel.
c) Nem minden fajta szarka farka tarka, csak a tarka farkú szarka farka tarka.

1.3. Axiómák és a bizonyítások formái

Bizonyításon egy állításnak más állításokból meghatározott logikai következtetési szabályokkal való levezetését értjük. Ha bonyolultabb állításokat megkísérlünk egyszerűbbekre visszavezetni, gyorsan olyan tételekbe ütközhetünk, amelyeket korábbi tételekből sehogy sem lehet levezetni. Ezért először igaznak tekintett állításokat, ***axiómákat*** fektetünk le, amelyekhez a bizonyításoknál vissza lehet nyúlni. Így végső soron minden bizonyítást axiómákra lehet visszavezetni. Az, hogy mit lehet egy axiómarendszerből levezetni, attól függ, hogy melyik logikai rendszer mellett döntünk, és milyen következtetési szabályokat engedünk meg.

Lényeges kérdés egy meghatározott axiómákra felépített matematikai elmélet ***ellentmondásmentessége***, vagyis annak megmutatása, hogy olyan ellentmondá-

A	B	$A \Rightarrow B$	$\neg B$	$\neg A$	$\neg B \Rightarrow \neg A$	$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$
I	I	I	H	H	I	I
I	H	H	I	H	H	I
H	I	I	H	I	I	I
H	H	I	I	I	I	I

1.2. ábra. Az $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$ kijelentés igazságtáblázata.

sos kijelentéseket, mint például $A \wedge \neg A$, nem lehet levezetni. Hasonlóan fontos az axiómarendszer ***teljessége***, vagyis hogy valamennyi tételt le lehessen vezetni. Ez a kijelentés és predikátumkalkulus esetén elérhető (GÖDEL *teljességi tétele*). Lényeges még az axiómarendszer ***függetlensége***, vagyis egyik axiómát se lehessen a többiből levezetni.

A matematikai tételek, állítások jelentős része $A \Rightarrow B$ típusú implikáció. Itt A a tétel feltételeit jelöli, amelyeket *premisszáknak* nevezünk („az, amit tudunk"), B pedig a tétel állítását jelöli, amelyet *konklúziónak* is mondunk („amit tudni szeretnénk"). Az ilyen típusú tételek bizonyításának legismetebb formája a ***közvetlen*** vagy ***direkt bizonyítás***, amelynek az alapja a

$$((A \Rightarrow B) \wedge A) \Rightarrow B$$

modus ponens.

Ha egy M axiómarendszerből az A állítást kell levezetni, ez úgy is elvégezhető, hogy a $\neg A$ feltételezésével olyan B állításra következtetünk, amelynek a tagadását M-ből le lehet vezetni. Ekkor $\neg A \Rightarrow B$-ből és $\neg B$-ből a *modus tollens* miatt $\neg\neg A$ és így A következik (***közvetett*** vagy ***indirekt bizonyítás***). Ekkor tehát

$$((A \Rightarrow B) \wedge \neg B) \Rightarrow \neg A.$$

Indirekt bizonyításra talán a legismertebb példa a középiskolai matematikából jól ismert $\sqrt{2}$ irracionális voltának bizonyítása.

Ha egy állítás $A \Rightarrow B$ alakú, akkor gyakran a $\neg B \Rightarrow \neg A$ kontrapozíciót bizonyítjuk. Az 1.2. ábra azt mutatja, hogy ez miért tehető meg. Egy állítás hamis voltának bizonyításához mindig elegendő egyetlen ***ellenpélda.***

A modus ponens és a modus tollens következtetési szabályok indokolják a ***szükséges*** illetve ***elégséges feltételek*** elnevezéseket: ha $A \Rightarrow B$ érvényes, akkor A-t B elégséges feltételének, B-t pedig A szükséges feltételének nevezzük. Általánosan, azt, hogy az $A \Rightarrow B$ implikáció igaz, az alábbi kifejezési módok bármelyikével leírhatjuk:

„A-ból következik B";

„A csak akkor teljesül, ha B is teljesül";

„A elégséges feltétele annak, hogy B teljesüljön";

„B teljesülésének szükséges feltétele A";

A matematikai tételek jelentős része $A \Leftrightarrow B$ típusú ekvivalencia. Azt, hogy $A \Leftrightarrow B$ igaz, az alábbi kifejezési módokkal írhatjuk le:

„A ekvivalens B-vel";

„A akkor és csak akkor teljesül, ha B is";

„A teljesülésének szükséges és elégséges feltétele B";
„A pontosan akkor teljesül, ha B;"

Nagyon fontos és hasznos bizonyítási módszer a ***teljes indukció***, ami a természetes számoknak az 5. PEANO-axiómában (4.1. fejezet) megfogalmazott tulajdonságára épül. Ennek az eljárásnak az általánosítása a ***transzfinit indukció*** (5.17. tétel).

Definíción egy fogalom pontos leírását értjük, esetleg más fogalmak felhasználásával. Itt hasonló problémák adódnak, mint a bizonyításnál. Sok fogalmat nem explicit módon ($A \overset{\text{def}}{\Leftrightarrow} B$), hanem implicit módon, kölcsönös összefüggések alapján definiálunk (például a síkgeometriában az egyenest, a távolságot, a területet stb.). A későbbiekben hasznos lesz annak ismerete, hogy egy reláció vagy függvény minden, az elsőrendű predikátumkalkulus eszközeivel leírt implicit definícióját explicit alakban is meg lehet adni (BETH tétele).

Megjegyzések a fejezethez

A logika a helyes következtetés tudománya. Ha egy logikai rendszerben csak egyetlen ellentmondás is van, akkor azon a rendszeren belül bármilyen állítás bebizonyítható. Sőt, GÖDEL megmutatta, hogy ha egy „megfelelően erős" formális rendszer ellentmondásmentes, akkor megfogalmazható benne olyan állítás, amely a rendszer keretein belül sem nem bizonyítható, sem nem cáfolható. GÖDEL eredményeire a kötet végén még visszatérünk.

Az első fennmaradt axiómarendszert EUKLIDÉSZ Elemek [7] című munkája tartalmazza. EUKLIDÉSZ arra törekedett, hogy minél kevesebb axiómát mondjon ki, és tételként bizonyított mindent, amit csak lehet. A későbbiekben látni fogjuk, hogy az axiómák kiválasztása meglehetősen önkényes, egy adott témakörhöz több különböző axiómarendszer is megalkotható. Egy axiómarendszer „erősségét" lényegében az adja, hogy „mennyi mindent" lehet bizonyítani belőle.

Javasolt irodalom: MENDELSON [28], PÁSZTORNÉ [30], PENROSE [31], QUINE [32], és SZENDREI [39].

2. Halmazok, relációk, függvények

A *halmaz* fogalma a modern matematikában alapvető szerepet játszik. A halmazelmélet alapjait CANTOR rakta le, de az általa lefektetett ún. ***naív halmazelméletben*** ellentmondásokat lehet konstruálni. Egyszerűsége miatt a gyakorlatban mégis ezt használjuk, és lehetőség szerint kerüljük az olyan halmazok konstrukcióját, amelyekkel az elmélet ellentmondásosnak bizonyulna. A halmazelmélet ellentmondásmentességének kívánt szigorúságát az ***axiomatikus halmazelméletben*** érjük el, amelyet a fejezet végén ismertetünk.

2.1. Naív halmazelmélet

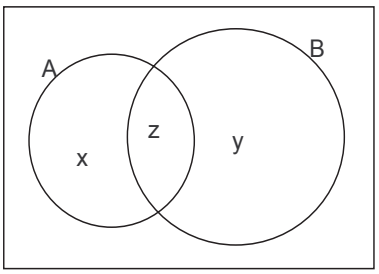
2.1.1. Bevezető fogalmak

A ***halmaz*** és a halmaz ***eleme*** fogalmakat a matematikában nem definiáljuk, ezek ún. alapfogalmak. Körülírva őket, a halmaz egymástól jól megkülönböztethető objektumok (dolgok, tárgyak) együttese, összessége. Az objektumokat a halmaz elemeinek nevezzük.

Az „ objektumok együttese, összessége" kifejezés arra utal, hogy valamilyen objektum vagy benne van az adott halmazban, vagy nincsen benne, de a kettő egyidejűleg nem teljesül. A „jól megkülönböztethetőség" pedig azt jelenti, hogy minden objektum legfeljebb egy példányban van benne az adott halmazban.

Valamely halmaz elemeire az $a, b, c, \ldots$ betűket, a halmazokra az $A, B, C, \ldots$ jelölést alkalmazva jelentse $a \in A$ azt, hogy a eleme A-nak, $b \notin B$ pedig azt, hogy b nem eleme B-nek. A halmazok lehetnek végesek vagy végtelenek (5. fejezet). Véges halmazokat meg lehet adni elemeik felsorolásával, szokás szerint kapcsos zárójelek között, míg tetszőleges halmazokat az elemeiket definiáló feltételek megadásával. Ilyenkor röviden $\{x \in H \mid T(x)\}$-et írunk azon H-beli x objektumok halmazára, amelyekre a $T(x)$ tulajdonság teljesül. Amennyiben a $\mid$ elválasztójel zavaró, akkor az $\{x \in H \,:\, T(x)\}$ is használatos. Ha a H halmaz nyilvánvaló, kiírása elhagyható.

2.1. példa. Példák halmazokra:
$H_1 = \{2, 3, 5, 7\}$,
$\mathbb{N} = \{0, 1, 2, \ldots\}$,



2.1. ábra. Az A és B halmazok Venn-diagramos szemléltetése.

$H_2 = \{x \in \mathbb{N} \mid x^4 - 17x^3 + 101x^2 - 247x + 210 = 0\}$,
H_3 legyen a négy legkisebb pozitív prímből álló halmaz,
$H_4 = \{x \in \mathbb{N} \mid x \text{ prím}\}$.

Ekkor H_1, H_2, H_3 véges halmazok, valamint az 5. fejezetben látni fogjuk, hogy H_4 végtelen halmaz. Az $\mathbb{N}$-nel jelölt halmazt a ***természetes számok halmazának*** nevezzük. Ez a halmaz olyan lényeges szerepet játszik a matematikában, hogy axiomatikus felépítésére a 4. fejezetben visszatérünk. Addig $\mathbb{N}$-et mint a számlálás eszközét használjuk.

2.1. definíció. *Halmazokat akkor nevezünk egyenlőeknek, ha ugyanazokból az elemekből állnak, vagyis*

$$A = B \overset{\text{def}}{\Leftrightarrow} \forall x\ (x \in A \Leftrightarrow x \in B).$$

Az elemek sorrendjének nincs tehát jelentősége. Az iménti példában $H_1 = H_2 = H_3$. Ha az A és B halmazok nem egyenlőek, akkor ezt úgy jelöljük, hogy $A \neq B$.

2.2. definíció. *Azt a halmazt, amelynek nincs eleme,* ***üres halmaznak*** *nevezzük és $\varnothing$-zal jelöljük.*

Az egyenlőség definíciója szerint csak egyetlen üres halmaz létezik.

Halmazok szemléltetéseként egy halmaz elemeit a sík pontjaiként is felfoghatjuk, amelyeket körrel vagy más zárt görbével körülfogunk (Euler vagy Venn-*diagram*, 2.1. ábra). A Venn-diagrammal való ábrázolás csak vizuális szemléletet ad, állítások bizonyítására nem alkalmas.

2.1.2. Részhalmazok és hatványhalmazok

Előfordulhat, hogy az A halmaz minden eleme egy B halmaznak is eleme. Ekkor A-t a B ***részhalmazának*** nevezzük, jelölése $A \subseteq B$.

2.3. definíció. $A \subseteq B \overset{\text{def}}{\Leftrightarrow} \forall x\ (x \in A \Rightarrow x \in B)$.

Ekkor a ***valódi részhalmaz*** definíciója az alábbi lesz.

2.4. definíció. $A \subset B \overset{\text{def}}{\Leftrightarrow} A \subseteq B \wedge A \neq B$.

Ebben az esetben a B halmaznak léteznek olyan elemei, amelyek nem tartoznak A-hoz. Minden A halmazra érvényes, hogy $\varnothing \subseteq A$. Ha $A \neq \varnothing$, akkor $\varnothing \subset A$ szintén teljesül.

2.2. példa. Felhívjuk a figyelmet az $\in$ és $\subset$ kölönbözőségére. A $2 \in \{2,3,5,7\}$ érvényes, ugyanakkor $2 \subset \{2,3,5,7\}$ nem, ezzel szemben $\{2\} \subset \{2,3,5,7\}$ szintén igaz.

A halmazokat mint elemeket összefogva újabb halmazokat alkothatunk, ezeket ***halmazrendszereknek*** nevezzük. Különleges halmazrendszer egy A halmaz valamennyi részhalmazának halmaza, amelyet az adott halmaz ***hatványhalmazának*** nevezünk, és $\wp(A)$-val jelölünk.

2.5. definíció. $\wp(A) \overset{\text{def}}{\Leftrightarrow} \{x \mid x \subseteq A\}$.

A későbbiekben megmutatjuk, hogy egy n-elemű halmaz hatványhalmaza 2^n elemből áll.

2.1.3. Halmazműveletek

A halmazelmélet alkalmazhatósága szempontjából kiemelt jelentősége van a halmazok közötti műveleteknek. Ezek, amint látni fogjuk, szoros kapcsolatban állnak a kijelentéskalkulus műveleteivel.

2.6. definíció. $A \setminus B \overset{\text{def}}{\Leftrightarrow} \{x \mid x \in A \wedge x \notin B\}$.

$A \setminus B$-t úgy olvassuk, hogy „A mínusz B”, mivel ez a halmaz A-nak pontosan azon elemeiből áll, amelyek B-hez nem tartoznak (***különbséghalmaz***).

Ha $A \subseteq H$, akkor $H \setminus A$-t A-nak H-ra vonatkozó ***kiegészítőjének*** vagy ***komplementerének*** nevezzük, és $\overline{A}_H$-val jelöljük. Ha az összefüggésekből világos, hogy mely H ***alaphalmazról*** van szó, akkor az $\overline{A}$ jelölés használatos. Felhívjuk a figyelmet, hogy a komplementerképzésnél mindig tisztában kell lennünk, hogy mely H halmazról is van szó. A komplementerképzésnek a negációval való összefüggése nyilvánvaló:

$$x \in H \Rightarrow (x \in \overline{A} \Leftrightarrow x \notin A \Leftrightarrow \neg(x \in A)).$$

A halmazok közötti legfontosabb művelet a metszet és az unió.

2.7. definíció. $A \cap B \overset{\text{def}}{\Leftrightarrow} \{x \mid x \in A \wedge x \in B\}$.

$A \cap B$ (olvasd: A és B ***metszete*** vagy ***közös része***) mindazokból az elemekből áll, amelyek egyidejűleg A-hoz és B-hez is hozzátartoznak. Ha $A \cap B = \varnothing$, akkor A-t és B-t ***diszjunktnak*** (vagy idegennek) nevezzük.

2.8. definíció. $A \cup B \overset{\text{def}}{\Leftrightarrow} \{x \mid x \in A \vee x \in B\}$.

$A \cup B$ (olvasd: A és B ***uniója*** vagy ***egyesítése***) mindazokból az elemekből áll, amelyek A-hoz vagy B-hez tartoznak (a „vagy” nem kizáró értelemben).

Az unió és a metszet legfontosabb tulajdonságai:

(1) $A \cap B = B \cap A$ (2) $A \cup B = B \cup A$
(3) $(A \cap B) \cap C = A \cap (B \cap C)$ (4) $(A \cup B) \cup C = A \cup (B \cup C)$
(5) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ (6) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
(7) $A \cap (A \cup B) = A$ (8) $A \cup (A \cap B) = A$
(9) $A \cap A = A$ (10) $A \cup A = A$.

Az (1)–(2) tulajdonságot *kommutativitásnak*, a (3)–(4)-et *asszociativitásnak*, az (5)–(6) tulajdonságot *disztributivitásnak*, (7)–(8)-at *elnyelési tulajdonságnak*, a (9)–(10) tulajdonságot *idempotenciának* nevezzük.

Az üres halmazra és a H alaphalmazra a következő tulajdonságok érvényesek:

$A \cap \varnothing = \varnothing$ $A \cup \varnothing = A$
$A \cap H = A$ $A \cup H = H$
$A \cap \overline{A} = \varnothing$ $A \cup \overline{A} = H$.

Érvényesek továbbá a De Morgan-törvények:

$\overline{A \cap B} = \overline{A} \cup \overline{B}$ és $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

2.3. példa. Legyen $H = \{a, b, c, d, e, f, g, h\}$, $A = \{a, c, e, g\} \subset H$, $B = \{e, f, g, h\} \subset H$. Ekkor $A \cup B = \{a, c, e, f, g, h\}$, $A \cap B = \{e, g\}$, $A \setminus B = \{a, c\}$, $\overline{A} = \{b, d, f, h\}$.

A metszetet és az uniót nem csak két halmazra lehet definiálni. A műveletek asszociativitása miatt a kettőnél több halmazból álló metszetet és uniót zárójelek nélkül írhatjuk, a kommutativitás miatt pedig a tagok sorrendje is lényegtelen. (Ennek bizonyítására a 4.13. tételben visszatérünk.)

Legyen X tetszőleges halmaz, $\mathcal{H} \subseteq \wp(X)$.

2.9. definíció. $\cap\mathcal{H} \overset{\text{def}}{\Leftrightarrow} \{x \mid \forall A \in \mathcal{H} \text{ esetén } x \in A\}$

2.10. definíció. $\cup\mathcal{H} \overset{\text{def}}{\Leftrightarrow} \{x \mid \exists A \in \mathcal{H} \text{ olyan, hogy } x \in A\}$

Így tehát a $\cap\mathcal{H}$ elemei a halmazrendszer minden halmazához hozzátartoznak, $\cup\mathcal{H}$ pedig mindazon elemekből áll, amelyek a halmazrendszer valamely halmazának elemei.

2.11. definíció. *Legyen X tetszőleges halmaz, és tekintsük a $\mathcal{H} \subset \wp(X)$, $\cup\mathcal{H} = X$ halmazrendszert. Ha minden $A \in \mathcal{H}$ esetén $A \neq \varnothing$, és minden $A, B \in \mathcal{H}$ $(A \neq B)$ esetén $A \cap B = \varnothing$, akkor a $\mathcal{H}$ halmazrendszert* ***X osztályokra való felbontásának*** *vagy* ***osztályfelbontásának*** *nevezzük.*

A halmazalgebra műveletei a matematika csaknem minden területén előbukkannak. Például az algebrában egy egyenletrendszer megoldáshalmaza az egyes egyenletek megoldáshalmazainak metszete.

Gyakorlatok

2.1-1. Legyenek az A, B, C halmazok a H alaphalmaz részhalmazai. Bizonyítsuk be, hogy ekkor $A \cap B \subseteq C \Leftrightarrow A \subseteq \overline{B} \cup C$.

2.1-2. Igaz-e az alábbi állítás minden A, B, C halmaz esetén:
$A \in B \wedge B \in C \Rightarrow A \in C$?

2.1-3. Bizonyítsuk be, hogy minden A, B, C halmaz esetén
a) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
b) $A \setminus (B \cup C) = (A \setminus B) \setminus C$.
2.1-4. Bizonyítsuk be a DE MORGAN-törvényeket.
2.1-5. Bizonyítsuk be, hogy tetszőleges A, B halmazokra
a) $A \cap B \subseteq A$, $B \subseteq A \cup B$,
b) $A \subseteq B \Leftrightarrow A \cup B = B \Leftrightarrow A \cap B = A \Leftrightarrow A \cap \overline{B} = \varnothing$.
2.1-6. Definiáljunk az A, B halmazokon egy új műveletet: $A \triangle B = (A \setminus B) \cup (B \setminus A)$.
a) Bizonyítsuk be, hogy $A \triangle (A \triangle B) = B$.
b) Fejezzük ki a $\triangle$ és a $\cap$ műveletek segítségével $A \cup B$-t és $A \setminus B$-t.
A $\triangle$ műveletet ***szimmetrikus különbségnek*** vagy ***szimmetrikus differenciának*** nevezzük.
2.1-7. Magyarázzuk meg az alábbi történet osztályfelbontással való kapcsolatát.

A programozók fizetésemelést szeretnének, mire a munkaadó így válaszol: – Nem szégyellik magukat? Tudják Önök tulajdonképpen hány napot dolgoznak egy évben? Nem? Akkor elmondom. Az év 365 napból áll. Naponta 8 órát alszanak, ami 122 napot tesz ki. Marad 243 nap. Naponta 7 órát szabadok, ami összesen 106 nap. Marad 137 nap. Egy évben 52 vasárnap van, amikor szabadok. Marad 85 nap. Szombaton is szabadok, ez plusz 52 nap. Ezen kívül van 3 hét szabadság. Marad 12 nap. Egy évben van még 11 szabadnap valami ünnep miatt. Mi marad még? Egyetlen nap! Igen, a május elseje. És maguk akkor is szabadnaposak!

2.2. Relációk

A reláció fogalma különösen fontos a matematikában. Ennek alapját a halmazok DESCARTES-féle direkt szorzata képezi. A relációk összefüggést állítanak fel egy halmaz vagy különféle halmazok elemei között. A reláció speciális eseteként eljutunk a függvény fogalmához, sőt, a relációk különféle struktúrákat is létrehozhatnak halmazokon. A relációk fontos szerepet játszanak az adatbázis-kezelő rendszerekben is.

2.2.1. DESCARTES-féle direkt szorzat és reláció

Ha egy halmaz a_1, a_2 elemének sorrendje is lényeges, és a sorrendiségben a_1 előbb szerepel, mint a_2, akkor az (a_1, a_2) ***rendezett pár*** fogalmát használjuk.

2.12. definíció. $(a_1, a_2) \overset{\text{def}}{\Leftrightarrow} \{\{a_1\}, \{a_1, a_2\}\}$.

Az (a_1, a_2) rendezett párban a_1 az első, a_2 a második komponens. Az (a_1, a_2) és (b_1, b_2) rendezett párok pontosan akkor egyenlőek, ha $a_1 = b_1$ és $a_2 = b_2$. Nyilván $(a_1, a_2) \neq \{a_1, a_2\}$. Kettőnél nagyobb n esetén a rendezett n-eseket a rendezett párok általánosításaként definiáljuk.

2.13. definíció. *Legyenek* $A_1, A_2, \ldots, A_n$ *halmazok. Az*

$$A_1 \times A_2 \times \ldots \times A_n \overset{\text{def}}{\Leftrightarrow} \{(a_1, \ldots, a_n) \mid a_i \in A_i\}$$

halmazt az $A_1, A_2, \ldots, A_n$ *halmazok* DESCARTES*-féle* ***direkt szorzatának*** *nevezzük.* $A = A_1 = A_2 = \ldots = A_n$ *esetén az* A^n *jelölés használatos. Megállapodás szerint* $A^0 = \{\varnothing\}$.

Két rendezett n-es egyenlősége ugyancsak a komponensenkénti egyenlőségből adódik.

2.14. definíció. *A* $\rho \subseteq A_1 \times A_2 \times \ldots \times A_n$ *részhalmazt* ***n-változós relációnak*** *nevezzük. Az* $n = 2$ *esetben* ***binér relációról****, a* $\rho \subseteq A^n$ *esetben* ***homogén relációról*** *beszélünk.*

2.4. példa. Legyen az A halmaz a magyar keresztnevek halmaza. Ekkor a $\rho = \{(\text{Antal}), (\text{Imre}), (\text{József})\}$ egy *unáris* reláció A-n.

2.5. példa. Az n-változós relációk szoros kapcsolatban állnak az n-változós predikátumokkal. Minden $P(x_1, \ldots, x_n)$ predikátum meghatároz egy ρ relációt az alábbi módon:

$$\rho = \{(a_1, \ldots, a_n) \in A_1 \times \cdots \times A_n \mid P(a_1, \ldots, a_n) \text{ logikai értéke IGAZ}\},$$

és hasonlóan, minden ρ reláció (logikai értékét tekintve) egy egyértelműen meghatározott $P(x_1, \ldots, x_n)$ predikátumhoz tartozik, amely így adható meg:

$$P(a_1, \ldots, a_n) \text{ logikai értéke } \begin{cases} \text{IGAZ}, & \text{ha } (a_1, \ldots, a_n) \in \rho \\ \text{HAMIS}, & \text{ha } (a_1, \ldots, a_n) \notin \rho. \end{cases}$$

A predikátumok tehát a relációk leírásai a logika nyelvén.

2.2.2. Binér relációk

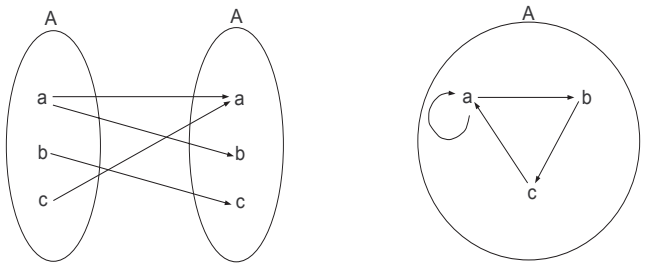
A $\rho \subseteq A \times B$ binér relációt úgy is értelmezhetjük, hogy B elemeit meghatározott módon „hozzárendeljük" A elemeihez. Az $(a, b) \in \rho$ helyett gyakran szokás $a\rho b$-t írni. Véges halmazok esetén ez a hozzárendelés „nyíldiagrammal" (a reláció irányított gráfjával) szemléltethető (2.2. ábra).

2.6. példa. Binér relációra példa a „$\subseteq$" tartalmazás a halmazrendszerekben, vagy a „$\perp$" merőlegesség az egyenesek egy halmazában.

2.7. példa. Legyen egy adott számítógépes program összes lehetséges bemenetének halmaza A, összes lehetséges kimenetének halmaza pedig B. Ekkor megadható egy $\rho \subseteq A \times B$ reláció oly módon, hogy $a\rho b$ pontosan akkor, ha a program az a bemenetre a b eredményt adja.

2.15. definíció. *A* $\rho \subseteq A \times B$ *reláció* ***értelmezési tartománya***

$$D_\rho \overset{\text{def}}{\Leftrightarrow} \{a \in A \mid \exists b \in B \ : \ (a, b) \in \rho\},$$



2.2. ábra. Legyen $A = \{a, b, c\}$, $\rho = \{(a, a), (a, b), (b, c), (c, a)\} \subset A \times A$. Az a) ábra mutatja a ρ reláció gráfját. Homogén binér relációk esetében a nyíldiagramos ábrázolás tovább egyszerűsíthető, ezt szemlélteti a b) ábra.

***értékkészlete** pedig*

$$R_\rho \overset{\text{def}}{\Leftrightarrow} \{b \in B \mid \exists a \in A \ : \ (a, b) \in \rho\}.$$

2.8. példa. Az $A = \{a, b\}$, $B = \{c, d, e\}$, $\rho = \{(a, d), (a, e)\} \subset A \times B$ reláció esetén $D_\rho = \{a\}, R_\rho = \{d, e\}$.

2.16. definíció. *A ρ binér relációt a σ binér reláció **kiterjesztésének**, illetve σ-t a ρ **leszűkítésének** (vagy megszorításának) nevezzük, ha $\sigma \subseteq \rho$. Ha H egy halmaz, a ρ reláció H-**ra való leszűkítésén** a*

$$\rho|_H \overset{\text{def}}{\Leftrightarrow} \{(a, b) \in \rho, \ a \in H\}$$

relációt értjük.

Tekintsük a $\rho \subseteq A \times A$ alakú (homogén binér) relációkat. Ekkor

(1) ρ *reflexív* $\overset{\text{def}}{\Leftrightarrow} \forall a \in A \ (a \rho a)$

(2) ρ *irreflexív* $\overset{\text{def}}{\Leftrightarrow} \forall a \in A \ \neg(a \rho a)$

(3) ρ *szimmetrikus* $\overset{\text{def}}{\Leftrightarrow} \forall a, b \in A \ (a \rho b \Rightarrow b \rho a)$

(4) ρ *antiszimmetrikus* $\overset{\text{def}}{\Leftrightarrow} \forall a, b \in A \ (a \rho b \wedge b \rho a \Rightarrow a = b)$

(5) ρ *szigorúan antiszimm.* $\overset{\text{def}}{\Leftrightarrow} \forall a, b \in A \ (a \rho b \Rightarrow \neg(b \rho a))$

(6) ρ *tranzitív* $\overset{\text{def}}{\Leftrightarrow} \forall a, b, c \in A \ (a \rho b \wedge b \rho c \Rightarrow a \rho c)$

(7) ρ *intranzitív* $\overset{\text{def}}{\Leftrightarrow} \forall a, b, c \in A \ (a \rho b \wedge b \rho c \Rightarrow \neg(a \rho c))$

(8) ρ *trichotom* $\overset{\text{def}}{\Leftrightarrow} \forall a, b \in A \left(\begin{array}{l} a \rho b \vee b \rho a \vee a = b \\ \text{és pontosan az egyik} \end{array} \right)$

(9) ρ *gyengén trichotom* $\overset{\text{def}}{\Leftrightarrow} \forall a, b \in A \ (a \rho b \vee b \rho a, \text{ esetleg mindkettő})$

A gyengén trichotom relációt gyakran dichotomnak, lineárisnak vagy konnexnek mondjuk. Ezek a tulajdonságok a rendezési struktúrákhoz és a hányadoshalmazok

konstrukciójához lesznek lényegesek.

Az Olvasóra bízzuk annak belátását, hogy a 2.2. ábrán látható homogén binér reláció esetében a fenti tulajdonságok közül csak az antiszimmetria teljesül.

2.2.3. Ekvivalenciareláció, hányadoshalmaz

Kiemelkedően fontos szerepet játszanak az alábbi tulajdonságokkal rendelkező relációk:

2.17. definíció. *Valamely* $\rho \subseteq A \times A$ *relációt* ***ekvivalenciarelációnak*** *nevezünk, ha reflexív, szimmetrikus és tranzitív.*

2.9. példa. Ekvivalenciareláció például az egyenesek párhuzamossága, szakaszok egybevágósága.

2.18. definíció. *Adott* $\rho \subseteq A \times A$ *ekvivalenciareláció esetén az* A *halmaz mindazon elemeinek halmazát, amelyek egy* $a \in A$ *elemmel* ρ *relációban állnak, az* a *által meghatározott* $[a]$ ***ekvivalenciaosztálynak*** *nevezzük:*

$$[a] \overset{\text{def}}{\Leftrightarrow} \{\, b \in A |\ a \rho b\}.$$

Lényeges kapcsolat van az A halmaz ekvivalenciarelációi és A osztályfelbontásai között.

2.19. tétel (ekvivalenciareláció és osztályfelbontás kapcsolata). *Valamely* A *halmazon értelmezett* ρ *ekvivalenciareláció az* A*-nak egy osztályfelbontását határozza meg. Megfordítva, az* A *halmaz minden osztályfelbontása egy ekvivalenciarelációt definiál* ρ *elemei között.*

Bizonyítás. Legyen adott az A halmazon egy ρ ekvivalenciareláció. Megmutatjuk, hogy a $\mathcal{H} = \{[a] \mid a \in A\}$ egy osztályozása A-nak. Nyilván $\cup\mathcal{H} = A$, valamint ρ reflexivitása miatt $a \in [a]$, így az osztályok nem üresek. Azt kell csak belátnunk, hogy a különböző osztályok metszete üres. Legyen $c \in [a] \cap [b]$. Ekkor $c \rho a$ és $c \rho b$, amiből a szimmetria és a tranzitivitás miatt $a \rho b$. Ha most $d \in [a]$, akkor a szimmetria és a tranzitivitás miatt $d \in [b]$. Ugyanígy, ha $d \in [b]$, akkor $d \in [a]$. Végeredményben tehát $[a] = [b]$, azaz ha két ekvivalenciaosztálynak van közös eleme, akkor azonosak. Eszerint A minden eleme pontosan egy ekvivalenciaosztályban fordul elő, és az osztályok páronként diszjunktak.

Megfordítva, ha $\mathcal{H}$ az A halmaz egy osztályfelbontása, akkor a

$$\rho = \{(a, b) \in A \times A \mid a \text{ és } b \text{ a } \mathcal{H} \text{ ugyanazon halmazának eleme}\}$$

reláció reflexív, szimmetrikus és tranzitív, vagyis ekvivalenciareláció. □

Egy ekvivalenciareláció tehát egy osztályfelbontást hoz létre, az A ekvivalenciaosztályainak halmazát.

2.20. definíció. *Az*

$$A/\rho \overset{\text{def}}{\Leftrightarrow} \{[a] \mid a \in A\}$$

elnevezése A*-nak* ρ *szerinti* ***hányadoshalmaza*** *(vagy faktorhalmaza). Egy* $b \in [a]$ *elem az* $[a]$ *osztály* ***reprezentánsa****. A* T *halmazt az* A/ρ ***teljes reprezentánsrendszerének*** *nevezzük, ha* T *pontosan egy elemet tartalmaz* A/ρ *minden osztályából.*

A hányadoshalmaz egy absztrakciós folyamat eredménye: az ekvivalenciaosztályt létrehozó tulajdonságot az osztályfelbontással lehet azonosítani. Ha az A halmaz ρ ekvivalenciareláció szerinti hányadoshalmazából mint osztályfelbontásból indulunk ki, és képezzük a hozzá tartozó ekvivalenciarelációt, akkor az eredeti relációt kapjuk vissza. Hasonlóan, ha egy osztályozásból képezzük a hozzá tartozó ekvivalenciarelációt, majd ebből a hányadoshalmazt, az eredeti osztályozást kapjuk.

2.10. példa. Egyenesek párhuzamossága az „irány”, szakaszok egybevágósága a „hosszúság” fogalmához vezet.

2.2.4. Relációk kompozíciója, inverze

2.21. definíció. *Ha* $\rho \subseteq A \times B$ *és* $\sigma \subseteq B \times C$*, akkor a*

$$\sigma \circ \rho \overset{\text{def}}{\Leftrightarrow} \{(x, z) \in A \times C \mid \exists y \in B \ (x \rho y \wedge y \sigma z)\}$$

relációt a ρ *és* σ ***relációk kompozíciójának*** *vagy* ***szorzatának*** *nevezzük.*

Figyeljük meg, hogy relációk kompozíciója lehet üres reláció is.

2.22. tétel (relációszorzat asszociativása). *Legyen* $\rho \subseteq A \times B, \sigma \subseteq B \times C, \tau \subseteq C \times D$. *Ekkor a relációszorzat asszociatív, vagyis* $(\tau \circ \sigma) \circ \rho = \tau \circ (\sigma \circ \rho)$.

Bizonyítás. Először a $(\tau \circ \sigma) \circ \rho \subseteq \tau \circ (\sigma \circ \rho)$ tartalmazást látjuk be. Ha $(a, d) \in (\tau \circ \sigma) \circ \rho$, akkor létezik olyan $b \in B$, amelyre $(a, b) \in \rho$ és $(b, d) \in \tau \circ \sigma$. A második összefüggésből következik, hogy létezik olyan $c \in C$, amelyre $(b, c) \in \sigma$ és $(c, d) \in \tau$. Ekkor viszont erre a c-re $(a, c) \in \sigma \circ \rho$ és $(c, d) \in \tau$. Így pedig $(a, d) \in \tau \circ (\sigma \circ \rho)$ is teljesül. Hasonlóképpen bizonyítható a $\tau \circ (\sigma \circ \rho) \subseteq (\tau \circ \sigma) \circ \rho$ összefüggés is, amiből a két reláció egyenlősége következik. □

2.23. definíció. *A* $\rho \subseteq A \times B$ *reláció* ***inverzének*** *a*

$$\rho^{-1} \overset{\text{def}}{\Leftrightarrow} \{(b, a) \in B \times A \mid (a, b) \in \rho\}$$

relációt nevezzük.

Megfigyelhetjük, hogy $D_{\rho^{-1}} = R_\rho$ és $R_{\rho^{-1}} = D_\rho$.

Gyakorlatok

2.2-1. Adjunk példákat a homogén binér relációk (1)–(9) tulajdonságai közül mindegyikre.

2.2-2. Hogyan lehet eldönteni egy homogén binér reláció gráfja alapján, hogy a reláció reflexív?
2.2-3. Legyen adott egy $\rho \subseteq A \times B$ reláció, és legyen $A_1, A_2 \subseteq A$. Bizonyítsuk be az alábbiakat:
a) Ha $A_1 \subseteq A_2$, akkor $R_{\rho|_{A_1}} \subseteq R_{\rho|_{A_2}}$.
b) $R_{\rho|_{A_1 \cup A_2}} = R_{\rho|_{A_1}} \cup R_{\rho|_{A_2}}$.
c) $R_{\rho|_{A_1 \cap A_2}} \subseteq R_{\rho|_{A_1}} \cap R_{\rho|_{A_2}}$.
2.2-4. Legyen $E = \{\text{sík egyenesei}\}$. Az alábbi $E \times E$-n értelmezett relációkról állapítsuk meg, hogy ekvivalenciarelációk-e:
a) $\rho = \{(a, b) \mid a \text{ egy pontban metszi } b\text{-t}\}$
b) $\sigma = \{(a, b) \mid a\text{-nak és b-nek van közös pontja}\}$.
2.2-5. Elemei felsorolásával határozzuk meg azt az ekvivalenciarelációt, amelyhez a megfelelő alaphalmazon az alábbi osztályfelbontás tartozik: $\{a, d, g\}$, $\{b\}$, $\{e\}$, $\{c, f\}$.

2.2-6. Az $\{1, 2, 3\}$ halmazon keressünk két olyan homogén binér relációt, amelyek szimmetrikusak, de a szorzatuk nem szimmetrikus.
2.2-7. Legyen $\rho \subseteq A \times A$. Vizsgáljuk meg $\rho \circ \rho^{-1}$ reflexivitását, szimmetriáját és tranzitivitását.
2.2-8.* Legyen $\rho \subseteq A \times A$. Bizonyítsuk be, hogy a

$$\hat{\rho} = \rho \cup \rho^2 \cup \ldots = \bigcup_{n=1}^{\infty} \rho^n$$

reláció tranzitív. $\hat{\rho}$-t a ρ reláció ***tranzitív lezártjának*** nevezzük.
($\rho^n = \underbrace{\rho \circ \rho \circ \ldots \circ \rho}_{n\text{-szer}}$, ami a relációszorzat asszociativitása miatt egyértelmű.)

2.3. Függvények

Az alábbiakban speciális relációkkal foglalkozunk.

2.3.1. A függvény definíciója

2.24. definíció. *Legyen* $A \neq \varnothing$, $B \neq \varnothing$, *továbbá* $\varnothing \neq f \subseteq A \times B$. *Az* f *relációt* A*-ból* B*-be képező* ***parciális függvénynek*** *vagy* ***leképezésnek*** *nevezzük, ha bármely* $x \in D_f$ *esetén az* $\{y \in B \mid (x, y) \in f\}$ *halmaz egyetlen elemből áll. Ezt az egyetlen elemet az* x*-hez rendelt* ***függvényértéknek*** *nevezzük, jele* $f(x)$.

Az $f(x)$-et úgy olvassuk: „ef iksz”, vagy f értéke az x helyen. Azt a tényt, hogy az x-hez rendelt függvényérték y, úgy jelöljük, hogy $x \mapsto y$, $f : x \mapsto y$, $f : x \overset{f}{\mapsto} y$, $x \mapsto f(x)$ vagy $y = f(x)$. Mivel a függvények speciális relációk, ezért a relációknál megismert definíciók (értelmezési tartomány, értékkészlet, kompozíció, inverz) a függvényekre is vonatkoznak. A függvény definíciója szerint az értelmezési tartomány bármely eleméhez létezik a hozzá rendelt függvényérték, ezért magát a függvényt *hozzárendelésnek* vagy *leképezésnek* is szokás nevezni. Bizonyos speciális esetekben találkozhatunk a *transzformáció, operáció, operátor, funkcionál* elnevezésekkel is.

Az $\{(x, f(x)) | \ x \in D_f\} \subseteq A \times B$ neve a ***függvény gráfja***. Számhalmazoknál a gráfot koordináta-rendszerben lehet ábrázolni.

A továbbiakban az A-ból B-be képező függvények $\{f \subseteq A \times B \mid f \text{ függvény}\}$ halmazát $A \to B$ (olv: A nyíl B) fogja jelölni. Ha f egy A-ból B-be képező függvény, akkor ezt úgy jelöljük, hogy $f \in A \to B$. Tetszőleges $f, g \in A \to B$ függvények esetén

$$f = g \Leftrightarrow D_f = D_g, \text{ és } \forall x \in D_f \text{ esetén } f(x) = g(x).$$

2.11. példa. Véges halmazokon értelmezett parciális függvényeket úgy is megadhatunk, hogy felsoroljuk az értelmezési tartomány elemeit és mindegyikük alá odaírjuk a képüket. Legyen például $A = \{a, b, c, d, e\}$ és $B = \{x, y, z\}$. Ekkor

$$f = \begin{pmatrix} a & b & c & d & e \\ x & y & x & & z \end{pmatrix}$$

az $f \in A \to B$ függvény egy megadási módja.

2.12. példa. A számítógépes programokban kulcsszerepet játszanak az ún. ***logikai függvények***, amikor $f \in A \to B$ esetén $B = \{\text{IGAZ}, \text{HAMIS}\}$. Az első fejezetben látott predikátumok példák logikai függvényekre.

2.25. definíció. *Legyen* $f \in A \to B$*, továbbá* $H \subseteq A$*. Az*

$$f[H] \overset{\text{def}}{\Leftrightarrow} \{f(x) \mid x \in H \cap D_f\} \subseteq R_f \subseteq B$$

halmazt a H *(*f *által létesített)* ***képének*** *nevezzük.*

Gyakori eset, hogy $H \subseteq D_f$. Ekkor $H \cap D_f = H$, tehát $f[H] = \{f(x) \mid x \in H\}$. Továbbá $H \cap D_f = \varnothing$ esetén $f[H] = \varnothing$, speciálisan $f[\varnothing] = \varnothing$.

2.26. definíció. *Legyen* $f \in A \to B$*, továbbá* $H \subseteq B$*. Az*

$$f^{-1}[H] \overset{\text{def}}{\Leftrightarrow} \{x \in D_f \mid f(x) \in H\} \subseteq D_f \subseteq A$$

halmazt a H *(*f *által létesített)* ***ősképének*** *nevezzük.*

A $H \cap R_f = \varnothing$ esetben $f^{-1}[H] = \varnothing$, speciálisan $f^{-1}[\varnothing] = \varnothing$. Megjegyezzük, hogy f^{-1} itt reláció, nem függvény.

Nagyon fontosak azok a függvények, amelyek értelmezési tartománya a teljes A halmaz.

2.27. definíció. *Legyen* $f \in A \to B$*. Azt mondjuk, hogy* f *egy* **A-n értelmezett, B-be képező függvény***, ha* $D_f = A$*. Ezt a tényt* $f : A \to B$*-vel jelöljük.*

Ha azt mondjuk, hogy f az A-t B-be képező függvény, akkor ez alatt azt értjük, hogy f egy olyan függény, amelynek az értelmezési tartománya A, az értékkészlete pedig B.

2.3.2. Függvények típusai, leszűkítés, kiterjesztés, indexelés

2.28. definíció. *Legyen adott egy* $f \in A \to B$ *függvény. Az* f *függvény* ***szürjektív,*** *ha* $R_f = B$, ***injektív,*** *ha* $\forall x_1, x_2 \in D_f$ $(x_1 \neq x_2)$ *esetén* $f(x_1) \neq f(x_2)$. *A leképezést* ***bijektívnek*** *nevezzük, ha szürjektív és injektív egyszerre.*

2.13. példa.
(1) Legyen $A_1, \ldots, A_n$ nem üres halmaz, és $i \in \{1, \ldots, n\}$. A $p_i : A_1 \times \ldots \times A_n \to A_i$, $(x_1, \ldots, x_n) \mapsto x_i$ függvény szürjektív. A leképezést ***i-edik projekciónak*** vagy ***vetítésnek*** nevezzük.

(2) Legyen $A \neq \varnothing$, és ρ egy ekvivalenciareláció A-n. A $k : A \to A/\rho$, $x \mapsto [x]$ függvény szürjektív, amelyet ***kanonikus függvénynek*** nevezünk.

(3) Az $A \to A$, $a \mapsto a$ leképezés bijektív, amit ***identikus leképezésnek, identitásnak*** vagy ***azonosságnak*** nevezünk, és id_A-val jelölünk.

(4) Véges halmazon értelmezett $f : A \to A$ bijektív függvények nagyon gyakoriak a matematikában, fizikában, és a számítástudományban. Ha például $A = \{a_1, a_2, \ldots, a_n\}$, akkor az $f : A \to A$ függvény szokásos jelölése

$$f = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ f(a_1) & f(a_2) & \ldots & f(a_n) \end{pmatrix}.$$

Ezeket a függvényeket ***permutációfüggvényeknek*** nevezzük.

(5) Az $f \in A \to B$ leképezést ***konstansfüggvénynek*** nevezzük, ha $f(x) = f(y)$ minden $x, y \in D_f$ esetén.

(6) Az $\varnothing \neq A \subseteq H$ halmaz ***karakterisztikus függvényén*** a

$$\chi_A(x) = \begin{cases} 1 & \text{ha } x \in A \\ 0 & \text{ha } x \in H \setminus A. \end{cases}$$

függvényt értjük. Ha jelölni akarjuk a H alaphalmazt is, akkor szokásos jelölés $\chi_A^{(H)}(x)$.

2.14. példa. Az $A = \{1, 2, 3\}$ halmazon értelmezett permutációfüggvények az alábbiak lesznek:

$$id_A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$
$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\ f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

2.29. definíció. *A* $g \in C \to B$ *függvényt az* $f \in A \to B$ *függvény (*C*-re való)* ***leszűkítésének*** *(vagy megszorításának) nevezzük, ha* $\varnothing \neq C \subseteq D_f$, *és* $f(x) = g(x)$ *minden* $x \in C$ *esetén.* g *helyett gyakran* $f|_C$*-t írunk (olvasd:* f *leszűkítése* C*-re).*

2.30. definíció. *A* $g \in C \to B$ *függvényt az* $f \in A \to B$ *függvény* ***kiterjesztésének*** *nevezzük, ha* $D_f \subseteq D_g$ *és* $g|_{D_f} = f$.

Vegyük észre, hogy a leszűkítés egyértelmű, a kiterjesztés nem.

Sokszor egy függvény esetében nem a hozzárendelés, hanem az értékkészlet elemeinek „rendszere" kap hangsúlyt. A „rendszer" valami olyant jelent, hogy az értékkészlet elemeit az értelmezési tartomány elemeinek segítségével adjuk meg, azaz „megindexeljük".

2.31. definíció. *Legyen* $I \neq \varnothing$ *és* $A \neq \varnothing$. *Az* $a : I \to A$ *függvényeket (*A*-beli) indexelt rendszereknek nevezzük. Az* I *halmazt* ***indexhalmaznak****, elemeit* ***indexeknek*** *nevezzük.*

Az $i \in I$ indexhez tartozó $a(i) \in A$ elemet i-indexű tagnak hívjuk, és $a(i)$ helyett általában a_i-vel jelöljük. Az indexelt rendszerek egyéb jelölései: $(a_i)_{i\in I}$, $(a_i, i \in I)$, $a_i \in A$ $(i \in I)$. Az $(a_i, i \in I)$ rendszert az különbözteti meg az $\{a_i \in A \mid i \in I\}$ halmaztól, hogy a rendszerben többször is (akár végtelen sokszor) előfordulhat ugyanaz az A-beli elem, hiszen nem követeljük meg az $a : I \to A$ leképezés injektivitását.

Ha A elemei mind halmazok, akkor ***halmazcsaládról*** beszélünk. Halmazcsaládokra is érvényes számos halmazelméleti azonosság, például kommutativitás, asszociativitás, disztributivitás, vagy a DE MORGAN-szabályok.

2.15. példa. Legyen $I = \{\text{piros, fehér, zöld}\}$, $A = \{\text{red, white, green}\}$. Az
$a : I \to A$,
$a_{\text{piros}} = \text{red}$,
$a_{\text{fehér}} = \text{white}$,
$a_{\text{zöld}} = \text{green}$
függvény egy indexelt rendszer.

2.3.3. Függvények kompozíciója, inverze, műveletei halmazokkal

Ha $g \in A \to B$ és $f \in B \to C$ függvények, akkor $f \circ g$ analóg a relációk kompozíciójával: $f \circ g \in A \to C$ az a függvény, amelyre

$$D_{f\circ g} = \{x \in D_g \mid g(x) \in D_f\} \subseteq D_g \subseteq A$$

halmaz nem üres, és ekkor a kompozíció

$$(f \circ g)(x) = f(g(x)) \ (x \in D_{f\circ g}).$$

A felírásban szereplő g-t ***belső függvénynek***, f-et ***külső függvénynek*** nevezzük. Könnyen megmutatható, hogy függvények kompozíciója szintén függvény.

A relációkkal analóg módon, a $h \in A \to B, g \in B \to C$ és $f \in C \to D$ függvényekre érvényes az asszociativitás törvénye, azaz $f\circ(g\circ h) = (f\circ g)\circ h$. A kompozíció az identikus leképezéssel a következőket adja: $\mathrm{id}_B \circ h = h$ és $h \circ \mathrm{id}_A = h$.

Valamely $f \in A \to B$ leképezés inverze, f^{-1} (mint relációinverz), általában nem függvény.

2.16. példa. Legyen $A = B = \{a, b\}$ és $f = \{(a, b), (b, b)\}$. Ekkor az $f^{-1} = \{(b, a), (b, b)\}$ reláció nem függvény.

Bizonyos feltétel teljesülése esetén azonban f^{-1} függvény.

2.32. tétel. *Az* $f \in A \to B$ *függvény inverze pontosan akkor függvény, ha* f *injektív. Ekkor* f^{-1} *maga is injektív, továbbá* $f^{-1} \circ f = \mathrm{id}_{D_f}$ *és* $f \circ f^{-1} = \mathrm{id}_{R_f}$.

Bizonyítás. Az f^{-1} reláció pontosan azokból a $(b, a) \in B \times A$ párokból áll, ahol a az f leképezésnél a b elem őse. Ezért f^{-1} pontosan akkor parciális függvény, ha minden $b \in B$ elemnek legfeljebb egy őse van, azaz f injektív. Mivel f^{-1} inverze f, ezért az iménti gondolatot ismételten alkalmazva kapjuk f^{-1} injektivitását. Az állítás többi része a szorzat és az inverz definíciójából következik. □

Az injektív függvényeket ***invertálható függvényeknek*** nevezzük.

2.17. példa. Számítsuk ki a 2.14. példa f_4 függvényének inverzét és az $f_3 \circ f_2$ függvénykompozíciót.

Megoldás: $p_4^{-1} = \{(3,1),(1,2),(2,3)\}$, vagy másként $f_4^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_3$. A keresett függvénykompozíció pedig $f_3 \circ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_5$.

2.33. definíció. *Legyenek* $A_1, \ldots, A_n$ *nem üres halmazok. Ha egy* $f \in A \to B$ *függvény esetén* $D_f \subseteq A_1 \times \ldots \times A_n$, *akkor* ***n-változós függvényről*** *beszélünk.*

Jelölésben $f((a_1, \ldots, a_n))$ helyett általában $f(a_1, \ldots, a_n)$-et írunk.

Gyakorlatok

2.3-1. Válasszuk ki az alábbi $\rho \subseteq \{1,2,3\} \times \{a,b,c,d\}$ relációk közül a függvényeket:
$\rho = \{(1,a),(1,c),(2,b),(2,d),(3,a)\}$
$\rho = \{(1,d),(2,a),(3,c)\}$
$\rho = \{(1,a),(2,a),(3,d)\}$.

2.3-2. Bizonyítsuk be, hogy tetszőleges $\phi : A \to B$ függvény esetén a $\mathrm{Ker}(\phi) \subseteq A \times A$, $a_1 \mathrm{Ker}(\phi) a_2 \Leftrightarrow \phi(a_1) = \phi(a_2)$ reláció ekvivalenciareláció. A $\mathrm{Ker}(\phi)$ relációt a ϕ függvény *magjának* nevezzük.

2.3-3. Legyen $A, B \subseteq H$, χ_A és χ_B pedig sorban a karakterisztikus függvényeik. Mi lesz ekkor $\overline{A}, A \cup B$ és $A \cap B$ karakterisztikus függvénye?

2.3-4. Bizonyítsuk be, hogy injektív függvények kompozíciója injektív, szürjektív függvények kompozíciója szürjektív függvény.

2.3-5. Legyen $f : A \to B$ és $g : B \to C$ invertálható fügvények. Bizonyítsuk be, hogy ekkor $g \circ f$ is invertálható, továbbá $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

2.3-6. Legyenek $f : X \to Y$ és $g : Y \to Z$ függvények. Bizonyítsuk be a függvényekre és halmazműveletekre vonatkozó alábbi összefüggéseket:

$$\begin{array}{rcll} f[A \cap B] & \subseteq & f[A] \cap f[B] & \text{minden } A, B \subseteq X\text{-re} \\ f[A \cup B] & = & f[A] \cup f[B] & \text{minden } A, B \subseteq X\text{-re} \\ f^{-1}[A \cap B] & = & f^{-1}[A] \cap f^{-1}[B] & \text{minden } A, B \subseteq Y\text{-ra} \\ f^{-1}[A \cup B] & = & f^{-1}[A] \cup f^{-1}[B] & \text{minden } A, B \subseteq Y\text{-ra} \\ f^{-1}[A \setminus B] & = & f^{-1}[A] \setminus f^{-1}[B] & \text{minden } A, B \subseteq Y\text{-ra} \\ (g \circ f)^{-1}[A] & = & f^{-1}[g^{-1}[A]] & \text{minden } A \subseteq Z\text{-re.} \end{array}$$

2.4. Axiomatikus halmazelmélet

A naív halmazelméletben, mint látni fogjuk, ellentmondásokat lehet konstruálni. Az ilyen ellentmondásokhoz vezető meggondolásokat ***antinómiáknak*** nevezzük. Ezeknek az elemzése a halmazelmélet új felépítéséhez vezetett. Példák antinómiákra:

(1) EPIMENDÉSZ (Kr. e. 600 körül)
A krétai EPIMENDÉSZ azt állítja: „Amit most mondok, hazugság." Ha EPIMENDÉSZ hazudott, akkor állítása hamis, és nem hazudott. Ha EPIMENDÉSZ nem hazudott, akkor állítása igaz, és hazudott.

(2) PROKLOSZ (Kr. e. 450 körül)
PROTAGORASZ egy tanítványát jogra tanítja, és megállapodik vele, hogy a tanítványnak csak akkor kell a tandíjat megfizetnie, ha első perét megnyerte. Mivel a tanítvány tanulmányai befejeztével nem vállalt pert, PROTAGORASZ végül beperelte a tandíj meg nem fizetése miatt. Így érvelt: „Ha megnyerem a pert, akkor megkapom a pénzemet az ítélet alapján, ha elveszítem, akkor a korábbi megállapodás alapján kapom meg." A tanítvány fordítva érvel: „A tandíjat egyik esetben sem kell megfizetnem, vagy a megállapodás vagy a bírói ítélet alapján."

(3) RUSSEL (1903)
Képezzük valamennyi olyan halmaz H halmazát, amely magát elemként nem tartalmazza. Az a feltevés, hogy ez a H halmaz magát elemként tartalmazza, arra a következtetésre vezet, hogy saját magát nem tartalmazza, és az a feltevés, hogy H saját magát tartalmazza, arra vezet, hogy H önmagát nem tartalmazza. Formalizálva, legyen $H = \{x |\ x \notin x\}$. Ekkor $H \in H \Leftrightarrow H \notin H$.

EPIMENDÉSZ és PROTAGORASZ állításai logikai értelemben tehát nem kijelentések. A RUSSEL-paradoxon szerint minden halmaz halmaza ellentmondásos fogalom. Az antinómiák kiküszöbölésének legjobb eszköze a HILBERT által tanácsolt axiomatikus módszer. Az ***axiomatikus halmazelmélet*** alapgondolata abban áll, hogy csak bizonyos axiomatikusan lerögzített tulajdonságokkal rendelkező dolgokat nevez halmazoknak. Az alábbiakban ismertetünk egy egyszerű, a számítógépes-algebrai rendszerekhez jól illeszkedő axiómarendszert, ami ZERMELO nevéhez fűződik.

(1) *A meghatározottság axiómája.* Két halmaz akkor és csak akkor egyenlő, ha elemeik ugyanazok.

(2) *A részhalmaz axiómája.* Minden A halmazra és minden $\mathcal{F}(x)$ kijelentésformulára (kifejezésre) létezik egy B halmaz, amelyhez A-nak pontosan azon x elemei tartoznak, amelyekre $\mathcal{F}(x)$ IGAZ.

(3) *Az üres halmaz axiómája.* Van olyan halmaz, amelynek nincs eleme.

(4) *Páraxióma.* Bármely a, b dologhoz van olyan halmaz, amelynek ezek és csak ezek az elemei.

(5) *Unióaxióma.* Ha A egy halmaz, akkor van olyan halmaz, amely pontosan azokat a dolgokat tartalmazza, amelyek A valamely elemének az elemei.

(6) *A hatványhalmaz axiómája.* Minden A halmazhoz lézetik egy olyan halmazrendszer, amelynek elemei pontosan A részhalmazai.

(7) *A végtelenségi axióma.* Van olyan A halmaz amelynek $\varnothing$ eleme, és ha az x halmaz eleme A-nak, akkor $x \cup \{x\}$ is eleme A-nak.

(8) *A kiválasztási axióma.* Nem üres halmazok bármely családjához lézetik ki-

választási függvény. (Az $X_i, i \in I$ halmazcsaládhoz tartozó kiválasztási függvénynek nevezzük azokat az $f : I \to \cup_{i\in I} X_i$ függvényeket, amelyekre $f_i \in X_i$ minden $i \in I$-re.)

Ebből az axiómarendszerből Fraenkel kihagyta a kiválasztási axiómát, és kizárt mindent az elméletből, ami nem halmaz, továbbá hozzávette az alábbi axiómát.

(9) *A pótlás axiómája.* Ha $\mathcal{F}(x, y)$ olyan kijelentésformula, hogy az A halmaz minden x elemére $\{y : \mathcal{F}(x, y)\}$ halmaz, akkor létezik az A halmazon értelmezett olyan f függvény, amelyre az $f(x) = \mathcal{F}(x, y)$ egyenlőség fennáll minden $x \in A$ esetén.

Az így kapott axiómarendszert Zermelo-Fraenkel-axiómarendszernek (ZF) nevezzük. Ha hozzávesszük a kiválasztási axiómát, akkor a Zermelo-Fraenkel-choice axiómarendszerhez (ZFC) jutunk.

A Zermelo-féle axiómarendszer végtelenségi axiómája biztosítja végtelen halmazok létezését, különösen a természetes számok $\mathbb{N}$ halmazáét. A hatványhalmaz axiómája miatt minden x halmazhoz létezik egy $\wp(x)$ hatványhalmaz. A kiválasztási axióma a legproblematikusabb. A kiválasztási függvény minden halmazból kiválasztja ennek a halmaznak egy elemét. Az axióma nem ad meg semmit arra vonatkozóan, hogy *hogyan* lehet az egyes esetekben ilyen függvényt konstruálni, csak az *egzisztenciáját* követeli meg. Meg lehet mutatni, hogy az axiomatikus halmazelmélet ellentmondásmentességét feltételezve a kiválasztási axióma a többitől független. A kiválasztási axiómát magában foglaló halmazelmélet mellett így van létjogosultsága a kiválasztási axióma nélküli halmazelméletnek is, de a matematikusok többsége az elsőhöz ragaszkodik.

Gyakorlatok

2.4-1. A végtelenségi axióma felhasználásával adjunk tetszőleges n pozitív egészhez olyan n elemű A_n halmazt, hogy $x, y \in A_n$ esetén az alábbiak közül pontosan az egyik teljesüljön: $x \in y, y \in x$ vagy $x = y$.

Megjegyzések a fejezethez

A halmazelmélet axiomatikus megalapozása először Zermelo-nak sikerült 1908-ban. Axiómarendszerét Fraenkel izraeli matematikus egészítette ki. A halmazelmélet egy másik axiómarendszerét Neumann János állította össze, majd később ehhez hasonlót fogalmazott meg Bernays zürichi matematikus. Ezekben az axiómarendszerekben az összes halmazok halmaza nem halmaz. Az axiomatikus halmazelmélet további izgató problémaköre a kontinuumhipotézis köré csoportosul. A problémát az 5. fejezet végén ismertetjük.

Javasolt irodalom: Hajnal és Hamburger [16], Halmos és Siegler [18], Lavrov és Maximova [26], valamint Totik [40].

3. Struktúrák

A matematika részterületeinek axiomatikus megalapozása során kiderült, hogy közös alapstruktúrákon nyugszanak. A fejezetben két alapstruktúrával foglalkozunk: a rendezési és az algebrai struktúrával. Létezik egy harmadik alapstruktúra is, a topologikus struktúra, amelynek részletes ismertetése a matematikai analízis keretein belül történik (harmadik rész). Az algebrai és a rendezési struktúrákra fogunk támaszkodni a következő fejezetben tárgyalt számfogalom felépítéséhez. Az alapstruktúrákon kívül a vegyes és a származtatott struktúrákat is megvizsgáljuk.

3.1. Rendezési struktúrák

Egy halmazhoz ***rendezési struktúrát*** rendelünk hozzá, ha az elemein valamilyen „rendezés" van értelmezve. Ez azt jelenti, hogy a halmaz elemei meghatározott szabályok szerint „összehasonlíthatóak". A rendezési struktúrák elmélete szoros kapcsolatban áll a halmazelmélettel.

3.1.1. Részbenrendezés

3.1. definíció. *Egy* $\rho \subseteq A \times A$ *relációt* ***részbenrendezésnek*** *nevezünk, ha reflexív, antiszimmetrikus és tranzitív.*

3.2. definíció. *Egy* $\sigma \subseteq A \times A$ *relációt* ***szigorú részbenrendezésnek*** *nevezünk, ha irreflexív és tranzitív.*

Az irreflexivitásból és a tranzitivitásból a szigorú antiszimmetria következik.

3.3. definíció. *Egy* $\Delta \subseteq A \times A$ *relációt* ***diagonális relációnak*** *nevezünk, ha* $\Delta = \{(a, a) |\ a \in A\}$.

3.4. tétel (részbenrendezés és szigorú részbenrendezés kapcsolata).
Ha ρ *részbenrendezés és* σ *szigorú részbenrendezés egy* A *halmazon, akkor*
(1) $\rho \setminus \Delta$ *szigorú részbenrendezés,*
(2) $\sigma \cup \Delta$ *részbenrendezés, és*
(3) $\sigma = \rho \setminus \Delta$ *pontosan akkor, ha* $\sigma \cup \Delta = \rho$.

Bizonyítás.
(1) $\rho\setminus\Delta$ nyilván irreflexív. Ha $(a,b)\in\rho\setminus\Delta$, akkor $a\neq b$, amiből ρ antiszimmetriája miatt $(b,a)\notin\rho$. Ezért $(b,a)\notin\rho\setminus\Delta$, amiből a szigorú antiszimmetria adódik. Tegyük most fel, hogy $(a,b),(b,c)\in\rho\setminus\Delta$. Ekkor ρ tranzitivitásából $(a,c)\in\rho$. Mivel $\rho\setminus\Delta$ szigorúan antiszimmetrikus, ezért $c\neq a$, így $(a,c)\in\rho\setminus\Delta$. Ezzel $\rho\setminus\Delta$ tranzitivitását is bebizonyítottuk.
(2) $\sigma\cup\Delta$ reflexívitása a diagonális reláció definíciójából következik. Ha $(a,b)\in\sigma$, akkor $(b,a)\notin\sigma$. Vagyis $(a,b),(b,a)\in\sigma\cup\Delta$ csak akkor lehetséges, ha $(a,b),(b,a)\in\Delta$. Ez pedig $\sigma\cup\Delta$ antiszimmetriáját jelenti. Tegyük fel, hogy $(a,b),(b,c)\in\sigma\cup\Delta$. Ha $(a,b),(b,c)\in\sigma$, akkor a tranzitivitás miatt $(a,c)\in\sigma$. Ha egyikük σ-nak eleme, a másik pedig Δ-beli, akkor (a,c) megegyezik (a,b) és (b,c) valamelyikével, és így ugyancsak σ-beli. Amennyiben pedig $(a,b),(b,c)\in\Delta$, akkor (a,c) is az. Vagyis (a,c) mindig eleme $\sigma\cup\Delta$-nak, ami bizonyítja a tranzitivitást.
(3) következik (1)-ből és (2)-ből. □

A tétel szerint bármely részbenrendezés egyértelműen meghatároz egy szigorú részbenrendezést, és viszont. Ha egy halmazon adott egy rögzített részbenrendezés, akkor ezt a $\leq$ jel fogja jelölni. A megfelelő szigorú részbenrendezésre pedig a $<$ jelet használjuk. A ρ részbenrendezéssel együtt ρ^{-1} is az. Ekkor a $\leq$ és $<$ relációk inverzét $\geq$ és $>$ fogja jelölni.

3.5. definíció. *Ha $\leq$ részbenrendezés az A halmazon, akkor $(A;\leq)$-t* ***részbenrendezett struktúrának****, az A halmazt pedig* ***részbenrendezett halmaznak*** *nevezzük.*

3.6. definíció. *Ha $B\subseteq A$, akkor az $(A;\leq)$ részbenrendezésnek a B-re való leszűkítése is részbenrendezés, amit* ***indukált részbenrendezésnek*** *nevezünk.*

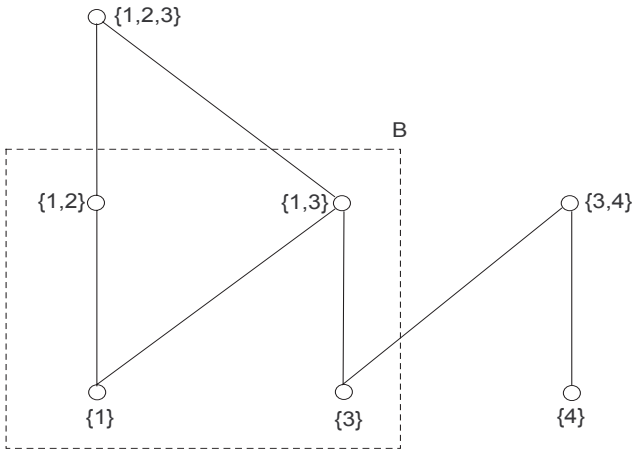
Az alábbi definícióknál mindig feltesszük, hogy B az $(A;\leq)$ részbenrendezett halmaz egy tetszőleges részhalmaza.

3.7. definíció. *A B halmaz m elemét* ***minimális elemnek*** *nevezzük, ha nem létezik olyan $x\in B$ $(x\neq m)$, amelyre $x\leq m$. A B halmaz k elemét* ***legkisebb elemnek*** *nevezzük, ha $k\leq x$ minden $x\in B$ esetén.*

Analóg módon definiálhatjuk egy részhalmaz ***maximális elemeit,*** illetve ***legnagyobb elemét.*** A definícióból világos, hogy egy tetszőleges részbenrendezett halmaz bármely véges részhalmazának van minimális eleme. Ezzel szemben legkisebb elem még véges részbenrendezett halmazok esetében sem mindig létezik. Ha viszont legkisebb elem létezik, akkor a szigorú antiszimmetria miatt az egyértelmű, és ez az elem minimális is. Ha A-nak létezik egyértelmű minimális eleme, akkor azt $\min A$-val, ha pedig létezik egyértelmű maximális eleme, azt $\max A$-val jelöljük.

3.8. definíció. *Az $a\in A$ elemet a B halmaz* ***alsó korlátjának*** *nevezzük, ha $a\leq b$ minden $b\in B$-re. Ha minden $b\in B$-re $b\leq f$, akkor f a B* ***felső korlátja.***

Lehet, hogy egy részbenrendezett halmaznak nincs alsó vagy felső korlátja, de az is lehet, hogy több van. Ha van az alsó korlátok között eleme B-nek, akkor csak egy van, és ez B legkisebb eleme. Hasonló állítás igaz a felső korlátokra.



3.1. ábra. Legyen $H = \{1,2,3,4\}$, $A = \{\{1\},\{3\},\{4\},\{1,2\},\{1,3\},\{3,4\},\{1,2,3\}\} \subset \wp(H)$ és tekintsük a „$\subseteq$" relációt $A \times A$-n. Az Olvasóra bízzuk annak belátását, hogy az így definiált reláció részbenrendezés. Az ábra a részbenrendezés Hasse-diagramját mutatja. Az A halmaz minimális elemei az $\{1\},\{2\},\{3\}$, maximális elemei az $\{1,2,3\},\{3,4\}$, legkisebb és legnagyobb elemei nincsenek. Legyen $B = \{\{1\},\{3\},\{1,2\},\{1,3\}\}$ és tekintsük az indukált részbenrendezést. Ekkor a B halmaz (A-beli) felső korlátja és szuprémuma az $\{1,2,3\}$ elem, alsó korlátja és infimuma nincs.

3.9. definíció. *Ha* B *alsó korlátjai halmazában van legnagyobb elem, azt a* B *halmaz* ***legnagyobb alsó korlátjának (alsó határának**, idegen szóval **infimumának**) nevezzük, és* $\inf B$*-vel jelöljük. Hasonlóan, ha* B *felső korlátjai halmazában van legkisebb elem, azt* B ***legkisebb felső korlátjának (felső határának**, idegen szóval **szuprémumának**) nevezzük, és* $\sup B$*-vel jelöljük.*

Véges halmaz rendezési struktúráját egyszerű esetekben áttekinthető módon lehet ún. ***rendezési diagramon*** (Hasse-féle diagramon) ábrázolni. A halmaz minden eleméhez a rajz síkjában egy pontot rendelünk hozzá azzal a megállapodással, hogy a b elemet az a elem fölé rajzoljuk, ha $a \leq b$ illetve $a < b$ érvényes. Azzal a további megállapodással, hogy b-t nem kötjük össze a-val, ha a b már más pontokon keresztül össze van kötve a-val (tranzitivitás), a vonalak számát nagyban lecsökkenthetjük (3.1. ábra).

3.10. definíció. *Legyen* $(A, \leq_1)$ *és* $(B; \leq_2)$ *részbenrendezett struktúra. Az* $f \in A \to B$ *függvényt* ***monoton növőnek*** *nevezzük, ha* $x, y \in D_f$, $x <_1 y$ *esetén* $f(x) \leq_2 f(y)$*, és* ***szigorúan monoton növőnek*** *nevezzük, ha* $x, y \in D_f$, $x <_1 y$ *esetén* $f(x) <_2 f(y)$.

Analóg módon definiálhatók a monoton és szigorúan monoton ***csökkenő*** függvények.

3.11. definíció. *Az* $(A; \leq)$ *részbenrendezés esetén* $[x, y]$*-al jelöljük mindazon* $z \in A$ *elemek halmazát, amelyekre* $x \leq z$ *és* $z \leq y$*, vagy rövidebben* $x \leq z \leq y$*. Hasonlóan,* $]x, y[$*-al jelöljük mindazon* z*-ket, melyekre* $x < z$ *és* $z < y$*, vagy másként* $x < z < y$*. Első esetben* ***zárt****, második esetben* ***nyílt intervallumról*** *beszélünk.*

Nyílt intervallumok jelölésére szokásos még az (x, y) jelölés, amelynek hátránya, hogy megegyezik a rendezett pár jelölésével. Analóg módon definiálhatók a balról zárt (nyílt), jobbról nyílt (zárt) intervallumok.

3.1.2. Teljes rendezés, jólrendezés

3.12. definíció. *Az $(A; \leq)$ részbenrendezés* ***teljes rendezés*** *(rendezés, lineáris rendezés, konnex rendezés), ha a $\leq$ reláció dichotom, azaz ha A bármely két eleme összehasonlítható. Ekkor az A halmaz teljesen rendezett.*

Ha $(A; \leq)$ teljes rendezés, akkor a legkisebb és minimális elem, valamint a legnagyobb és maximális elem fogalma egybeesik, továbbá az indukált részbenrendezésnél egy teljesen rendezett halmaz minden részhalmaza is teljesen rendezett.

3.13. definíció. *Egy részbenrendezett halmaz valamely részhalmazát* ***láncnak*** *nevezzük, ha az indukált részbenrendezésnél teljesen rendezett.*

A teljesen rendezett halmazok további specializálását adja az alábbi definíció.

3.14. definíció. *Az $(A; \leq)$ részbenrendezésnél az A halmaz* ***jólrendezett****, ha minden nem üres részhalmazának van legkisebb eleme.*

Jólrendezett halmazok esetén tehát bármely kételemű részhalmaznak is van legkisebb eleme, amiből következik, hogy jólrendezett halmazok teljesen rendezettek. De vajon melyek a jólrendezhető halmazok?

3.15. tétel (jólrendezési tétel). *Minden halmaz jólrendezhető.* □

Megjegyezzük, hogy a jólrendezési tétel következményképpen adódik a kiválasztási axiómát is tartalmazó axiomatikus halmazelméletből. Megfordítva, a jólrendezési tételből le lehet vezetni a kiválasztási axiómát. A kiválasztási axióma kritikája tehát az ekvivalencia miatt a jólrendezési tételt is illeti. A jólrendezési tétel alkalmazásánál a probléma az, hogy a jólrendezésnek csak a létezése van biztosítva. Ezt a hiányosságot küszöböli ki a jólrendezési tétellel ekvivalens Zorn-féle lemma, amely szerint, ha egy részbenrendezett halmaz minden lánca felülről korlátos, akkor a halmaznak van maximális eleme. A jólrendezési tétel helyett a Zorn-lemmát alkalmazva, az adott halmazhoz rendezési struktúrát tudunk tehát hozzákapcsolni.

Gyakorlatok

3.1-1. Mutassuk meg, hogy az alábbi, $\leq$-vel jelölt relációk minegyike részbenrendezés:

a) az $\{a, b, c, d\}$ halmaz legalább kételelmű részhalmazainak a halmazán $A \leq B$ pontosan akkor, ha $A \subseteq B$

b) az $\{a, b, c, d\}$ halmaz legfeljebb kételelmű részhalmazainak a halmazán $A \leq B$ pontosan akkor, ha $B \subseteq A$.

Készítsük el a részbenrendezések Hasse-féle diagramjait és keressük meg a maximális, minimális, legnagyobb, illetve legkisebb eleme(ke)t.

3.1-2. Bizonyítsuk be, hogy egy részbenrendezett halmaz bármely nem üres véges részhalmazának van maximális és minimális eleme.

3.1-3. Bizonyítsuk be, hogy ha $\rho \subseteq A \times A$ részbenrendezés, akkor ρ^{-1} is az. Mutassuk meg, hogy ha $(A;\rho)$-n valamely elem maximális, akkor (A,ρ^{-1})-en minimális és fordítva.
3.1-4.* Legyen $A \neq \varnothing$, és ρ egy A-n értelmezett reláció. Bizonyítsuk be, hogy ρ pontosan akkor terjeszthető ki részbenrendezéssé, ha a $\tilde{\rho} = \Delta \cup \hat{\rho}$ reláció részbenrendezés A-n (Δ a diagonális relációt, $\hat{\rho}$ a ρ reláció tranzitív lezártját jelenti.) Ekkor $\tilde{\rho}$ a ρ reláció ***reflexív-tranzitív lezártja***.
3.1-5. Mutassuk meg, hogy ha A és B teljesen rendezettek, akkor minden $f : A \to B$ szigorúan monoton növő (illetve csökkenő) függvény injektív. Állíthatunk-e hasonlót f inverzéről?

3.2. Algebrai struktúrák

Egy halmazhoz ***algebrai struktúrát*** rendelünk, ha benne egy vagy több műveletet értelmezünk. Ilyen művelet például számhalmazokon a „hagyományos" összeadás vagy szorzás. Műveleteket azonban nem csak számhalmazokon definiálhatunk. Kézenfekvő, hogy az definíciót általánosan fogalmazzuk meg.

3.2.1. Belső műveletek

3.16. definíció. *Tetszőleges A nem üres halmaz és n nemnegatív egész esetén A-n értelmezett n-változós* ***belső műveleten*** *egy $A^n \to A$ függvényt értünk, ahol n-et a művelet* ***változószámának*** *vagy* ***aritásának*** *nevezzük.*

Az $n = 0$ eset különleges. Mivel A^0 egyelemű halmaz, ezért egy A-n értelmezett nullaváltozós művelet egy A-beli elem kijelölését jelenti. Jelölésben a szokásos írásmódot alkalmazzuk. Például tetszőleges $a, b, c \in A$ elemekre a 3-változós f művelet eredményét $f(a, b, c)$-vel jelöljük. Egy-, illetve kétváltozós műveletek esetén betűk helyett általában egyéb műveleti jeleket (például $+, \cdot, \circ, \oplus, \otimes$, stb.) használunk. Ilyenkor a kétváltozós műveleti jelekre a binér relációknál látott „közéírást" (infix írásmódot) alkalmazunk. Ha tehát $\oplus$ 2-változós művelet A-n, akkor tetszőleges $a, b \in A$-ra a művelet eredményét $a \oplus b$-vel jelöljük, valamint a-t és b-t a művelet ***operandusainak*** nevezzük. Ha a műveleti jel a szorzás, akkor a szorzópontot általában elhagyjuk, vagyis $a \cdot b$ helyett ab-t írunk.

A műveletek megadása a függvények megadásához hasonlóan történhet. Véges halmazokra (5. fejezet) a műveleteket ***műveleti táblákkal*** lehet ábrázolni (3.2. ábra).

3.1. példa. Ha A egy tetszőleges nem üres halmaz, akkor $\cup, \cap$ és $\setminus$ binér műveletek, a komplementerképzés pedig unér művelet $\wp(A)$-n.

Ha infix műveletek eredményére újabb műveleteket alkalmazunk, akkor valamilyen módon (általában zárójelekkel) jelölni kell, hogy milyen sorrendben kell azokat elvégezni. Szokás megállapodni a műveletek ***precedenciájában***. Például először a nullér, majd az unér, azután a binér műveleteket végezzük el, a binér műveletek között is valamilyen végrehajtási sorrendet állítva fel. Megjegyezzük, hogy a záró-

$\oplus$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

3.2. ábra. Egy $\oplus$ kétváltozós művelet műveleti táblázata az $A = \{a, b, c, d\}$ halmazon.

jelek teljesen elhagyhatók, ha a műveleti jeleket mindig az operandusok elé írjuk. Ezt a jelölésmódot Łukasiewicz tiszteletére *lengyel jelölésnek* szokás nevezni. Az informatikában még elterjedtebb a *fordított lengyel jelölés*, ahol a műveleti jelek az operandusok után következnek. Néhány zsebszámológép mellett a PostScript nyomtatóvezérlő nyelv és a fordítóprogramok is ezt használják.

3.17. definíció. *Az* $(A; F)$ *párt, ahol* A *nem üres halmaz,* F *pedig* A*-n értelmezett műveletek egy rendezett halmaza,* ***algebrai struktúrának****, vagy röviden* ***algebrának*** *nevezzük.*

Ha az $(A; F)$ algebrai struktúrában F véges, mondjuk $F = (\oplus, \otimes)$, akkor az algebrát úgy is szokás jelölni, hogy $(A; \oplus, \otimes)$.

A továbbiakban az *egyetlen* kétváltozós művelettel rendelkező struktúrák, az ún. ***grupoidok*** tulajdonságait vizsgáljuk.

3.18. definíció. *Az* $(S; \oplus)$ *grupoid egy* s *elemét* bal *illetve* jobb oldali semleges elemnek *nevezzük, ha* $s \oplus a = a$ *illetve* $a \oplus s = a$ *minden* $a \in S$ *elemre. Ha* s *bal és jobb oldali semleges elem egyszerre, akkor* ***semleges elemnek*** *nevezzük.*

A semleges elemet idegen szóval neutrális elemnek is nevezzük. Általában semmi sem garantálja, hogy létezik bal és jobb oldali semleges elem, és a számukról sem állíthatunk semmit. De ha mindkét oldali semleges elem létezik, akkor azok szükségképpen megegyeznek, így ekkor egyetlen semleges elem létezik.

3.19. definíció. *Ha az* $(A; \oplus)$ *algebrai struktúra minden* $a, b, c \in A$ *elemére érvényes, hogy* $(a \oplus b) \oplus c = a \oplus (b \oplus c)$*, akkor azt mondjuk, hogy a struktúra művelete* ***asszociatív****, vagy a struktúrában érvényes az asszociativitás törvénye.*

Ha az asszociativitás érvényes, akkor több tényező esetén sem függ az eredmény a zárójelezéstől (4.13. tétel), így a zárójeleket bárhová lehet tenni, vagy akár el is hagyhatóak.

3.20. definíció. *Az* $(S; \oplus)$ *algebrai struktúrát* ***félcsoportnak*** *nevezzük, ha a művelete asszociatív.*

3.21. definíció. *A semleges elemet tartalmazó félcsoportot egységelemes félcsoportnak nevezzük.*

3.22. definíció. *Ha egy* $(S;\oplus)$ *egységelemes félcsoportban* s *a semleges elem és* $a_b \oplus a_j = s$*, akkor azt mondjuk, hogy* a_b *az* a_j *elem* bal oldali inverze*,* a_j *pedig az* a_b *elem* jobb oldali inverze*. Ha az* a *elemnek* ugyanaz *az elem a bal- illetve jobb oldali inverze is, akkor ezt az elemet* a ***inverzének*** *nevezzük.*

Az a elem inverzének jelölése $\oplus$ típusú (ún. additív) műveleteknél $\ominus a$, és $\otimes$ típusú (multiplikatív) műveleteknél a^{-1}. Az additív típusú műveleteknél az inverzet ***ellentettnek*** is nevezzük. Az algebrai struktúrák behatóbb tanulmányozása során bebizonyítjuk, hogy ha egységelemes félcsoportban egy elemnek létezik bal és jobb oldali inverze, akkor azok megegyeznek, így az inverz egyértelmű.

3.23. definíció. *A* $(G;\oplus)$ *algebrai struktúrát* ***csoportnak*** *nevezzük, ha*

I. *a művelet asszociatív,*
II. *létezik semleges eleme,*
III. *minden elemnek létezik inverze.*

3.24. definíció. *Az* $(A;\oplus)$ *algebrai struktúrában a műveletet* ***kommutatívnak*** *nevezzük, ha* $a \oplus b = b \oplus a$ *minden* $a, b \in A$*-ra, azaz ha bármely két elem felcserélhető.*

A 4.13. tétel szerint kommutatív félcsoportban a többtényezős szorzatok függetlenek a tényezők sorrendjétől.

3.25. definíció. *A* $(G;\oplus)$ *csoportot* Abel-***csoportnak*** *nevezzük, ha művelete kommutatív.*

3.2. példa.

(1) Tetszőleges H halmazra a $(\wp(H);\cap)$ és az $(\{\text{igaz},\text{hamis}\};\wedge)$ algebrai struktúrák kommutatív egységelemes félcsoportok.

(2) A 3.2. ábrán látható algebrai struktúra kommutatív csoport, az ún. Klein-féle csoport.

Az algebrai struktúrák elméletében különösen használhatónak bizonyultak azok a struktúrák, amelyekben *két* kétváltozós belső művelet is van. Jelöljük ezeket a műveleteket sorrendben $\oplus$-szal és $\otimes$-rel.

3.26. definíció. *Ha az* $(A;\oplus,\otimes)$ *algebrai struktúra minden* $a, b, c \in A$ *elemére érvényes, hogy*

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c), \quad \textit{illetve}$$
$$(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c),$$

akkor azt mondjuk, hogy a struktúrában a $\otimes$ *művelet az* $\oplus$ *műveletre nézve* ***bal*** *illetve* ***jobb oldalról disztributiv****.*

Vegyük észre, hogy ha a $\otimes$ művelet kommutatív, akkor elegendő az egyik a fenti két tulajdonságból.

3.27. definíció. *Az* $(R;\oplus,\otimes)$ *algebrai struktúrát* ***gyűrűnek*** *nevezzük, ha*

I. $(R;\oplus)$ *kommutatív csoport,*
II. $(R;\otimes)$ *félcsoport,*
III. *érvényesek a disztributivitás törvényei.*

A $\oplus$-ra vonatkozó semleges elemet ***nullelemnek*** *vagy* ***zéruselemnek*** *nevezzük, és 0-val jelöljük. Ha létezik a $\otimes$ műveletre semleges elem, akkor ezt az elemet* ***egységelemnek****, a gyűrűt* ***egységelemes gyűrűnek*** *nevezzük. Az egységelemet 1-gyel vagy e-vel jelöljük.*

3.28. definíció. *Valamely $(R;\oplus,\otimes)$* ***gyűrűt kommutatívnak*** *nevezünk, ha benne a $\otimes$ művelet kommutatív.*

A gyűrűk disztributív tulajdonságából a nullelem különleges szerepe adódik:

$$(a = 0 \text{ vagy } b = 0) \Rightarrow a \otimes b = 0.$$

Ha például $b = 0$, akkor $a \otimes 0 = a \otimes (0 \oplus 0) = (a \otimes 0) \oplus (a \otimes 0)$, majd mindkét oldalhoz hozzáadva az $a \otimes 0$ elem $\oplus$ műveletre vett inverzét, adódik, hogy $a \otimes 0 = 0$. Bizonyos esetekben ennek megfordítása is igaz:

3.29. definíció. *Ha egy gyűrű bármely a, b elemére $a \otimes b = 0 \Rightarrow (a = 0$ vagy $b = 0)$, akkor a gyűrűt* ***nullosztómentesnek*** *nevezzük.*

Ellenkező esetben létezik olyan $a \neq 0$ és $b \neq 0$, amelyekre $a \otimes b = 0$. Ekkor a-t bal oldali, b-t jobb oldali ***nullosztónak,*** az a, b párt ***nullosztópárnak*** nevezzük. Nullosztómentes gyűrűben nem nulla elemmel való szorzásnál lehet jobbról is, balról is egyszerűsíteni, hiszen ha $a \otimes b = a \otimes c$, akkor $a \otimes (b \ominus c) = 0$, így $c = b$, és hasonlóan megy a jobb oldali szorzásnál is.

3.30. definíció. *A legalább két elemet tartalmazó nullósztómentes kommutatív gyűrűt* ***integritási tartománynak*** *nevezzük.*

Gyűrűre legegyszerűbb példa a ***nullgyűrű***, amely csak egyetlen elemet tartalmaz, ez nyilván 0. Másik példa lehet egy tetszőleges kommutatív csoport, amelyben egy új műveletet értelmezünk úgy, hogy a művelet eredménye minden esetben a 0 legyen. Ezeket a gyűrűket ***zérógyűrűknek*** nevezzük. Vegyük észre, hogy a zérógyűrű tetszőleges sok elemet tartalmazhat.

Ha $(R;\oplus,\otimes)$ legalább két elemú egységelemes gyűrű, akkor $0 \otimes a = 0 \neq 1$, ezért a $\otimes$ műveletre nézve inverz elemek csak $R \setminus \{0\}$-ban lehetnek.

3.31. definíció. *Az $(F;\oplus,\otimes)$ algebrai struktúrát* ***testnek*** *nevezzük, ha*

I. *$(F;\oplus,\otimes)$ gyűrű és*

II. *$(F \setminus \{0\};\otimes)$ kommutatív csoport.*

Ha II.*-ben lemondunk a kommutativitásról, akkor a struktúrát* ***ferdetestnek*** *nevezzük.*

Természetesen minden test egységelemes integritási tartomány.

3.3. példa. Tetszőleges H halmazra a $(\wp(H);\triangle,\cap)$ struktúra test. ($A \triangle$ a szimmetrikus differencia művelete, lásd a 2.1-6. gyakorlatot.)

3.2.2. Külső műveletek

A belső műveletek mellet az ún. külső műveletek is fontos algebrai struktúrákat eredményeznek. A nem üres A halmazhoz itt egy további halmaz, az ***operátortartomány*** csatlakozik. Az operátortartomány elemeit A elemeivel kapcsoljuk össze úgy, hogy ismét A egy elemét kapjuk. A művelet jeléül a $\circ$-t választjuk.

3.32. definíció. *Az A halmazon és az Ω operátortartományon a $\circ : \Omega \times A \to A$, $(\omega, a) \mapsto \omega \circ a$ $(\omega \in \Omega, a \in A)$ függvényt **külső műveletnek** nevezzük. A külső műveletet $(A, \Omega, \circ)$-rel jelöljük.*

Általában gyűrűket és testeket alkalmazunk mint operátortartományokat, és gyakran A-ra vonatkozó külső műveletről beszélünk.

3.33. definíció. *Legyen $(A; +)$ kommutatív csoport, $(\Omega; \oplus, \otimes)$ gyűrű, $(A, \Omega, \circ)$ pedig egy külső művelet. Ekkor A-t (bal oldali) Ω-**modulusnak** nevezzük, ha minden $a, b \in A$ és $\gamma, \delta \in \Omega$ esetén*

$$\begin{array}{lrcl} \text{I.} & \omega \circ (a + b) & = & (\omega \circ a) + (\omega \circ b) \\ \text{II.} & (\omega \oplus \mu) \circ a & = & (\omega \circ a) + (\mu \circ a) \\ \text{III.} & (\omega \otimes \mu) \circ a & = & \omega \circ (\mu \circ a). \end{array}$$

Az Ω-modulusok definíciója eltér az algebrai struktúrák „szokásos” definíciójától, hiszen az egyik „művelet” nem az Ω-modulus elemeire van értelmezve. De ha Ω minden ω eleméhez hozzárendeljük azt az f_ω egyváltozós műveletet, amelyre minden $a \in A$-ra $f_\omega(a) = \omega \circ a$, akkor az Ω-modulus immár (esetleg végtelen sok művelettel rendelkező) algebrai struktúrává válik.

A modulusok közül azok, amelyeknek operátortartománya test vagy ferdetest, különleges szerepet töltenek be a matematikában.

3.34. definíció. *Ha egy Ω-modulus operátortartománya test, akkor a modulust az Ω test feletti **vektortérnek** vagy **lineáris térnek** nevezzük.*

Az A halmaz elemeit ekkor ***vektoroknak***, Ω elemeit pedig ***skalároknak*** hívjuk.

Gyakorlatok

3.2-1. Bizonyítsuk be, hogy tetszőleges A nem üres halmaz esetén a
(1) $(\wp(A); \cup)$ struktúra kommutatív egységelemes félcsoport,
(2) $(\{\text{IGAZ,HAMIS}\}; \vee)$ struktúra kommutatív egységelemes félcsoport,
(3) $(\wp(A); \triangle)$ struktúra kommutatív csoport,
(4) $(\{\text{IGAZ,HAMIS}\}; \Leftrightarrow)$ struktúra kommutatív csoport.

3.2-2. Tetszőleges A nem üres halmaz esetén a $(\wp(A); \setminus)$ struktúrában milyen tulajdonságok évényesek?

3.2-3. Bizonyítsuk be, hogy ha az $(R; \oplus, \otimes)$ gyűrű legalább kételemű, akkor a nullelem és az egységelem mindig különbözőek.

3.2-4. Bizonyítsuk be, hogy az $(\{\text{IGAZ,HAMIS}\}; \Leftrightarrow, \vee)$ struktúra test.

3.3. Vegyes és származtatott struktúrák

Az alapstruktúrából álló vegyes struktúrákat ***többszörös struktúráknak*** nevezzük. Például algebrai struktúrák együtt léphetnek fel rendezési struktúrákkal. Számunkra a rendezett testek lesznek különösen fontosak. Amennyiben többszörös struktúrákat tekintünk, a struktúrák összekapcsolhatóságát külön feltételek szabályozzák.

3.35. definíció. *Az* $(R;\oplus,\otimes;\leq)$ *struktúrát* ***rendezett integritási tartománynak*** *nevezzük, ha* $(R;\oplus,\otimes)$ *integritási tartomány,* $(R;\leq)$ *(teljesen) rendezett, és*

(1) $x,y,z\in R$ *és* $x\leq y\Rightarrow x\oplus z\leq y\oplus z$ *(az „összeadás" monoton)*

(2) $x,y,z\in R$ *és* $z\geq 0$ *és* $x\leq y\Rightarrow x\otimes z\leq y\otimes z$ *(a „szorzás" monoton).*

Fontos lesz még az alábbi definíció is.

3.36. definíció. *Egy algebrai struktúrát* ***rendezett testnek*** *nevezünk, ha test, és rendezett integritási tartomány.*

Az alapstuktúrákból új struktúrák konstruálhatók. Ennek három lényegesen különböző módozata van.

a) ***Részstruktúra.*** Részstruktúra keletkezik, ha a struktúrára jellemző tulajdonságokat csak egy *részhalmazra* korlátozzuk. Ilyenek lehetnek: részcsoportok, részgyűrűk, vektorterek alterei, indukált részbenrendezések, stb.

b) ***Szorzatstruktúra.*** Szorzatstruktúra keletkezik, ha azonosan struktúrált halmazok Descartes-szorzatát tekintjük, az alapstruktúrákat komponensenként rendelve egymáshoz.

c) ***Hányadosstruktúra (faktorstruktúra).*** Hányadosstruktúra keletkezik, ha az A halmaz alapstruktúráját egy A-n értelmezett ρ ekvivalenciarelációval, a műveletek „összeférhetőségét" feltételezve az A/ρ hányadoshalmazra értelmezzük. Ilyenek például: faktorcsoport, faktorgyűrű. Grupoidoknál az összeférhetőség az alábbiakat jelenti:

3.37. definíció. *Legyen* $\odot$ *egy binér művelet az* A *halmazon, és legyen adott* A*-n egy* ρ *ekvivalenciareláció (vagy* A *egy osztályozása). A* $\odot$ ***művelet összeférhető*** *(idegen szóval kompatibilis)* ***az ekvivalenciarelációval*** *(vagy az osztályozással), ha*

$$a\rho b \text{ és } c\rho d \Rightarrow (a\odot c)\rho(b\odot d).$$

Több műveletet is tartalmazó algebrai struktúráknál összeférhetőség esetén az iménti tulajdonságnak minden egyes műveletre teljesülnie kell.

Tanulmányaink során bőven látunk példákat mindhárom említett konstrukcióra. Ízelítőül tekintsünk egy szorzatstruktúrát a rendezési struktúrák közül.

3.4. példa. Legyenek $(A;\leq_1)$ és $(B;\leq_2)$ részbenrendezett struktúra és legyen $A\times B$-ben $(a_1,b_1)\leq_3(a_2,b_2)$, ha $a_1\leq_1 a_2$ A-ban és $b_1\leq_2 b_2$ B-ben. Ekkor $(A\times B;\leq_3)$ is részbenrendezett struktúra, aminek a bizonyítását az Olvasóra bízzuk. Figyeljük meg, hogy $(A\times B;\leq_3)$ nem teljesen rendezett, még akkor sem, ha A és B is teljesen rendezettek. Az iménti $\leq_3$ rendezést definiáljuk másképp:

$$(a_1,b_1)\leq_4(a_2,b_2),\ \overset{\text{def}}{\Leftrightarrow}\ (a_1<_1 a_2)\vee(a_1=a_2\wedge b_1\leq_2 b_2).$$

Ekkor $(A \times B; \leq_4)$ újra egy részbenrendezés, amelynek a neve ***lexikografikus rendezés***. Ha A és B teljesen rendezett, illetve jólrendezett, akkor $A \times B$ is teljesen illetve jólrendezett.

3.5. példa. Legyen A a magyar ábécé betűinek halmaza, $<$ pedig a szokásos ábécésorrend $(a < á < b < \ldots)$. Ekkor $A \times A$-n a lexikografikus rendezés a kétbetűs „szavak" ábécérendbe szedését adja.

Függvények segítségével struktúrált halmazok *között* is létesíthetünk összefüggéseket. Lényeges szempont ugyanakkor, hogy a függvény mindkét struktúrával összeférjen. Ilyen, a struktúra szempontjából összeférő leképezéseket ***morfizmusoknak*** nevezzük. A struktúra lényeges jellegzetességei ekkor megőrződnek (például a csoport tulajdonság csoporthomomorfizmusoknál). Az algebrai struktúrák morfizmusait a XX. fejezetben tárgyaljuk. A számfogalom felépítésekor (kétműveletes algebrai struktúrák között) az alábbi fogalmat fogjuk felhasználni.

3.38. definíció. *Az* $(A; +, \cdot)$ *algebrai struktúrát* ***beágyazzuk*** *a* $(B; \oplus, \otimes)$ *algebrai struktúrába, ha megadható olyan* $C \subseteq B$ *halmaz és* $\varphi : A \to C$ *bijektív függvény, amely művelettartó, vagyis minden* $a, b \in A$ *esetén*

(1) $\varphi(a + b) = \varphi(a) \oplus \varphi(b)$

(2) $\varphi(a \cdot b) = \varphi(a) \otimes \varphi(b)$.

Ha tehát a definícióban szereplő C halmaz és φ függvény létezik, akkor a műveletek szempontjából C ugyanúgy viselkedik, mint A. Megjegyezzük, hogy a beágyazás tetszőleges, azonos műveletszámú algebrai struktúrák között is értelmezhető.

Gyakorlatok

3.3-1. Általánosítsuk a lexikografikus rendezést n darab részbenrendezett halmazra.

3.4. Egyéb konstrukciók: polinomok, mátrixok

3.4.1. Polinomok

A polinomok kiemelkedő szerepet játszanak a matematikában. Az XX. fejezetben részletesen foglalkozunk velük, most csak a polinomstruktúrák lényegesebb fogalmait emeljük ki.

3.39. definíció. *Az* $(R; +, \cdot)$ *gyűrű feletti* ***egyhatározatlanú polinomok*** *az*

$$f = a_0 + a_1 x + \cdots + a_n x^n \quad (a_i \in R,\ n \in \mathbb{N}) \tag{3.1}$$

alakú formális kifejezések azzal a megállapodással, hogy $n \leq m$ *esetén az* $a_0 + a_1 x + \cdots + a_n x^n$ *és a* $b_0 + b_1 x + \cdots + b_m x^m$ $(a_i, b_j \in R)$ *kifejezések pontosan akkor jelölik ugyanazt a polinomot, ha* $a_0 = b_0, a_1 = b_1, \ldots a_n = b_n$ *és* $b_{n+1} = \cdots = b_m = 0$.

(3.1)-ben az $a_0, a_1, \ldots, a_n \in R$ értékeket ***együtthatóknak*** nevezzük. Az R gyűrű feletti egyhatározatlanú polinomok halmazát R[x]-szel jelöljük, ahol x az ún. határozatlan. Nyilván x helyett más betű is szerepelhet. Az $f \in R[x]$ polinomra gyakran

használjuk az $f(x)$ jelölést.

3.40. definíció. *Egy* $f = a_0 + a_1x + \cdots + a_nx^n$ *polinomnak az* $r \in R$ *helyen felvett* ***helyettesítési értéke*** *az* $f(r) = a_0 + a_1r + \cdots + a_nr^n \in R$ *elem, ahol* r^i *alatt az* $\overbrace{r \cdot r \cdot \ldots \cdot r}^{i \text{ darab}}$ *szorzatot értjük. Ha* f *helyettesítési értéke az* r *helyen* 0*, akkor azt mondjuk, hogy* r *az* f ***gyöke*** *(vagy* ***zérushelye****). Azt a legnagyobb természetes* n *számot, amelyre* $a_n \neq 0$*, a* ***polinom fokának*** *nevezzük és* $\deg(f)$*-el vagy* $\operatorname{grad}(f)$*-el jelöljük. Ekkor* $a_n \in R$ *a polinom* ***főegyütthatója****. Ha* R *egységelemes, akkor azokat a polinomokat, amelyeknek a főegyütthatója* R *egységeleme,* ***főpolinomoknak*** *nevezzük. Az azonosan nulla polinom fokát a* $-\infty$ *szimbólumnak definiáljuk.*

A XX. fejezetben bebizonyítjuk, hogy tetszőleges R gyűrű esetén $R[x]$ a „polinomösszeadás" és „polinomszorzás" műveleteivel szintén gyűrűt alkot.

3.4.2. Mátrixok

Az előző részben már említettük az algebrai struktúrák morfizmusait. Vektortereknél a modulus-morfizmusok helyett ***lineáris leképezésekről*** beszélünk. Lineáris leképezések vizsgálata a ***lineáris algebra*** területéhez tartozik.

3.41. definíció. *Legyen* $(R; +, \cdot)$ *gyűrű,* $m, n \in \mathbb{N} \setminus \{0\}$*. Az*

$$A : \{1, \ldots, m\} \times \{1, \ldots, n\} \to R$$

függvényeket R*-feletti* $m \times n$*-es (olv. „emszer ennes")* ***mátrixoknak*** *nevezzük, ezen függvények halmazát* $R^{m \times n}$*-nel (olv. er ad em kereszt en) jelöljük.*

Egy mátrixot, mint véges halmazon értelmezett függvényt, táblázattal is megadhatunk:

$$A = [a_{ij}]_{\substack{1 \le i \le m \\ 1 \le j \le n}} = \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mn} \end{bmatrix} \in R^{m \times n}.$$

Ekkor az $(i, j) \in \{1, \ldots, m\} \times \{1, \ldots, n\}$ helyen felvett $A(i, j) \in R$ függvényérték szokásos jelölése a_{ij}. Mivel az a_{ij} függvényérték a táblázat i-edik sorának és j-edik oszlopának kereszteződésébe kerül, ezért a_{ij}-t az A mátrix i-edik sora j-edik elemének nevezzük.

Mátrixok között műveleteket értelmezhetünk.

3.42. definíció. *Az* $m \times n$*-es* $A = [a_{ij}]$ *és* $B = [b_{ij}]$ ***mátrixok összege*** *az* $m \times n$*-es* $C = [c_{ij}]$ *mátrix, ahol*

$$[c_{ij}] = [a_{ij}] \oplus [b_{ij}] = [a_{ij} + b_{ij}] \quad (1 \le i \le m, 1 \le j \le n).$$

$(R^{m \times n}; \oplus)$ neutrális eleme a ***zérusmátrix*** (vagy nullmátrix), melynek minden eleme 0. Erre a zérusmátrixra minden $A = [a_{ij}]$ mátrixnak létezik ellentettje, nevezetesen az a mátrix, amelynek i-edik sora j-edik eleme $-a_{ij}$. Vagyis ha $(R; +)$ Abel-csoport, akkor $(R^{m \times n}; \oplus)$ is az.

3.43. definíció. *Azt mondjuk, hogy az* $A \in R^{m\times n}$ *és* $B \in R^{k\times l}$ *mátrixok* ***kompatibilisek*** *(azaz ebben a sorrendben összeszorozhatók), ha* $n = k$*, vagyis ha* A *oszlopainak száma megegyezik* B *sorainak számával.*

3.44. definíció. *Legyen* $A = [a_{ij}]$ *egy* $m \times n$*-es,* $B = [b_{jk}]$ *pedig egy* $n \times p$ *típusú mátrix. Az* $m\times p$*-es* $C = [c_{ik}]$ *mátrixot az* A *és* B ***mátrixok szorzatának*** *nevezzük, ha*

$$[c_{ik}] = [a_{ij}] \otimes [b_{jk}] = [a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{in}b_{nk}]$$

minden $1 \le i \le m$ *és* $1 \le k \le p$ *esetén.*

A mátrixszorzás kompatibilis A, B, C mátrixok esetén asszociatív, vagyis

$$A \otimes (B \otimes C) = (A \otimes B) \otimes C.$$

A 3.4-1. gyakorlat annak bizonyítását kéri, hogy a mátrixszorzás disztributív. Kommutatívak természetesen csak az (n, n)-es mátrixok lehetnének, de az $n = 1$ esettől eltekintve általában nem azok. Például ha

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{és} \quad B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix},$$

akkor

$$A \otimes B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{és} \quad B \otimes A = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

3.45. definíció. *Az* $n \times n$*-es mátrixokat* ***négyzetes*** *(vagy kvadratikus)* ***mátrixoknak*** *nevezzük.*

Könnyű észrevenni, hogy az $(R^{n\times n}; \otimes)$ struktúra semleges eleme az

$$I_n = [\delta_{ik}], \quad \delta_{ik} = \begin{cases} 1 & \text{ha } i = k, \\ 0 & \text{egyébként} \end{cases}$$

egységmátrix. Az eddigieket összegezve az alábbi tételt bizonyítottuk.

3.46. tétel. *Ha* R *egységelemes gyűrű, akkor* $(R^{n\times n}; \oplus, \otimes)$ $(n \in \mathbb{N} \setminus \{0\})$ *szintén egységelemes gyűrűt alkot.*

3.6. példa. Mátrixok segítségével könnyen lehet az $A = \{a_1, a_2, \ldots, a_m\}$ és $B = \{b_1, b_2, \ldots, b_n\}$ halmazok közötti $\rho \subseteq A \times B$ binér relációt ábrázolni az alábbi módon: legyen $M_\rho = [m_{ij}]$, ahol

$$m_{ij} = \begin{cases} 1 & \text{ha } (a_i, b_j) \in \rho, \\ 0 & \text{ha } (a_i, b_j) \notin \rho. \end{cases}$$

Az M_ρ mátrixot ekkor a ρ ***reláció mátrixának*** nevezzük.

Mátrixokról bővebben az XX. fejezetben olvashatunk.

Gyakorlatok

3.4-1. Bizonyítsuk be, hogy kompatibilis A, B, C, D mátrixokra a mátrixszorzás disztributív művelet, vagyis

$$\begin{aligned} A \otimes (B \oplus C) &= (A \otimes B) \oplus (A \otimes C) \\ (B \oplus C) \otimes D &= (B \otimes D) \oplus (C \otimes D). \end{aligned}$$

Megjegyzések a fejezethez

A matematikai struktúrák jelentik a világ megismerésének, a természet jelenségeinek struktúrált vizsgálatához szükséges matematikai módszerek alapjait. Rendezési, algebrai és topológiai struktúrák nélkül csak jóval körülményesebben lehetne leírni és jellemezni mindazt, ami körülvesz minket, és mindazt, ami megfordul a fejünkben.

Ajánlott irodalom: Bálintné, Czédli, Szendrei [2], Birkhoff és Bartee [3], Gavrilov és Szapozsenko [14], Kalmár [21], valamint Tremblay és Mahonar [41].

4. A számfogalom felépítése

Ha a gyakorlati életben használt számokkal való számolást axiomatikusan szeretnénk megalapozni, akkor kiindulhatunk a legátfogóbb számtartományból, és részstruktúrák vizsgálatára szorítkozhatunk, vagy, mint az alábbiakban, a természetes számokkal lehet kezdeni, és fölépíjük alkalmas struktúrákat konstruálni.

4.1. Természetes számok

4.1.1. Peano-axiómák

A természetes számok halmazának első jellemzése Peano-tól származik. Axiómái kis módosítással a következők:

(1) $0 \in \mathbb{N}$. A nulla természetes szám.

(2) $\forall\, n\ (n \in \mathbb{N} \Rightarrow \exists!\ n' \in \mathbb{N})$. Minden n természetes számhoz egyértelműen létezik egy n' természetes szám, amelyet n ***rákövetkezőjének*** nevezünk.

(3) $\forall\, n\ (n \in \mathbb{N} \Rightarrow n' \neq 0)$. A 0 nem rákövetkezője egyetlen természetes számnak sem.

(4) $\forall\, n\ \forall\, m\ (n \in \mathbb{N} \wedge m \in \mathbb{N} \wedge n' = m' \Rightarrow n = m)$. Ha két természetes számnak ugyanaz a rákövetkezője, akkor egymással egyenlők.

(5) $\forall\ M\ (M \subseteq \mathbb{N} \wedge 0 \in M \wedge \forall\ n(n \in M \Rightarrow n' \in M) \Rightarrow M = \mathbb{N})$. Ha a természetes számok egy M részhalmaza tartalmazza a 0-át és minden természetes számmal együtt a rákövetkezőjét is, akkor $M = \mathbb{N}$.

Az 5. axiómára az alábbi ekvivalens megfogalmazás ismeretes:

(5′) $\forall\ P\ (P(0) \wedge \forall\ n(n \in \mathbb{N} \wedge P(n) \Rightarrow P(n')) \Rightarrow \forall\ n(n \in \mathbb{N} \Rightarrow P(n)))$. Valamely (a „megfelelő eszközökkel”, „megfelelőképpen megfogalmazott”) tulajdonság, amely a nullának és minden természetes számmal együtt a rákövetkezőjének is megvan, az összes természetes számra teljesül. Ezt az axiómát a ***teljes indukció*** elvének nevezzük.

4.1. tétel. *Ha* $n \in \mathbb{N}$, *akkor* $n' \neq n$.

Bizonyítás. Tekintsük az $M = \{n \in \mathbb{N}\ :\ n' \neq n\}$ halmazt. (3) szerint M tartalmazza a 0-t, továbbá, ha tartalmazza n-et, akkor n'-t is, mert (4) miatt $(n')' = n'$-ből $n' = n$ következne. Ekkor viszont (5) miatt $M = \mathbb{N}$. □

4.2. tétel. *Minden* $0 \neq n \in \mathbb{N}$*-hez egyértelműen létezik olyan* $m \in \mathbb{N}$*, amelyre* $m' = n$.

Bizonyítás. Az egyértelműség a negyedik Peano-axiómából következik. A létezést teljes indukcióval bizonyítjuk. Tekintsük az

$$M = \{0\} \cup \{n \in \mathbb{N} \ : \ \text{van olyan } m \in \mathbb{N}, \text{ amelyre } m' = n\}$$

halmazt. Ekkor $0 \in M$, és ha $n \in M$, akkor $n' = (m')' \in M$, így (5) miatt $M = \mathbb{N}$. □

A 4.1. és 4.2. tételek miatt a rákövetkezési relációval a 0 alapfogalomból a többi természetes számot explicit módon lehet definiálni:

4.3. definíció. $1 \overset{\text{def}}{\Leftrightarrow} 0'$, $2 \overset{\text{def}}{\Leftrightarrow} 1'$, $3 \overset{\text{def}}{\Leftrightarrow} 2'$ ....

Az így konstruált halmazt a ***természetes számok halmazának*** nevezzük és $\mathbb{N}$-el jelöljük. Két kérdés merül fel. Az egyik, hogy az axiómák egyértelműen meghatározzák-e $\mathbb{N}$-et, a másik, hogy létezik-e $\mathbb{N}$ egyáltalán. Megmutatható, hogy az axiomatikus halmazelmélet végtelenségi axiómája által definiált halmaz teljesíti a Peano-axiómákat. Az első kérdésre is igenlő a válasz, ami az alábbi, bizonyítás nélkül közölt fontos tétel felhasználásával látható be. A tétel $\mathbb{N}$-en értelmezett függvények ***rekurzióval*** való definíciójának módszerét tárgyalja.

4.4. tétel (rekurziótétel). *Legyen* A *egy halmaz,* $a \in A$*, és* $f : A \to A$ *egy tetszőleges függvény. Ekkor a* Peano*-axiómák teljesülése esetén egyértelműen létezik olyan* $g : \mathbb{N} \to A$ *függvény, amelyre* $g(0) = a$*, és* $g(n') = f(g(n))$ *minden* $n \in \mathbb{N}$ *esetén.* □

A teljes indukció kitüntetett szerepet játszik a matematikában. Az alábbiakban egy halmazelméleti problémát oldunk meg a segítségével.

4.1. példa. Legyenek $A_1, A_2, \ldots, A_n$ tetszőleges halmazok, $n \geq 2$. Megmutatjuk, hogy

$$\overline{\left(\bigcup_{i=1}^{n} A_i\right)} = \bigcap_{i=1}^{n} \overline{A_i}.$$

Teljes indukcióval bizonyítunk. Az $n = 2$ eset a már látott De Morgan szabály. Tegyük fel, hogy $2 < k < n$-re igaz az állítás (indukciós feltétel). Bebizonyítjuk, hogy ekkor $k+1$-re is igaz:

$$\begin{aligned}
\overline{\left(\bigcup_{i=1}^{k+1} A_i\right)} &= \overline{A_1 \cup A_2 \cup \cdots \cup A_k \cup A_{k+1}} \\
&= \overline{(A_1 \cup A_2 \cup \cdots \cup A_k) \cup A_{k+1}} \\
&= \overline{A_1 \cup A_2 \cup \cdots \cup A_k} \cap \overline{A_{k+1}} \\
&= \left(\bigcap_{i=1}^{k} \overline{A_i}\right) \cap \overline{A_{k+1}} \\
&= \bigcap_{i=1}^{k+1} \overline{A_i}.
\end{aligned}$$

A levezetés során először a művelet asszociativitását, majd a két halmazra vonatkozó De Morgan szabályt, végül pedig az indukciós feltételt használtuk.

4.1.2. Műveletek természetes számokkal

Az összeadás és szorzás számolási műveleteit nem vontuk be az axiómarendszerbe, ezeket induktív módon definiáljuk.

Összeadás
A rekurziótétel alapján minden $m \in \mathbb{N}$-re létezik olyan $s_m : \mathbb{N} \to \mathbb{N}$ függvény, amelyre $s_m(0) = m$, és minden $n \in \mathbb{N}$-re $s_m(n') = (s_m(n))'$. Az $s_m(n)$ számot $m + n$-el fogjuk jelölni, és az m és n természetes számok ***összegének*** nevezzük. Megjegyezzük, hogy az összeadásból visszakapjuk a rákövetkezést, hiszen $m' = (s_m(0))' = s_m(0') = s_m(1) = m + 1$.

4.5. tétel. *Ha* $k, m, n \in \mathbb{N}$, *akkor*
(1) $(k + m) + n = k + (m + n)$ *(asszociativitás);*
(2) $0 + n = n + 0 = n$*;*
(3) $m + n = n + m$ *(kommutativitás).*

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

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

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

$$\begin{aligned}(k + m) + n' &= s_k(m) + n' = (s_k(m) + n)' \\ &= ((k + m) + n)' = (k + (m + n))' \quad \text{(az indukciós feltevés miatt)} \\ &= (k + s_m(n))' = (k + s_m(n')) = (k + s_m(n')) \\ &= k + (m + n').\end{aligned}$$

(2) bizonyítása n szerinti indukcióval történik. $0 + n = n$ az $n = 0$ esetben nyilvánvaló. Tegyük fel, hogy $n \in \mathbb{N}$-re igaz az állítás. Ekkor $0 + n' = (0 + n)' = n'$, így az állítás minden $n \in \mathbb{N}$-re teljesül. Az $n + 0 = n$ egyenlőség az összeadás definíciójából következik. A kommutativitást két darab indukcióval bizonyítjuk. Először belátjuk, hogy rögzített $m \in \mathbb{N}$ esetén $m' + n = (m + n)'$ minden $n \in \mathbb{N}$-re. n szerinti indukcióval dolgozunk. Az $n = 0$ eset $m' + 0 = m' = (m + 0)'$ miatt teljesül. Tegyük fel, hogy $m' + n = (m + n)'$ valamilyen $n \in \mathbb{N}$-re. Ekkor

$$m' + n' = (m' + n)' = \big((m + n)'\big)' = (m + n')',$$

vagyis az állítás minden $n \in \mathbb{N}$-re igaz. Most megmutatjuk, hogy $m + n = n + m$ minden $n \in \mathbb{N}$-re. Az $n = 0$ eset nyilvánvaló. Indukcióval bizonyítva tegyük fel, hogy valamilyen $n \in \mathbb{N}$-re igaz az állítás. Ekkor

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

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

Szorzás
A rekurziótétel alapján minden $n \in \mathbb{N}$-re létezik olyan $p_m : \mathbb{N} \to \mathbb{N}$ függvény, amelyre $p_m(0) = 0$ és minden $n \in \mathbb{N}$-re $p_m(n') = p_m(n)+m$. A $p_m(n)$ számot $m \cdot n$-nel, vagy gyakran a rövidebb mn-nel jelöljük, és az m és n számok ***szorzatának*** nevezzük. A szorzat definíciója miatt $1 \cdot 1 = p_1(1) = p_1(0') = p_1(0) + 1 = 1$.

4.6. tétel. *Ha* $k, m, n \in \mathbb{N}$*, akkor*
(1) $k \cdot (m + n) = k \cdot m + k \cdot n$ (disztributivitás)
(2) $(k \cdot m) \cdot n = k \cdot (m \cdot n)$ (asszociativitás)
(3) $0 \cdot n = n \cdot 0 = 0$
(4) $1 \cdot n = n \cdot 1 = n$
(5) $m \cdot n = n \cdot m$ (kommutativitás)

Bizonyítás. Először a disztributivitást bizonyítjuk, amihez n szerinti indukciót használunk. $n = 0$-ra

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

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

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

Az asszociativitást n szerinti indukcióval bizonyítjuk. $n = 0$-ra $(k \cdot m) \cdot 0 = 0 = k \cdot 0 = k \cdot (m \cdot 0)$. Tegyük fel, hogy $n \in \mathbb{N}$-re igaz az állítás. Ekkor

$$\begin{aligned} (k \cdot m) \cdot n' &= p_k(m) \cdot (n + 1) = p_k(m) \cdot n + p_k(m) \\ &= (k \cdot m) \cdot n + k \cdot m = k \cdot (m \cdot n) + k \cdot m = k \cdot (m \cdot n + m) \\ &= k \cdot p_m(n') = k \cdot (m \cdot n'). \end{aligned}$$

(3) 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 valamely $n \in \mathbb{N}$-re $0 \cdot n = 0$. Ekkor

$$0 \cdot n' = p_0(n') = p_0(n) + 0 = 0 \cdot n + 0 = 0.$$

A következőkben bebizonyítjuk, hogy

$$m' \cdot n = m \cdot n + n \tag{4.1}$$

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

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

(4) bizonyítása n szerinti indukcióval történik. Az $n = 0$ eset (3) miatt teljesül. Tegyük fel, hogy $n \in \mathbb{N}$-re $1 \cdot n = n$. Ekkor

$$1 \cdot n' = p_1(n') = p_1(n) + 1 = 1 \cdot n + 1 = n + 1 = n'.$$

Hasonlóan, tegyük fel, hogy $n \cdot 1 = n$ valamilyen $n \in \mathbb{N}$-re. Ekkor (4.1) miatt

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

Az $m \cdot n = n \cdot m$ kommutativitás bizonyítása n szerinti indukcióval történik. Az $n = 0$ eset (3) miatt teljesül. Tegyük fel, hogy $n \in \mathbb{N}$-re igaz az állítás. Ekkor (4.1)-et felhasználva

$$m \cdot n' = m \cdot n + m = n \cdot m + m = n' \cdot m.$$

□

Az előző két tétel azt mutatja, hogy $(\mathbb{N}; +)$ kommutatív félcsoport a 0 nullelemmel, és $(\mathbb{N}; \cdot)$ is kommutatív félcsoport az 1 egységelemmel.

A természetes számok rendezési struktúrája

4.7. definíció. $n \leq m \overset{\text{def}}{\Leftrightarrow} \exists\, k \in \mathbb{N} \,:\, n + k = m.$

Belátható, hogy $(\mathbb{N}; \leq)$ teljes rendezés, sőt, jólrendezés. Mi, Peano-val ellentétben 1 helyett a 0-t választottuk legkisebb számnak. $(\mathbb{N}; \leq)$ jólrendezése miatt $0 < 1$, $n < n'$, és használhatjuk azokat a kifejezésmódokat, hogy „ az $n + 1$ szám 1-gyel nagyobb n-nél," „az $n + k$ szám k-val nagyobb n-nél", továbbá, mivel $\mathbb{N}$-nek nincs felső korlátja, „bármilyen nagy természetes szám van", vagyis „akármeddig el lehet számolni."

A rendezési struktúra az összeadással és a szorzással adott algebrai struktúrával összefér abban az értelemben, hogy érvényesek a

4.8. tétel (monotonia tételei).

$$\begin{aligned} n \leq m &\quad\Leftrightarrow\quad n + k \leq m + k, \\ n \leq m \text{ \textit{és} } k \neq 0 &\quad\Leftrightarrow\quad n \cdot k \leq m \cdot k. \end{aligned}$$

Bizonyítás. Ha $n \leq m$, akkor létezik olyan $s \in \mathbb{N}$, hogy $n + s = m$, így $n + s + k = m + k$ minden $k \in \mathbb{N}$-re, vagyis a 4.7. definíció miatt $n + k \leq m + k$. Megfordítva, ha $n + k \leq m + k$ minden $k \in \mathbb{N}$-re, akkor nyilván $k = 0$-ra is igaz, vagyis $n \leq m$. A szorzásra vonatkozó ekvivalencia bizonyítását az Olvasóra hagyjuk. □

A tétel egyenlőségre vonatkozó állításai az alábbi

4.9. tétel (egyszerűsítési szabályok).

$$\begin{aligned} n + k = m + k &\quad\Rightarrow\quad n = m, \\ n \cdot k = m \cdot k \text{ \textit{és} } k \neq 0 &\quad\Rightarrow\quad n = m. \end{aligned}$$

Észrevehetjük, hogy ha egy halmaz tartalmaz egy k természetes számot, és minden természetes számmal együtt a rákövetkezőjét is, akkor a teljes indukció miatt tartalmaz minden $n \geq k$ természetes számot.

A 4.7. definícióból az $n + x = m$ egyenlet megoldhatósága is következik, feltéve, hogy $n \leq m$ érvényes. Ezt az egyértelműen meghatározott megoldást m és n ***különbségének*** nevezzük, és úgy írjuk, hogy $x = m - n$.

Sorozatok, összegek, szorzatok

4.10. definíció. *Azokat a leképezéseket, amelynek az értelmezési tartománya a természetes számok $\mathbb{N}$ halmaza,* ***sorozatnak*** *nevezünk.*

A sorozat tehát egy olyan indexelt rendszer, ahol az indexhalmaz a természetes számok halmaza. Ha $\mathbb{N}^+$-szal jelöljük az $\mathbb{N} \setminus \{0\}$ halmazt, sorozatokat $\mathbb{N}^+$-on is értelmezhetünk. Ilyenkor a sorozatnak nincs nulladik eleme, csak első, második, stb.

4.2. példa. A sorozat fogalma nagyon lényeges a számítástudományban, ahol gyakran listaként vagy lineáris tömbként értelmezzük őket. Például egy V lineáris tömb (vagy vektor) pozíciók (tárhelyek) sorozatának is tekinthető, ahol az n-edik pozícióban lévő elemet $V[n]$ jelöli.

Legyen $(G;+)$ csoport, $a : \mathbb{N} \to G$ egy sorozat. Mivel $\mathbb{N}$ jólrendezett, az $(a_0, a_1, \ldots)$ sorozatra ***összeget*** definiálhatunk.

4.11. definíció.

$$\sum_{i=m}^{n} a_i \overset{\text{def}}{\Leftrightarrow} \begin{cases} a_m + a_{m+1} + \ldots + a_{n-1} + a_n, & \text{ha } m \leq n, \\ 0, & \text{ha } n = m-1, \\ -a_{n+1} - a_{n+2} - \ldots - a_{m-1}, & \text{ha } n < m-1. \end{cases}$$

Ugyanez a gondolat alkalmazható a $(G;\cdot)$ csoport esetén is. Ilyenkor a ***szorzat*** definíciója

4.12. definíció.

$$\prod_{i=m}^{n} a_i \overset{\text{def}}{\Leftrightarrow} \begin{cases} a_m \cdot a_{m+1} \cdots a_{n-1} \cdot a_n, & \text{ha } m \leq n, \\ 1, & \text{ha } n = m-1, \\ (a_{n+1} \cdot a_{n+2} \cdot \ldots \cdot a_{m-1})^{-1}, & \text{ha } n =< m-1. \end{cases}$$

Ha az összeg minden ***tagja*** ugyanaz az $a \in G$ szám, a szokásos jelölés szerint $\sum_{i=m}^{m+n-1} a = na$. Hasonlóan, ha a szorzat minden ***tényezője*** ugyanaz az $a \in G$ szám, akkor ezt úgy jelöljük, hogy $\prod_{i=m}^{m+n-1} a = a^n$. Az összegek esetében ***additív írásmódról***, a szorzatok esetében ***multiplikatív írásmódról*** beszélünk. Megjegyezzük, hogy amennyiben $m \leq n$, az összeg és a szorzat tetszőleges félcsoportban értelmezhető. Az összegek és szorzatok jóldefiniáltságához szükséges még, hogy a műveletek asszociativitása *akárhány* elemre érvényes legyen. Azt is megvizsgáljuk, hogy a kommutativitás és disztributivitás akárhány elemre érvényes-e. A tételt a lehető legáltalánosabban fogalmazzuk meg.

4.13. tétel (általános asszociativitás, kommutativitás és disztributivitás tétele).
(1) *Tetszőleges* $(A;\cdot)$ *félcsoport bármely* $a_1, a_2, \dots, a_k$ $(k \in \mathbb{N}^+)$ *elemeire az* $a_1 a_2 \cdots a_k$ *szorzat független attól, hogy milyen (szabályos) zárójelezéssel végezzük el a műveletet.*
(2) *Kommutatív félcsoportban a többtényezős szorzatok nem függnek a tényezők sorrendjétől.*
(3) *Tetszőleges* $(R;+,\cdot)$ *gyűrű bármely* $a_1, \dots, a_m, b_1, \dots, b_n, \dots, z_1, \dots, z_t \in R$ *elemeire*

$$(a_1 + \cdots + a_m)(b_1 + \cdots + b_n)\cdots(z_1 + \cdots + z_t) = \sum_{i=1}^{m}\sum_{j=1}^{n}\cdots\sum_{l=1}^{t} a_i b_j \cdots z_l.$$

Bizonyítás. (1) bizonyítása k szerinti teljes indukcióval történik. A bizonyítás során $\langle a_1 \dots a_k\rangle$ jelentse azt, hogy „az $a_1 \dots a_k$ szorzat valamilyen zárójelezéssel". A $k = 1, 2$ esetben nincs szerepe a zárójelezésnek, a $k = 3$ eset pedig a félcsoport asszociativitása miatt nyilván igaz. Legyen $k \geq 4$, és tegyük fel, hogy az állítás k-nál kevesebb tényezős szorzatokra igaz. Bebizonyítjuk, hogy

$$\langle a_1 \dots a_k\rangle = \big(\dots((a_1 a_2)a_3)a_4 \dots\big)a_k.$$

A $\langle a_1 \dots a_k\rangle$ kifejezésben van egy legutolsó szorzás, mondjuk

$$\langle a_1 \dots a_k\rangle = \langle a_1 \dots a_i\rangle\langle a_{i+1} \dots a_k\rangle \quad (1 \leq i \leq k-1).$$

Először a második tényezőre az indukciós feltevést, majd az asszociativitást, végül újra az indukciós feltevést alkalmazva

$$\begin{aligned}\langle a_1 \dots a_k\rangle &= \langle a_1 \dots a_i\rangle\langle a_{i+1} \dots a_k\rangle \\ &= \overbrace{\langle a_1 \dots a_i\rangle}\big(\overbrace{(\dots(a_{i+1}a_{i+2})a_{i+3}\dots)}\overbrace{a_k}\big) \\ &= \langle a_1 \dots a_{k-1}\rangle a_k \\ &= \big(\dots((a_1 a_2)a_3)a_4 \dots\big)a_k.\end{aligned}$$

Ha $i = k-1$, akkor a második lépés szükségtelen, így az első sor jobb oldala és a harmadik sor azonos. Azt kaptuk, hogy bármely félcsopotban a többtényezős szorzatok zárójelek nélkül írhatók. (2) bizonyítása: ha az $a_1 \dots a_k$ elemekből képzett bármely k-tényezős szorzatban két szomszédos elemet felcserélünk, a két elemre vonatkozó kommutativitás miatt a szorzat értéke nem változik. Szomszédos elemek felcserélgetésével pedig az $a_1 \dots a_k$ szorzatból kiindulva a tényezők tetszőleges sorrendje véges sok lépésben elérhető. A bizonyításban az asszociativitást teljes mértékben kihasználtuk. (3) bizonyítása többlépéses teljes indukcióval történik, a technikai részleteket mellőzzük. □

Gyakorlatok

4.1-1. Bizonyítsuk be, hogy $(\mathbb{N};\leq)$ gyengén trichotom teljes rendezés.
4.1-2. Bizonyítsuk be, hogy $(\mathbb{N};<)$ jólrendezés.
4.1-3. Bizonyítsuk be, hogy $\forall\, n\ (n \in \mathbb{N} \Rightarrow 3\sum_{k=1}^{n} k(k+1) = n(n+1)(n+2))$.
4.1-4.* Bizonyítsuk be az általános disztributivitás tételét.

4.2. Egész számok

Az összeadás és a szorzás inverz művelete $\mathbb{N}$-ben általában nem értelmezhető. Az iménti alfejezetben definiált kivonásnak mint az összeadás inverz műveletének korlátlan végrehajthatóságához a „negatív számok” hozzákapcsolásával juthatunk el, más szóhasználattal élve $\mathbb{N}$-et az egész számok gyűrűjébe ágyazzuk.

4.2.1. Konstrukció

Rögzített $m, n \in \mathbb{N}$, $m \leq n$ esetén végtelen sok olyan számpár van $\mathbb{N}\times\mathbb{N}$-en, amelyek különbsége $n - m$. Ha $n_1 - m_1 = n_2 - m_2$, akkor $n_1 + m_2 = n_2 + m_1$ is teljesül. Ez az alábbi ρ relációt sugallja $\mathbb{N} \times \mathbb{N}$-en:

$$(n_1, m_1)\rho(n_2, m_2) \overset{\text{def}}{\Leftrightarrow} n_1 + m_2 = n_2 + m_1.$$

Könnyen belátható, hogy ρ ekvivalenciareláció, ezért osztályoz. Az ekvivalenciaosztályokat egy párnak szögletes zárójelek közötti megadásával írjuk fel.

4.3. példa. $(3, 8) \in [(1, 6)]$, mivel $(3, 8)\rho(1, 6)$.

4.14. definíció. $\mathbb{Z} \overset{\text{def}}{\Leftrightarrow} (\mathbb{N} \times \mathbb{N})/\rho = \{[n, m] \mid (n, m) \in \mathbb{N} \times \mathbb{N}\}$.

4.2.2. Műveletek, rendezésük

$\mathbb{Z}$ algebrai struktúráját az alábbi műveletekkel definiáljuk:

4.15. definíció.

$$\begin{aligned} [(n, m)] + [(k, l)] &\overset{\text{def}}{\Leftrightarrow} [(n + k, m + l)], \\ [(n, m)] \cdot [(k, l)] &\overset{\text{def}}{\Leftrightarrow} [(nk + ml, nl + mk)]. \end{aligned}$$

Az így definiált műveletek kommutativitása, asszociativitása és disztributivitása az $\mathbb{N}$-ben érvényes műveletek tulajdonságai alapján könnyen belátható. Ennél több is igaz: az $[(n, m)] + x = [(k, l)]$ egyenlet tetszőleges $[(n, m)]$ és $[(k, l)]$ esetén egyértelműen megoldható, a megoldás a (4.15) definíció és ρ definíciója, valamint a 4.9. tétel miatt $x = [(k+m, n+l)]$. Az összeadás műveletét tekintve az egyenlet megoldhatósága garantálja egy semleges elem ($[(0, 0)]$) és erre az elemre vonatkozó inverz elemek létezését. Ezzel pedig gyűrűt konstruáltunk. Fennmarad a kérdés, hogy $\mathbb{N}$-et valóban beágyaztuk-e $\mathbb{Z}$-be.

$\mathbb{Z}$ konstrukcióját alaposan szemügyre véve kézenfekvőnek tűnik a $\varphi : \mathbb{N} \to \mathbb{Z}$, $\varphi(n) = [(n, 0)]$ leképezés vizsgálata. Ekkor

$$\varphi(n + m) = [(n + m, 0)] = [(n, 0)] + [(m, 0)] = \varphi(n) + \varphi(m),$$

továbbá

$$\varphi(nm) = [nm, 0] = [(n, 0)] \cdot [(m, 0)] = \varphi(n) \cdot \varphi(m).$$

Ha $\varphi(n) = \varphi(m)$, akkor $[(n,0)] = [(m,0)]$, így a 4.14. definíció miatt $n = m$, vagyis φ injektív.

A továbbiakban 0-t írunk $[(0,0)]$ helyett, 1-et írunk $[(1,0)]$ helyett, és általánosan a-t írunk az $[(a,0)]$ osztály helyett. A beágyazás következtében az $\mathbb{N}$-beli műveletekre vonatkozó egyszerűsítési szabályok minden további nélkül működnek $\mathbb{Z}$-ben is. Mivel $\mathbb{Z}$ egységelemes, és a szorzásra vonatkozó egyszerűsítési szabály miatt nullosztómenes, ezért az alábbi tételt bizonyítottuk.

4.16. tétel. *$\mathbb{Z}$ integritási tartomány.* □

A természetes számokkal ellentétben $\mathbb{Z}$-ben minden számnak nemcsak rákövetkezője, hanem „megelőzője" is van. $\mathbb{Z}$-t $\mathbb{N}$-hez hasonlóan lehet rendezni.

4.17. definíció. $a \leq b \overset{\text{def}}{\Leftrightarrow} b - a \in \mathbb{N}$.

Ez a rendezés teljes, de nem jólrendezés. Könnyű megmutatni, hogy a beágyazás során definiált φ függvény rendezéstartó is, vagyis ha $a \leq b$ $\mathbb{N}$-ben, akkor $\varphi(a) \leq \varphi(b)$ $\mathbb{Z}$-ben. $\mathbb{Z}$-t a HASSE-diagramja alapján számegyenesen lehet ábrázolni. A nullánál kisebb számokat negatív egész számoknak, a nagyobbakat pozitív egész számoknak nevezzük, és $\mathbb{Z}^-$-szal illetve $\mathbb{Z}^+$-szal jelöljük. Ha a 0-t is beleértjük, a szokásos jelölés $\mathbb{Z}_0^-$ és $\mathbb{Z}_0^+$. Az eddigiek alapján tehát kijelenthetjük, hogy $\mathbb{N} = \mathbb{Z}_0^+$.

$\mathbb{Z}$-ben tehát az összeadást, kivonást és a szorzást korlátozás nélkül el lehet végezni. A számolási szabályok formalizálásához, amelyben a $\mathbb{Z}$-ben való számolást az $\mathbb{N}$-ben való számolásra vezetjük vissza, előnyösen használhatjuk az „ellentett előjelű szám" és az „abszolút érték" fogalmát. $0-a$ helyett $-a$-t írunk, az a és $-a$ számokat egymás ***ellentettjeinek*** nevezzük. A kettő közül az egyik mindig természetes szám, ezt a ***abszolút értékének*** nevezzük, és $|a|$-kel jelöljük.

A 4.2-1. gyakorlat a $\mathbb{Z}$-beli „szokásos" számolási szabályokat sorolja fel. A gyakorlat (7)–(8) állításai a $\mathbb{Z}$-beli műveletek monotonitását jelentik, ezért a 3.35. definíciónak megfelelően azt is mondhatjuk, hogy $(\mathbb{Z}; +, \cdot; \leq)$ ***rendezett integritási tartomány.***

4.4. példa. Tekintsük a $\mathbb{Z}$ feletti $A = \begin{bmatrix} 2 & 1 \\ 3 & -2 \end{bmatrix}$ és $B = \begin{bmatrix} 1 & -1 \\ 2 & -3 \end{bmatrix}$ mátrixokat. Ekkor $A \otimes B = \begin{bmatrix} 4 & -5 \\ -1 & 3 \end{bmatrix}$, $B \otimes A = \begin{bmatrix} -1 & 3 \\ -5 & 8 \end{bmatrix}$, ami azt mutatja, hogy a mátrixszorzás nem kommutatív (pedig a szorzás kommutatív $\mathbb{Z}$-ben).

Gyakorlatok

4.2-1. Bizonyítsuk be a $\mathbb{Z}$ elemeire vonatkozó alábbi állításokat:

(1) $a \in \mathbb{Z}^+ \wedge b \in \mathbb{Z}^- \wedge |a| \geq |b| \Rightarrow a + b = |a| - |b|$
(2) $a \in \mathbb{Z}^+ \wedge b \in \mathbb{Z}^- \wedge |a| \leq |b| \Rightarrow a + b = -(|b| - |a|)$
(3) $a \in \mathbb{Z}^- \wedge b \in \mathbb{Z}^- \Rightarrow a + b = -(|a| + |b|)$
(4) $a \in \mathbb{Z} \wedge b \in \mathbb{Z} \Rightarrow a - b = a + (-b)$
(5) $a \in \mathbb{Z}^+ \wedge b \in \mathbb{Z}^- \Rightarrow ab = -|a| \cdot |b|$
(6) $a \in \mathbb{Z}^- \wedge b \in \mathbb{Z}^- \Rightarrow ab = |a| \cdot |b|$
(7) $a, b, c \in \mathbb{Z} \wedge a \leq b \Rightarrow a + c \leq b + c$

(8) $a, b \in \mathbb{Z}_0^+ \Rightarrow a \cdot b \in \mathbb{Z}_0^+$
(9) $a < b \wedge c \in \mathbb{Z}^+ \Rightarrow ac < bc$
(10) $a < b \wedge c \in \mathbb{Z}^- \Rightarrow ac > bc$
(11) $a \neq 0 \Rightarrow a^2 \in \mathbb{Z}^+$.

4.2-2. Az előző fejezetben megmutattuk, hogy minden jólrendezett halmaz lánc. Bizonyítsuk be, hogy az állítás megfordítása nem igaz.

4.3. Racionális számok

Az egész számok körében a szorzás invertálhatóságára vonatkozó kérdés a $bx = a$ egyenlet megoldhatóságát jelenti tetszőleges $a, b \in \mathbb{Z}$ esetén. Ha létezik megoldás, akkor ezt az a és b ***hányadosának*** nevezzük, és a/b-vel jelöljük. Ilyen ***osztást*** $\mathbb{Z}$-ben általában nem lehet végrehajtani. Ezért olyan struktúrát keresünk, amelyben az osztás „korlátozás nélkül" elvégezhető, és amelyben a $\mathbb{Z}$-ben megismert tulajdonságok érvényben maradnak. Ezt ismét egy beágyazással érjük el.

A 0 számnak mindenesetre kitüntetett szerepe van, hiszen $\forall\, c\ (c \in \mathbb{Z} \Rightarrow c \cdot 0 = 0)$. A $0x = a$ egyenletet $a = 0$ esetén nem lehet $\mathbb{Z}$-ben egyértelműen megoldani, sőt, $a \neq 0$ esetén egyáltalán nem lehet megoldani. Ezért célszerű, hogy a bővített halmazban a $bx = a$ megoldhatóságát csak $b \neq 0$-ra követeljük meg.

4.3.1. Konstrukció

A $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ párok halmazán vezessünk be egy ϑ ekvivalenciarelációt. Most azt vesszük figyelembe, hogy az osztás elvégezhetősége esetén $a_1/b_1 = a_2/b_2$-ből $a_1 b_2 = a_2 b_1$ következik.

$$(a_1, b_1)\vartheta(a_2, b_2) \overset{\text{def}}{\Leftrightarrow} a_1 b_2 = a_2 b_1.$$

Könnyű belátni, hogy ϑ valóban ekvivalenciareláció. Jelöljük $\mathbb{Q}$-val az ekvivalenciaosztályok halmazát.

4.18. definíció. $\mathbb{Q} \overset{\text{def}}{\Leftrightarrow} (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/\vartheta = \{[(a, b)] \mid (a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\}$.

$\mathbb{Q}$ elemeit ***racionális számoknak*** nevezzük.

4.3.2. Műveletek, rendezésük

Szem előtt tartva, hogy a racionális számokkal való számoláskor a törtekkel való szokásos számolási szabályoknak kell teljesülnie, célszerűnek tűnik az összeadás és szorzás alábbi definíciója.

4.19. definíció.

$$[(a, b)] + [(c, d)] \overset{\text{def}}{\Leftrightarrow} [(ad + bc, bd)],$$
$$[(a, b)] \cdot [(c, d)] \overset{\text{def}}{\Leftrightarrow} [(ac, bd)].$$

Könnyű belátni, hogy $(\mathbb{Q}; +)$ kommutatív csoport a $[(0, 1)]$ semleges elemmel, továbbá az $[(a, b)]$-hez tartozó, az összeadásra vonatkozó inverz elem $-[(a, b)] =$

$[(-a,b)]$. A $(\mathbb{Q}\setminus\{[(0,1)]\};\cdot)$ kommutatív csoport az $[(1,1)]$ semleges elemmel. $a\neq 0$ esetén az $[(a,b)]$-hez tartozó, a szorzásra vonatkozó inverz elem (*reciprok*) $[(a,b)]^{-1}=[(b,a)]$. Azt is könnyű belátni, hogy a két műveletet összekapcsoló disztributiv törvények is igazak, ezért $(\mathbb{Q};+,\cdot)$ ***test***.

Meg kell még vizsgálnunk, hogy $\mathbb{Z}$-t valóban beágyaztuk-e $\mathbb{Q}$-ba. Tekintsük a $\varphi:\mathbb{Z}\to\mathbb{Q}$, $\varphi(a)=[(a,1)]$ függvényt. Ekkor

$$\varphi(a+b)=[(a+b,1)]=[(a,1)]+[(b,1)]=\varphi(a)+\varphi(b),$$

és

$$\varphi(ab)=[(ab,1)]=[(a,1)]\cdot[(b,1)]=\varphi(a)\cdot\varphi(b).$$

Mivel ϑ definíciója miatt $\varphi(a)=\varphi(b)\Rightarrow a=b$, ezért φ injektív. Vagyis $\mathbb{Z}$-t tényleg beágyaztuk $\mathbb{Q}$-ba.

A továbbiakban 0-t írunk $[(0,1)]$ helyett, 1-et írunk $[(1,1)]$ helyett, és általánosan a-t írunk az $[(a,1)]$ osztály helyett. Minden $[(a,b)]$ racionális szám egy $[(b,1)]\cdot x=[(a,1)]$ alakú egyenlet megoldása, ezért egész számok hányadosaként írható. A szokásos jelölés szerint

$$\frac{a}{b}\overset{\text{def}}{\Leftrightarrow}[(a,b)].$$

Észrevehetjük, hogy $[(a,b)]=[(-a,-b)]$ miatt minden racionális számot elő lehet állítani $[(a,b)]$, $b>0$ alakban. Továbbá ϑ definíciója miatt az előbbi konstrukció esetén $[(a_1,b_1)]=[(a_2,b_2)]$-ből következik, hogy vagy $a_1,a_2\in\mathbb{Z}^+$, vagy $a_1,a_2\in\mathbb{Z}^-$, vagy mindkettő 0.

Egy $[(a,b)]$ racionális számot, ahol $b>0$, ***pozitívnak*** nevezünk, ha $a>0$, és ***negatívnak*** nevezünk, ha $a<0$. A pozitív racionális számokat $\mathbb{Q}^+$-szal, a negatívokat $\mathbb{Q}^-$-szal jelöljük. Ha a 0-t is beleértjük, akkor $\mathbb{Q}_0^+$-t, illetve $\mathbb{Q}_0^-$-t írunk. Így, ahogy az egész számoknál, egy tetszőleges $a\in\mathbb{Q}$ esetén a vagy $-a$ közül azt, amelyik természetes szám, a ***abszolút értékének*** nevezzük, és $|a|$-kel jelöljük.

Vezessünk be $\mathbb{Q}$-ban egy rendezési relációt.

4.20. definíció. $p\leq q\overset{\text{def}}{\Leftrightarrow}q-p\in\mathbb{Q}_0^+$.

Ez a rendezés $\mathbb{Z}$ rendezésének kiterjesztését jelenti, hiszen az egész számok $\mathbb{Q}$-ba történő beágyazása rendezéstartó is (ellenőrizzük!). Kijelenthetjük, hogy $\mathbb{Z}\subset\mathbb{Q}$, és $\mathbb{Q}$ elemei ábrázolhatóak a számegyenesen. A rendezés az algebrai struktúrával összefér, a monotoniára vonatkozó törvények (4.2-1. gyakorlat (7)–(8) pontjai) $\mathbb{Q}$-ban is érvényesek. Ezért a 3.36. definíciónak megfelelően $(\mathbb{Q};+,\cdot;\leq)$ ***rendezett test.***

4.21. definíció. *Egy* $(T;+,\cdot;\leq)$ *rendezett testet* ***arkhimédeszi tulajdonságúnak*** *nevezünk, ha minden* $a,b\in T$, $a>0$ *esetén van olyan* $n\in\mathbb{N}$, *hogy* $na\geq b$.

Az alábbi tételt bizonyítás nélkül közöljük.

4.22. tétel. $(\mathbb{Q};+,\cdot;\leq)$ *arkhimédeszi tulajdonságú.*

$\mathbb{Q}$ arkhimédeszi tulajdonságából fontos és érdekes tételek adódnak. Bebizonyítható, hogy minden $a,b\in\mathbb{Q}$, $a<b$ esetén létezik olyan $r\in\mathbb{Q}$, amelyre $a<r<b$ (például $r=(a+b)/2$), vagyis $\mathbb{Q}$ „mindenütt sűrű”. Másrészt minden $r\in\mathbb{Q}^+$-ra $0<r/2<r$, vagyis $\mathbb{Q}^+$-nak nincs legkisebb eleme.

4.4. Valós számok

Mivel $\mathbb{Q}$-ban a négy alapművelet korlátozás nélkül elvégezhető (az egyetlen megszorítás, hogy nem oszthatunk 0-val), az algebrai struktúra nem ad okot újabb általánosításra. Mégis, a rendezési (és a topológiai) struktúra hiányosságokat mutat. Ezek kiküszöbölése vezet el a valós számokhoz.

4.4.1. Konstrukció

Az előző fejezetben láttuk, hogy $(\mathbb{Q};\leq)$ teljesen rendezett, így elemei a számegyenesen ábrázolhatóak. Noha a racionális számok „mindenütt sűrűn" helyezkednek el a számegyenesen, mégsem töltik ki azt „teljesen." Például Püthagorasz szerint az egységnyi oldalú négyzet átlójának hossza nem racionális szám. Meg lehet adni közelítő értékek egy sorozatát $(1, 1.4, 1.41, 1.414, \ldots)$, mégis, az $\{x \in \mathbb{Q} \mid x^2 < 2\}$ halmaznak ($\mathbb{Q}$-ban) nincs felső határa.

4.23. definíció. *Egy* $(T;+,\cdot;\leq)$ *rendezett testet* ***felső határ tulajdonságúnak*** *nevezünk, ha minden nem üres felülről korlátos részhalmazának létezik (*T*-ben) felső határa.*

Az iménti példa szerint $\mathbb{Q}$ nem felső határ tulajdonságú. Belátható, hogy létezik felső határ tulajdonságú test, mégpedig lényegében egyértelműen. Az alábbiakban csak a létezést vizsgáljuk.

4.24. definíció. *A* $(\mathbb{Q};\leq)$ *halmaznak a* $p \in \mathbb{Q}$ *elem által meghatározott* ***nyílt kezdőszeletén*** *a* $\mathbb{Q}_p = \{x \in \mathbb{Q} \mid x < p\} \subset \mathbb{Q}$ *halmazt értjük.*

4.25. definíció. *Legyen* $\varnothing \neq \alpha \subset \mathbb{Q}$. *Azt mondjuk, hogy* α ***nyílt kezdet****, ha*
(1) $\forall\, p \in \alpha \;:\; \mathbb{Q}_p \subset \alpha$,
(2) $\forall\, p \in \alpha \;\; \exists\, q \in \alpha \;:\; q > p$.

A nyílt kezdetek tehát $\mathbb{Q}$ bizonyos részhalmazai. Ha a számegyenesen való ábrázolásban gondolkodunk, akkor egy nyílt kezdet egy balra végtelenbe nyúló, jobb oldali végpontot nem tartalmazó nyílt félegyenes racionális pontjainak halmaza. Észrevehetjük, hogy minden nyílt kezdőszelet egyúttal nyílt kezdet is, de ennek megfordítása nem igaz: a $\mathbb{Q}^- \cup \{x \in \mathbb{Q} \mid x \in \mathbb{Q}_0^+ \text{ és } x^2 < 2\} \subset \mathbb{Q}$ bár nyílt kezdet $\mathbb{Q}$-ban, de nem kezdőszelete egyetlen racionális számnak sem. Könnyen meggondolható, hogy pontosan azok a nyílt kezdetek nyílt kezdőszeletek, melyeknek a „jobb oldali vége" nem racionális szám.

4.26. definíció. *Az összes* $\mathbb{Q}$*-beli nyílt kezdet halmazát* $\mathbb{R}$*-rel jelöljük és elemeit* ***valós számoknak*** *nevezzük.*

A valós számokat tehát racionális számok halmazaiként definiáljuk.

4.27. definíció. *Azokat a valós számokat, amelyek nem nyílt kezdőszeletei racionális számoknak,* ***irracionális számoknak*** *nevezzük.*

4.28. tétel. *A valós számok halmaza felső határ tulajdonságú.* □

Mivel egy felső határ tulajdonságú test mindig arkhimédeszi tulajdonságú is, (4.4-1. feladat) ezért $\mathbb{R}$ arkhimédeszi tulajdonságú.

4.4.2. Műveletek, rendezésük

$\mathbb{R}$ az alábbi rendezéssel teljesen rendezett struktúra lesz:

4.29. definíció. $\alpha \leq \beta \overset{\text{def}}{\Leftrightarrow} \alpha \subseteq \beta$ $(\alpha, \beta \in \mathbb{R})$.

A valós számokat $\mathbb{Q}$ algebrai struktúrájának felhasználása nélkül vezettük be. Az alábbi műveletekkel mégis lehetséges algebrai struktúra konstruálása $\mathbb{R}$-en.

4.30. definíció. $\alpha, \beta \in \mathbb{R}$ *esetén*

$$\begin{aligned} \alpha + \beta &\overset{\text{def}}{\Leftrightarrow} \{r + s \in \mathbb{Q} \mid r \in \alpha \text{ és } s \in \beta\} \subset \mathbb{Q}, \\ \alpha \cdot \beta &\overset{\text{def}}{\Leftrightarrow} \mathbb{Q}^- \cup \{rs \mid r \in \alpha \setminus \mathbb{Q}^- \text{ és } s \in \beta \setminus \mathbb{Q}^-\}, \text{ ha } \alpha, \beta \geq 0. \end{aligned}$$

Tetszőleges valós számok szorzatát az $\alpha\beta = (-\alpha)(-\beta) = -((-\alpha)\beta) = -(\alpha(-\beta))$ egyenlőségek alapján az iménti definíció szerint adhatjuk meg. Láthatjuk, hogy az összeadás és a szorzás is kétváltozós belső művelet $\mathbb{R}$-ben. A műveletekre az alábbi tulajdonságok teljesülnek:

4.31. tétel.

- $(\mathbb{R}; +)$ *kommutatív csoport, amelynek semleges eleme az* $\{r \in \mathbb{Q} \mid r < 0\}$ *nyílt kezdet (amely egyúttal nyílt kezdőszelet is). Ezt az elemet a továbbiakban* 0*-val jelöljük.*
- $(\mathbb{R} \setminus \{0\}; \cdot)$ *kommutatív csoport, melynek semleges eleme az* $\{r \in \mathbb{Q} \mid r < 1\}$ *nyílt kezdet (amely szintén nyílt kezdőszelet). Ezt az elemet a továbbiakban* 1*-gyel jelöljük.*
- *Minden* $\alpha, \beta, \gamma \in \mathbb{R}$ *esetén* $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$.
- *Minden* $\alpha, \beta, \gamma \in \mathbb{R}$ *esetén* $\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$.
- *Minden* $\alpha, \beta, \gamma \in \mathbb{R}$, $\gamma \geq 0$ *esetén* $\alpha \leq \beta \Rightarrow \alpha\gamma \leq \beta\gamma$.

Azt kaptuk tehát, hogy

4.32. tétel. $(\mathbb{R}; +, \cdot; \leq)$ *rendezett test.*

Vajon hogy viszonyulnak egymáshoz a $\mathbb{Q}$ és az $\mathbb{R}$ rendezett testek? Tekintsük a $\varphi : \mathbb{Q} \to \mathbb{R}$, $\varphi(p) = \mathbb{Q}_p$ függvényt. Bebizonyítható, hogy φ injektív, valamint művelet- és rendezéstartó, így a $(\mathbb{Q}; +, \cdot; \leq)$ rendezett test természetes módon azonosítható $\{\mathbb{Q}_p \mid p \in \mathbb{Q}\}$-val. Vagyis $\mathbb{Q}$-t beágyaztuk $\mathbb{R}$-be. Ebben az értelemben kijelenthetjük, hogy $\mathbb{Q} \subset \mathbb{R}$. A pozitív valós számokat $\mathbb{R}^+$-szal, a negatívokat $\mathbb{R}^-$-szal jelöljük. Ha a 0-t is beleértjük, akkor $\mathbb{R}_0^+$-t, illetve $\mathbb{R}_0^-$-t írunk. A valós számkörben az egészeknél és a racionális számoknál látott módon értelmezzük az ***abszolút értéket***.

4.33. definíció. *Legyen* $x \in \mathbb{R}$. *Ekkor*

$$|x| \overset{\text{def}}{\Leftrightarrow} \begin{cases} x & \text{ha } x \geq 0, \\ -x & \text{ha } x < 0. \end{cases}$$

Megjegyezzük továbbá, hogy ha $a \in \mathbb{Z}^+$, akkor a beágyazások tulajdonságai miatt $a \in \mathbb{Q}^+$ és $a \in \mathbb{R}^+$ is teljesül.

4.34. definíció. *Legyen* $x \in \mathbb{R}$. *Ekkor*

$$\operatorname{sgn}(x) \overset{\text{def}}{\Leftrightarrow} \begin{cases} 0 & \text{ha } x = 0, \\ x/|x| & \text{egyébként.} \end{cases}$$

A sgn függvényt ***előjelfüggvénynek*** nevezzük. $\mathbb{R}$ arkhimédeszi tulajdonsága miatt definiálhatjuk egy valós szám „egészrészét".

4.35. definíció.

$$\begin{aligned} \lfloor x \rfloor &\overset{\text{def}}{\Leftrightarrow} \text{az } x\text{-nél nem nagyobb egészek legnagyobbika,} \\ \lceil x \rceil &\overset{\text{def}}{\Leftrightarrow} \text{az } x\text{-nél nem kisebb egészek legkisebbike.} \end{aligned}$$

Az első esetben x ***alsó egészrészéről***, a második esetben x ***felső egészrészéről*** beszélünk. Ennek megfelelően definiáljuk x ***törtrészét*** [1]:

4.36. definíció. $\{x\} \overset{\text{def}}{\Leftrightarrow} x - \lfloor x \rfloor$.

4.5. példa. $\lfloor \frac{3}{2} \rfloor = 1$, $\lfloor -\frac{31}{10} \rfloor = -4$, $\lceil \frac{3}{2} \rceil = 2$, $\lceil -\frac{31}{10} \rceil = -3$, $\{\frac{3}{2}\} = \frac{1}{2}$, $\{-\frac{31}{10}\} = \frac{9}{10}$, $\lfloor \pi \rfloor = 3$.

A valós számok helyiértékes előállítására vonatkozó módszereket analízisből tanuljuk. Az alábbi tételt bizonyítás nélkül közöljük.

4.37. tétel. *Minden valós szám előállítható* ***véges*** *vagy* ***végtelen tizedes törtként.*** □

Ha eltekintünk azoktól a tizedes törtektől, amelyek kifejtésében valahonnan kezdve csupa 9-es áll, akkor a többi tizedes tört kölcsönösen egyértelműen megfeleltethető a valós számoknak. Belátható, hogy minden racionális szám véges vagy végtelen szakaszos tizedes törtnek felel meg, az irracionális számok pedig a nem szakaszos végtelen tizedes törtekkel azonosíthatók.

Az összeadás, kivonás, szorzás és osztás műveleteken kívül a valós számkörben új műveleteket lehet bevezetni, a gyökvonást és a logaritmuskeresést.

4.38. definíció. $\sqrt[n]{r} \overset{\text{def}}{\Leftrightarrow} \mathbb{Q}^- \cup \{x \in \mathbb{Q}_0^+ \mid x^n \in r\}$, *ahol* $n \in \mathbb{N}^+, r \in \mathbb{R}_0^+$.

Ezt a számot az r nemnegatív valós szám n***-edik gyökének***, meghatározását ***gyökvonásnak*** nevezzük. Analízisből látni fogjuk, hogy a gyökvonást „tetszés szerinti pontossággal" el lehet végezni. Megjegyezzük, hogy valós számok racionális kitevőjű, és valós számok valós kitevőjű hatványozása is értelmezhető.

Az $r^x = t$ egyenletnek $1 \neq r \in \mathbb{R}^+$-ra és $t \in \mathbb{R}^+$-ra a hatványozás monotonitása és a felső határ tulajdonság miatt mindig pontosan egy megoldása van, amit $x = \log_r t$ alakban írunk és ***logaritmuskeresésnek*** nevezünk. A logaritmuskeresésről és tulajdonságairól analízisből tanulunk.

Megjegyezzük, hogy a valós számok konstrukciójának léteznek egyéb megközelítései is. Weierstrass a valós számoknak az ún. intervallumskatulyázással történő

[1] A törtrész jelölés sajnos összetéveszthető az egyedül az x-et tartalmazó halmazzal, mégis ez a jelölés terjedt el, ezért mi is ezt használjuk.

jellemzését adta. CANTOR a racionális számok topológiai struktúrájának nem teljes voltából indult ki és jutott el a valós számokhoz. A részleteket könyvünk harmadik részében tárgyaljuk. Megjegyezzük továbbá, hogy az eddig látott számkörök úgy is felépíthetőek lettek volna, hogy axiomatizáljuk a valós számokat, majd különböző megszorítások révén jutunk el a racionális, egész és természetes számokhoz (DEDEKIND).

4.6. példa. Az $\mathbb{R}$ valós számtest feletti vektortér jól ismert a középiskolai matematikából, ahol síkgeometriai feladatok megoldására és szemléltetésére használtuk őket.

Gyakorlatok

4.4-1. Mutassuk meg, hogy egy felső határ tulajdonságú test mindig arkhimédeszi tulajdonságú is.

4.4-2.* Hogyan lehetne megadni a valós számok valós kitevőjű hatványozását nyílt kezdetek segítségével?

4.5. Komplex számok

A valós számok műveleteinél érdekes dologra lehetünk figyelmesek: a gyökvonást nem lehet tetszőleges valós számra definiálni. Ilyen például a $\sqrt{-1}$ szimbólum. Ez a szimbólum először az általános harmadfokú egyenletek megoldásánál bukkant elő, ami a reneszánsz matematika egyik felfedezése volt. CARDANO és FERRO észrevették, hogy bizonyos harmadfokú egyenletek megoldása során (amikor három különböző valós gyök létezik) a négyzetgyökjel alatt negatív szám szerepel, így az összes megoldás a korábbi módon nem volt számolható. Ezt hívták „casus irreducibilisnek." Azt is észrevették azonban, hogy negatív számok négyzetgyökeire is bevezethetők bizonyos számolási szabályok, így fokozatosan tisztázódtak a „képzetes" számokkal való műveletek szabályai. A komplex számok fogalmát GAUSS tisztázta véglegesen, bebizonyítva az algebra alaptételét.

4.5.1. Konstrukció

A komplex számokat többféleképpen is be lehet vezetni, mi most az eddig megszokott utat követjük.

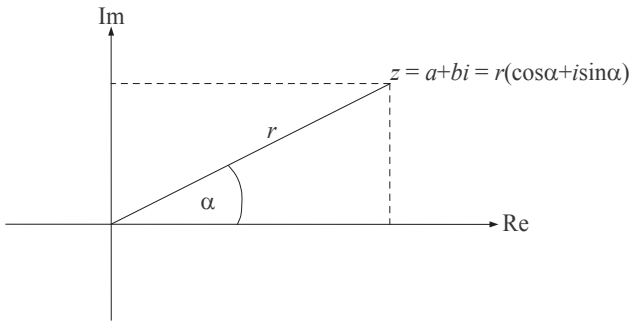
4.39. definíció. $\mathbb{C} \overset{\text{def}}{\Leftrightarrow} \mathbb{R} \times \mathbb{R}$.

$\mathbb{C}$ elemeit ***komplex számoknak*** nevezzük. Az összeadás és szorzás definíciója a következő:

4.40. definíció. *Legyen* $(a, b), (c, d) \in \mathbb{C}$. *Ekkor*

$$\begin{aligned} (a, b) + (c, d) &\overset{\text{def}}{\Leftrightarrow} (a + c, b + d), \\ (a, b) \cdot (c, d) &\overset{\text{def}}{\Leftrightarrow} (ac - bd, ad + bc). \end{aligned}$$

Belátható, hogy $(\mathbb{C}; +)$ kommutatív csoport a $(0, 0)$ semleges elemmel, továbbá az (a, b)-hez tartozó, az összeadásra vonatkozó inverz elem $-(a, b) = (-a, -b)$. Ezen



4.1. ábra. A z komplex szám algebrai és trigonometrikus alakja.

kívül $(\mathbb{C} \setminus \{(0,0)\}; \cdot)$ kommutatív csoport az $(1,0)$ semleges elemmel. Az (a,b)-hez tartozó, a szorzásra vonatkozó inverz elem $(a,b)^{-1} = (a/(a^2+b^2), -b/(a^2+b^2))$. Az inverzképzés pontosan akkor zárt $\mathbb{C}$-ben, ha $a^2+b^2 \neq 0$. A két műveletet összekapcsoló disztributiv törvények is igazak, ezért

4.41. tétel. $(\mathbb{C}; +, \cdot)$ *test.*

Meg kell még vizsgálnunk, hogy $\mathbb{R}$-et valóban beágyaztuk-e $\mathbb{C}$-be. Tekintsük a $\Phi : \mathbb{R} \to \mathbb{C}$, $\Phi(a) = (a,0)$ függvényt. Ekkor

$$\Phi(a+b) = (a+b,0) = (a,0) + (b,0) = \Phi(a) + \Phi(b)$$

és

$$\Phi(ab) = (ab,0) = (a,0) \cdot (b,0) = \Phi(a) \cdot \Phi(b).$$

Mivel $\Phi(a) = \Phi(b) \Rightarrow a = b$, ezért Φ injektív. Vagyis $\mathbb{R}$-et valóban beágyaztuk $\mathbb{C}$-be, az összes $(a,0), a \in \mathbb{R}$ alakú komplex számokat azonosíthatjuk $\mathbb{R}$-rel.

4.5.2. Szemléltetésük és műveleteik

A továbbiakban i-t írunk $(0,1)$ helyett, és általánosan, $a + bi$-t írunk $(a,b) = (a,0)+(b,0)\cdot(0,1)$ helyett. Ha $z = a+bi \in \mathbb{C}$, akkor megkülönböztetjük a z komplex szám ***valós*** $(\Re)$ és ***képzetes*** (imaginárius, $\Im$) ***részét***: $\Re(z) = a$, $\Im(z) = b$. Ennek megfelelően a komplex számokat a síkbeli DESCARTES-féle koordináta-rendszer pontjaiként is felfoghatjuk, vagyis minden komplex számnak a sík egy pontja felel meg és fordítva (GAUSS-féle számsík, 4.1. ábra). Más felfogásban a komplex számok az origóból induló vektoroknak is tekinthetők, és a komplex számok összeadása megfelel a vektorok szokásos összeadásának. Egy komplex szám ***abszolút értéke*** vagy ***hossza*** ennek a vektornak a hossza. A komplex számok abszolút értékének algebrai bevezetéséhez szükségünk lesz az előző fejezetben látott gyökvonás fogalmára.

4.42. definíció. $|z| = |a+bi| = \sqrt{a^2+b^2}$.

A valós számokra a szokásos abszolút értéket kapjuk: $|(a,0)| = |a|$.

4.43. definíció. *A* $z = a + bi$ *komplex szám* ***konjugáltján*** *a* $\overline{z} = a - bi$ *számot értjük.*

Egy komplex szám tehát pontosan akkor valós, ha megegyezik konjugáltjával. Ha egy nem nulla komplex szám valós része nulla, akkor ***képzetesnek*** nevezzük. Ha $z, w \in \mathbb{C}$, akkor az alábbi összefüggések könnyen igazolhatók (4.5-1. gyakorlat).

4.44. tétel.

(1) $\overline{\overline{z}} = z$,
(2) $\overline{z+w} = \overline{z} + \overline{w}$,
(3) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$,
(4) $z + \overline{z} = 2\Re(z)$,
(5) $z - \overline{z} = 2i\Im(z)$,
(6) $z\overline{z} = |z|^2$,
(7) $z \neq 0$ *esetén* $z^{-1} = \overline{z}/|z|^2$,
(8) $|0| = 0$, *és* $z \neq 0$ *esetén* $|z| > 0$,
(9) $|z| = |\overline{z}|$,
(10) $|z \cdot w| = |z| \cdot |w|$ (mert nem negatívak és mindkét oldal négyzete $z\overline{z}w\overline{w}$),
(11) $|\Re(z)| \leq |z|$, $|\Im(z)| \leq |z|$,
(12) $|z + w| \leq |z| + |w|$ ***(háromszög-egyenlőtlenség)***. □

Az alábbiakban felhasználjuk a sin, cos függvények, valamint az e és a π számok definícióit és tulajdonságait. Ezeket az analízis tárgyalása során szokás bizonyítani. Ha a GAUSS-féle számsíkon a $z \neq 0$ vektor (komplex szám) koordinátáit a szinusz és koszinusz függvények segítségével írjuk fel, azt kapjuk, hogy $z = r(\cos\varphi + i\sin\varphi)$, ahol $r = |z|$ és $0 \leq \varphi < 2\pi$. A $\varphi \in \mathbb{R}$ számot a z komplex szám ***argumentumának*** (vagy arkuszának) nevezzük, és $\arg(z)$-vel jelöljük (4.1. ábra). Megmutatható, hogy $\cos\varphi + i\sin\varphi = e^{i\varphi}$, így a komplex számok $z = re^{i\varphi}$ alakjához jutunk. Az iménti jelölésekkel tehát egy $z \neq 0$ komplex számot többféle alakban is felírhatunk:

$z = a + bi$ (algebrai alak),
$z = r(\cos\varphi + i\sin\varphi)$ (trigonometrikus alak),
$z = re^{i\varphi}$ (EULER-féle alak).

A 4.44. tételben megvizsgáltuk a komplex számok algebrai alakjával történő műveleteket. Most a trigonometrikus alakkal vett műveleteket vizsgáljuk.

Legyen $z, w \in \mathbb{C}$, $z = |z|(\cos\varphi + i\sin\varphi)$, $w = |w|(\cos\psi + i\sin\psi)$, $0 \leq \varphi, \psi < 2\pi$, $\varphi, \psi \in \mathbb{R}$. Ekkor

$$\begin{aligned} zw &= |z| \cdot |w|(\cos\varphi + i\sin\varphi) \cdot (\cos\psi + i\sin\psi) \\ &= |zw|(\cos\varphi\cos\psi - \sin\varphi\sin\psi + i(\cos\varphi\sin\psi + \cos\psi\sin\varphi)) \\ &= |zw|(\cos(\varphi+\psi) + i\sin(\varphi+\psi)). \end{aligned}$$

Ez az ún. MOIVRE-***azonosság***. Hasonlóan, a 4.44. tétel (7) tulajdonsága miatt a $w \neq 0$ esetben

$$\frac{z}{w} = \frac{|z|}{|w|}(\cos(\varphi - \psi) + i\sin(\varphi - \psi)).$$

Ha z, w nem nulla komplex számok, akkor a $0 \leq \arg(zw) < 2\pi$ esetben $\arg(zw) = \arg(z) + \arg(w)$, ha pedig $\arg(zw) \geq 2\pi$, akkor $\arg(zw) = \arg(z) + \arg(w) - 2\pi$.

Hasonlóan, a $0 \le \arg(z/w) < 2\pi$ esetben $\arg(z/w) = \arg(z) - \arg(w)$, az $\arg(z/w) < 0$ esetben pedig $\arg(z/w) = \arg(z) - \arg(w) + 2\pi$. Geometriai értelemben tehát komplex számok szorzásánál a hosszak összeszorzódnak, az „x tengely pozitív felével" bezárt szögek pedig „összeadódnak". Hasonlóan, komplex számok osztásánál az eredmény hossza a hosszak hányadosa, az „x tengely pozitív felével" bezárt szögek pedig „kivonódnak". A műveletek eredményének arkuszát mindig a $[0, 2\pi)$ intervallumban vesszük.

A valós számok hatványozását a komplex számokra általánosítva a MOIVRE-azonosságból azt kapjuk, hogy $n \in \mathbb{N}$ esetén

$$z^n = |z|^n(\cos n\varphi + i \sin n\varphi).$$

4.7. példa. Az $(1+i)^{2004}$ szám algebrai alakja:

$$\begin{aligned}(1+i)^{2004} &= \left(\sqrt{2}(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})\right)^{2004} = \\ &= (\sqrt{2})^{2004}(\cos 501\pi + i\sin 501\pi) = \\ &= (\sqrt{2})^{2004}(\cos\pi + i\sin\pi) = -2^{1002}.\end{aligned}$$

4.5.3. Komplex számok gyökei

A hatványozáshoz hasonlóan lehet a komplex számokból való gyökvonást valós számokkal való számolásra visszavezetni.

4.45. definíció. *Legyen $z \in \mathbb{C}$, $n \in \mathbb{N}^+$. A $w \in \mathbb{C}$ komplex számot a z* ***n-edik gyökének*** *nevezzük, ha $w^n = z$.*

$z = 0$ esetén nyilván $w = 0$. Ha $0 \neq z = |z|(\cos\varphi + i\sin\varphi)$, akkor a

$$w_k = \sqrt[n]{|z|}\left(\cos\left(\frac{\varphi + 2k\pi}{n}\right) + i\sin\left(\frac{\varphi + 2k\pi}{n}\right)\right),\ k = 0, 1, \ldots, n-1$$

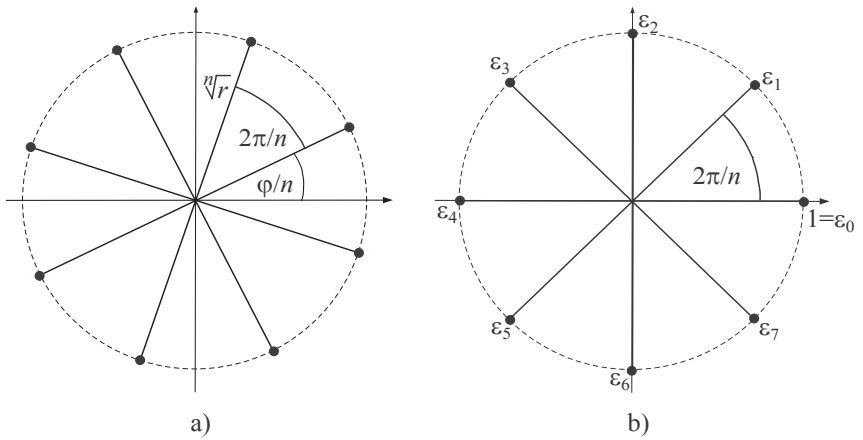
különböző komplex számok, és csak ezek azok, amelyeknek n-edik hatványa z. Eszerint minden 0-tól különböző komplex számnak n különböző n-edik gyöke van. Vagyis $n > 1$ esetén a $z \mapsto z^n$ hatványfüggvény inverze nem függvény. A gyököket jobban szemügyre véve láthatjuk, hogy a $z \neq 0$ komplex szám gyökei a GAUSS-féle számsíkon szabályos n oldalú sokszög csúcsai. A csúcsok origótól mért távolsága $\sqrt[n]{|z|}$, az egyik csúcsnak a valós tengellyel bezárt szöge φ/n (4.2. ábra).

4.8. példa. Számítsuk ki a $\sqrt[6]{\frac{1-i}{\sqrt{3}+i}}$ kifejezés értékét. Mivel

$$\begin{aligned}1 - i &= \sqrt{2}(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}) = \sqrt{2}(\cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4}) \text{ és} \\ \sqrt{3} + i &= 2(\frac{\sqrt{3}}{2} + \frac{1}{2}i) = 2(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}),\end{aligned}$$

továbbá

$$\frac{7\pi}{4} - \frac{\pi}{6} = \frac{19\pi}{12},$$



4.2. ábra. a) Az $r(\cos\varphi + i\sin\varphi) = z \neq 0$ komplex szám n-edik gyökei egy origó középpontú, $\sqrt[n]{r}$ sugarú szabályos n-szög csúcsai. Ezen szabályos n-szög egyik csúcsa az a pont, amelybe mutató helyvektor a valós tengely pozitív felével φ/n szöget zár be. b) A komplex n-edik egységgyökök. Mindkét ábrán $n = 8$.

ezért

$$\sqrt[6]{\frac{1-i}{\sqrt{3}+i}} = \frac{1}{\sqrt[12]{2}}\left(\cos\frac{19\pi+24k\pi}{72} + i\sin\frac{19\pi+24k\pi}{72}\right), \quad 0 \le k \le 5.$$

Speciálisan, ha $z = 1$, akkor az $\varepsilon^n = 1$ feltételnek az

$$\varepsilon_k = \varepsilon_k^{(n)} = \left(\cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)\right), \; k = 0, 1, \ldots, n-1$$

komplex számok tesznek eleget. Ezeket ***n-edik komplex egységgyököknek*** nevezzük. Némely n-edik egységgyök természetes kitevőjű hatványaiként az összes többi előáll. Például a negyedik egységgyökök $(\pm 1, \pm i)$ közül az i ilyen, a -1 azonban nem.

4.46. definíció. *Azt az n-edik egységgyököt, amelynek különböző természetes kitevőjű hatványai előállítják a többi n-edik egységgyököt,* ***primitív n-edik egységgyöknek*** *nevezzük.*

Tetszőleges $n \in \mathbb{N}^+$-ra $\varepsilon_1^{(n)}$ mindig primitív egységgyök. Belátható, hogy $\varepsilon_k^{(n)}$ pontosan akkor lesz primitív n-edik egységgyök, ha k és n relatív prímek, tehát nincs egynél nagyobb közös osztójuk.

4.47. tétel. *Legyen $0 \neq z \in \mathbb{C}$, $n \in \mathbb{N}^+$ és $w_1^n = z$. Ekkor z többi n-edik gyöke $w_1\varepsilon_k$ $(1 \le k \le n-1)$, ahol ε_k n-edik egységgyök.*

Bizonyítás. Felhasználva, hogy $\varepsilon_k^n = 1$ azt kapjuk, hogy $(w_1\varepsilon_k)^n = w_1^n\varepsilon_k^n = w_1^n = z$. Másrészt $w_1\varepsilon_k$ $(1 \le k \le n-1)$ mind különbözőek, mert ha $w_1\varepsilon_k = w_1\varepsilon_s$, akkor

$w_1 \neq 0$ miatt $\varepsilon_k = \varepsilon_s$. □

4.48. következmény. *Ha $n \in \mathbb{N}$, $n > 1$, akkor a $z \in \mathbb{C}$ szám n-edik gyökeinek összege 0.*

Valóban,

$$\sum_{k=0}^{n-1} w_1 \varepsilon_k = \sum_{k=0}^{n-1} w_1 \varepsilon_1^k = w_1 \frac{\varepsilon_1^n - 1}{\varepsilon_1 - 1} = w_1 \frac{1-1}{\varepsilon_1 - 1} = 0.$$

4.5.4. $\mathbb{C}$ algebrai zártsága és rendezési struktúrája

Vizsgáljuk meg a komplex együtthatós másodfokú egyenletek megoldhatóságát, vagyis keressük meg az $f(x) = ax^2 + bx + c \in \mathbb{C}[x]$ polinom zérushelyeit ($a \neq 0$). Az egyenletet $4a$-val megszorozva és átrendezve azt kapjuk, hogy $(2ax+b)^2 = b^2 - 4ac$, majd gyökvonás és átrendezés után

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

A komplex számok körében nem csupán a másodfokú egyenleteknek létezik megoldása. Távolról sem elemi általánosításként érvényes az

4.49. tétel (algebra alaptétele). *Minden $\mathbb{C}[x]$-beli, $n > 0$ fokú polinomnak legalább egy zérushelye van $\mathbb{C}$-ben.*

A tételnek több különböző bizonyítása ismeretes. Mindenesetre a bizonyítás nem végezhető el tisztán algebrai eszközökkel. A $\mathbb{C}$ testet ezen tulajdonsága miatt ***algebrailag zártnak*** nevezzük.

Míg $\mathbb{C}$ algebrai struktúrája $\mathbb{R}$ algebrai struktúrájának kiterjesztése, az $\mathbb{R}$-ből a $\mathbb{C}$-be való átmenetnél a rendezési struktúra elvész. $\mathbb{C}$ teljesen rendezhető, például úgy, hogy

$$z_1 \leq z_2 = \begin{cases} |z_1| < |z_2| \text{ vagy} \\ (|z_1| = |z_2| \text{ és } \arg z_1 \leq \arg z_2), \end{cases}$$

mégsem lehetséges olyan rendezés, amely az algebrai struktúrával összefér, vagyis érvényes lenne rá a műveletek monotonitása.

4.50. tétel. *Nem létezik olyan rendezési reláció, amellyel $\mathbb{C}$ rendezett test lenne.*

Bizonyítás. Indirekt bizonyítunk. Tegyük fel, hogy $\mathbb{C}$ rendezett test a $\leq$ relációval. Mivel $\leq$ teljes rendezés, ezért a $0 \leq i$ és az $i \leq 0$ összefüggések közül valamelyiknek (pontosan az egyiknek) teljesülnie kell. Az utóbbi esetben az összeadás monotonitása miatt $0 \leq -i$. Figyelembe véve, hogy $i \cdot i = -1 = (-i) \cdot (-i)$, a szorzás monotonitása miatt ezért $0 \leq -1$ mindenképpen fennáll. Újból felhasználva a szorzás monotonitását azt kapjuk, hogy $0 \leq (-1) \cdot (-1) \leq 1$, amiből az összeadás monotonitása miatt $-1 \leq 0$ adódik. Azt kaptuk tehát, hogy $0 \leq -1$ és $-1 \leq 0$ is teljesül. De az antiszimmetria miatt egyenlőség áll fenn, ami ellentmondás. □

Gyakorlatok

4.5-1. Bizonyítsuk be a 4.44. tétel állításait.

·	1	i	j	k
1	1	i	j	k
i	i	−1	k	−j
j	j	−k	−1	i
k	k	j	−i	−1

4.3. ábra. A kvaterniók szorzási táblázata.

4.5-2. Számítsuk ki i^n értékét, ahol $n \in \mathbb{Z}$.
4.5-3. Határozzuk meg az

$$f(x) = (2+i)x^2 - (5-i)x + (2+2i) \in \mathbb{C}[x]$$

polinom gyökeit.
4.5-4. Mely z komplex számok elégítik ki a $\overline{z} = z^3$ egyenletet?
4.5-5. Igazoljuk, hogy egy m-edik és egy n-edik egységgyök szorzata mn-edik egységgyök.

4.6. Algebrai és transzcendens számok, kvaterniók

Vizsgáljuk meg a racionális együtthatós polinomok gyökeit.

4.51. definíció. *Egy $\mathbb{Q}[x]$-beli polinom gyökét ($\mathbb{Q}$ feletti)* ***algebrai számnak*** *nevezzük.*

Az algebrai számok halmaza a komplex műveletekkel testet alkot. Algebrai szám például a $\sqrt{2}$ és az i.

4.52. definíció. *A $\mathbb{Q}$ felett nem algebrai komplex számokat* ***transzcendens*** *számoknak nevezzük.*

Ezek közé tartozik két fontos szám, az e és a π. $\mathbb{Q}$ és az algebrai számok teste közé végtelen sok közbülső test konstruálható.

A komplex számok konstrukciója azt a kérdést veti fel, hogy lehet-e $\mathbb{C}$-t tovább bővíteni, vagyis léteznek-e $\mathbb{R}$-nek más bővítései, amelyeket ugyancsak $\mathbb{R}$ feletti véges dimenziós vektortérként lehet felfogni. Erre a kérdésre a válasz tagadó. De ha lemondunk a szorzás kommutativitásáról, Frobenius szerint $\mathbb{C}$-n kívül még pontosan egy ilyen struktúra létezik, a ***kvaterniók*** négydimenziós ***ferdeteste***. Ha báziselemként az $1, i, j, k$ szimbólumokat választjuk, akkor K minden eleme $\alpha = a + bi + cj + dk$ $(a, b, c, d \in \mathbb{R})$ alakban írható. K-beli elemek összeadása koordinátánként, míg szorzása a 4.3. ábrán látható szorzótábla szerint a disztributivitás felhasználásával történik. A kvaterniókat a térbeli mozgással való kapcsolata miatt robotok vezérlésénél használják.

Megjegyzések a fejezethez

PEANO öt axiómája egyértelműen meghatározza a természetes számokat, de ezek közül bármelyiket elhagyva már nem teljesül az egyértelműség. PEANO az egyes esetekre az alábbi példákat adta:

(1) Legyen N a pozitív egész számok halmaza. Ekkor a $2,3,4,5$ axiómák teljesülnek, de az első nem.

(2) Legyen $\mathsf{N} = \{0,1,2\}$, $0' = 1$, és $1' = 2$, de nem értelmezzük a $2'$ jelölést. Ekkor az $1,3,4,5$ axiómák teljesülnek, de a második nem.

(3) Legyen $\mathsf{N} = \{0,1,2,\ldots,23\}$, és a rákövetkezést definiáljuk az órák múlásának megfelelően, vagyis $0' = 1, 1' = 2, \ldots, 23' = 0$. Ekkor az $1,2,4,5$ axiómák teljesülnek, de a harmadik nem.

(4) Legyen $\mathsf{N} = \{0,1\}$, és $0' = 1, 1' = 1$. Ekkor az $1,2,3,5$ axiómák teljesülnek, de a negyedik nem.

(5) Legyen N a nemnegatív racionális számok halmaza, és minden elem rákövetkezője legyen a nála 1-gyel nagyobb racionális szám. Ekkor az $1,2,3,4$ axiómák teljesülnek, de az ötödik nem.

Ezek a példák azt is mutatják, hogy az öt axióma független, hiszen sem az axiómák, sem azok tagadása nem vezet ellentmondásra.

A valós számok axiomatikus felépítéséhez a test és rendezési axiómákon kívül a teljességi axiómára (DEDEKIND-axióma vagy szétválasztási axióma) van még szükség: legyen A és B valós számok két nemüres részhalmaza. Ha minden $a \in A$ és minden $b \in B$ elemre $a \le b$, akkor létezik olyan c valós szám, amelyre

$$\forall a \in A \text{ és } \forall b \in B \text{ esetén } a \le c \le b \text{ teljesül.}$$

A valós számok rendezett teste az alábbi intervallum-skatulyázási tulajdonsággal is rendelkezik (WEIERSTRASS): ha a_n, b_n $(n = 1,2,\ldots)$ valós számsorozatok, $a_n < b_n$, $a_n < a_{n+1}$, és $b_n > b_{n+1}$ $(n = 1,2,\ldots)$, akkor

$$\bigcap_{n=1}^{\infty} [a_n, b_n] \neq \varnothing.$$

A matematikai logikában a különböző axiómarendszereket azok „konzisztenciaerőssége" segítségével tanulmányozzák. Egy axiómarendszernek akkor nagyobb a konzisztenciaerőssége egy másikénál, ha a konzisztenciájából a másik konzisztenciája következik, speciálisan, ha benne a másikat modellezni lehet. Az egyik leggyengébb rendszer a PEANO axiómái által formalizált aritmetika (elsőrendű aritmetika). Az analízishez viszont ennél erősebbre (másodrendű aritmetikára) van szükség. Még erősebb rendszerek keletkeznek, ha magát a halmazelméletet axiomatizáljuk, ahogy tettük ezt a 2.4. fejezetben. Bizonyos matematikai eredmények bizonyításához az analízisnél többet, de az egész ZERMELO-FRAENKEL-féle halmazelméletnél még mindig kevesebbet használunk fel.

A transzcendens számok létezését CANTOR és LIOUVILLE mutatta meg. A π transzcendens mivolta sokáig foglalkoztatta a matematikusokat, mert a görögök kizárólag körzővel és vonalzóval vett szerkesztési feladatát szerették volna megoldani: szerkesszünk olyan négyzetet, amelynek a területe egy adott kör területével egyenlő.

Mivel a kör négyszögesítése egy π hosszúságú szakasz szerkesztésével ekvivalens, a π transzcendenciája egyben a szerkesztési feladat megoldhatatlanságát bizonyítja.

Hilbert 1900-as párizsi előadásán vetette fel azt a kérdést, hogy egy hatványról, ahol az alap 0-tól és 1-től különböző algebrai szám, a kitevő pedig irracionális algebrai szám, állítható-e, hogy mindig transzcendens. Hilbert a problémát igen nehéznek gondolta, de Gelfond és Schneider 1934-ben megoldották. Később a megoldási módszert még élesíteni is sikerült (Baker, 1966.).

Ajánlott irodalom: Dringó és Kátai [6], Láng [24], valamint Szendrei [39].

5. Halmazok számossága

Ezidáig csak intuitív fogalmunk volt arról, hogy mit is jelent a véges és a végtelen. Hány eleme is van egy adott halmaznak? – kérdezhetjük. A pontos válasz csak az „elemek száma", a „halmaz számossága" fogalmak egzakt definíciója útján lehetséges. A fejezetben erre a kérdésre keressük a választ. A halmazok számossága elméletének alapjait CANTOR fektette le.

5.1. Számosság

5.1. definíció. *Legyen* A *és* B *két halmaz. Ha létezik közöttük egy* $A \to B$ *bijekció, akkor* A*-t és* B*-t* ***azonos számosságúnak*** *mondjuk és ezt a tényt* $A \sim B$*-vel jelöljük.*

Gyakran úgy is mondjuk, hogy „A ekvivalens B-vel." Ebben az értelemben például a $\{2, 3, 5, 7\}$ és $\{a, b, c, d\}$ halmazok ekvivalensek, csakúgy mint az $\{1, 3, 5, 7, 9, 11, \ldots\}$ és az $\{1, 6, 12, 18, 24, \ldots\}$ halmazok.

A halmazok azonos számossága alapján a halmazok számosságáról még semmit nem mondtunk. De ha jobban megfigyeljük, az azonos számosság $\sim$ relációja reflexív, szimmetrikus és tranzitív reláció, amit bijektív leképezések tulajdonságainak felhasználásával könnyen be is láthatunk.

5.2. definíció. *A* $\mathcal{H}$ *halmazrendszerben a* $\mathcal{H}/\sim$ *hányadoshalmaz egy elemét* ***számosságnak*** *nevezzük.*

Egy halmazrendszer minden A halmazához számosságot (idegen szóval kardinális számot) lehet hozzárendelni, $\mathcal{H}/\sim$ azon osztályát, amelyben A benne van, vagyis a $\text{card} : \mathcal{H} \to \mathcal{H}/\sim$, $A \mapsto \text{card}(A) = [A]$ függvényt definiáljuk. Jelölésben $\text{card}(A)$ helyett gyakran $|A|$-t vagy $\sharp A$-t írunk.

5.2. Véges, végtelen halmazok

5.3. definíció. *Egy* A *halmazt* ***végtelennek*** *nevezünk, ha létezik egy valódi* $B \subset A$ *részhalmaza, amelyre* $A \sim B$*. Ellenkező esetben* A*-t végesnek mondjuk.*

A definíció szerint $\mathbb{N}$ végtelen halmaz, míg $\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$, stb. véges halmazok. Figyeljük meg, hogy az azonos számosság fogalma által a véges és végtelen halmazok definíciója nem támaszkodik a természetes számok halmazára. Sőt, a $\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$, stb. által reprezentált számosságok tették lehetővé a természetes számok halmazának halmazelméleti megalapozását (4.1. fejezet). Véges halmazok esetén azonban a számosságot a természetes számokkal a legkönnyebb jellemezni.

5.4. definíció. *Legyen* $n \in \mathbb{N}^+$, A *pedig egy tetszőleges halmaz. Azt mondjuk, hogy az* A *halmaz* n*-elemű (vagy elemeinek száma* n*), ha létezik* $\{1, \dots, n\} \to A$ *bijekció.*

Valamely halmazrendszer számosságainak halmazán értelmezni lehet az összeadást, a szorzást és a hatványozást. Ennek során az összeadást halmazok egyesítésével, a szorzást a DESCARTES-féle szorzattal és a hatványozást az összes leképezés halmazával lehet definiálni:

$$\begin{aligned} \operatorname{card}(A) + \operatorname{card}(B) &\overset{\text{def}}{\Leftrightarrow} \operatorname{card}(A \cup B), \quad \text{ha } A \cap B = \varnothing, \\ \operatorname{card}(A) \cdot \operatorname{card}(B) &\overset{\text{def}}{\Leftrightarrow} \operatorname{card}(A \times B), \\ \operatorname{card}(A)^{\operatorname{card}(B)} &\overset{\text{def}}{\Leftrightarrow} \operatorname{card}(A^B), \quad \text{ahol } A^B = \{f \mid f : B \to A\}. \end{aligned}$$

Érvényesek továbbá a kommutativitás, asszociativitás és a disztributivitás törvényei, valamint a hatványokra vonatkozó szokásos törvények.

Valamely halmazrendszer számosságainak halmazában rendezési relációt lehet definiálni.

5.5. definíció. $\operatorname{card}(A) \preceq \operatorname{card}(B) \overset{\text{def}}{\Leftrightarrow} \exists C\ (C \subseteq B \wedge A \sim C)$.

A rövidség kedvéért gyakran csak $A \preceq B$-t írunk, és azt mondjuk, hogy B ***majorálja*** A-t. Ha $A \preceq B$, de $A \not\sim B$, akkor $A \prec B$-t írunk, és azt mondjuk, hogy B ***szigorúan majorálja*** A-t.

Világos, hogy minden halmazra $A \preceq A$ (reflexivitás), és az is, hogy ha $A \preceq B$ és $B \preceq C$, akkor $A \preceq C$ (tranzitivitás). Nem világos azonban, hogy ha $A \preceq B$ és $B \preceq A$, akkor ebből következik-e, hogy $A \sim B$. Az sem világos, hogy bármely két halmaz számossága összehasonlítható-e, azaz bármely A, B halmazokra $A \preceq B$ és $B \preceq A$ közül valamelyik fennáll ($\preceq$ gyengén trichotom). Az alábbi tételek (melyeket bizonyítás nélkül közlünk) választ adnak ezekre a kérdésekre.

5.6. tétel (Schröder–Bernstein). *Ha* $A \preceq B$ *és* $B \preceq A$*, akkor* $A \sim B$. □

5.7. tétel. *A* $\preceq$ *reláció gyengén trichotom.* □

Megmutatható, hogy a $\preceq$ reláció jólrendezés.

5.3. Megszámlálható és nem megszámlálható halmazok

A legkisebb végtelen halmazt a természetes számok alkotják. $\mathbb{N}$ számosságát $\aleph_0$-lal jelöljük (ejtsd: alef null vagy alef zéró[1]). Eszerint $\aleph_0$ a legkisebb végtelen számosság.

[1] $\aleph$ a héber ábécé első betűje.

5.8. definíció. *Valamely* A *halmazt* ***megszámlálhatónak*** *nevezünk, ha* $card(A) \preceq \aleph_0$*,* ***megszámlálhatóan végtelennek,*** *ha* $card(A) = \aleph_0$*, és* ***nem megszámlálhatónak*** *mondjuk, ha* $card(A) \succ \aleph_0$*.*

Ha A végtelen és B megszámlálható halmaz, akkor

$$\text{card}(A) \succeq \aleph_0 \text{ és } \text{card}(B) \preceq \aleph_0 \Rightarrow \text{ card}(A \cup B) \sim \text{card}(A).$$

Ennek megfelelően megszámlálható halmaz bármely részhalmaza is megszámlálható. Egy végtelen halmaz pontosan akkor megszámlálható számosságú, ha elemei sorozatba rendezhetőek.

5.9. tétel. *Az* $\mathbb{N} \times \mathbb{N}$ *halmaz megszámlálhatóan végtelen.*

Bizonyítás. Soroljuk fel a természetes számpárokat az alábbi táblázat szerint:

$$\begin{array}{cccc} (0,0) & (0,1) & (0,2) & (0,3) & \dots \\ (1,0) & (1,1) & (1,2) & (1,3) & \dots \\ (2,0) & (2,1) & (2,2) & (2,3) & \dots \\ (3,0) & (3,1) & (3,2) & (3,3) & \dots \\ \vdots & \vdots & \vdots & \vdots & \end{array}$$

A táblázat elemei egyetlen sorozatba rendezhetőek:

$$(0,0), (0,1), (1,0), (2,0), (1,1), (0,2), (0,3), (1,2), (2,1), (3,0), \dots$$

$\mathbb{N} \times \mathbb{N}$ elemeiből álló halmaz tehát megszámlálhatóan végtelen. □

5.10. tétel. $\mathbb{Q}$ *megszámlálhatóan végtelen.*

Bizonyítás. Az 5.9. tétel bizonyításhoz hasonlóan járunk el. Ha az alábbi táblázat elemeit az iménti „átlós eljárással" sorba rendezzük, egy szürjektív $f : \mathbb{N} \to \mathbb{Q}$ leképezést kapunk.

$$\begin{array}{cccccc} 0, & \frac{1}{1} & -\frac{1}{1} & \frac{2}{1} & -\frac{2}{1} & \dots \\ & \frac{1}{2} & -\frac{1}{2} & \frac{2}{2} & -\frac{2}{2} & \dots \\ & \frac{1}{3} & -\frac{1}{3} & \frac{2}{3} & -\frac{2}{3} & \dots \\ & \vdots & \vdots & \vdots & \vdots & \end{array}$$

Ha minden olyan törtet „átugrunk", amely más előállításban korábban már szerepelt, akkor a leképezés bijektív lesz. □

5.11. tétel. *Megszámlálhatóan végtelen halmazok megszámlálhatóan végtelen családjának egyesítése megszámlálhatóan végtelen.*

Bizonyítás. Legyen I megszámlálhatóan végtelen, és A_i megszámlálhatóan végtelen minden $i \in$ I-re. $I \sim \mathbb{N}$ ismeretében készítsük el az alábbi halmazokat:

$$\begin{aligned} B_0 &= A_0 \\ B_i &= A_i \setminus (\cup_{j<i} B_j) \quad i = 1, 2, 3, \dots \end{aligned}$$

Ekkor $B_i \cap B_j = \varnothing \ \ (i \neq j)$ és $\cup A_i = \cup B_i$. Mivel minden $i \in$ I-re $B_i \subseteq A_i$, ezért a B_i halmazok is megszámlálható számosságúak, így elemeik sorozatba rendezhetőek:

$$\begin{aligned} B_0 &= \{b_{00}, b_{01}, b_{02,\dots}\} \\ B_1 &= \{b_{10}, b_{11}, b_{12,\dots}\} \\ B_2 &= \{b_{20}, b_{21}, b_{22,\dots}\} \\ &\vdots \end{aligned}$$

Ezekből a sorozatokból az „átlós eljárással" újat készítve bijektív módon képeztük le $\cup A_i$ $(i \in I)$ elemeit $\mathbb{N}$-be. □

5.12. következmény. $\mathbb{Z}, \mathbb{N}^n \ (n \in \mathbb{N}^+), \cup_{n=0}^{\infty} \mathbb{N}^n$ *megszámlálhatóan végtelen halmazok.*

Vajon minden végtelen halmaz megszámlálható?

5.13. tétel (Cantor). *Bármely* A *halmazra* $A \prec \wp(A)$.

Bizonyítás. Az $a \mapsto \{a\}$ kölcsönösen egyértelmű leképezése A-nak $\wp(A)$-ba, ezért $A \preceq \wp(A)$. A továbbiakban indirekt módon tegyük fel, hogy létezik egy f bijektív leképezés A-ból $\wp(A)$-ba. Legyen $B = \{a \in A \mid a \notin f(a)\}$. Ha valamely $b \in$ B-re $f(b) = B$, akkor a B halmaz definíciója szerint $b \in B$ nem lehetséges. De $b \notin B$ sem lehetséges, mert $f(b) = B$ miatt $b \in B$ következne. Ez ellentmond f bijektivitásának. □

Az iménti bizonyítás alapeszméje, hogy ha adott végtelen 0–1 sorozatok egy $(f_n, n \in \mathbb{N})$ végtelen sorozata, akkor a $g(n) = 1 - f_n(n)$ sorozat az iménti felsorolásban nem szerepel. Ezt a konstrukciót Cantor-***féle átlós eljárásnak*** nevezzük.

Az 5.13. tétel következménye, hogy $\mathbb{N}$-ből könnyen lehet nagyobb számosságú végtelen halmazt konstruálni, más szóval a végtelen halmazok számossága nem azonos.

5.14. tétel. $\mathbb{R}$ *nem megszámlálható.*

Bizonyítás. Legyen $J = \{x \mid 0 < x < 1, \ x \in \mathbb{R}\}$. Mivel az $f : J \to \mathbb{R}$,

$$f(x) = \frac{x - \frac{1}{2}}{x(x-1)}$$

függvény bijektív, ezért elegendő J nem megszámlálhatóságát bizonyítani. Indirekt módon tegyük fel, hogy létezik egy $\mathbb{N} \to J$ bijekció. A 4.37. tételnél említettük, hogy eltekintve azoktól a tizedes törtektől, amelyek kifejtésében valahonnan kezdve csupa 9-es áll, a többi tizedestört kölcsönösen egyértelműen megfeleltethető a valós számoknak. Ennek megfelelően soroljuk fel J összes elemét, és írjuk fel ezeket az

elemeket tizedes tört alakban:

$$\begin{aligned} j_0 &= 0.z_{00}z_{01}z_{02}z_{03}\dots \\ j_1 &= 0.z_{10}z_{11}z_{12}z_{13}\dots \\ j_2 &= 0.z_{20}z_{21}z_{22}z_{23}\dots \\ &\vdots \end{aligned}$$

Ekkor a $0.\hat{z}_0\hat{z}_1\hat{z}_2\dots$ szám biztosan nem szerepel az iménti felsorolásban, amennyiben $\hat{z}_i \neq z_{ii}$ és $\hat{z}_i \neq 9$. Ez ellentmond J felsorolhatóságának. □

5.15. definíció. *Valamely A halmazt* ***kontinuum-számosságúnak*** *nevezünk, ha ekvivalens $\mathbb{R}$-rel.*

Kontinuum-számosságú halmazok természetesen végtelenek. Az alábbi tételt bizonyítás nélkül közöljük.

5.16. tétel. $\wp(\mathbb{N}), \mathbb{R}^n$ $(n \in \mathbb{N}^+)$ *(és így a komplex számok $\mathbb{C}$ halmaza és a kvaterniók is) kontinuum-számosságúak.*

A tételnek megfelelően egy egyenes pontjainak halmaza és a háromdimenziós euklideszi tér pontjainak halmaza azonos számosságú.[2]

A fejezetben megmutattuk, hogy $\mathbb{N} \prec \mathbb{R}$. Cantor vetette fel azt a kérdést, hogy van-e valami a kettő között, azaz létezik-e olyan A halmaz, amelyre $\mathbb{N} \prec A \prec \mathbb{R}$. Az az állítás, hogy ilyen halmaz nincs a ***kontinuumsejtés*** vagy ***kontinuumhipotézis.*** Általánosabban, mivel bármely A halmazra $A \prec \wp(A)$, megkérdezhetjük, hogy van-e olyan B végtelen halmaz és A halmaz, hogy $B \prec A \prec \wp(B)$. Az az állítás, hogy ilyen halmazok nincsenek, az ***általánosított kontinuumsejtés***. 1963-ban Cohen bebizonyította, hogy a válasz attól függ, milyen halmazelméletet választunk. A standard változat, a Zermelo–Fraenkel–choice halmazelmélet (ZFC) ellentmondásmentességét feltételezve (ezt reméljük) a kontinuumhipotézist sem benne megcáfolni, sem bebizonyítani nem lehet.

A fejezet végén azzal a kérdéssel foglalkozunk, hogy milyen bizonyítási módszerek és konstrukciók lehetségesek a különféle végtelen halmazokon. A 4. fejezetben láttuk, hogy a természetes számokon a teljes indukció és a rekurziótétel nyújt kiváló lehetőségeket. De mi a helyzet más (végtelen) számhalmazokon? Az alábbi, bizonyítás nélkül közölt tételek választ adnak erre a kérdésre. Az általánosítás alapját a jólrendezett halmazok képezik.

Legyen $(W; <)$ egy jólrendezés. Adott $t \in W$-re vezessük be az alábbi jelölést:

$$\operatorname{seg} t = \{x \in W \mid x < t\}.$$

A $\operatorname{seg} t$ halmaz tehát egy jólrendezett halmaz t-nél kisebb elemeit tartalmazza (szelet).

[2] Néha magát Cantor-t is kétségek gyötörték. Amikor három évi ellenkező irányú próbálkozás után bebizonyította, hogy az n-dimenziós térnek pontosan ugyanannyi pontja van, mint az egydimenziósnak, ezt írta: „Látom, de nem hiszem el." Reymond egyenesen úgy fogalmazott: „A józan ész számára visszataszító." Ám a Cantor-i gondolat segítségével a matematikai analízis számos problémáját sikerült a „helyére tenni," olyannyira, hogy korának vezető matematikusa, Hilbert 1926-ban ezt írta: „Senki sem űzhet ki minket a Cantor által teremtett paradicsomból."

5.17. tétel (transzfinit indukció). *Legyen* $(W;<)$ *egy jólrendezés. Tegyük fel, hogy a* $B \subseteq W$ *halmaz minden* $t \in W$ *elemére*

$$\operatorname{seg} t \subseteq B \Rightarrow t \in B.$$

Ekkor $B = W$.

A módszer a teljes indukció (4.1. fejezet) általánosítása. Felhasználhatóságát a jólrendezési tétel biztosítja. A tételt általában arra használjuk, hogy megmutassuk, egy W jólrendezett halmaz minden elemére teljesül valamilyen tulajdonság. Először azon elemeket gyűjtjük össze egy B halmazba, amelyekre teljesül a tulajdonság, majd az indukciós lépésben megmutatjuk, hogy ha minden $x < t$ elemnek megvan az adott tulajdonsága, akkor t-nek is megvan. A teljes indukcióval ellentétben tehát itt nincs külön alapeset.

Emlékezzünk vissza a 4.4. rekurziótételre, miszerint egy sorozatot megadhatunk úgy, hogy megadjuk a 0 helyen felvett értékét, és megadunk egy képzési szabályt, amely alapján a sorozat n helyen felvett értékéből kiszámítjuk az $n+1$ helyen felvett értékét. De mi van akkor, ha a sorozat egy tagja nemcsak az őt közvetlen megelőzőtől függ? Ilyenkor a rekurziótétel nem használható. A rekurziótétel alábbi általánosabb változata lehetővé teszi, hogy egy sorozat egy tagját az *összes* előző tag függvényeként adhassuk meg. A tételt általában $\mathbb{N}$-re alkalmazzuk, de tetszőleges jólrendezett halmazra érvényes, innen ered a neve. A tételt bizonyítás nélkül közöljük.

5.18. tétel (transzfinit rekurziótétel). *Legyen* $(W;<)$ *egy jólrendezés, és* A *egy tetszőleges nem üres halmaz. Tegyük fel, hogy minden* $x \in \wp(W)$ *halmazhoz egyértelműen létezik olyan* $y \in \wp(A)$ *halmaz, amelyre a* $\gamma(x, y)$ *kijelentésformula* IGAZ. *Ekkor egyértelműen létezik olyan* $f : \wp(W) \to \wp(A)$ *függvény, amikor minden* $t \in W$*-re* $\gamma(f|_{\operatorname{seg} t}, f(t))$ IGAZ.

A tétel jelentősége a számítástudományban ott van, hogy segítségével olyan f rekurzív függvények, eljárások adhatók, amelyeknél minden $f(t)$ függvényérték a már korábban kiszámolt $f(x), x < t$ értékek függvénye. Másszóval a rekurziótétel és a transzfinit rekurziótétel következményeként használhatunk rekurzív eljárásokat és függvényeket a számítógépek programozásánál. A következő fejezetben példát is látunk a tétel alkalmazására.

Gyakorlatok

5.3-1. Adjunk bijektív leképezést
(a) két különböző hosszúságú szakasz pontjai között,
(b) a $[0, 1]$ intervallum és az egységnyi oldalú négyzet pontjai között.

5.3-2. Tekintsük az $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$,

$$f(m, n) = \frac{k(k+1)}{2} + m$$

függvényt, ahol $k = m + n$. Bizonyítsuk be, hogy f bijektív. Ezzel az 5.9. tétel egy alternatív bizonyítását adtuk.

5.3-3. Bizonyítsuk be, hogy az algebrai számok halmazának számossága megszámlálhatóan végtelen. Ennek felhasználásával lássuk be azt is, hogy léteznek transzcendens számok, ráadásul a számosságuk nagyobb az algebrai számok halmazának

számosságánál.

5.3-4. A 4. fejezetben láttuk, hogy $(\mathbb{Q};\leq)$ és $(\mathbb{R};\leq)$ nem jólrendezettek, mert $(\mathbb{Z};\leq)$ sem az. Adjunk meg $\mathbb{Q}$-ra egy jólrendezést. A módszer $\mathbb{R}$ esetében miért nem működik? Megjegyezzük, hogy $\mathbb{R}$-re nem ismeretes jólrendezés, holott a jólrendezési tétel értelmében minden halmaz jólrendezhető.

Megjegyzések a fejezethez

A számosságokkal kapcsolatos legalapvetőbb ismeretek megtalálhatók Dringó és Kátai [6], valamint Szendrei [39] könyvében. Axiomatikus tárgyalást olvashatunk továbbá Hajnal és Hamburger [16] munkájában.

6. Kombinatorika

A kombinatorika véges halmazok elemeinek elrendezéseivel, az elrendezések különböző lehetőségeinek megszámlálásával foglalkozik. Ilyenek például emberek ülésrendje egy teremben, figurák elrendezése a sakktáblán, betűk elrendezése egy szóban, nyerési lehetőségek egy szerencsejátékban, stb. Számos kérdés ered a valószínűségszámításból és a szórakoztató matematikából. A kombinatorikának szoros kapcsolata van a számelmélettel, csoportelmélettel, geometriával és a gráfelmélettel is. A fejezet első részében megkíséreljük a problémákat alapmintákra visszavezetni, és általános módszereket kifejleszteni. A fejezet második részében kombinatorikai problémák megoldása során jól használható tételeket bizonyítunk, a binomiális- és polinomiális tételt, a skatulya-elvet és a logikai szita formulát. A fejezet végén speciális számokkal és kombinatorikai összefüggésekkel foglalkozunk.

6.1. Permutáció, variáció, kombináció

6.1. definíció. *Legyen A egy tetszőleges n elemű halmaz. Az n elem valamely sorrendben való felsorolását (elrendezését) az A halmaz* ***permutációjának*** *nevezzük.*

Keressük az A halmaz összes különböző permutációinak számát. Jelöljük ezt a számot P_n-el. A problémát máshogy megfogalmazva, ha $S_n = \{\varphi \mid \varphi : A \to A, \text{bijektív}\}$, akkor $P_n = |S_n|$ keresett. Láthatjuk, hogy S_n az A halmazon értelmezett permutációfüggvények száma. Bevezetjük az $n!$ (olvasd „n faktoriális") jelölést az első n pozitív természetes szám szorzatára, tehát $n! = 1 \cdot 2 \cdot \ldots \cdot n$. Megállapodunk abban, hogy $0! = 1$.

6.2. tétel. $P_n = n!$.

Bizonyítás. Teljes indukcióval bizonyítunk. $n = 1$ esetén $P_1 = 1 = 1!$, tehát az állítás igaz. Legyen $n > 1$ és tegyük fel, hogy $n-1$-ig igaz az állítás. Létesítsünk relációt az n elemű permutációk halmazán. Legyen két permutáció relációban, ha az elrendezésben az első elemük megegyezik. Ez a reláció ekvivalenciareláció, tehát osztályoz. Az osztályok száma n, hiszen ennyi különböző elem állhat az első helyen. Egy-egy osztályba P_{n-1} elem kerül, így az összes permutáció száma $P_n = n \cdot P_{n-1}$. Az indukciós feltevés szerint $P_n = n \cdot (n-1)! = n!$. □

n	0	1	2	3	4	5	6	7	8	9	10
$n!$	1	1	2	6	24	120	720	5040	40320	362880	3628800

6.1. ábra. A faktoriális függvény első néhány értéke.

6.1. példa. 10 ember 10 széken való különböző ülésrendjeinek a száma $P_{10} = 10! = 3\,628\,800$.

6.2. példa. A 3 elemű halmazon értelmezett permutációfüggvények száma $3! = 6$, a konkrét függvényeket a 2.14. példa mutatja.

A 6.1. ábra a faktoriális függvény értékeit mutatja az első néhány helyen. Hasznos megjegyeznünk az első hat faktoriális értékét, valamint azt a tényt, hogy $n!$ jegyeinek a száma meghaladja n-et, ha $n \geq 25$. Nagy n értékekre $n!$ kiszámítása műveletigényes ($n-1$ szorzás), ilyenkor a STIRLING-formula ad jól használható becslést:

$$n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

Permutációkkal kapcsolatban időnként felmerül a ***ciklikus permutálás*** fogalma. Egy adott permutációban lévő elemeket ciklikusan permutálunk, ha minden elem helyére a rákövetkezőt, az utolsó elem helyére pedig az elsőt írjuk. Hasonlóan lehet a „másik irányba" ciklikusan permutálni. Nyilvánvaló, hogy egy n elemű permutációt n-szer egymás után ciklikusan permutálva visszakapjuk a kiindulásul vett permutációt.

A permutációk egy általánosabb elrendezési probléma speciális esetét képezik. Ahelyett, hogy n számú elemből n elemű sorozatokat képeznénk, tekinthetünk k számú elemből álló sorozatokat, ahol $k \leq n$.

6.3. definíció. *Egy n elemű halmaz elemeiből képezhető k tagú ($k \leq n$), különböző elemekből álló sorozatát az n elem k-ad osztályú (ismétlés nélküli)* ***variációjának*** *nevezünk.*

Jelölje V_n^k az n elem összes k-ad osztályú variációinak számát.

6.4. tétel. $V_n^k = P_n/P_{n-k} = n(n-1)\dots(n-k+1)$.

Bizonyítás. Tekintsük ismét az n elem összes permutációját, és létesítsünk a permutációk között relációt az alábbi módon: két permutáció akkor legyen relációban, ha az első k elemük megegyezik. Könnyű belátni, hogy ekvivalenciarelációt kapunk. Az összes permutációt megkapjuk, ha megnézzük, hogy egy osztályban hány elem található, és hány osztály van. Az egy osztályba kerülő elemek száma P_{n-k}, vagyis annyi, ahányféleképpen a többi $n-k$ elem felsorolható. Különböző osztályokba pedig akkor kerül két permutáció, ha az első k helyen valahol van köztük eltérés. Így tehát annyi osztály van, ahányféleképpen n elemből k tagú sorozatot képezhetünk, vagyis V_n^k. Ezek szerint $P_n = V_n^k \cdot P_{n-k}$, amiből a tétel állítása következik. □

6.3. példa. Arra, hogy 6 ember 10 széken foglaljon helyet, $V_{10}^6 = 10!/4! = 151\ 200$ lehetőség van (feltéve, hogy minden ember más-más széken ül).

A legtöbb kártyajátékban nincs jelentősége annak, hogy a kártyákat a leosztásnál milyen sorrendben kapjuk meg, mivel a nálunk lévő lapok tetszés szerint átrendezhetők. Itt tehát az adott n elemű halmaz részhalmazai érdekelnek bennünket.

6.5. definíció. *Egy n elemű halmaz k elemű részhalmazait a halmaz k-ad osztályú (ismétlés nélküli)* ***kombinációinak*** *nevezzük.*

A kombinációk számát jelöljük C_n^k-val. Vezessük be az

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

jelölést (olvasd „n alatta k"). Mivel $0! = 1$, ezért $\binom{n}{0} = 1$ és $\binom{n}{n} = 1$, valamint, ha $n < k$, akkor legyen $\binom{n}{k} = 0$.

6.6. tétel. *Ha $n \geq k$, akkor*

$$C_n^k = \frac{V_n^k}{P_k} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

Bizonyítás. n elem k-ad osztályú variációinak száma V_n^k. Ezeket a variációkat úgy is előállíthatjuk, hogy képezzük az n elemű halmaz k elemű részhalmazait, majd a kapott k elemet az összes lehetséges módon sorba rakjuk. Ez a sorbarakás P_k-féleképpen történhet. Ily módon minden variációt pontosan egyszer kapunk meg, ezért $V_n^k = C_n^k P_k$, amiből a tétel állítása következik. □

6.4. példa. Ahhoz, hogy az ötös lottón biztos telitalálatunk legyen, $\binom{90}{5} = 43\ 949\ 268$ darab szelvényt kell kitöltenünk (természetesen különbözőképpen).

Most azt az esetet vizsgáljuk, hogy egy n darab kártyát tartalmazó csomagból sorban k darabot húzunk, az eredményeket mindig feljegyezzük, és minden húzás után a kihúzottat visszatesszük a csomagba. Így ugyanis fennáll annak a lehetősége, hogy egy kártyát többször is kihúzunk.

6.7. definíció. *Egy n elemű halmaz elemeiből készíthető olyan k tagú sorozatokat, ahol egy elem többször is előfordulhat, a halmaz k-ad osztályú* ***ismétléses variációjának*** *nevezzük.*

Jelölje az ilyen sorozatok számát $V_n^{k,i}$.

6.8. tétel. $V_n^{k,i} = n^k$.

Bizonyítás. A bizonyítást rögzített n-re k szerinti indukcióval végezzük. Legyen $k = 1$. Ekkor $V_n^{1,i} = n$, tehát az állítás igaz. Legyen $k > 1$, és tegyük fel, hogy $k-1$-ig igaz az állítás. k-ad osztályú ismétléses variációkat úgy is képezhetünk, hogy sorban vesszük a $k-1$ osztályúakat, és a k-adik helyre elhelyezünk még egy elemet. Ezt n-féleképpen tehetjük meg, így $V_n^{k,i} = V_n^{k-1,i} \cdot n = n^{k-1} \cdot n = n^k$. □

6.5. példa. Egy totószelvényt (13 helyre 1,x vagy 2 kerülhet) $3^{13} = 1\,594\,323$-féleképpen lehet kitölteni.

6.6. példa. Mennyi egy n elemű A halmaz összes részhalmazai száma?

Megoldás: Mivel minden elem A valamely részhalmazához való tartozása a karakterisztikus függvénnyel egyértelműen jellemezhető, így az összes részhalmazok száma megegyezik az n-tagú $0, 1$ jegyekből álló különböző sorozatok számával, ami $V_2^n = 2^n$.

6.7. példa. Tegyük fel, hogy egy érvényes számítógépes azonosító hét karakterből áll, az első karakter az $\{A, B, C, D, E, F, G\}$ betűk valamelyike, a többi hat karakter pedig a 26 betűs angol ábécé vagy a 10 számjegy közül való. A kis és nagybetűket különbözőnek tekintjük.

Megoldás: Az első betűt $\binom{7}{1}$-féleképpen választhatjuk, a többit pedig 62^6-féleképpen $(62 = 2 \cdot 26 + 10)$. Ez mindösszesen 397 601 649 088 lehetőség.

6.9. definíció. *Egy n-elemű halmazból k elem oly módon történő kiválasztását, hogy egy elem többször is kiválasztható, a sorrendre viszont nem vagyunk tekintettel, a halmaz k-ad osztályú* ***ismétléses kombinációjának*** *nevezzük.*

Az ismétléses kombinációk számát $C_n^{k,i}$-vel jelöljük.

6.10. tétel. $C_n^{k,i} = C_{n+k-1}^k$.

Bizonyítás. Valamely n-elemű halmaz k-ad osztályú ismétléses kombinációja úgy is megadható, hogy a k elemet tetszőleges sorrendben felsoroljuk, például növekvően, vagyis az ismétléses kombinációk száma az n elemből képezhető k-elemű monoton növekvő sorozatok számával egyezik meg. Hasonló gondolattal valamely n elemű halmaz k-ad osztályú ismétlés nélküli kombinációi száma az n elemből képezhető k elemű szigorúan monoton sorozatok számával egyezik meg. Ennek megfelelően definiáljunk két halmazt:

$$\begin{aligned} A &= \{(a_1, a_2, \ldots, a_k) \mid a_j \in \mathbb{N},\ 1 \le a_1 \le a_2 \le \ldots \le a_k \le n\}, \\ B &= \{(b_1, b_2, \ldots, b_k) \mid b_j \in \mathbb{N},\ 1 \le b_1 < b_2 < \ldots < b_k \le n + k - 1\}. \end{aligned}$$

Mivel $|A| = C_n^{k,i}$ és $|B| = C_{n+k-1}^k$, a tétel bizonyításához elegendő egy bijekciót létesíteni a két halmaz között. Más megfogalmazásban bijekciót keresünk egy $f_1 : [1, k] \to [1, n]$ monoton növekedő és egy $f_2 : [1, k] \to [1, n+k-1]$ szigorúan monoton növekedő függvény között. A $h(j) = f_1(j) + j - 1$ összefüggéssel definiált függvény pontosan megfelel a követelményeknek. □

6.8. példa. 5 darab szabályos dobókockával $C_6^{5,i} = \binom{10}{5} = 252$ különböző dobás lehetséges.

6.11. definíció. *Ha egy n számú elemből álló sorozatban az elemek között k számú egymástól különböző van $(k \le n)$, ezek rendre $n_1, n_2, \ldots, n_k$ gyakorisággal fordulnak elő, és $n = n_1 + n_2 + \ldots + n_k$, akkor n-elemű* ***permutációról*** *beszélünk $n_1, n_2, \ldots, n_k$ számú* ***ismétléssel****.*

Jelölje ezen permutációk számát $P_n^{n_1,n_2,\dots,n_k}$.

6.12. tétel.

$$P_n^{n_1,n_2,\dots,n_k} = \frac{n!}{n_1!n_2!\cdots n_k!}.$$

Bizonyítás. A bizonyítást k szerinti indukcióval végezzük. $k = 1$ esetén $P_n^n = 1 = n!/n!$. Legyen $k > 1$ és tegyük fel, hogy $k-1$ számú különböző elem esetén igaz az állítás. Legyen ezek után k különböző elem $n_1, n_2, \dots, n_k$ előfordulási gyakoriságokkal adott. Az ismétléses permutációk között készítsünk relációt: két permutáció akkor legyen relációban, ha elhagyva belőlük az n_k-szor előforduló elemet, azonos permutációhoz jutunk. Könnyű belátni, hogy ez a reláció ekvivalenciareláció, az osztályok száma $P_{n-n_k}^{n_1,n_2,\dots,n_{k-1}}$. Most számoljuk össze az osztályok elemszámát. A $k-1$ különböző elemből álló permutációból annyiféleképpen tudunk k eleműt készíteni, ahányféleképpen az $n-n_k+1$ lehetséges hely közül (s darab sorbarakott tárgy között $s-1$ darab helyre, valamint az első elé és az utoló mögé lehet rakni) n_k darab kiválasztható, megengedve egy hely többszöri kiválasztását is. Egy osztályban tehát $C_{n-n_k+1}^{n_k,i} = C_n^{n_k}$ elem lesz. Ezért az ismétléses permutációk száma

$$P_n^{n_1,n_2,\dots,n_k} = P_{n-n_k}^{n_1,\dots,n_{k-1}} C_n^{n_k} = \frac{(n-n_k)!}{n_1!n_2!\cdots n_{k-1}!}\frac{n!}{n_k!(n-n_k)!} = \frac{n!}{n_1!n_2!\cdots n_k!}.$$

□

6.9. példa. Két piros, négy fehér, egy zöld, valamint egy sárga golyót $8!/(2!4!1!1!) = 840$-féleképpen lehet sorbarakni.

Jegyezzük meg, hogy az ismétléses permutáció fogalma különbözik az ismétléses variáció és kombináció fogalmától. Az ismétléses permutáció esetében rögzítjük, hogy melyik típusú elemből hányat választhatunk, míg az utóbbiaknál bármelyik elemet akárhányszor felhasználhatjuk.

A fejezetben látott alapesetek a gyakorlatban nem önállóan, hanem vegyesen fordulnak elő.

6.10. példa. Egy trafikban kapható k fajta képeslap közül $\binom{k}{2}^n$-féleképpen küldhetünk n barátunknak 2-2 különbözőt.

6.11. példa. 5 lapot húzunk egy 52 lapos francia kártyacsomagból. Az összes lehetőség közül hány esetben lesz a lapok között

a) legalább egy ász;

b) pontosan egy ász;

c) legfeljebb egy ász?

Az a) esetben célszerű először a „rossz" eseteket összeszámlálni. A csomagban 4 ász van, ezért $\binom{48}{5}$ esetben nincs a kihúzott lapok között ász. Az összes lehetséges húzások száma $\binom{52}{5}$, így legalább egy ász $\binom{52}{5} - \binom{48}{5}$ esetben lesz. A b) kérdésnél az egyetlen ászt négyféleképpen választhatjuk, és bármely választásnál a maradék 4 lapot $\binom{48}{4}$-féleképpen. Tehát a válasz $4 \cdot \binom{48}{4}$. A c) esetben vagy egyetlen ászt húzunk vagy egyet sem, így a korábbi megfontolások alapján $4 \cdot \binom{48}{4} + \binom{48}{5}$ esetben húzunk legfeljebb egy ászt.

Gyakorlatok

6.1-1. Hány csupa különböző jegyből álló hatjegyű szám képezhető? Ezen számok közül hány olyan van, amelyikben pontosan 4 páratlan számjegy szerepel?
6.1-2. Az n-elemű A halmazon hány homogén binér reláció van?
6.1-3. Hányféleképpen ültethet le Hófehérke egy hosszú asztal mellé a 7 törpe közül ötöt, ha Tudor és Kuka nem ülhet egymás mellé?
6.1-4. Artúr király kerekasztala körül 12 lovag ül. Mindegyikük hadilábon áll a szomszédjával (és csak velük). Hányféleképpen választhat a király a hercegnő kiszabadítására 5 lovagot úgy, hogy ne legyenek közöttük ellenségek? És n lovag közül k-t?

6.2. Binomiális és polinomiális tétel

Az alábbiakban két lényeges állítást vizsgálunk összegek hatványairól. Az állítások tetszőleges egységelemes kommutatív gyűrűben igazak, de mi az egyszerűség kedvéért testben ($\mathbb{R}$ vagy $\mathbb{C}$) mondjuk ki őket. Mindkét állítás bizonyításakor messzemenően kihasználjuk az általános asszociativitás, kommutativitás és disztributivitás tételét (4.13. tétel).

6.13. tétel (binomiális tétel). *Legyen* $x, y \in \mathbb{R}$ *és legyen* $n \in \mathbb{N}^+$. *Ekkor*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Bizonyítás. Az n tényezős $(x+y)^n$ szorzatot kifejtve $x^k y^{n-k}$ alakú tagokat kapunk ($0 \le k \le n$). Egy ilyen tag úgy keletkezik, hogy az n tényező közül k-ból az x-et, $n-k$-ból az y-t választjuk. Rögzített k-ra az $x^k y^{n-k}$ tag annyiszor fog előállni, ahányszor az n tényezőből a k darab x-et kiválaszthatjuk, vagyis $\binom{n}{k}$-szor. k-ra összegezve kapjuk a tétel állítását. □

Az $\binom{n}{k}$ alakú számok innen kapták a ***binomiális együttható*** elnevezést.

6.14. következmény. *Legyen* $n \in \mathbb{N}^+$. *Ekkor,* $x = y = 1$, *illetve* $x = 1, y = -1$ *behelyettesítésével az előző tételbe kapjuk, hogy*

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n,$$

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0.$$

□

Vajon mi a helyzet akkor, ha kettő helyett több tagú összeg n-edik hatványát szeretnénk kiszámítani?

6.15. tétel (polinomiális tétel). *Legyen* $x_1, x_2, \ldots, x_r \in \mathbb{R}$ *és legyen* $r, n \in \mathbb{N}^+$. *Ekkor*

$$(x_1 + x_2 + \ldots + x_r)^n = \sum_{i_1+i_2+\ldots+i_r=n} P_n^{i_1,i_2,\ldots,i_r} x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r}.$$

Bizonyítás. A bizonyítást r szerinti teljes indukcióval végezzük. Az $r = 1$ eset nyilvánvaló. Legyen $r > 1$ és tegyük fel, hogy $r-1$-ig igaz az állítás. Végezzük el az $x_2 + \ldots + x_r = u$ helyettesítést és tekintsük a binomiális tételt. Ekkor

$$(x_1 + x_2 + \ldots + x_r)^n = (x_1 + u)^n = \sum_{i_1=0}^{n} \binom{n}{i_1} x_1^{i_1} u^{n-i_1}.$$

Az indukciós feltevést u^{n-i_1}-re alkalmazva

$$\sum_{i_1=0}^{n} \binom{n}{i_1} x_1^{i_1} \sum_{i_2+i_3+\ldots+i_r=n-i_1} P_{n-i_1}^{i_2,i_3,\ldots,i_r} x_2^{i_2} x_3^{i_3} \cdots x_r^{i_r} =$$

$$= \sum_{i_1+i_2+\ldots+i_r=n} \binom{n}{i_1} P_{n-i_1}^{i_2,i_3,\ldots,i_r} x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r}.$$

Felhasználva, hogy

$$\binom{n}{i_1} P_{n-i_1}^{i_2,i_3,\ldots,i_r} = \frac{n!}{i_1!(n-i_1)!} \frac{(n-i_1)!}{i_2! \cdots i_r!} = P_n^{i_1,\ldots,i_r},$$

a bizonyítás kész. □

6.3. A skatulya-elv és a logikai szita-formula

Egyszerű, de igen hasznos gondolatot fogalmazunk meg az alábbiakban.

6.16. tétel (skatulya-elv). *Ha* $n+1$ *darab dolgot* n *skatulyába kell elhelyeznünk, akkor legalább egy skatulyába legalább két dolog kerül.* □

Ez másrészt azt jelenti, hogy egy n-elemű halmaz n-elemű halmazra való leképezése akkor és csak akkor injektív, ha szürjektív.

6.12. példa. Megmutatjuk, hogy az $A = \{1, 2, \ldots, 7, 8\}$ halmazból bárhogy is választunk ki ötöt, közülük valamelyik kettőnek az összege pontosan 9.

Konstruáljunk 4 halmazt az alábbi módon: $A_1 = \{1, 8\}$, $A_2 = \{2, 7\}$, $A_3 = \{3, 6\}$, $A_4 = \{4, 5\}$. Az A halmazból kiválasztott öt szám mindegyike benne lesz $A_1, \ldots, A_4$ valamelyikében. De mivel ez csak négy halmaz, valamelyik két szám ugyanabba a halmazba fog tartozni. Márpedig a halmazokon belüli számok összege mindig 9.

6.17. tétel (Általános skatulya-elv). *Ha* n *darab dolgot* m *darab skatulyába kell elhelyeznünk, akkor lesz olyan skatulya, ahol legalább* $\lfloor (n-1)/m \rfloor + 1$ *dolog kerül.*

Bizonyítás. Indirekt bizonyítunk. Ha a skatulyák legfeljebb $\lfloor (n-1)/m \rfloor$ elemet tartalmaznának, akkor összesen legfeljebb $m \cdot \lfloor (n-1)/m \rfloor \leq m \cdot (n-1)/m = n-1$ elemünk lenne. □

6.13. példa. Megutatjuk, hogy 30 tetszőlegesen választott ember közül mindig van 5 olyan, akik a hét ugyanazon napján születtek.

A hét napjai lesznek a skatulyák, így az iménti tételnek megfelelően $n = 30$ és $m = 7$. Ekkor $\lfloor (30-1)/7 \rfloor + 1 = 5$ ember biztosan a hét ugyanazon napján ünnepli a születésnapját.

Az alábbi módszer számos kombinatorikai feladat megoldásának kulcsa.

Legyen adott N objektum, amelyek közül bizonyosak rendelkeznek az előre megadott $\alpha_1, \alpha_2, \ldots, \alpha_n$ tulajdonságok közül egyesekkel. Az N objektum bármelyikének lehet több tulajdonsága is, vagy akár egy sem. Jelölje $N(\alpha_i, \alpha_j, \ldots, \alpha_k)$ azon objektumok számát, amelyek az $\alpha_i, \alpha_j, \ldots, \alpha_k$ tulajdonságok mindegyikével (esetleg továbbiakkal is) rendelkeznek. Ha hangsúlyozni akarjuk, hogy olyan objektumot választunk ki, amelyik valamelyik tulajdonsággal nem rendelkezik, akkor azt fölülvonással jelöljük. Például $N(\alpha_1, \alpha_3, \overline{\alpha}_4)$ jelenti azon objektumok számát, amelyek az α_1 és α_3 tulajdonságokkal rendelkeznek, az α_4 tulajdonsággal azonban nem. Az egyik tulajdonsággal sem rendelkező objektumok számát így $N(\overline{\alpha}_1, \overline{\alpha}_2, \ldots, \overline{\alpha}_n)$ jelöli. Vezessük be az alábbi jelöléseket.

$$\begin{aligned}
S_0 &= N, \\
S_1 &= N(\alpha_1) + N(\alpha_2) + \ldots + N(\alpha_n), \\
S_2 &= N(\alpha_1, \alpha_2) + N(\alpha_1, \alpha_3) + \ldots + N(\alpha_1, \alpha_n) + \ldots + N(\alpha_{n-1}, \alpha_n), \\
S_3 &= N(\alpha_1, \alpha_2, \alpha_3) + \ldots + N(\alpha_{n-2}, \alpha_{n-1}, \alpha_n), \\
&\vdots \\
S_n &= N(\alpha_1, \alpha_2, \ldots, \alpha_n).
\end{aligned}$$

Az összegzés az $\alpha_1, \ldots, \alpha_n$ tulajdonságok minden lehetséges kombinációjára értendő a sorrend figyelembevétele nélkül.

6.18. tétel (logikai szita-formula). *Az iménti jelölésekkel*

$$N(\overline{\alpha}_1, \overline{\alpha}_2, \ldots, \overline{\alpha}_n) = S_0 - S_1 + S_2 - S_3 + \ldots + (-1)^n S_n.$$

Bizonyítás. Legyen P egy olyan objektum, amelyre az $\alpha_1, \alpha_2, \ldots, \alpha_n$ tulajdonságok közül pontosan k darab teljesül. Ekkor P k-szor fordul elő a legalább egy tulajdonsággal rendelkező objektumok számának felsorolásában, $\binom{k}{2}$-ször a legalább két tulajdonsággal rendelkező objektumok számának felsorolásában, $\binom{k}{3}$-szor a legalább három tulajdonsággal rendelkező objektumok számának felsorolásában, és így tovább, $\binom{k}{k}$-szor a legalább k tulajdonsággal rendelkező objektumok számának felsorolásában. Így, ha $k \geq 1$, akkor a 6.14. következmény szerint a P objektum előfordulásainak száma az egyenlet jobb oldalán

$$1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \ldots + (-1)^k \binom{k}{k} = (1-1)^k = 0.$$

Ha $k = 0$, akkor P egy olyan objektum, amely az $\alpha_1, \alpha_2, \ldots, \alpha_n$ tulajdonságok közül egyikkel sem rendelkezik, így pontosan egyszer fordul elő az egyenlet jobb oldalán.

Ezzel a tételt bebizonyítottuk. □

6.14. példa. Egy vállalatnál 67 ember dolgozik, közülük 47-en angolul, 35-en németül, 20-an franciául, 23-an angolul és németül is, 12-en angolul és franciául is, 11-en németül és franciául is, végül mindhárom nyelven 5-en beszélnek, akkor hány munkatárs nem beszéli a felsorolt nyelvek egyikét sem? A szita formula szerint $67-(47+35+20)+(23+12+11)-5 = 6$.

6.15. példa. Hány szürjektív leképezése létezik egy k-elemű X halmaznak egy n elemű Y halmazra, ahol $1 \leq n \leq k$?

Az általánosság megszorítása nélkül feltehető, hogy $X = \{1, \dots, k\}$ és $Y = \{1, \dots, n\}$. Jelölje A_i $(1 \leq i \leq n)$ azon $X \to Y$ leképezések halmazát, ahol i nem képelem. Ekkor az $X \to Y$ szürjektív leképezések halmaza $\overline{A_1 \cup \dots \cup A_n}$. Tetszőleges $1 \leq r \leq n$ és $1 \leq i_1 < \dots < i_r \leq n$ esetén $A_{i_1} \cap \dots \cap A_{i_r}$ pontosan azokból a leképezésekből áll, ahol $i_1, \dots, i_r$ elemek egyike sem képelem. Ezek száma $(n-r)^k$. Ilyen r-es kiválasztása pedig $\binom{n}{r}$-féleképpen lehetséges. Így a szita-formula alapján

$$|\overline{A_1 \cup \dots \cup A_n}| = n^k + \sum_{r=1}^{n} (-1)^r \binom{n}{r} (n-r)^k = \sum_{r=0}^{n} (-1)^r \binom{n}{r} (n-r)^k.$$

Gyakorlatok

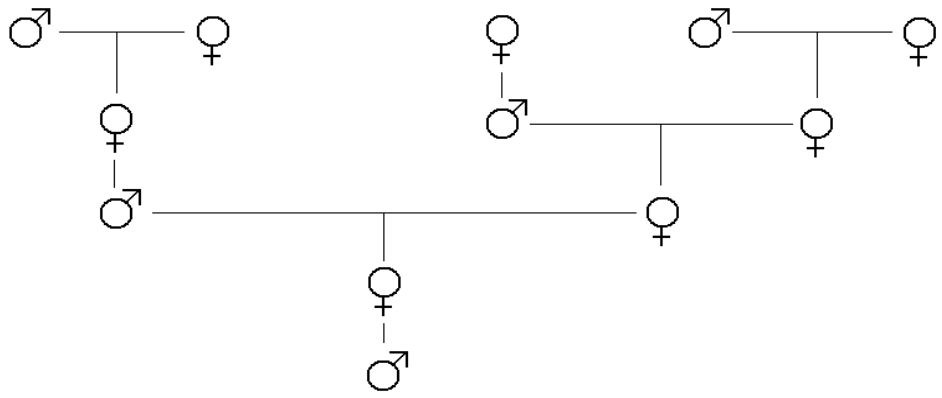
6.3-1. Bizonyítsuk be, hogy minden $n \in \mathbb{N}^+$-hoz létezik olyan $k \in \mathbb{N}^+$, hogy az nk szorzat tizes számrendszerbeli alakja csupa 1 és 0 jegyekből áll.

6.3-2. Egy ismerősünknek el akarunk küldeni 8 különböző fényképet. Hányféleképpen tehetjük meg, ha 5 különböző borítékot akarunk felhasználni? (Egy borítékon belül nem számít a képek sorrendje, és minden borítékba kerül kép.)

6.3-3. Egy toronyház legfelső emeletére 10 ember megy fel a rendelkezésre álló négy lift valamelyikével. Hányféleképpen történhet ez, ha egyik lift sem üres?

6.4. Speciális számok és sorozatok

A transzfinit rekurziótétel szerint, ha egy rekurzív sorozat valamelyik elemére vagyunk kíváncsiak, akkor kiszámításához az azt megelőző elemeket is ismernünk kell. A gyakorlatban valamilyen „explicit formulát", ún. ***zárt alakot*** próbálunk adni a sorozat tagjainak kiszámítására. A ***generátorfüggvények módszerének*** segítségével számos rekurzió zárt alakja (általános megoldása) számítható ki. Ámbár a módszer részletes tárgyalása túlmutat jegyzetünk keretein, szerencsére léteznek olyan sorozatok, ahol a zárt alak könnyen kiszámítható. Ezek közül bizonyos sorozatok olyan sűrűn fordulnak elő a matematikában, hogy külön nevet is adtak nekik. Ebben a fejezetben ilyen speciális sorozatokról lesz szó.



6.2. ábra. A hímnemű méhek családfájának első négy szintje.

6.4.1. Fibonacci-számok

A FIBONACCI-számokat az alábbi rekurzióval definiáljuk:

$$\begin{aligned} F_0 &= 0, \\ F_1 &= 1, \\ F_n &= F_{n-1} + F_{n-2} \qquad (n > 1). \end{aligned}$$

Ez a legegyszerűbb olyan rekurziós szabály, amelyben a következő tag mindig az előző kettőtől függ. Jegyezzük meg, hogy egy rekurziót a kezdeti értékek *és* a képzési szabály *együtt* határozza meg. A FIBONACCI-rekurziónál a kezdeti értékek a lehető legegyszerűbbek: a FIBONACCI-számok a legváltozatosabb körülmények között bukkanak fel.

A „méhek családfája" jó példa arra, hogyan lehet a FIBONACCI-számokat természetes módon bevezetni. Vizsgáljuk meg egy hímnemű méh (here) családfáját. Egy herének egy szülője van, a királynő, mivel a herék a királynő megtermékenyítetlen petéiből kelnek ki. Minden nőnemű méhnek (dolgozó vagy királynő) azonban két szülője van, egy hím és egy nőnemű (királynő). A 6.2. ábra a családfa első négy szintjét mutatja be. Egy herének tehát egy nagyapja és egy nagyanyja, egy dédapja és két dédanyja, két ükapja és három ükanyja van. Általánosan, egy herének pontosan F_{n+1} „n-edrendű nagyapja" és F_{n+2} „n-edrendű nagyanyja" van, ahol a nagyszülők esetén $n = 0$, a dédszülőknél $n = 1$, stb.

A FIBONACCI-számok gyakran fordulnak elő a természetben: egy tipikus napraforgó tányérján például a szorosan egymás mellett levő kis virágok spirálisokban rendeződnek el, amelyek általában 34 teljes körből állnak az egyik, 55-ből pedig a másik forgási irányban. Kisebb tányérok esetén ez a szám 21 és 34, vagy 13 és 21. Hasonló elrendezés figyelhető meg a fenyőtobozokon is. A FIBONACCI-számok a számítástudományban is sokszor bukkannak elő. A 6.3. ábra a FIBONACCI-sorozat első néhány tagját mutatja.

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

6.3. ábra. A FIBONACCI-sorozat első néhány tagja.

6.19. tétel. *A* FIBONACCI*-sorozat* n*-edik tagja*

$$F_n = \frac{1}{\sqrt{5}}\left(\phi^n - \bar{\phi}^n\right) \qquad (n = 1, 2, 3, \ldots), \tag{6.1}$$

ahol

$$\phi = \frac{1+\sqrt{5}}{2}, \qquad \textit{és} \qquad \bar{\phi} = \frac{1-\sqrt{5}}{2}.$$

Bizonyítás. n szerinti teljes indukcióval bizonyítunk. $n = 1$-re az állítás nyilvánvaló. Tegyük fel, hogy $n = k-1$-ig igaz az állítás. Megvizsgáljuk az $n = k$ esetet.

$$\begin{aligned} F_k &= F_{k-1} + F_{k-2} = \frac{1}{\sqrt{5}}(\phi^{k-1} - \bar{\phi}^{k-1}) + \frac{1}{\sqrt{5}}(\phi^{k-2} - \bar{\phi}^{k-2}) = \\ &= \frac{1}{\sqrt{5}}\left(\phi^{k-1} + \phi^{k-2} - (\bar{\phi}^{k-1} + \bar{\phi}^{k-2})\right) = \\ &= \frac{1}{\sqrt{5}}\left(\phi^{k-2}(\phi+1) - \bar{\phi}^{k-2}(\bar{\phi}+1)\right) = \\ &= \frac{1}{\sqrt{5}}(\phi^k - \bar{\phi}^k). \end{aligned}$$

□

Bármilyen meglepő, a (6.1) egyenletben F_n minden n-re egész szám. A $\phi \approx 1.61803$ szám nagyon fontos a matematika számos területén, de nemcsak ott, hanem a képzőművészetben is, ahol ***aranymetszés*** néven ismert. A görög ϕ betű PHEIDIAS tiszteletére utal, aki állítólag tudatosan használta ezt a számot a szobrászatban. (Tapasztalati tény, hogy az emberek köldökmagasságának és teljes magasságának aránya kb. 1.618.) A tételben szereplő állítást először EULER bizonyította 1765-ben. Az alábbi egyenlőségek bizonyítását az Olvasóra bízzuk:

$$\begin{aligned} \phi^2 &= \phi + 1 \\ \bar{\phi}^2 &= \bar{\phi} + 1 \\ \bar{\phi} &= -1/\phi. \end{aligned}$$

6.4.2. A szubfaktoriális

Vajon hányféle módon lehet egy n számú különböző elemből álló sorzatot úgy átrendezni, hogy egyik elem se maradjon a helyén ($n \geq 2$)? Jelöljük ezeknek az ún. ***fixpont nélüli permutációknak*** a számát D_n-el. Ezt az értéket az n elem ***szubfaktoriálisának*** nevezzük. A probléma elemzését nézzük egy konkrét példán.

Tegyük fel, hogy n ember örömében feldobja a kalapját. Hány esetben történik meg, hogy mindenki pontosan egy kalapot kap el, de senki sem a sajátját? Az, hogy az A_i személy a j sorszámú kalapot kapja el ($i \neq j$) $D_{n-1} + D_{n-2}$ esetben

n	0	1	2	3	4	5	6	7	8	9	10
D_n	1	0	1	2	9	44	265	1 854	14 833	133 496	1 334 961

6.4. ábra. A szubfaktoriális-sorozat első néhány tagja.

lehetséges, ugyanis A_j vagy az i sorszámú kalapot kapja el (D_{n-2} számú lehetőség), vagy nem (D_{n-1} számú lehetőség). Mivel A_i egy i-től különböző sorszámú kalapot $n-1$ féleképpen kaphat el, az alábbi rekurzív képlet adódik:

$$D_n = (n-1)(D_{n-1} + D_{n-2}).$$

A szubfaktoriális elnevezés a faktoriálisokkal vett hasonlóságból ered. Könnyen igazolható ugyanis, hogy

$$n! = (n-1)\big((n-1)! + (n-2)!\big).$$

A rekurzióra vonatkozó zárt alak meghatározása helyett az eredeti problémát oldjuk meg a szita-formula segítségével.

Jelöljük S_k-val azon permutációk számát, ahol valamelyik k darab személy biztosan a saját kalapját kapja el. Ezt a k személyt $\binom{n}{k}$ féleképpen lehet kiválasztani. A többi $n-k$ személy bármelyik kalapot kaphatja, ez $(n-k)!$ lehetőség. Összesen tehát $S_k = \binom{n}{k}(n-k)!$. A szita-formula szerint a minket érdeklő permutációk száma

$$D_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = n!\big(1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^n \frac{1}{n!}\big).$$

(Az analízisben járatosak észrevehetik, hogy D_n éppen e^{-1} sorfejtésének kezdete.)

A formulából következik, hogy célszerű a $D_0 = 1$ megállapodás. Ekkor $D_1 = 0, D_2 = 1, D_3 = 2$, stb. A 6.4. ábrán a szubfaktoriálisok sorozatának első néhány tagját láthatjuk.

6.4.3. Binomiális együtthatók

Vizsgáljuk meg a korábban látott binomiális együtthatók néhány tulajdonságát. Írjuk fel az $\binom{n}{k}$ értékeket kis n esetén. Ezt a táblázatot PASCAL-***háromszögnek*** nevezzük (6.5. ábra). Ha a táblázatot alaposan szemügyre vesszük, számtalan érdekes összefüggés tárul elénk. Az első a táblázat sorainak szimmetriája. Az

$$\binom{n}{k} = \binom{n}{n-k}$$

összefüggés következik a definícióból, de abból is, hogy n elemből pontosan annyiféleképpen választhatunk ki k darabot, ahányféleképpen a fennmaradó $n-k$ darabot. További észrevétel, hogy a táblázat n-edik sorának ($n > 0$) k-adik eleme a fölötte lévő és a fölötte lévő bal oldali szomszédja összege, vagyis

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$	$\binom{n}{7}$	$\binom{n}{8}$	$\binom{n}{9}$	$\binom{n}{10}$
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1

6.5. ábra. A Pascal-háromszög első néhány sora.

Az állítás bizonyítása minden n-re és k-ra elemi feladat (a definícióból következik), amit gyakorlásképpen az Olvasóra bízunk. Ha a fenti egyenlet jobb oldalán a második tagra ismételten alkalmazzuk ezt a gondolatot, azt kapjuk, hogy $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-2}{k-1} + \binom{n-2}{k}$. Tovább folytatva a felbontást, és figyelembe véve a $\binom{k}{k} = \binom{k-1}{k-1}$ azonosságot azt kapjuk, hogy

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-2}{k-1} + \ldots + \binom{k}{k-1} + \binom{k-1}{k-1}.$$

Ez azt jelenti, hogy a táblázatban egy elem a tőle balra lévő oszlopban a fölötte lévő elemek összege.

Néha a binomiális együtthatók becslésére van szükségünk. $1 \leq k \leq n$ esetén az alábbi alsó korlátot kapjuk:

$$\begin{aligned}\binom{n}{k} &= \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1} \\ &= \left(\frac{n}{k}\right)\left(\frac{n-1}{k-1}\right)\cdots\left(\frac{n-k+1}{1}\right) \\ &\geq \left(\frac{n}{k}\right)^k.\end{aligned}$$

A Stirling-formulából származó $k! \geq (k/e)^k$ egyenlőtlenség segítségével az alábbi felső korlátot kapjuk:

$$\begin{aligned}\binom{n}{k} &= \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1} \\ &\leq \frac{n^k}{k!} \\ &\leq \left(\frac{en}{k}\right)^k.\end{aligned}$$

Gyakorlatok

6.4-1. Határozzuk meg azon csupa 1-ből és 0-ból álló n-esek számát, amelyek nem tartalmaznak két szomszédos 1-est.
6.4-2. Helyezzünk két üvegtáblát egymásra. Hányféle módon haladhat át vagy verődhet vissza egy fénysugár, ha közben pontosan n-szer változtatott irányt?
6.4-3. 15 házaspár hányféleképpen táncolhat úgy, hogy egyik férj sem táncol a saját feleségével?
6.4-4. Mennyi 11^{10} értéke? Miért könnyű kiszámítani, ha ismerjük a binomiális együtthatókat?
6.4-5. Bizonyítsuk be a hexagon-tulajdonságot (a Pascal-háromszög valamely elemét „szimmetrikusan körülfogó" számok egy hexagont képeznek, például 21 esetén a hexagon elemei $15, 6, 7, 28, 56, 35$):

$$\binom{n-1}{k-1}\binom{n}{k+1}\binom{n+1}{k} = \binom{n-1}{k}\binom{n+1}{k+1}\binom{n}{k-1}.$$

6.4-6.⋆ Igazoljuk, hogy

$$\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}.$$

6.4-7.⋆ Bizonyítsuk be az

$$\binom{n}{k} \leq \frac{n^n}{k^k(n-k)^{n-k}}$$

egyenlőtlenséget.

Megjegyzések a fejezethez

A Pascal-háromszög számos további érdekes tulajdonsággal is rendelkezik, az érdeklődő Olvasónak javasoljuk a Konkrét Matematika című tankönyv [15] 5. fejezetét. További ajánlott irodalom: Hajnal [17], Knuth [22], Szendrei [39], valamint Vilenkin [42].

7. Elemi számelmélet

A számelmélet eredeti tárgya az egész számok $\mathbb{Z}$ gyűrűje, amelyben az összeadást, a kivonást és a szorzást korlátozás nélkül el lehet végezni, ezzel szemben az osztást nem. A számelmélet nagy része lényegében az oszthatósági viszonyokat vizsgálja. A fejezetben a legáltalánosabb oszthatósági vonatkozásokra építünk, elsősorban azért, mert a definíciók többsége nemcsak $\mathbb{Z}$-re, hanem tetszőleges egységelemes integritási tartományra vonatkozik. Az elemi számelmélethez tartozik még $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ elemei különböző ábrázolási lehetőségeinek vizsgálata is.

7.1. Általános alapfogalmak

A fejezetben a definíciókat, tételeket az $(R; +, \cdot)$ egységelemes integritási tartományban értelmezzük.

7.1. definíció. *Az* $a \in R$ *számot a* $b \in R$ *szám* ***osztójának*** *nevezünk, ha létezik olyan* $q \in R$ *szám, amelyre* $b = aq$.

Jelölése: $a \mid b$. Az $a = b = 0$ esetet kivéve egyetlen ilyen q létezik, mert ha $b = aq'$ is teljesülne, akkor $0 = a(q - q')$ miatt a nullosztó lenne. Ugyanezt a kapcsolatot úgy is kifejezhetjük, hogy b ***osztható*** a-val, illetve hogy b ***többszöröse*** vagy ***többese*** a-nak. Ha nem létezik olyan $q \in R$, amelyre $b = aq$, akkor az a nem osztója b-nek, amit $a \nmid b$-vel jelölünk.

A 0 minden számmal osztható (a 0-val is!), hiszen minden a-ra $0 = a \cdot 0$. Másrészt az 1 minden szám osztója.

7.1. példa. $\mathbb{Z}$-ben $2 \mid 10$, mert $2 \cdot 5 = 10$, de $4 \nmid 6$.

Az alábbiakban az oszthatóság fontosabb tulajdonságait láthatjuk. A bizonyítást az Olvasóra bízzuk.

7.2. tétel (az oszthatóság tulajdonságai).

(1) $a \mid a$ *minden* $a \in R$*-re,*
(2) $a \mid b$ *és* $b \mid c \Rightarrow a \mid c$,
(3) $a_1 \mid b_1$ *és* $a_2 \mid b_2 \Rightarrow a_1a_2 \mid b_1b_2$,
(4) $a \mid b \Rightarrow ac \mid bc$ *minden* $c \in R$*-re,*
(5) $ac \mid bc$ *és* $c \neq 0 \Rightarrow a \mid b$,
(6) $a \mid b_i$ *és* $c_i \in R$ $(i = 1, 2, \ldots, k) \Rightarrow a \mid \sum_{i=1}^{k} b_i c_i$.

Az (1)–(3) tulajdonságok azt fejezik ki, hogy az oszthatóság reflexív, tranzitív, de nem szimmetrikus reláció. (6)-ot lineáris kombinációs tulajdonságnak nevezzük.

7.2. példa. Érdemes megjegyezni az alábbi, oszthatósággal kapcsolatos összefüggéseket:
1) $a - b \mid a^n - b^n$, mert

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

2) $a + b \mid a^{2n+1} + b^{2n+1}$, mert

$$a^{2n+1} + b^{2n+1} = (a + b)(a^{2n} - a^{2n-1}b + \cdots - ab^{2n-1} + b^{2n}).$$

3) $a + b \mid a^{2n} - b^{2n}$, mert

$$a^{2n} - b^{2n} = (a^n)^2 - (b^n)^2.$$

7.3. definíció. *Azt a számot, ami minden számnak osztója* ***egységnek*** *nevezzük.*

Az egységek R azon elemei, amelyeknek a szorzásra nézve létezik inverzük. Megjegyezzük, hogy az egységek halmaza változatos képet mutat. Tekintsük például a $(\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}; +, \cdot)$ egységelemes integritási tartományt. Ebben a struktúrában, amint azt később látni fogjuk, végtelen sok egység van.

7.4. tétel. *Ha* $a \mid b$ *és* ε, δ *egységek, akkor* $\varepsilon a \mid \delta b$ *is teljesül.*

Bizonyítás. Mivel $\varepsilon \mid 1$, ezért alkalmas r-rel $1 = \varepsilon r$. Ha $b = aq$, akkor $\delta b = \delta(\varepsilon r)(aq) = (\varepsilon a)(\delta q r)$, tehát valóban $\varepsilon a \mid \delta b$. □

A tétel azt fejezi ki, hogy egy szám és egységszerese oszthatósági szempontból teljesen azonosan viselkednek. Így az egész számok oszthatósági vizsgálatát leszűkíthetjük majd a nemnegatív egészekre, sőt, a 0 speciális szerepének tisztázása után a pozitív egészekre.

7.5. definíció. *Azt mondjuk, hogy* $a \in R$ *és* $b \in R$ ***asszociáltak,*** *ha létezik olyan* $\varepsilon \in R$ *egység, amellyel* $b = \varepsilon a$.

Az asszociáltság reflexív, szimmetrikus és tranzitív reláció, tehát osztályoz. A nullának önmagán kívül nincs más asszociáltja. Az $a \in R$ szám asszociáltjai az εa alakú számok, ahol ε egység.

7.3. példa. Tekintsük a $G = \{a + bi \mid a, b \in \mathbb{Z}\}$ halmazt, az ún. ***Gauss-egészeket.*** A halmaz elemei a komplex sík egész rácspontjai. Belátható, hogy $(G; +, \cdot)$ struktúra a komplex

műveletekkel egységelemes integritási tartomány. Keressük meg a struktúra egységeit. Ha ε egység, akkor $\varepsilon \mid 1$. A konjugáltakat tekintve ekkor $\overline{\varepsilon} \mid \overline{1}$ is teljesül, amiből $\varepsilon \cdot \overline{\varepsilon} \mid 1 \cdot \overline{1} = 1$ következik, vagyis $|\varepsilon|^2 \mid 1$. Ha $\varepsilon = a + bi$ $(a, b \in \mathbb{Z})$, akkor tehát $a^2 + b^2 \mid 1$, ami csak az $a^2 + b^2 = 1$ esetben lehetséges. Ekkor $a = \pm 1, b = 0$, illetve $a = 0, b = \pm 1$ a megoldások. A Gauss-egészek gyűrűjében tehát négy egység van, így az asszociáltak osztálya négy elemű.

A 7.4. tétel szerint bármely $0 \neq a \in R$ nem egység és bármely ε egység esetén $\varepsilon \mid a$ és $\varepsilon a \mid a$ teljesül. Ezeket az a ***triviális osztóinak*** nevezzük. Lényeges szerepet játszanak azok a számok, amelyeknek csak triviális osztói vannak:

7.6. definíció. *Legyen $0 \neq a \in R$ nem egység. Az a számot **felbonthatatlannak** vagy **irreducibilisnek** nevezzük, ha $a = bc \Rightarrow b$ vagy c egység.*

Az $a = bc$ szorzatban nem lehet b is és c is egység, mert akkor a is az lenne. Eszerint a definícióban „kizáró vagy" szerepel. Másrészt a 7.6. definíció miatt a felbonthatatlan számoknak csak triviális osztói vannak. Ha egy nemnulla és nem egység számnak a triviálistól különböző osztója is van, akkor ***összetett számnak*** nevezzük.

7.7. definíció. *Legyen $0 \neq p \in R$ nem egység. A p számot **prímnek** nevezzük, ha $p \mid bc \Rightarrow p \mid b$ vagy $p \mid c$.*

A definícióban most „megengedő vagy" szerepel, hiszen előfordulhat, hogy p a bc szorzat mindkét tényezőjét osztja.

7.4. példa. Az egész számok körében a 7 és a 11 felbonthatatlanok és egyben prímek is. A 4 nem prím, mert például $4 \mid 12 = 2 \cdot 6$, de $4 \nmid 2$ és $4 \nmid 6$.

7.8. tétel. *Minden prímelem felbonthatatlan.*

Bizonyítás. Legyen p prím és $p = xy$. Mivel egységelemes integritási tartományban dolgozunk, ezért $p \mid xy$. A 7.7. definíció szerint ekkor $p \mid x$ vagy $p \mid y$. Feltehető, hogy $p \mid x$. Így $x = pz = x(yz)$ miatt $yz = 1$, amiből következik, hogy y és z egységek, x és p pedig asszociáltak. □

Vajon teljesül-e a tétel állításának megfordítása, vagyis hogy minden felbonthatatlan elem prím? A későbbiekben látni fogjuk, hogy a válasz nemleges.

7.9. definíció. *Legyenek $a_1, a_2, \ldots, a_n$ az R egységelemes integritási tartomány tetszőleges elemei. Legyen $L \subseteq R$ egy olyan részhalmaz, melynek minden l elemére $l \mid a_i$ $(i = 1, 2, \ldots, n)$, valamint ha $l' \mid a_i$ $(i = 1, 2, \ldots, n)$, akkor $l' \mid l$. L elemeit **legnagyobb közös osztóknak** nevezzük.*

Ez a legnagyobb közös osztó fogalom látszólag eltér a középfokú oktatásban $\mathbb{Z}$-ben látott legnagyobb közös osztó fogalomtól, de előnye, hogy tetszőleges egységelemes integritási tartományban érvényes. Látni fogjuk, hogy $\mathbb{Z}$-re a két megközelítés ugyanazt szolgáltatja.

L az $a_1, a_2, \ldots, a_n$ elemek közös osztóinak osztályai között maximális az oszthatóságra nézve, és ha L nem üres, akkor elemei egymás asszociáltjai.

7.5. példa. $\mathbb{Z}$-ben a 6 és 8 elemekre $L = \{-2, 2\}$.

7.10. definíció. *Ha* L *elemei az egységek, akkor azt azt mondjuk, hogy* $a_1, a_2, \ldots, a_n$ ***relatív prímek.***

7.11. definíció. *Az* $a_1, a_2, \ldots, a_n \in R$ *elemek* ***páronként relatív prímek,*** *ha közülük semelyik kettőnek sincs az egységtől különböző osztója.*

Megjegyezzük, hogy az $a_1, a_2, \ldots, a_n \in R$ elemekre sokkal „erősebb" feltételt jelent, hogy páronként relatív prímek, mintha „csak" relatív prímek lennének. Amennyiben az adott n elem páronként relatív prim, akkor ebből következik, hogy relatív prímek, míg megfordítva ez nem igaz.

7.6. példa. $\mathbb{Z}$-ben a $6, 9, 16$ számok relatív prímek, de nem páronként relatív prímek, mert $3 \mid 6$ és $3 \mid 9$, továbbá $2 \mid 6$ és $2 \mid 16$.

7.12. definíció. *Legyenek* $a_1, a_2, \ldots, a_n$ *az* R *egységelemes integritási tartomány tetszőleges elemei. Legyen* $T \subseteq R$ *egy olyan részhalmaz, melynek minden* t *elemére* $a_i \mid t$ $(i = 1, 2, \ldots, n)$*, valamint ha* $a_i \mid t'$ $(i = 1, 2, \ldots, n)$*, akkor* $t \mid t'$*.* T *elemeit* ***legkisebb közös többszörösöknek*** *nevezzük.*

T az $a_1, a_2, \ldots, a_n$ elemek közös többszöröseinek osztályai között minimális az oszthatóságra nézve, valamint ha T nem üres, akkor elemei egymás asszociáltjai.

7.7. példa. $\mathbb{Z}$-ben a 6 és 8 elemekre $T = \{-24, 24\}$.

Gyakorlatok

7.1-1. Bizonyítsuk be, hogy ha a és b asszociáltak, akkor $a \mid b$ és $b \mid a$.
7.1-2.* Bizonyítsuk be, hogy egységelemes integritási tartományban az egységek a szorzásra nézve Abel-csoportot alkotnak.

7.2. Oszthatóság az egész számok körében

7.13. tétel. *Az egész számok körében két egység van,* $\varepsilon = \pm 1$*.*

Bizonyítás. Nyilván minden $a \in \mathbb{Z}$-re $\pm 1 \mid a$, hiszen $a = (\pm 1)(\pm a)$. Másrészt ha ε egység, akkor $\varepsilon \mid 1$, azaz alkalmas q-val $1 = \varepsilon q$. Ekkor $|1| = |\varepsilon q| = |\varepsilon||q|$. Mivel $|\varepsilon| \geq 1$ és $|q| \geq 1$, ezért $|\varepsilon| = 1$, azaz csak $\varepsilon = \pm 1$ lehetséges. □

7.14. következmény. *Ha* $a \mid b$ *és* $b \mid a$*, akkor* $|a| = |b|$*.*

Bizonyítás. Ha a vagy b valamelyike 0, akkor a szükségszerűen a másik is, így feltehető, hogy $a, b \neq 0$. A feltétel szerint ekkor léteznek olyan a' és b' egészek, amelyekkel $aa' = b$ és $bb' = a$. Ekkor a $bb'a' = b$ összefüggést kapjuk, amiből $b \neq 0$ miatt $b'a' = 1$, vagyis $a = \pm 1$ és $b = \pm 1$. A bizonyítás kész. □

7.15. tétel. *Legyenek* $a, b \in \mathbb{Z}$*,* $a \mid b$ *és* $b \neq 0$*. Ekkor* $|a| \leq |b|$*.*

Bizonyítás. Mivel $a \mid b$, ezért $\exists q \in \mathbb{Z}$, amelyre $aq = b$, így $|aq| = |a| \cdot |q| = |b|$. $|q| < 1$ esetén $b = 0$ lenne, ezért $|q| \geq 1$. Ebből $|b| = |a| \cdot |q| \geq |a|$ következik. □

A tétel következménye, hogy $0 \neq b \in \mathbb{Z}$ esetén b-nek véges sok osztója van.

7.2.1. Maradékos osztás

7.16. tétel (maradékos osztás tétele). *Tetszőleges a és $b \neq 0$ egész számokhoz egyértelműen léteznek olyan q és r egész számok, melyekre $a = bq + r$ és $0 \leq r < |b|$.*

Bizonyítás. Legyen először $b > 0$. A $0 \leq r = a - bq < b$ feltétel pontosan akkor teljesül, ha $bq \leq a < b(q+1)$, azaz $q \leq a/b < q + 1$. Ilyen q egész szám pedig pontosan egy létezik, $q = \lfloor a/b \rfloor$. Ha $b < 0$, akkor a $0 \leq r = a - bq < |b| = -b$ feltétel $q \geq a/b > q - 1$ teljesülésével ekvivalens, ami pontosan egy q egészre áll fenn, amikor $q = \lceil a/b \rceil$. □

A maradékos osztásnál kapott q számot ***hányadosnak***, r-et pedig (legkisebb nemnegatív) ***maradéknak*** nevezzük.

7.8. példa. Most délután 1 óra van. Mennyi idő lesz 101 óra múlva?

Megoldás: Legyen $b = 24$ és $a = 13 + 101 = 114$. Ekkor $114 = 4 \cdot 24 + 18$. Vagyis 101 óra múlva 18 óra (délután 6 óra) lesz.

A maradékos osztás tétele felhasználható a pozitív egészek ***számrendszeres*** ábrázolásához.

7.17. tétel (számrendszerek). *Legyen $q > 1$ rögzített egész. Ekkor bármely N pozitív egész szám egyértelműen írható fel*

$$N = \sum_{i=0}^{n} a_n q^n$$

alakban, ahol $0 \leq a_i < q$ és $a_n \neq 0$.

Bizonyítás. A $0 \leq a_0 < q$ és $q \mid N - a_0$ feltétel miatt a_0 az N-nek a q-val történő maradékos osztásakor keletkező legkisebb nemnegatív maradéka, tehát pontosan egy megfelelő a_0 létezik. Ezt N-ből kivonva és q-val osztva jelöljük a hányadost N_0-al. Ekkor az

$$N_0 = \frac{N - a_0}{q} = a_n q^{n-1} + a_{n-1} q^{n-2} + \ldots + a_2 q + a_1$$

felírásból az előző eljárást folytatva kapjuk a megfelelő a_i-k létezését és egyértelműségét. □

Az iménti előállításban q-t a ***számrendszer alapszámának*** nevezzük, az a_i számok pedig a q alapú számrendszer ***számjegyei***. Legismertebb ilyen ábrázolás $q = 10$ esetén a tízes alapú és $q = 2$ esetén a bináris (2-es alapú) számrendszerek. Az iménti számot

$$N = (a_n a_{n-1} \ldots a_1 a_0)_q$$

alakban jelöljük. A $q = 10$ esetén a zárójelet és az alapszám feltüntetését általában elhagyjuk.

mennyiség	elnevezés	rövidítés
10^{18}	exa	E
10^{15}	peta	P
10^{12}	tera	T
10^{9}	giga	G
10^{6}	mega	M
10^{3}	kilo	K
10^{-3}	milli	m
10^{-6}	mikro	μ
10^{-9}	nano	n
10^{-12}	pico	p
10^{-15}	femto	f
10^{-18}	atto	a

7.1. ábra. A tízes számrendszerbeli mennyiségek szokásos jelölése.

7.9. példa. $21 = (21)_{10} = (10101)_2$, hiszen $21 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1$.

7.10. példa. Az informatikában gyakran nagyon kicsi (például processzor tervezés), máskor nagyon nagy (például tárolókapacitás) mennyiségeket kell felírnunk a 10-es számrendszerben. Ezekben az esetekben a 7.1. ábrán látható jelölések használhatók. Például 3 GHz, 8 TByte, stb.

7.2.2. Legnagyobb közös osztó

Ha létezik az $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ számok legnagyobb közös osztója, akkor a legnagyobb közös osztók közül az egyik nemnegatív, ezt $\text{lnko}(a_1, a_2, \ldots, a_n)$-nel jelöljük. (A $\gcd(a_1, a_2, \ldots, a_n)$ és az $(a_1, a_2, \ldots, a_n)$ jelölés is elterjedt; ha nem okoz félreértést, akkor ez utóbbit fogjuk használni). Nyilván $(0, \ldots, 0) = 0$, egyébként pedig a 0-kat elhagyva a közös osztók nem változnak. Az, hogy $a_1, a_2, \ldots, a_n$ relatív prímek, azt jelenti, hogy $(a_1, a_2, \ldots, a_n) = 1$. Hasonlóan, ha létezik az $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ számok legkisebb közös többszöröse, akkor a legkisebb közös többszörösök közül az egyik nemnegatív, ezt $\text{lkkt}(a_1, a_2, \ldots, a_n)$-nel jelöljük. (A $\text{lcm}(a_1, a_2, \ldots, a_n)$ és az $[a_1, a_2, \ldots, a_n]$ jelölés is gyakori, a rövidség kedvéért mi ez utóbbit használjuk). Ha valamelyik a_i nulla, akkor az egyetlen közös többszörös a 0.

Egyáltalán nem magától értetődő azonban, hogy bármely két egész számnak létezik legnagyobb közös osztója.

7.18. tétel (két egész szám legnagyobb közös osztója létezése). *Bármely két egész számnak létezik legnagyobb közös osztója.*

Bizonyítás. A legnagyobb közös osztó létezését a matematika egyik legősibb eljárásával, az ***euklideszi algoritmussal*** bizonyítjuk (EUKLIDÉSZ i.e. 300 körül élt görög matematikus). Az algoritmus alapgondolata az, hogy az egyik számot maradékosan

elosztjuk a másikkal, majd a másik számot a maradékkal, és így tovább mindaddig, amíg 0 maradékhoz nem jutunk. Megmutatjuk, hogy az eljárás véges és az utolsó nem nulla maradék lesz a két szám (egyik) legnagyobb közös osztója.

Tegyük fel, hogy $a, b \in \mathbb{Z}$, $b \neq 0$. Ha $b \mid a$, akkor b nyilván legnagyobb közös osztó. Ha $b \nmid a$, akkor a maradékos osztás tételét alkalmazva alkalmas q_i, r_i egészekkel

$$\begin{aligned}
a &= bq_1 + r_1, && \text{ahol} \quad 0 < r_1 < |b|,\\
b &= r_1q_2 + r_2, && \text{ahol} \quad 0 < r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, && \text{ahol} \quad 0 < r_3 < r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n, && \text{ahol} \quad 0 < r_n < r_{n-1},\\
r_{n-1} &= r_nq_{n+1}, && (r_{n+1} = 0).
\end{aligned}$$

Az eljárás véges sok lépésben befejeződik, hiszen a maradékok nemnegatív egészek szigorúan monoton csökkenő sorozatát alkotják. Be kell még látnunk, hogy r_n valóban az a és b számok (egyik) legnagyobb közös osztója.

Az algoritmus során visszafelé haladva először azt igazoljuk, hogy r_n közös osztója a-nak és b-nek. Az utolsó egyenlőségből $r_n \mid r_{n-1}$. Az utolsó előtti egyenlőségből a 7.2. tétel lineáris kombinációs tulajdonsága miatt

$$r_n \mid r_{n-1} \text{ és } r_n \mid r_n \Rightarrow r_n \mid r_{n-1}q_n + r_n = r_{n-2}.$$

Az eljárást folytatva végül $r_n \mid b$, majd (az első egyenlőségből) $r_n \mid a$ adódik. A legnagyobb közös osztó tulajdonság bizonyításához felülről lefelé haladunk. Legyen $c \in \mathbb{Z}$ olyan, hogy $c \mid a$ és $c \mid b$. Ekkor az első egyenlőségből $c \mid a - bq = r_1$, majd a másodikból $c \mid b \wedge c \mid r_1 \Rightarrow c \mid b - r_1q_2 = r_2$. Ugyanígy folytatva végül az utolsó előtti egyenlőségből azt kapjuk, hogy $c \mid r_n$. □

7.19. következmény. *Bármely $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ számoknak létezik legnagyobb közös osztója és*

$$(a_1, a_2, \ldots, a_n) = ((\ldots((a_1, a_2), a_3), \ldots, a_{n-1}), a_n).$$

Bizonyítás. Két szám közös osztóinak halmaza megegyezik a két szám legnagyobb közös osztója osztóinak halmazával. A többit indukcióval kapjuk. □

7.20. következmény. *Ha $c > 0$, akkor $(ca, cb) = c(a, b)$.*

Bizonyítás. Tekintsük az (a, b) előállítására szolgáló euklideszi algoritmust, legyen az utolsó nemnulla maradék $r_n = (a, b)$. Ha minden egyenlőséget megszorzunk c-vel, akkor éppen a (ca, cb)-t előállító euklideszi algoritmushoz jutunk. Ebben az utolsó nemnulla maradék $(ca, cb) = cr_n = c(a, b)$. □

7.21. tétel. *Az a és b egész számok legnagyobb közös osztója alkalmas u és v egészekkel kifejezhető $(a, b) = au + bv$ alakban.*

Bizonyítás. Az euklideszi algoritmus első egyenlőségéből r_1-et kifejezve $r_1 = a - bq_1$ adódik. Ezt a második egyenletbe helyettesítve

$$r_2 = b - r_1q_2 = b - (a - bq_1)q_2 = a(-q_2) + b(1 + q_1q_2),$$

azaz r_2 felírható $aU+bV$ alakban. Ezzel a módszerrel továbbhaladva az utolsó előtti egyenlőségből azt kapjuk, hogy $(a,b) = r_n$ is kifejezhető $au + bv$ alakban. □

7.11. példa. Keressük meg 2004 és 56 legnagyobb közös osztóját.

$$\begin{aligned} 2004 &= 35 \cdot 56 + 44 \\ 56 &= 1 \cdot 44 + 12 \\ 44 &= 3 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4. \end{aligned}$$

Vagyis $(2004, 56) = 4$. Most fejezzük ki a legnagyobb közös osztót a 2004 és a 56 lineáris kombinációjaként.

$$\begin{aligned} 44 &= 1 \cdot 2004 - 35 \cdot 56 \\ 12 &= 56 - 44 = 56 - (2004 - 35 \cdot 56) = -2004 + 56 \cdot 36 \\ 8 &= 44 - 3 \cdot 12 = 2004 - 35 \cdot 56 - 3(-2004 + 56 \cdot 36) = 4 \cdot 2004 - 143 \cdot 56 \\ 4 &= 12 - 8 = -2004 + 56 \cdot 36 - (4 \cdot 2004 - 143 \cdot 56) = -5 \cdot 2004 + 56 \cdot 179. \end{aligned}$$

Ugyanehhez az eredményhez juthatunk, ha a lineáris kombinációt az euklideszi algoritmus maradéksorozata végéről indulva írjuk fel.

$$\begin{aligned} 4 &= 12 - 8 = 12 - (44 - 3 \cdot 12) = -44 + 4 \cdot 12 = -44 + 4(56 - 44) = -5 \cdot 44 + 4 \cdot 56 \\ &= -5(2004 - 35 \cdot 56) + 4 \cdot 56 = -5 \cdot 2004 + 179 \cdot 56. \end{aligned}$$

A 7.21. tétel szerint az euklideszi algoritmus segítségével tetszőleges a, b egészek esetén találhatóak olyan u, v egészek, amelyekkel $(a,b) = au + bv$. De nem csak egy ilyen számpár létezik. Ha ugyanis u_0, v_0 megfelelőek, akkor $u_1 = u_0 + bt$ és $v_1 = v_0 - at$ is azok minden $t \in \mathbb{Z}$ esetén:

$$au_1 + bv_1 = a(u_0 + bt) + b(v_0 - at) = au_0 + bv_0 = (a,b).$$

A 7.21. tétel fontos következménye a kétismeretlenes ***lineáris diofantikus egyenlet*** megoldhatóságára vonatkozó alábbi tétel. Diofantikus egyenletnek olyan egész együtthatós algebrai egyenletet nevezünk, melynek a megoldásait is az egész számok körében keressük. Az $ax + by = c$ egyenletben tehát a, b, c rögzített egész számok és megoldáson az egyenletet kielégítő x, y egész számpárt értjük.

7.22. tétel. *Rögzített a, b, c egész számok esetén az $ax+by = c$ diofantikus egyenletnek akkor és csak akkor létezik megoldása, ha $(a,b) \mid c$.*

Bizonyítás. Először tegyük fel, hogy létezik egy x_0, y_0 megoldás. Ekkor $(a,b) \mid a$ és $(a,b) \mid b$ alapján $(a,b) \mid ax_0 + by_0 = c$. Megfordíta, tegyük fel, hogy $(a,b) \mid c$, vagyis valamilyen t-re $c = (a,b)t$. Ekkor a 7.21. tétel miatt alkalmas u, v egészekkel $(a,b) = au + bv$. Az egyenletet t-vel szorozva azt kapjuk, hogy $c = a(ut) + b(vt)$, azaz $x = ut$ és $y = vt$ megoldása az $ax + by = c$ diofantikus egyenletnek. □

Megoldhatóság esetén az euklideszi algoritmus egyúttal eljárást is szolgáltat a lineáris diofantikus egyenlet (egyik) megoldásának megkereséséhez.

Az alábbi tétel fontos szerepet játszik a számelmélet alaptételének bizonyításánál.

7.23. tétel. *Ha* $c \mid (a, b)$ *és* $(c, a) = 1$*, akkor* $c \mid b$.

Bizonyítás. Elegendő azt az esetet vizsgálni, amikor a, b és c is pozitívak. Ekkor $c \mid ab$, $c \mid cb$ és a 7.20. következmény alapján $c \mid (ab, cb) = (a, c)b = b$. □

7.2.3. Prímek és felbonthatatlanok

7.24. tétel. *Az egész számok körében* p *akkor és csak akkor prím, ha felbonthatatlan.*

Bizonyítás. Nyilván feltehető, hogy $p \neq 0$ és $p \neq \pm 1$. Azt kell csak belátni, hogy ha p felbonthatatlan, akkor prím is. Legyen $p \mid bc$. Ha $p \mid b$, akkor készen vagyunk. Ha $p \nmid b$, akkor p felbonthatatlansága és $(p, b) \mid p$ miatt $(p, b) = 1$. A $p \mid bc$ és $(p, b) = 1$ feltételekből a 7.23. tétel alapján $p \mid c$ következik. □

Beláttuk tehát, hogy az egészek körében a prímek és a felbonthatatlan számok egybeesnek. Ezért tehető meg, hogy az egész számokra a középiskolában a felbonthatatlan számnak megfelelő tulajdonsággal értelmezik a prímszámokat, melyeket ezen esetben ***törzsszámoknak*** is szokás nevezni. A két fogalom azonban más számkörben nem feltétlenül ekvivalens. Ilyen például az $(\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}; +, \cdot)$ egységelemes integritási tartomány, ahol a $3, 2 \pm \sqrt{5}$ elemek irreducibilis elemek, de nem prímelemek. Ezekben a számkörökben az elemeknek többféle, lényegesen különböző felbontásuk is lehetséges. Az iménti számkörben $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$.

7.2.4. A számelmélet alaptétele

7.25. tétel (a számelmélet alaptétele). *Minden, a* 0*-tól és egységektől különböző egész szám véges sok felbonthatatlan szám szorzatára bontható, és ez a felbontás a tényezők sorrendjétől és egységszeresektől eltekintve egyértelmű.*

Az egyértelműség azt jelenti, hogy ha $a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$, ahol p_i és q_j számok felbonthatatlanok, akkor $r = s$ és és a p_i és q_j számok valamilyen sorrendben egymás egységszeresei.

7.12. példa. $20 = 2 \cdot 2 \cdot 5 = (-2) \cdot 2 \cdot (-5) = 5 \cdot (-2) \cdot (-2)$.

Bizonyítás. A felbonthatóság bizonyítása: legyen $a \in \mathbb{Z}$ nem nulla és nem egység. Ha a felbonthatatlan, akkor készen vagyunk. Ha a nem felbonthatatlan, akkor létezik nemtriviális osztója. Ezek közül a legkisebb pozitív szükségképpen felbonthatatlan. Ekkor $a = p_1 a_1$, ahol p_1 felbonthatatlan és a_1 nem egység. Ha a_1 felbonthatatlan, akkor készen vagyunk; ha nem, akkor létezik olyan p_2 felbonthatatlan, hogy $a_1 = p_2 a_2$, ahol a_2 nem egység. Hasonlóan járunk el a_2-vel, stb. Eljárásunk véges sok lépésben véget ér, mert az $|a_i|$ számok pozitív egészek szigorúan monoton csökkenő sorozatát alkotják. Így eljutunk egy olyan a_k-hoz, amely már felbonthatatlan. Ekkor az $a = p_1 p_2 \dots p_k$ előállítást nyerjük.
Az egyértelműség bizonyítása: tegyük fel indirekt, hogy a-nak (legalább) két lényegesen különböző felbontása létezik, vagyis

$$a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s \tag{7.1}$$

Ha itt valamelyik p_i egységszerese valamelyik q_j-nek, például $p_1 = \varepsilon q_1$, akkor q_1-el egyszerűsítve

$$a' = \frac{a}{q_1} = \varepsilon p_2 p_3 \dots p_r = q_2 q_3 \dots q_s,$$

vagyis a'-nek két lényegesen különböző felbontását kapjuk. Az eljárást folytatva végül egy olyan számhoz jutunk, amelynek kétféle felbontásában már nincsenek egységszeres tényezők. Feltehető, hogy az indirekt feltevésben szereplő (7.1) előállítás ilyen. Ekkor $p_1 \mid q_1 q_2 \dots q_s$. Mivel p_1 felbonthatatlan, ezért prím is, vagyis p_1 szükségképpen osztja legalább az egyik q_j tényezőt. Ha azonban $p_1 \mid q_j$, akkor q_j felbonthatatlansága miatt p_1 vagy egység vagy q_j egységszerese, de mindkettő ellentmondás. □

Figyeljük meg, hogy az egyértelműség bizonyítása lényegében a maradékos osztás elvégezhetőségére épült. Általában is igaz, hogy ha egy egységelemes integritási tartományban létezik a maradékos osztás megfelelője, akkor ott érvényes a számelmélet alaptétele. Viszont az állítás megfordítása nem igaz: léteznek olyan számkörök, amelyekben érvényes a számelmélet alaptétele, noha semmilyen értelemben nem létezik bennük maradékos osztás.

A következőkben pozitív számok pozitív osztóival foglalkozunk és prímszámon is pozitív prímszámot fogunk érteni. Ekkor a számelmélet alaptételében szereplő prímtényezős felbontás az alábbiakat jelenti:

7.26. tétel. *Minden $n > 1$ egész szám*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}$$

alakban írható, ahol $p_1, p_2, \dots, p_r$ különböző (pozitív) prímek és $\alpha_i > 0$ egészek. Ez a felírás a prímhatványtényezők sorrendjétől eltekintve egyértelmű. Az előállítást az n szám ***kanonikus alakjának*** *nevezzük.* □

7.13. példa. 123456 kanonikus alakja $2^6 \cdot 3 \cdot 643$, de nem kanonikus alakja például $2^5 \cdot 6 \cdot 643$.

Az n szám ***módosított kanonikus alakjához*** jutunk, ha a fenti előállításban az $\alpha_i = 0$ esetet is megengedjük. Természetesen az egyértelműség ekkor a fellépő felesleges tényezőktől eltekintve értendő.

7.14. példa. 123456 módosított kanonikus alakja $2^5 \cdot 3 \cdot 5^0 \cdot 643$ és $2^5 \cdot 3 \cdot 7^0 \cdot 643$ is.

A pozitív egészek osztói és azok száma a kanonikus alak segítségével könnyen áttekinthető.

7.27. tétel. *Az*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

kanonikus alakú szám
a) pozitív osztói pontosan a

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$$

alakú számok, ahol $0 \le \beta_i \le \alpha_i, i = 1, 2, \ldots, r$,
b) pozitív osztói száma

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_r + 1).$$

Az osztók esetén a módosított kanonikus alakot használtuk. A triviális osztókat a $\beta_i = 0$ és a $\beta_i = \alpha_i$ (minden i-re) speciális esetekben kapjuk. A $\tau(n)$ függvény az n pozitív osztói számának szokásos jelölése.

Bizonyítás. a) Ha $n = cd$, akkor c és d prímtényezős felbontásának szorzata n prímtényezős felbontása kell legyen. b) Az összes pozitív osztót úgy kapjuk, hogy a β_i kitevők minden i-re egymástól függetlenül végigfutnak a $0, 1, \ldots \alpha_i$ értékeken, a kitevők egymástól független megválasztására így $(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_r+1)$ lehetőség van. A pozitív osztók előállításának egyértelműségét felhasználva a tétel bizonyítása kész. □

7.15. példa. Ha $n = 2^7 3^4 7$, akkor $\tau(n) = 8 \cdot 5 \cdot 2 = 80$ és $d = 2^6 \cdot 7$ osztója n-nek.

Vajon a legkisebb közös többszörös is minden egész számpár esetén létezik?

7.28. tétel. *Tetszőleges a, b egész számnak létezik asszociáltság erejéig egyértelmű legkisebb közös többszöröse.*

Bizonyítás. Ha $a = 0$ vagy $b = 0$, akkor $[a, b] = 0$. Tegyük fel, hogy $a, b > 0$. Belátjuk, hogy a és b legkisebb közös többszöröse $t = ab/(a, b)$. Nyilván t többszöröse a-nak is és b-nek is, hiszen $a/(a, b)$, illetve $b/(a, b)$ is egészek. Másrészt t az a és b tetszőleges T közös többesének osztója, hiszen $(T/a, T/b) = (Ta/ab, Tb/ab) = T(a, b)/ab = T/t$ egész szám, vagyis $t \mid T$. Ha a és b valamelyike (vagy mindkettő) negatív, akkor hasonló megfontolással $t = [a, b] = |ab|/(a, b)$. □

7.29. következmény. *Legyen $a, b, c \in \mathbb{Z}$. Ekkor $(a, b)[a, b] = |ab|$.*

7.30. következmény. *Legyen $a, b, c \in \mathbb{Z}$, $(a, b) = 1$. Ekkor $|ab| = [a, b]$.*

7.31. tétel. *Ha $a, b, c \in \mathbb{Z}$, akkor $a \mid c$ és $b \mid c \Leftrightarrow [a, b] \mid c$.*

Bizonyítás. Az a és b egészek összes pozitív közös többszöröse kanonikus alakjában a p_i-k kitevője legalább akkora, mint $[a, b]$-ben, és emellett más prímek is előfordulhatnak. Így a közös többszörösök éppen $[a, b]$ többszörösei. □

7.32. tétel. (1) *Ha az a és b pozitív egészek módosított kanonikus alakja*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \quad \text{és} \quad b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}, \quad \text{ahol} \quad \alpha_i \ge 0,\ \beta_j \ge 0,$$

akkor

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \ldots p_r^{\min(\alpha_r, \beta_r)},$$
$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \ldots p_r^{\max(\alpha_r, \beta_r)}.$$

(2) $(ab, c) = 1 \Leftrightarrow (a, c) = 1$ *és* $(b, c) = 1$.

A fenti kifejezésben $\min(\alpha_i, \beta_i)$ és $\max(\alpha_i, \beta_i)$ az α_i, β_i számok közül a kisebbiket, illetve a nagyobbikat jelenti, ha $\alpha_i \neq \beta_i$, illetve a közös értéküket, ha $\alpha_i = \beta_i$.

Bizonyítás. (1) Egy d pozitív egész pontosan akkor közös osztója a-nak és b-nek, ha $d \mid a$ és $d \mid b$. Ez azt jelenti, hogy d módosított kanonikus alakjában minden p_i prím γ_i kitevőjére $\gamma_i \leq \alpha_i$ és $\gamma_i \leq \beta_i$, ez pedig azzal ekvivalens, hogy $\gamma_i \leq \min(\alpha_i, \beta_i)$. A legnagyobb közös osztót akkor kapjuk, ha a γ_i kitevőket a legnagyobbra választjuk. A legkisebb közös többszörösre vonatkozó egyenlőség bizonyítása analóg módon történik. (2) Két szám pontosan akkor relatív prím, ha nincs közös prímosztójuk. □

7.16. példa. Az $a = 2^3 \cdot 3^7 \cdot 7^2$ és $b = 2 \cdot 3^8 \cdot 5 \cdot 7^3$ esetén $(a, b) = 2 \cdot 3^7 \cdot 7^2$ és $[a, b] = 2^3 \cdot 3^8 \cdot 5 \cdot 7^3$.

A legnagyobb közös osztó, illetve a legkisebb közös többszörös iménti módon való meghatározása kényelmesnek tűnik, azonban nem túl hatékony eljárás. Nagy számok esetén nem ismerünk gyors algoritmust a kanonikus alak meghatározására. Ugyanakkor két egész szám legnagyobb közös osztóját az euklideszi algoritmus nagy számok esetén is gyorsan megadja. Megjegyezzük továbbá, hogy természetes számok prím mivoltának ellenőrzésére ismeretesek hatékony algoritmusok. Egy nagy egész szám prímsége tehát algoritmikusan eldönthető, míg faktorizálására nem ismerünk gyors módszert. Ez a tény titkosírások konstrukciójára használató, amit az XX fejezetben vizsgálunk meg részletesen.

7.2.5. A prímszámok problémaköre

A természetes számok prímjeinek világa olyan, mint a szerelem: titokzatos, tüneményes, érdekes és élvezetes. Már Euklidész Elemek című munkájában szerepel az alábbi tétel:

7.33. tétel. *A prímszámok száma végtelen.*

Bizonyítás. Tegyük fel indirekt, hogy csak véges sok prímszám van, $p_1, p_2, \ldots, p_k$, és legyen $n = \prod_{j=1}^{k} p_j$. Ekkor $n + 1$ nyilván $p_1 = 2, p_2, \ldots p_k$ egyikével sem osztható, ugyanakkor a számelmélet alaptétele miatt bizonyosan létezik prímosztója. Ez ellentmond az indirekt feltevésnek. □

A következő tételből az derül ki, hogy a prímek között tetszőlegesen nagy hézagok találhatók.

7.34. tétel. *Tetszőleges pozitív egész* N *számhoz megadható egy legalább* N *hosszú csupa összetett számot tartalmazó intervallum.*

Bizonyítás. Az előző bizonyításhoz hasonlóan okoskodunk. Jelölje n_k az összes, a p_k prímnél nem nagyobb prímek szorzatát. Ekkor $n_k + 2, n_k + 3, n_k + 4, \ldots, n_k + p_k$ mind összetettek. Találtunk tehát $N = p_k - 1$ egymás utáni összetett számot. □

A 2 és a 3 kivételével szomszédos természetes számok nem lehetnek egyidejűleg prímek, mert egyikük mindig páros. Ugyanakkor időnként előfordulhatnak egymáshoz igen közeli prímek, úgynevezett ***ikerprímek***, amikor p és $p + 2$ is prím. Az a probléma, hogy létezik-e végtelen sok ikerprímpár, máig megoldatlan. Az ikerprímprobléma általánosabban is megfogalmazható: a szomszédos prímek különbsége

vajon végtelen sokszor lesz-e „nagyon kicsi". A CSEBISEV-tétel szerint bármely $n > 1$ egész esetén létezik olyan p prím, amelyre $n < p < 2n$, vagyis a szomszédos prímek különbsége nem nőhet „túl gyorsan". Bebizonyítható, hogy ha p_k jelöli a k-adik prímet, akkor $p_{k+1} - p_k < (\log p_k)^{8/9}$ végtelen sok k esetén teljesül. Az ikerprímek mindenképpen „nagyon ritkán" helyezkednek el a prímek között, az ikerprímek reciprokösszege ugyanis konvergens (BRUN), míg a prímeké divergens. Ez utóbbi tény azt is mutatja, hogy „elég sok" prímszám van. Ha $\pi(x)$ jelöli az x-nél nem nagyobb prímek számát, akkor a prímszámtétel szerint

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

A tételt már GAUSS és LEGENDRE is sejtette, de HADAMARD és DE LA VALLÉE-POUSSIN bizonyította be az analízis segédeszközeivel. Ha adott n-ig nemcsak a prímek számára keresünk jó becslést, hanem egy prímtáblázatban fel is akarjuk sorolni őket, az alábbi algoritmus használható.

7.35. tétel (ERATHOSZTENESZI-szita). *Írjuk fel a számokat 2-től n-ig. Az első szám, a 2 prím, aminek összes többszöröse összetett, ezeket húzzuk ki. A megmaradt számok közül az első, a 3 prím, ennek többszörösei összetettek, ezeket húzzuk ki, stb. Ismételjük az eljárást $\sqrt{n}$-ig. A nem kihúzott számok együtt éppen az n-nél nem nagyobb prímszámokat adják.*

A szita algoritmusban azért elég a prímosztókat $\sqrt{n}$-ig vizsgálni, mert az n összetett szám legkisebb prímosztója nem lehet nagyobb $\sqrt{n}$-nél. Ha ugyanis p az n összetett szám legkisebb prímosztója, akkor nyilván $n = pk$ és $p \le k$. De ekkor $p^2 \le pk = n$, amiből $p \le \sqrt{n}$.

Érdekes kérdés, hogy bizonyos tulajdonságú sorozatokban van-e végtelen sok prím. Az alábbi tételt bizonyítás nélkül közöljük.

7.36. tétel (DIRICHLET-tétel). *Ha $a, d \in \mathbb{Z}$, $d > 0$ és $(a, d) = 1$, akkor az $a + kd$, $k = 0, 1, 2, \ldots$ számtani sorozat végtelen sok prímet tartalmaz.* □

A prímszámok elméletében számos nevezetes sejtés létezik, az alábbiakban kettőt sorolunk fel:

- Két egymást követő négyzetszám között mindig található prímszám.
- Minden 3-nál nagyobb páros szám felírható két prím összegeként (páros GOLDBACH-sejtés).

A speciális alakú prímek közül a $2^k + 1$ és a $2^k - 1$ alakú prímeket említjük meg, az előbbieket FERMAT-prímeknek, az utóbbiakat MERSENNE-prímeknek nevezzük. Megmutatható, hogy ha $2^k + 1$ prím, akkor k szükségképpen kettőhatvány, ha pedig $2^k - 1$ prím, akkor k maga is prím. Így a FERMAT-prímek $F_n = 2^{2^n} + 1$, a MERSENNE-prímek pedig $M_p = 2^p - 1$ (p prím) alakúak. Ismert, hogy F_n a $0 \le n \le 4$ esetén prím, míg $5 \le n \le 23$ esetén összetett. A FERMAT-prímek a szabályos sokszögek szerkesztésénél játszanak szerepet: GAUSS bebizonyította, hogy egy szabályos n-szög pontosan akkor szerkeszthető euklideszi szerkesztéssel (vagyis körzővel és vonalzóval), ha $n = 2^\alpha p_1 \ldots p_r$, ahol $\alpha \ge 0, r \ge 0$ és a p_i számok különböző FERMAT-prímek. Az első néhány érték: $3, 4, 5, 6, 8, 10, 12, 15$, stb.

A MERSENNE-féle számokhoz a ***tökéletes számok*** keresése során jutunk. Ezek olyan n természetes számok, amelyek n-től különböző osztóik összegével egyenlők. Például $6 = 1 + 2 + 3$. Pátatlan tökéletes számok 10^{20} alatt bizonyosan nincsenek, feltehetően egyáltalán nincsenek. A páros számok pontosan akkor tökéletesek, ha $n = M_k 2^{k-1}$ alakúak. 2005. május végéig 42 MERSENNE-prím volt ismeretes ($2, 3, 5, 7, 13, 17, 19, 31, 61$, stb.). A 42. MERSENNE-prím $2^{25964951} - 1$, ami 7 816 230 decimális jegyet tartalmaz. Máig megoldatlan az a kérdés, hogy a tökéletes számok (MERSENNE-prímek) sorozata véges, vagy végtelen.

7.2.6. Kongruenciák

Oszthatósági kérdések vizsgálatánál gyakran fordul elő, hogy maradékos osztást végezve a hányados értéke nem lényeges, valójában csak a maradékra van szükségünk. Ez indokolja az alábbi reláció bevezetését.

7.37. definíció. *Ha* $a, b, m \in \mathbb{Z}$ *és* $m \mid a - b$, *akkor azt mondjuk, hogy* a *és* b ***kongruensek*** *modulo* m. *Ezt a tényt* $a \equiv b \pmod{m}$*-el jelöljük. 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 még a tömörebb $a \equiv b\ (m)$ illetve $a \not\equiv b\ (m)$ jelölés is.

7.17. példa. $16 \equiv 4 \pmod{3}$, mert $3 \mid 16 - 4 = 12$.

Kongruenciák vizsgálatánál elegendő az $m > 1$ esetre szorítkozni, hiszen $m \mid a - b \Leftrightarrow -m \mid a - b$. Az $m = 0$ esetben $0 \mid a - b$ pontosan akkor teljesül, ha $a = b$, míg az $m = 1$ esetben $1 \mid a - b$, ami minden $a, b \in \mathbb{Z}$-re teljesül, így ezek az esetek kevésbé érdekesek.

7.38. tétel (a kongruencia tulajdonságai).

(1) $a \equiv a \pmod{m}$ *minden* a*-ra,*
(2) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$,
(3) $a \equiv b \pmod{m}$ *és* $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$,
(4) $a \equiv b \pmod{m}$ *és* $c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$,
(5) $a \equiv b \pmod{m}$ *és* $c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$,
(6) $f(x) \in \mathbb{Z}[x] \wedge a \equiv b \pmod{m} \Rightarrow f(a) \equiv f(b) \pmod{m}$.

Bizonyítás. Valamennyi állítás könnyen adódik a kongruencia definíciójából. Példaként először a (4) tulajdonságot igazoljuk. A feltétel szerint $m \mid a - b$ és $m \mid c - d$, amiből az oszthatóság lineáris kombinációs tulajdonsága alapján $m \mid (a+c) - (b+d)$, vagyis $a + c \equiv b + d \pmod{m}$. A (4) és (5) tulajdonságok $c = d$ esetére $a \equiv b \pmod{m} \Rightarrow a + c \equiv b + c \pmod{m}$ és $a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$, továbbá az (5) tulajdonság $c = a$, $d = b$ esetének többszöri alkalmazására $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$ adódik. Mindezek ismételt alkalmazásával jutunk el (6)-hoz. □

A tétel első három állítása azt fejezi ki, hogy a kongruencia reflexív, szimmetrikus és tranzitív reláció, azaz ekvivalenciareláció. A (4)–(5) tulajdonságok alapján az azonos

modulus szerinti kongruenciák „összeadhatók és összeszorozhatók." A tétel semmit sem állít az „osztásról." Az alábbi tétel szerint az egyszerűsítés csak úgy végezhető el, ha közben a modulust is megváltoztatjuk.

7.39. tétel. *Ha* $d = (c, m)$*, akkor*

$$ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{d}}.$$

Bizonyítás. A definíció alapján $m \mid (a-b)c$, vagyis

$$\frac{m}{d} \mid (a-b)\frac{c}{d}.$$

Mivel

$$(\frac{m}{d}, \frac{c}{d}) = 1,$$

ezért

$$\frac{m}{d} \mid a-b,$$

azaz

$$a \equiv b \pmod{\frac{m}{d}}.$$

Megfordítva, a kongruencia definíciója alapján lézetik olyan $q \in \mathbb{Z}$, amelyre

$$\frac{m}{d}q = a-b.$$

Az egyenletet c-vel szorozva kapjuk, hogy

$$\frac{mqc}{d} = c(a-b),$$

és mivel c/d is egész, ezért $m \mid ac-bc$, vagyis $ac \equiv bc \pmod{m}$. □

Nagyon lényeges az alábbi

7.40. következmény. $(c, m) = 1$ *és* $ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{m}$. □

A 7.38. tétel szerint az egészeket ekvivalenciaosztályokba sorolhatjuk. De vajon mely számok kerülnek egy osztályba?

7.41. tétel. *Az* $a \equiv b \pmod{m}$ *kongruencia pontosan akkor teljesül, ha az* a *és* b *számok* m*-mel vett osztási maradéka azonos.*

Bizonyítás. Osszuk el a-t és b-t maradékosan m-mel. Ekkor egyértelműen léteznek olyan q_a, r_a és q_b, r_b egészek, amelyekkel $a = mq_a + r_a$ és $b = mq_b + r_b$, ahol $0 \le r_a, r_b < m$. Ha $a \equiv b \pmod{m}$, akkor $m \mid m(q_a - q_b) + (r_a - r_b)$, amiből $m \mid r_a - r_b$ következik. De $|r_a - r_b| < m$ miatt $r_a - r_b = 0$, vagyis $r_a = r_b$. Megfordítva, ha $r_a = r_b$, akkor $m \mid (a-b)$, ezért $a \equiv b \pmod{m}$ teljesül. □

Így tehát azok az egészek kerülnek egy osztályba, amelyek m-mel osztva ugyanazt a maradékot szolgáltatják.

7.42. definíció. *Rögzített* m *modulus mellett az* a*-val kongruens elemek halmazát az* a *által reprezentált* ***maradékosztálynak*** *nevezzük és* $[a]_m$*-el jelöljük.*

A definíció szerint $[a]_m = \{a+km : k \in \mathbb{Z}\}$, valamint $a \equiv b \pmod{m} \Leftrightarrow [a]_m = [b]_m$.

7.18. példa. $[3]_7 = \{\ldots, -11, -4, 3, 10, 17, \ldots\} = [80]_7$.

Az összes maradékosztályt tartalmazó halmaz jelölése:

$$\mathbb{Z}_m = \{[a]_m \mid 0 \leq a \leq m-1\}.$$

7.43. definíció. *Ha az m szerinti maradékosztályok mindegyikéből kiemelünk pontosan egy reprezentáns elemet, akkor ezen elemek halmazát* ***teljes maradékrendszernek*** *nevezzük modulo m.*

Teljes maradékrendszer a modulo m vett legkisebb nemnegatív maradékok

$$\{a \in \mathbb{Z} \mid 0 \leq a \leq m-1\}$$

halmaza. Gyakran a legkisebb abszolút értékű maradékokat használjuk, mint teljes maradékrendszert.

7.19. példa. Teljes maradékrendszerek például a $\{13, -10, 31, -31, -8\}$, a $\{0, 1, 2, 3, 4\}$ és a $\{-2, -1, 0, 1, 2\}$ halmazok modulo 5.

A következőkben vizsgáljuk meg, hogy a modulushoz relatív prím egészek hogyan helyezkednek el a maradékosztályokban.

7.44. tétel. $a \equiv b \pmod{m} \Rightarrow (a, m) = (b, m)$.

Bizonyítás. A feltétel szerint $b = a + mc$ alkalmas c egésszel. Mivel $(a, m) \mid a$ és $(a, m) \mid m$ ezért $(a, m) \mid b$, így $(a, m) \mid (b, m)$. Hasonlóan adódik az $(b, m) \mid (a, m)$ oszthatóság is, ezért $(a, m) = (b, m)$. □

7.45. definíció. *Az $[a]_m$ maradékosztályt* ***redukált maradékosztálynak*** *nevezzük, ha $(a, m) = 1$.*

A 7.44. tétel miatt ha egy maradékosztály egy eleme relatív prím a modulushoz, akkor a maradékosztály összes eleme ilyen.

7.46. definíció. *Ha minden m szerinti redukált maradékosztályból pontosan egy reprezentáns elemet választunk, akkor* ***redukált maradékrendszert*** *kapunk.*

7.20. példa. A $\{-7, 7, 11, -11\}$ halmaz redukált maradékrendszer modulo 12.

7.47. definíció (Euler-féle φ függvény). *Tetszőleges m pozitív egész esetén jelentse $\varphi(m)$ az m-nél nem nagyobb, m-hez relatív prím természetes számok számát.*

7.21. példa. $\varphi(1) = 1$, $\varphi(7) = 6$, $\varphi(8) = 4$, $\varphi(10) = 4$.

Észrevehetjük, hogy $\varphi(m) = m-1 \Leftrightarrow m$ prím, valamint hogy $\varphi(m)$ éppen a modulo m redukált maradékosztályok száma. Az alábbi tétel a fenti definíciókból következik, bizonyítását a 7.2-3. gyakorlatra hagyjuk.

7.48. tétel. *Egész számok egy tetszőleges halmaza pontosan akkor alkot*
(1) *teljes maradékrendszert modulo* m*, ha a halmaz elemszáma* m *és elemei páronként inkongruensek modulo* m*,*
(2) *redukált maradékrendszert modulo* m*, ha a halmaz elemszáma* $\varphi(m)$*, elemei páronként inkongruensek modulo* m *és valamennyien relatív prímek* m*-hez.*

Az alábbi tétel szerint teljes maradékrendszer, illetve redukált maradékrendszer bizonyos tulajdonságú lineáris transzformációk után is teljes, illetve redukált maradékrendszer marad.

7.49. tétel (maradékrendszerek lineáris transzformációi). *Legyen* $\{a_1, a_2, \dots, a_m\}$ *teljes maradékrendszer,* $\{b_1, b_2, \dots, b_{\varphi(m)}\}$ *redukált maradékrendszer modulo* m*, és* $c, d \in \mathbb{Z}, (c, m) = 1$*. Ekkor*
(1) $\{ca_i + d : 1 \le i \le m\}$ *teljes maradékrendszer modulo* m*,*
(2) $\{cb_i : 1 \le i \le \varphi(m)\}$ *redukált maradékrendszer modulo* m*.*

Bizonyítás. (1) igazolása: mivel az új halmaz elemszáma is m, ezért a 7.48. tétel szerint már csak azt kell igazolni, hogy elemei páronként inkongruensek modulo m. Tegyük fel, hogy $ca_i + d \equiv ca_j + d \pmod m$, megmutatjuk, hogy $i = j$. Mindkét oldalból d-t kivonva $ca_i \equiv ca_j \pmod m$ adódik. Mivel $(c, m) = 1$, ezért a 7.40. következmény miatt c-vel egyszerűsíthetünk, így $a_i \equiv a_j \pmod m$, vagyis $i = j$, hiszen az a_i-k teljes maradékrendszert alkotnak. (2) igazolása hasonló: az új halmaz elemszáma is $\varphi(m)$, továbbá $cb_i \equiv cb_j \pmod m$ és $(c, m) = 1$ miatt $b_i \equiv b_j \pmod m$, vagyis $i = j$. Még azt kell igazolni, hogy az új halmaz elemei is relatív prímek m-hez. Ez abból adódik, hogy $(b_i, m) = 1$, $(c, m) = 1$ és a 7.32. tétel (3) állítása miatt ekkor $(cb_i, m) = 1$ is teljesül. □

A tétel egy nagyon fontos alkalmazása a következő.

7.50. tétel (Euler-tétel). *Legyen* $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$*. Ekkor* $a^{\varphi(m)} \equiv 1 \pmod m$.

Bizonyítás. Legyen $r_1, r_2, \dots r_{\varphi(m)}$ egy redukált maradékrendszer modulo m. Mivel $(a, m) = 1$, ezért $ar_1, ar_2, \dots, ar_{\varphi(m)}$ is redukált maradékrendszert alkot modulo m. A két redukált maradékrendszerben a megfelelő reprezentánsok párba állíthatók aszerint, hogy modulo m azonos osztályba esnek, vagyis $r_i \equiv ar_j \pmod m$ alkalmas $1 \le i, j \le \varphi(m)$ esetén. Ezeket a kongruenciákat összeszorozva kapjuk, hogy

$$a^{\varphi(m)} \prod_{j=1}^{\varphi(m)} r_j \equiv \prod_{j=1}^{\varphi(m)} r_j \pmod m.$$

$(r_i, m) = 1$ miatt az összes r_i-vel egyszerűsíthetünk, így $a^{\varphi(m)} \equiv 1 \pmod m$ adódik. □

A tételben szereplő $(a, m) = 1$ feltétel nemcsak elégséges, hanem szükséges is abban az értelemben, hogy csak akkor létezik olyan $k > 0$ kitevő, amelyre $a^k \equiv 1 \pmod m$, ha a és m relatív prímek. A tétel konkrétan megad egy ilyen k-t. Abban a speciális esetben, ha a modulus egy p prímszám, $\varphi(p) = p - 1$, így az alábbi összefüggést kapjuk.

7.51. következmény (FERMAT-tétel egyik alakja). *Ha* p *prímszám,* $a \in \mathbb{Z}$ *és* $p \nmid a$*, akkor* $a^{p-1} \equiv 1 \pmod{p}$.

7.52. következmény (FERMAT-tétel másik alakja). *Ha* p *prímszám és* $a \in \mathbb{Z}$*, akkor* $a^p \equiv a \pmod{p}$.

Bizonyítás. Ha $p \mid a$, akkor mindkét oldal osztható p-vel. Ha $p \nmid a$, akkor az előző következmény miatt lesz igaz. □

Felhívjuk a figyelmet, hogy a FERMAT-tétel első alakja csak $p \nmid a$ esetén, míg második alakja az a egészre vonatkozó megkötés nélkül is teljesül.

7.2.7. Műveletek maradékosztályokkal

A modulo m maradékosztályok között műveleteket értelmezhetünk.

$$\begin{aligned} [a]_m \oplus [b]_m &= [a+b]_m, \\ [a]_m \otimes [b]_m &= [ab]_m. \end{aligned}$$

Először is megmutatjuk, hogy a műveletek nem függnek attól, hogy az egyes maradékosztályokban melyik reprezentánst választottuk. Ha ugyanis $[a_1]_m = [a_2]_m$, akkor $a_1 \equiv a_2 \pmod{m}$ és ha $[b_1]_m = [b_2]_m$, akkor $b_1 \equiv b_2 \pmod{m}$, amiből $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$, vagy másképp $[a_1 + b_1]_m = [a_2 + b_2]_m$ következik. Hasonlóan járhatunk el a szorzás esetében is.

7.53. tétel. *A modulo* m *vett maradékosztályok az iménti összeadásra és szorzásra nézve egységelemes kommutatív gyűrűt alkotnak.*

Bizonyítás. Valamennyi tulajdonság azonnal következik a műveletek definíciójából. Példaképpen megmutatjuk, hogy a $\oplus$ művelet kommutativitása és asszociativitása a $+$ kommutativitásából és asszociativitásából adódik.

$$\begin{aligned} [a]_m \oplus [b]_m &= [a+b]_m \\ &= [b+a]_m \\ &= [b]_m \oplus [a]_m \ , \end{aligned}$$

$$\begin{aligned} ([a]_m \oplus [b]_m) \oplus [c]_m &= [a+b]_m \oplus [c]_m \\ &= [(a+b)+c]_m \\ &= [a+(b+c)]_m \\ &= [a]_m \oplus [b+c]_m \\ &= [a]_m \oplus ([b]_m \oplus [c]_m). \end{aligned}$$

□

Megjegyezzük, hogy a maradékosztályok között a kivonás is elvégezhető, vagyis bármely $[a]_m, [b]_m$ esetén pontosan egy olyan $[c]_m$ létezik, amelyre $[a]_m = [b]_m \oplus [c]_m$. A $[c]_m$ maradékosztályt $[a]_m \oplus [-b]_m$ alakban kaphatjuk meg.

Vizsgáljuk meg, hogy mely maradékosztályoknak létezik ***multiplikatív inverze,*** vagyis mely $[a]_m$ esetén létezik olyan $[c]_m$, amelyre $[a]_m \otimes [c]_m = [c]_m \otimes$

$[a]_m = [1]_m$. A feltétel pontosan azt jelenti, hogy $[ac]_m = [1]_m$, azaz $ac \equiv 1 \pmod{m}$. A későbbiekben bebizonyítjuk, hogy ezen kongruencia megoldhatóságának szükséges és elégséges feltétele, hogy $(a, m) = 1$ teljesüljön, vagyis $[a]_m$ redukált maradékosztály legyen. Az alábbi tételt kaptuk:

7.54. tétel. *A modulo m maradékosztályok között pontosan a redukált maradékosztályoknak létezik multiplikatív inverzük.*

7.55. következmény. *A modulo m maradékosztályok akkor és csak akkor alkotnak testet, ha m prím.*

7.2.8. Lineáris kongruenciák

Legyen $m > 1$ egész szám, valamint $a, b \in \mathbb{Z}$ adottak. Keressük az $ax \equiv b \pmod{m}$ lineáris kongruencia megoldásait. Nyilván, ha x_1 megoldása a kongruenciának, akkor minden $x_2 \equiv x_1 \pmod{m}$ is az, hiszen ekkor $ax_2 \equiv ax_1 \equiv b \pmod{m}$. Vagyis ha x_1 megoldás, akkor az $[x_1]$ maradékosztály összes eleme az. A megoldások megkereséséhez így elegendő egy teljes maradékrendszer elemeit végigpróbálni.

7.56. definíció. *Lineáris kongruencia megoldásszámán a páronként inkongruens megoldásokat értjük.*

7.57. tétel. *Az $ax \equiv b \pmod{m}$ kongruenciának pontosan akkor létezik megoldása, ha $(a, m) \mid b$. Ha létezik megoldás, akkor a megoldásszám (a, m).*

Bizonyítás. Az $ax \equiv b \pmod{m}$ kongruencia megoldhatósága azt jelenti, hogy létezik olyan x_1 egész, amelyre $ax_1 \equiv b \pmod{m}$. A kongruencia definíciója miatt ez azt jelenti, hogy létezik olyan x_2 egész, amelyre $mx_2 = b - ax_1$, vagyis $ax_1 + mx_2 = b$. Így az $ax \equiv b \pmod{m}$ kongruencia akkor és csak akkor oldható meg, ha az $ax_1 + mx_2 = b$ diofantikus egyenlet megoldható, aminek a szükséges és elégséges feltétele az, hogy $(a, m) \mid b$ teljesüljön (7.22. tétel).

Most vizsgáljuk meg a megoldásszámot, amennyiben létezik megoldás. Legyen $d = (a, m)$, $m_1 = m/d$, $a_1 = a/d$, $b_1 = b/d$. Ha $d = 1$, akkor amennyiben $\{c_1, c_2, \ldots, c_m\}$ teljes maradékrendszer, akkor a 7.49. tétel miatt $\{c_1 a, c_2 a, \ldots, c_m a\}$ is teljes maradékrendszer modulo m, így pontosan egy elem van köztük, amelyik b-vel kongruens. Ezen elem által reprezentált maradékosztály az egyetlen megoldás. Ha $d > 1$, akkor mivel az $ax \equiv b \pmod{m}$ és az $a_1 x \equiv b_1 \pmod{m_1}$ kongruenciákat ugyanazok az egész számok elégítik ki, így elég azt megvizsgálni, hogy a modulo m_1 egyetlen maradékosztályt alkotó megoldások hány inkongruens maradékosztályt jelentenek modulo m. Ha x_0 megoldása az $a_1 x \equiv b_1 \pmod{m_1}$ kongruenciának, akkor pontosan az

$$x_0, x_0 + m_1, x_0 + 2m_1, \ldots x_0 + (d-1)m_1$$

elemek esnek különböző maradékosztályokba modulo m. Ez pedig d darab inkongruens megoldást jelent. Vagyis a teljes megoldást a

$$[x_0], [x_0 + m_1], [x_0 + 2m_1], \ldots [x_0 + (d-1)m_1]$$

maradékosztályok elemei alkotják. □

A bizonyításból kiderült, hogy az $ax \equiv b \pmod{m}$ lineáris kongruencia és az $ax + my = b$ lineáris diofantikus egyenlet kölcsönösen visszavezethetők egymásra.

7.58. tétel. *Legyen* $(a, m) = 1$. *Ekkor az* $ax \equiv b \pmod{m}$ *kongruencia egyetlen megoldása az* $x_0 = a^{\varphi(m)-1}b \pmod{m}$ *számnak megfelelő osztály.*

Bizonyítás. Az előző tétel miatt a kongruenciának létezik megoldása, legyen ez x_0. Az $ax_0 \equiv b \pmod{m}$ kongruenciát $a^{\varphi(m)-1}$-gyel szorozva az $a^{\varphi(m)}x_0 \equiv a^{\varphi(m)-1}b \pmod{m}$ egyenletet kapjuk. Mivel $(a, m) = 1$, ezért az EULER-tételből az állítás következik. □

A $b = 1$ eset különleges, mivel a keresett x éppen az a multiplikatív inverze modulo m.

Összefoglalva, az $ax \equiv b \pmod{m}$ kongruencia megoldását (amennyiben megoldható) úgy is megkereshetjük, hogy (a, m)-mel osztva (természetesen a modulussal is osztunk) megoldjuk a kapott kongruenciát, majd ennek az x_0 megoldásából

$$x_k = x_0 + k\frac{m}{(a, m)}$$

segítségével előállítjuk a többit, ahol $0 \leq k < (a, m)$.

7.22. példa. Oldjuk meg a $12x \equiv 34 \pmod{1234}$ kongruenciát. Mivel $(12, 1234) = 2$ és $2 \mid 34$, ezért a kongruencia megoldható. A kongruenciát 2-vel osztva azt kapjuk, hogy $6x \equiv 17 \pmod{617}$. A jobb oldalból 617-et kivonva $6x \equiv -600 \pmod{617}$ adódik, majd 6-tal osztva kapjuk, hogy $x \equiv -100 \pmod{617}$. Így a megoldások $x \equiv 517 \pmod{1234}$ és $x \equiv 1134 \pmod{1234}$.

7.2.9. Szimultán kongruenciák

Lineáris kongruenciák után most lineáris kongruenciarendszerek közös megoldásait keressük.

Legyen $k \in \mathbb{N},\ m_1, m_2, \ldots m_k \in \mathbb{N},\ a_i, b_i \in \mathbb{Z}\ (1 \leq i \leq k)$. Az

$$\begin{aligned} a_1x &\equiv b_1 \pmod{m_1} \\ a_2x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_kx &\equiv b_k \pmod{m_k} \end{aligned}$$

kongruenciarendszer ***szimultán megoldása*** x_0, ha egyszerre elégíti ki az összes kongruenciát. Ha valamelyik kongruenciára nem teljesül a megoldhatóság feltétele, akkor nyilván a kongruenciarendszernek sincs megoldása. Másrészt, ha külön-külön létezik is az iménti kongruenciáknak megoldása, ez nem feltétlenül jár azzal, hogy létezik szimultán megoldás. A kérdésnek csak egy speciális esetét tárgyaljuk, amely a ***kínai maradéktétel*** néven ismert.

Időszámításunk szerint 100 körül Sun-Tsu kínai matematikus oldotta meg azt

a problémát, hogy hogyan lehet olyan x egészeket találni, amelyek 3-mal, 5-tel és 7-tel osztva rendre 2, 3, illetve 2 maradékot adnak. Egy ilyen megoldás az $x = 23$, az összes megoldás pedig a $23 + 105k$ alakú számok halmaza, ahol k tetszőleges egész számot jelöl. A kínai maradéktétel egy megfeleltetést létesít páronként relatív prím modulusú kongruenciák rendszere (például 3, 5 és 7) és egy olyan kongruencia között, amelynek modulusa az iménti modulusok szorzata (az előbbi példa szerint 105).

7.59. tétel (kínai maradéktétel). *Ha $m_1, \ldots, m_k$ páronként relatív prím modulusok, akkor a*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k}, \end{aligned} \tag{7.2}$$

kongruenciarendszernek bármely $a_1, \ldots, a_k$ egészek esetén van megoldása, s ez a megoldás modulo $M = m_1 \cdots m_k$ egyértelműen meghatározott.

Bizonyítás. Legyen

$$M_i = M/m_i \qquad (1 \le i \le k),$$

vagyis $M_i = m_1 m_2 \ldots m_{i-1} m_{i+1} \ldots m_k$. Tekintsük az

$$\begin{aligned} M_1 y &\equiv 1 \pmod{m_1} \\ M_2 y &\equiv 1 \pmod{m_2} \\ &\vdots \\ M_k y &\equiv 1 \pmod{m_k} \end{aligned}$$

kongruenciákat. Ezek külön-külön mind egyértelműen megoldhatók, mert M_i és m_i relatív prímek minden $1 \le i \le k$ esetén. Jelöljük megoldásaikat sorban $y_1, y_2, \ldots, y_k$-val és legyenek

$$c_i = M_i y_i \qquad (1 \le i \le k). \tag{7.3}$$

Legyen

$$x_0 \equiv (a_1 c_1 + a_2 c_2 + \ldots + a_k c_k) \pmod{M}. \tag{7.4}$$

Megmutatjuk, hogy ebből az egyenletből $x_0 \equiv a_i \pmod{m_i}$ $(1 \le i \le k)$ következik. Ha $i \ne j$, akkor $M_j \equiv 0 \pmod{m_i}$, amiből (7.3) miatt $c_j \equiv M_j \equiv 0 \pmod{m_i}$. Azt is észrevehetjük, hogy $c_i \equiv 1 \pmod{m_i}$ minden $1 \le i \le k$ esetén, így

$$\begin{aligned} x_0 &\equiv a_i c_i \pmod{m_i} \\ &\equiv a_i M_i y_i \pmod{m_i} \\ &\equiv a_i \pmod{m_i} \end{aligned}$$

minden i-re teljesül. A (7.4) szerint kiszámolt x_0 tehát valóban megoldás.

Tegyük fel, hogy a (7.2) kongruenciarendszernek több inkongruens megoldása is van modulo M, vagyis tegyük fel, hogy $x_0 \not\equiv x_1 \pmod{M}$ a kongruenciarendszer megoldásai. Mivel $x_0 \equiv x_1 \pmod{m_i}$ minden $1 \le i \le k$ esetén, ezért $m_i \mid a - b$. De $(m_i, m_j) = 1$ $(i \neq j)$, ezért $M \mid x_0 - x_1$, s így $x_0 \equiv x_1 \pmod{M}$, ami ellentmondás.

Megmutatjuk még, hogy a (7.2) kongruenciarendszer összes megoldását az $[x_0]_M$ maradékosztály elemei szolgáltatják. Legyen $x_1 \in [x_0]_M$, vagyis $x_0 \equiv x_1 \pmod{M}$. Ekkor $M \mid x_0 - x_1$, így $m_i \mid x_0 - x_1$ minden $1 \le i \le k$ esetén. Ez azt jelenti, hogy $x_0 \equiv x_1 \pmod{m_i}$, vagyis x_1 is kielégíti (7.2) minden egyenletét. □

A bizonyítás módszert is ad a szóban forgó kongruenciarendszer megoldására.

7.60. következmény. *Ha $m_1, \dots, m_k$ páronként relatív prím pozitív egészek, továbbá $M = m_1 \cdots m_k$, akkor az x és a egészekre az*

$$x \equiv a \pmod{m_i} \qquad (i = 1, 2, \dots, k)$$

egyenletek akkor és csak akkor teljesülnek egyidejűleg, ha

$$x \equiv a \pmod{M}.$$

□

7.61. tétel. *Legyenek $m_1, \dots, m_k$ páronként relatív prím pozitív egészek, $M = m_1 \cdots m_k$ és legyen $a \in \mathbb{Z}_M$. Legyenek továbbá $a_i \in \mathbb{Z}_{m_i}$ olyanok, hogy*

$$a_i \equiv a \bmod m_i \qquad (1 \le i \le k).$$

Tekintsük a

$$\phi : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$$
$$\phi(a) = (a_1, a_2, \dots, a_k)$$

megfeleltetést. Ekkor ϕ bijektív homomorfizmus (más szóval izomorfizmus), vagyis $\mathbb{Z}_M$ elemeivel végzett műveletek ekvivalensek a megfelelő szám k-asok minden egyes koordinátájával függetlenül végrehajtott ugyanolyan típusú műveletekkel: ha

$$a \leftrightarrow (a_1, a_2, \dots, a_k),$$

$$b \leftrightarrow (b_1, b_2, \dots, b_k),$$

akkor

$$\begin{aligned} (a + b) &\leftrightarrow ((a_1 + b_1) \bmod m_1, \dots, (a_k + b_k) \bmod m_k), \\ (a - b) &\leftrightarrow ((a_1 - b_1) \bmod m_1, \dots, (a_k - b_k) \bmod m_k), \\ (ab) &\leftrightarrow (a_1 b_1 \bmod m_1, \dots, a_k b_k \bmod m_k). \end{aligned}$$

Bizonyítás. A ϕ függvény bijektivitása a kínai maradéktételből következik. A művelettartás (homomorfia) a gyűrűelmélet homomorfiatétele miatt teljesül, amit a későbbiekben algebrából bizonyítunk. □

A tételt gyakran alkalmazzuk gyors algoritmusok készítésekor, mivel az egyes $\mathbb{Z}_{m_i}$

halmazokban hatékonyabban lehet műveleteket végezni (bitműveletekben számolva), mint $\mathbb{Z}_M$-ben.

7.23. példa. Tegyük fel, hogy olyan számítógép architektúránk van, ahol a gépi szó 4 bites, vagyis idealizált számítógépünk az $I_1 = [0, 2^4-1] = [0, 15]$ intervallum egészeivel képes egész aritmetikát végezni. Erre az aritmetikára építve valósítsunk meg az architektúránkon olyan egész aritmetikát (összeadás, kivonás, szorzás), amellyel az $I_2 = [0, 2000]$ intervallumban is számolni tudunk.

Válasszunk páronként relatív prím számokat az I_1 intervallumból úgy, hogy szorzatuk nagyobb legyen 2000-nél. Legyenek például $m_1 = 14, m_2 = 13, m_3 = 11$. Ekkor $M = m_1 \cdot m_2 \cdot m_3 = 2002$. Egy I_2 intervallumbeli egészet tehát egy I_1 intervallumból vett számhármassal ábrázolunk. Legyen például $a = 100$. Ekkor $100 \equiv 2 \pmod{14}, 100 \equiv 9 \pmod{13}$ és $100 \equiv 1 \pmod{11}$, így

$$100 \leftrightarrow (2, 9, 1).$$

Hasonlóan, ha mondjuk $b = 150$, akkor $150 \equiv 10 \pmod{14}, 150 \equiv 7 \pmod{13}$ és $150 \equiv 7 \pmod{11}$, vagyis

$$150 \leftrightarrow (10, 7, 7).$$

Ekkor a kínai maradéktétel 7.61. következménye szerint

$$a + b \leftrightarrow (2 + 10 \bmod 14, 9 + 7 \bmod 13, 1 + 7 \bmod 11) = (12, 3, 8).$$

Az ellenőrzéshez meg kell oldani a

$$\begin{aligned} x &\equiv 12 \pmod{14} \\ x &\equiv 3 \pmod{13} \\ x &\equiv 8 \pmod{11} \end{aligned}$$

kongruenciarendszert. A tétel jelöléseivel

$$M_1 = 13 \cdot 11 = 143,\ M_2 = 14 \cdot 11 = 154,\ M_3 = 14 \cdot 13 = 182.$$

A következőkben megoldjuk az alábbi egyenleteket:
(1) $143x \equiv 1 \pmod{14} \Leftrightarrow 3x \equiv 1 \pmod{14} \Leftrightarrow 3x \equiv 15 \pmod{14} \Leftrightarrow x \equiv 5 \pmod{14}$,
(2) $154x \equiv 1 \pmod{13} \Leftrightarrow 11x \equiv 1 \pmod{13} \Leftrightarrow -2x \equiv -12 \pmod{13} \Leftrightarrow x \equiv 6 \pmod{13}$,
(3) $182x \equiv 1 \pmod{11} \Leftrightarrow 6x \equiv 1 \pmod{11} \Leftrightarrow 6x \equiv 12 \pmod{11} \Leftrightarrow x \equiv 2 \pmod{11}$.
Kapjuk tehát, hogy

$$x \equiv 12 \cdot 5 \cdot 143 + 3 \cdot 6 \cdot 154 + 8 \cdot 2 \cdot 182 = 8580 + 2772 + 2912 \equiv 250 \pmod{2002}.$$

Valóban, $a + b = 100 + 150 = 250 \pmod{2002}$.

7.24. példa. Oldjuk meg az ősi indián problémát: ha kettesével, hármasával, négyesével, ötösével vagy hatosával veszünk ki tojásokat egy kosárból, a végén az iménti sorrendnek megfelelően $1, 2, 3, 4$, illetve 5 tojás marad. De ha hetesével emeljük ki őket, a végén nem marad egy sem. Minimálisan hány tojás lehetett a kosárban?

A kongruenciarendszer:

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 5 \pmod 6 \\ x &\equiv 0 \pmod 7. \end{aligned}$$

Mivel a modulusok páronként nem relatív prímek, ezért a kínai maradéktétel egyből nem alkalmazható. Először összevonásokat végzünk. Az $x \equiv 1 \pmod 2 \Leftrightarrow 2x \equiv 2 \pmod 4$ kongruenciát hozzáadva az $x \equiv 3 \pmod 4$ kongruenciához kajuk, hogy

$$3x \equiv 5 \pmod 4 \Leftrightarrow 3x \equiv 9 \pmod 4 \Leftrightarrow x \equiv 3 \pmod 4.$$

Persze ezt rögtön észrevehettük volna, hiszen ha egy szám 4-gyel osztva 3 maradékot ad, akkor szükségképpen 2-vel osztva 1-et. A technikát most három egyenletre alkalmazzuk:

$$\begin{aligned} x &\equiv 2 \pmod 3 \Leftrightarrow 4x \equiv 8 \pmod{12}, \\ x &\equiv 3 \pmod 4 \Leftrightarrow 3x \equiv 9 \pmod{12}, \\ x &\equiv 5 \pmod 6 \Leftrightarrow 2x \equiv 10 \pmod{12}. \end{aligned}$$

A kongruenciákat összeadva kapjuk, hogy

$$9x \equiv 27 \pmod{12} \Leftrightarrow 3x \equiv 9 \pmod 4 \Leftrightarrow x \equiv 3 \pmod 4.$$

Vagyis a megoldandó egyenletrendszer:

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 0 \pmod 7. \end{aligned}$$

Most már alkalmazható a kínai maradéktétel. Jelöléseinkkel $m_1 = 4, m_2 = 5, m_3 = 7, M = 3 \cdot 5 \cdot 7 = 140, M_1 = 140/4 = 35, M_2 = 140/5 = 28, M_3 = 140/7 = 20$, továbbá $a_1 = 3, a_2 = 4, a_3 = 0$. Most megoldjuk az alábbi egyenleteket:
(1) $35x \equiv 1 \pmod 4 \Leftrightarrow 3x \equiv 1 \pmod 4 \Leftrightarrow 3x \equiv -3 \pmod 4 \Leftrightarrow x \equiv -1 \pmod 4 \Leftrightarrow x \equiv 3 \pmod 4$,
(2) $28x \equiv 1 \pmod 5 \Leftrightarrow 3x \equiv 1 \pmod 5 \Leftrightarrow 3x \equiv 6 \pmod 5 \Leftrightarrow x \equiv 2 \pmod 5$.
A megoldás így

$$x \equiv 3 \cdot 3 \cdot 35 + 4 \cdot 2 \cdot 28 + 0 \pmod{140} \Leftrightarrow x \equiv 539 \pmod{140} \Leftrightarrow x \equiv 119 \pmod{140}.$$

A megoldás ellenőrzését az Olvasóra bízzuk.

7.2.10. Számelméleti függvények

7.62. definíció. *A számelméletben az* $\mathbb{N}^+ \to \mathbb{C}$ *leképezéseket* ***számelméleti függvényeknek*** *nevezzük.*

Ilyenek például a korábban definiált Euler-féle φ függvény, vagy a pozitív osztók számát jelölő τ függvény.

7.63. definíció. *Egy* f *számelméleti függvényt* ***additívnak*** *nevezünk, ha relatív prím* $m, n \in \mathbb{N}^+$ *számok esetén* $f(mn) = f(m)+f(n)$ *teljesül, és* ***teljesen*** *(vagy totálisan)* ***additívnak*** *nevezünk, ha ez tetszőleges* $m, n \in \mathbb{N}^+$ *esetén fennáll.*

Jelölje $v(n)$ az $1 < n \in \mathbb{N}^+$ különböző prímosztói számát és legyen $v(1) = 0$. Ha $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ az n kanonikus alakja, akkor $v(n) = r$. Könnyen látható, hogy a v függvény additív, de nem teljesen additív számelméleti függvény. Például $1 = v(4) \neq 2v(2) = 2$.

Legyen $1 < a \in \mathbb{N}$ és minden $n \in \mathbb{N}^+$-ra tekintsük az $n \mapsto \log_a n$ függvényt. Mivel $\log_a(mn) = \log_a m + \log_a n$ minden $m, n \in \mathbb{N}^+$ esetén, ezért az $\log_a n$ függvény teljesen additív.

7.64. definíció. *Egy* f *számelméleti függvényt* ***multiplikatívnak*** *nevezünk, ha relatív prím* $m, n \in \mathbb{N}^+$ *számok esetén* $f(mn) = f(m)f(n)$ *teljesül, és* ***teljesen*** *(vagy totálisan)* ***multiplikatívnak*** *nevezünk, ha ez tetszőleges* $m, n \in \mathbb{N}^+$ *esetén fennáll.*

Az $E(1) = 1$, $E(n) = 0$, ha $n > 1$ összefüggéssel definiált függvény teljesen multiplikatív. Az $f(n) = n^k$ ($k \in \mathbb{N}$) függvény teljesen multiplikatív, hiszen $f(mn) = (mn)^k = m^k n^k = f(m)f(n)$ minden $m, n \in \mathbb{N}^+$ esetén teljesül. Definiáljuk a $\mu : \mathbb{N}^+ \to \{-1, 0, 1\}$ MÖBIUS-függvényt:

$$\mu(n) = \begin{cases} 1 & \text{ha } n = 1, \\ (-1)^r & \text{ha } n = p_1 p_2 \cdots p_r \ (p_i\text{-k páronként különböző prímek}), \\ 0 & \text{különben.} \end{cases}$$

Könnyen ellenőrizhető, hogy a MÖBIUS-függvény multiplikatív, de nem teljesen multiplikatív, hiszen például $0 = \mu(4) \neq \mu(2)^2 = 1$.

A definíciókban az $m = 1$ helyetesítéssel azt kapjuk, hogy egy additív számelméleti függvény 1 helyen felvett értéke mindig nulla, valamint egy nem azonosan nulla multiplikatív számelméleti függvény 1 helyen felvett értéke mindig 1.

7.65. tétel. *Az* EULER*-féle* φ *függvény multiplikatív, és ha* $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ *az* $n > 1$ *természetes szám kanonikus alakja, akkor*

$$\varphi(n) = n \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right) = \prod_{j=1}^{k} (p_j^{\alpha_j} - p_j^{\alpha_j - 1}).$$

Bizonyítás. Először φ multiplikativitását látjuk be. Erre két különböző bizonyítást is adunk.
(1). Legyenek $m, n \in \mathbb{N}^+$, $(m, n) = 1$. Készítsük el az alábbi táblázatot:

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & m \\ m+1 & m+2 & m+3 & \cdots & 2m \\ 2m+1 & 2m+2 & 2m+3 & \cdots & 3m \\ \vdots & \vdots & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & (n-1)m+3 & \cdots & nm\,. \end{array}$$

A táblázatban $\varphi(mn)$ olyan szám van, amelyik mn-hez relatív prím, továbbá a 7.32.

tétel miatt ezek mindegyike relatív prím m-hez és n-hez is. Keressük meg a táblázatban azon elemek számát, amelyek m-hez és n-hez is relatív prímek. Mivel egy-egy oszlop elemei ugyanabba a maradékosztályba tartoznak, és minden sorban egy teljes maradékrendszer van modulo m, így $\varphi(m)$ olyan oszlop van, amelyek elemei relatív prímek m-hez. A 7.49. tétel miatt minden ilyen oszlop teljes maradékrendszert alkot modulo n, így ezen oszlopok mindegyike pontosan $\varphi(n)$ olyan elemet tartalmaz, amelyik n-hez relatív prím. Így az m-hez és n-hez egyszerre relatív prímek száma $\varphi(m)\varphi(n)$.

(2). Legyenek $m, n \in \mathbb{N}^+$ olyanok, hogy $(m, n) = 1$. Tudjuk, hogy $\varphi(1) = 1$, ezért ha $m = 1$ vagy $n = 1$, akkor az állítás nyilvánvaló. Feltehető tehát, hogy $m, n \geq 2$. Legyenek $\{r_1, \ldots, r_{\varphi(m)}\}$ és $\{s_1, \ldots, s_{\varphi(n)}\}$ redukált maradékrendszerek modulo m, illetve n. Rögzített (i, j) indexpárra $(1 \leq i \leq \varphi(m),\ 1 \leq j \leq \varphi(n))$ tekintsük az

$$\begin{aligned} x &\equiv r_i \pmod{m} \\ x &\equiv s_j \pmod{n}. \end{aligned} \tag{7.5}$$

kongruenciarendszert. A kínai maradéktétel miatt ennek pontosan egy megoldása van modulo mn, legyen ez a megoldás t_{ij}. Mivel tetszőleges (i, j) indexpár $(1 \leq i \leq \varphi(m),\ 1 \leq j \leq \varphi(n))$ esetén $(t_{ij}, m) = (r_i, m) = 1$ és $(t_{ij}, n) = (s_j, n) = 1$, ezért $(t_{ij}, mn) = 1$. Különböző (i, j), (i', j') indexpárokra $(1 \leq i, i' \leq \varphi(m),\ 1 \leq j, j' \leq \varphi(n))$ ha $i \neq i'$, akkor $t_{ij} \equiv r_i \not\equiv r_{i'} \equiv t_{i'j'} \pmod{n}$, ha $j \neq j'$, akkor $t_{ij} \equiv s_j \not\equiv s_{j'} \equiv t_{i'j'} \pmod{m}$, így $t_{ij} \not\equiv t_{i'j'} \pmod{mn}$. A kínai maradéktétel miatt tetszőleges t_{ij}-hez $(1 \leq t_{ij} \leq mn)$ van olyan (i, j) pár $(1 \leq i \leq \varphi(m),\ 1 \leq j \leq \varphi(n))$, hogy a (7.5) kongruenciarendszernek pontosan a t_{ij} a megoldása. Azt kaptuk, hogy a t_{ij} számok $(1 \leq t_{ij} \leq mn)$ redukált maradékrendszert alkotnak modulo mn, s így $\varphi(m)\varphi(n) = \varphi(mn)$.

Eszerint φ multiplikatív, vagyis $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$. Elég tehát azt belátni, hogy $\varphi(p^\alpha) = p^\alpha(1 - 1/p) = p^\alpha - p^{\alpha-1}$, ha p prím és $\alpha > 0$. Ez viszont következik abból, hogy $0 < x \leq p^\alpha$ pontosan akkor nem relatív prím p^α-hoz, ha többszöröse p-nek. □

7.25. példa. Határozzuk meg a 2003^{2003} utolsó két számjegyét a tízes számrendszerben. A feladat szerint meg kell oldani a

$$2003^{2003} \equiv x \pmod{100}$$

kongruenciát. Az egyenletben hatványozás szerepel, ezért az Euler-tételt próbáljuk alkalmazni. Mivel

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(4) \cdot \varphi(25) = (2^2 - 2)(5^2 - 5) = 2 \cdot 20 = 40,$$

valamint $(3, 100) = 1$, ezért $3^{\varphi(100)} \equiv 1 \pmod{100}$, így

$$x \equiv 2003^{2003} \equiv 3^{2003} \equiv 3^{40 \cdot 50 + 3} \equiv (3^{40})^{50} \cdot 3^3 \equiv 3^3 \equiv 27 \pmod{100}.$$

Gyakorlatok

7.2-1. Bizonyítsuk be, hogy $a, b \in \mathbb{Z}$ esetén $a \mid b$ és $b \mid a \Rightarrow |a| = |b|$.

7.2-2. Bizonyítsuk be a LEGENDRE-formulát: az $n!$ kanonikus alakja

$$n! = \prod_{p \le n} p^{\alpha_p}, \quad \text{ahol} \quad \alpha_p = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

7.2-3. Hogyan olvasható le egy szám kanonikus alakjából, hogy négyzetszám, köbszám, illetve általában k-adik hatvány?

7.2-4. Melyek igazak az alábbi állítások közül?

a) $(a, b) = (a + b, ab)$.
b) $(a, bc) = (ab, ac)$.
c) $(a^3, b^3) = (a, b)^3$.
d) $[a, (b, c)] = ([a, b], [a, c])$.

7.2-5. Bizonyítsuk be a 7.48. tételt.

7.2-6. A kegyetlen várúr pincebörtöne 666 szűk cellájának mindegyikében egy-egy rab sínylődik. A várúr születésnapja alkalmából sorban leküldi egy-egy emberét. Az i.-nek leküldött ember minden i. cella zárján állít egyet, vagyis, ha nyitva volt, bezárja, ha zárva volt, kinyitja. Azok a rabok, akiknek a legvégén nyitva marad a cellája, szabadon elmehetnek. Hányan és mely cellák lakói szabadulnak?

7.2-7. Lássuk be kongruenciák segítségével a természetes számok 9-cel, illetve 11-gyel való oszthatóságára vonatkozó szabályokat.

7.2-8. Oldjuk meg az alábbi kongruenciák közül a megoldhatókat:

a) $3x \equiv 5 \pmod 7$,
b) $123x \equiv 456 \pmod{78}$,
c) $111x \equiv 1111 \pmod{11}$.

7.2-9. Süsünek csupa 7 és tízfejű unokatestvérei vannak, akiknek összesen 116 fejük van. Hány unokatestvére van a sárkánygyereknek?

7.2-10. Oldjuk meg az $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$, $x \equiv 1 \pmod 5$ kongruenciarendszert.

7.2-11. Bizonyítsuk be a 7.65. tételt a logikai szita formula segítségével.

7.2-12. Mi a $39^{39^{39}}$ szám utolsó két számjegye?

7.3. Lánctörtek

A fejezetben már megvizsgáltuk a természetes számok helyiértékes ábrázolását (7.17. tétel). Az egész számok is leírhatók ily módon, szükség szerint előjellel egészítve ki őket. A racionális számok egyrészt két egész szám hányadosaként, másrészt helyiértékesen ábrázolva, véges vagy végtelen szakaszos tizedes törtként is megadhatók (4.37. tétel). Az irracionális számokat végtelen nem szakaszos tizedes törtekkel írhatjuk le. A következőkben a valós számok másfajta előállítását vizsgáljuk. Fel fogjuk használni a 4.35.-ben és 4.36.-ban definiált egészrész és törtrész függvényeket.

Tetszőleges α valós szám esetén tekintsük az alábbi algoritmust. Legyen

$$q_1 = \lfloor \alpha \rfloor, \quad \alpha_1 = \{\alpha\}.$$

Ekkor $\alpha = q_1 + \alpha_1$. Ha $\alpha_1 \neq 0$, akkor legyen

$$q_2 = \left\lfloor \frac{1}{\alpha_1} \right\rfloor, \quad \alpha_2 = \left\{ \frac{1}{\alpha_1} \right\}.$$

Ekkor

$$\alpha = q_1 + \alpha_1 = q_1 + \frac{1}{q_2 + \alpha_2}.$$

Ha $\alpha_2 \neq 0$, akkor $1/\alpha_2$ egész és törtrészét képezzük, stb. Általában, ha a $q_1, q_2, \ldots, q_n$ és $\alpha_1, \alpha_2, \ldots, \alpha_n$ értékeket már meghatároztuk, és $\alpha_n \neq 0$, akkor legyen

$$q_{n+1} = \left\lfloor \frac{1}{\alpha_n} \right\rfloor, \quad \alpha_{n+1} = \left\{ \frac{1}{\alpha_n} \right\}.$$

Ekkor

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots \; q_n + \cfrac{1}{q_{n+1} + \alpha_{n+1}}}}}.$$

Eljárásunk akkor ér véget, ha valamilyen m-re $\alpha_m = 0$.

Az iménti kifejezést ***lánctörtnek*** nevezzük és az egyszerűbb írásmód kedvéért bevezetjük rá a $//q_1, q_2, \ldots, q_n, q_{n+1} + \alpha_{n+1}//$ jelölést. Az ily módon kapott $q_1, q_2, \ldots$ egész számokat a lánctört előállítás ***jegyeinek*** nevezzük. A konstrukció alapján világos, hogy a lánctörtjegyek egyértelműen meghatározott egész számok és $q_i > 0$, ha $i > 1$. (Lánctörtek felírására szokásos még a $\langle q_1, q_2, \ldots \rangle$, illetve a $[q_1, q_2, \ldots]$ jelölés is.)

7.26. példa. Legyen $\alpha = 355/113 = 3.14159292035398230088$. Ekkor

$$\begin{aligned} \frac{355}{113} &= 3 + \frac{16}{113}, \quad q_1 = 3, \\ \frac{113}{16} &= 7 + \frac{1}{16}, \quad q_2 = 7, \\ \frac{16}{1} &= 16 + 0, \quad q_3 = 16. \end{aligned}$$

Azt kaptuk tehát, hogy $\alpha = //3, 7, 16//$.

7.27. példa. Legyen $\alpha = \sqrt{2}$. Ekkor

$$\begin{aligned} \sqrt{2} &= 1 + (\sqrt{2} - 1), \quad q_1 = 1, \\ \frac{1}{\sqrt{2}-1} &= \sqrt{2} + 1 = 2 + (\sqrt{2} - 1), \quad q_2 = 2, \\ \frac{1}{\sqrt{2}-1} &= \sqrt{2} + 1 = 2 + (\sqrt{2} - 1), \quad q_3 = 2, \\ &\vdots \end{aligned}$$

Vagyis $\sqrt{2} = //1, 2, 2, \ldots//$.

7.66. tétel. *Az α valós szám lánctörtjegyeinek sorozata pontosan akkor véges, ha α racionális.*

Bizonyítás. Ha a lánctörtjegyek sorozata véges, mondjuk $//q_1, q_2, \ldots, q_n//$, akkor az emeletes törteket lebontva α végül két egész szám hányadosaként írható fel, vagyis α racionális.

Megfordítva, legyen $\alpha = a/b$, ahol $b > 0$ és a egész számok, $(a, b) = 1$. Megmutatjuk, hogy ekkor a lánctörtjegyeket megadó algoritmus lépései pontosan az a-ra és b-re vonatkozó euklideszi algoritmus lépéseinek felelnek meg, így a lánctörtjegyeket előállító algoritmus véges sok lépésben befejeződik.

Hajtsuk végre az euklideszi algoritmust az a, b számokon.

$$\begin{aligned}
a &= bq_1 + r_1, & 0 < r_1 < b,\\
b &= r_1 q_2 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2 q_3 + r_3, & 0 < r_3 < r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1} q_n + r_n, & 0 < r_n < r_{n-1},\\
r_{n-1} &= r_n q_{n+1}.
\end{aligned}$$

Osszuk el az euklideszi algoritmus egyenlőségeit rendre b-vel, r_1-gyel, r_2-vel, …, r_n-nel.

$$\begin{aligned}
\frac{a}{b} &= q_1 + \frac{1}{b/r_1},\\
\frac{b}{r_1} &= q_2 + \frac{1}{r_1/r_2},\\
\frac{r_1}{r_2} &= q_3 + \frac{1}{r_2/r_3},\\
&\vdots\\
\frac{r_{n-2}}{r_{n-1}} &= q_n + \frac{1}{r_{n-1}/r_n},\\
\frac{r_{n-1}}{r_n} &= q_{n+1}.
\end{aligned}$$

Lépésről lépésre elvégezve a behelyettesítéseket (a második egyenlőségből az azt megelőző egyenletbe b/r_1-et, a harmadikból r_1/r_2-t, és így tovább) pontosan az a/b szám $//q_1, q_2, \ldots, q_{n+1}//$ lánctört előállítását kapjuk. □

A továbbiakban feltesszük, hogy α valós, és megmutatjuk, hogy a lánctörtek segítségével α-t jól közelítő racionális számokat tudunk előállítni. Ezek α lánctörtalakjának „szeletei” lesznek.

7.67. definíció. *Az α valós szám $//q_1, q_2, \ldots, q_n, \ldots//$ lánctört alakjának **n-edik szeletén** a $\delta_n = //q_1, q_2, \ldots, q_n//$ lánctörtet értjük.*

A 7.66. tétel szerint ha α megegyezik lánctört alakjának valamely szeletével, akkor racionális.

7.68. tétel. *Legyen az α valós szám lánctört alakja $//q_1, q_2, \ldots, q_n, \ldots//$.*

(1) *Ekkor a*

$$\begin{array}{lllllll} P_0 & = & 1 & & Q_0 & = & 0 \\ P_1 & = & q_1 & & Q_1 & = & 1 \\ P_k & = & q_k P_{k-1} + P_{k-2} & & Q_k & = & q_k Q_{k-1} + Q_{k-2} \end{array}$$

rekurzió a lánctört szeleteit állítja elő, vagyis ha $1 \le k \le n$, akkor $\delta_k = P_k/Q_k$, ahol a P_k és Q_k egészek relatív prímek.

(2) *Minden $1 < k \le n$ esetén*

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_k Q_{k-1}}.$$

(3) *Minden $1 < k \le n$ esetén*

$$|\alpha - \delta_{k-1}| \le \frac{1}{Q_k Q_{k-1}},$$

és egyenlőség csak $\delta_n = \alpha$ esetén áll.

Bizonyítás. Az (1) állítást indukcióval bizonyítjuk. $k = 1$-re $P_1 = q_1$, $Q_1 = 1$, és $\delta_1 = q_1 = P_1/Q_1$. $k = 2$ esetén $P_2 = q_1 q_2 + 1$, $Q_2 = q_2$, és $\delta_2 = (q_1 q_2 + 1)/q_2 = P_2/Q_2$. Tegyük fel, hogy $2 < k - 1$-ig az állítás igaz. Vegyük észre, hogy δ_k-t úgy kapjuk $\delta_{k-1} = //q_1, q_2, \ldots, q_{k-1}//$-ből, hogy q_{k-1} helyébe $q_{k-1} + 1/q_k$-t írunk. Így

$$\delta_{k-1} = \frac{P_{k-1}}{Q_{k-1}} = \frac{q_{k-1} P_{k-2} + P_{k-3}}{q_{k-1} Q_{k-2} + Q_{k-3}}$$

felhasználásával

$$\begin{array}{rcl} \delta_k & = & \dfrac{(q_{k-1} + 1/q_k) P_{k-2} + P_{k-3}}{(q_{k-1} + 1/q_k) Q_{k-2} + Q_{k-3}} = \dfrac{q_k (q_{k-1} P_{k-2} + P_{k-3}) + P_{k-2}}{q_k (q_{k-1} Q_{k-2} + Q_{k-3}) + Q_{k-2}} \\ & = & \dfrac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}} = \dfrac{P_k}{Q_k}. \end{array}$$

Most indukcióval megmutatjuk, hogy minden $1 \le k \le n$ esetén $P_k Q_{k-1} - Q_k P_{k-1} = (-1)^k$. $k = 1$ esetén $P_1 Q_0 - Q_1 P_0 = -1$, vagyis az állítás igaz. $k = 2$-re $P_2 Q_1 - P_1 Q_2 = (q_1 q_2 + 1) - q_1 q_2 = 1 = (-1)^2$. Tegyük fel, hogy az állítás teljesül $2 < k - 1$-re. Ekkor

$$\begin{array}{rcl} P_k Q_{k-1} - Q_k P_{k-1} & = & (q_k P_{k-1} + P_{k-2}) Q_{k-1} - (q_k Q_{k-1} + Q_{k-2}) P_{k-1} \\ & = & Q_{k-1} P_{k-2} - P_{k-1} Q_{k-2} = (-1) \cdot (-1)^{k-1} = (-1)^k. \end{array}$$

Ebből egyrészt következik (2), másrészt hogy P_k és Q_k legnagyobb közös osztója osztója $(-1)^k$-nak is, azaz hogy P_k és Q_k relatív prímek. Az $\alpha - \delta_{k-1}$ különbség $(2 \le k \le n)$ becsléséhez a (2) állítást és az $\alpha = //q_1, q_2, \ldots, q_k, \alpha_{k+1}//$ összefüggést használjuk fel. Ekkor ugyanis

$$\alpha - \delta_{k-1} = \frac{(-1)^k}{Q_{k-1}\big((q_k + \alpha_{k+1}) Q_k + Q_{k-1}\big)},$$

ahol a nevező $q_k > 0$ miatt mindig pozitív. Ez azt is jelenti, hogy ha k páros, akkor $\alpha - \delta_{k-1}$ mindig pozitív, ha k páratlan, akkor $\alpha - \delta_{k-1}$ mindig negatív, továbbá a (2) állítás miatt a páratlan indexű közelítő törtek növekvő, a páros indexűek csökkenő sorozatot alkotnak. Azt kaptuk tehát, hogy

$$\frac{P_1}{Q_1} < \frac{P_3}{Q_3} < \ldots \leq \alpha \leq \ldots < \frac{P_4}{Q_4} < \frac{P_2}{Q_2},$$

amiből a (3) állítás következik. Egyenlőség nyilván csak az $\alpha = \delta_n$ esetben állhat fenn. □

Történeti érdekesség, hogy a görögök lánctörteket használtak az irracionális számok leírására. Megmutatható, hogy egy β irracionális szám lánctört kifejtése pontosan akkor periodikus valahonnan kezdve, ha β gyöke valamilyen racionális együtthatós másodfokú egyenletnek.

A 7.68. tétel szerint ha α irracionális, akkor végtelen sok olyan $p, q \in \mathbb{Z}$, $q \neq 0$ pár létezik, amelyre

$$|\alpha - \frac{p}{q}| < \frac{1}{q^2},$$

nevezetesen bármely P_k, Q_k pár ilyen. Az is megmutatható, hogy két egymás utáni lánctört közelítés közül az egyik eleget tesz a

$$|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$$

egyenlőltenségnek, sőt, három egymás utáni lánctört közelítés közül az egyikre teljesül az

$$|\alpha - \frac{p}{q}| < \frac{1}{\sqrt{5}q^2}$$

egyenlőtlenség. Az $\alpha = (1+\sqrt{5})/2$ esetén további élesítés már nem tehető úgy, hogy még mindig végtelen sok p, q párra álljon fenn az egyenlőtlenség.

Még fonosabb tény, hogy az adott korlátnál nem nagyobb nevezőjű törtek közül a lánctört kifejtések adják a legjobb közelítéseket.

7.69. tétel. *Legyen α egy irracionális szám. Az előző tétel jelöléseivel, ha $p \in \mathbb{Z}$, $q \in \mathbb{N}^+$ és*

$$|\alpha - p/q| < |\alpha - P_k/Q_k|$$

valamely $k > 1$-re, akkor $q > Q_k$. Sőt, ha

$$|\alpha q - p| < |\alpha Q_k - P_k|$$

valamely $k > 0$-ra, akkor $q \geq Q_{k+1}$. □

Gyakorlatok

7.3-1. Határozzuk meg az alábbi valós számok lánctörtjegyeit:
a) $123/21$, b) $\sqrt{3}$, c) $(1+\sqrt{5})/2$.

7.3-2. Igaz-e, hogy $//q_1, q_2, \ldots, q_n// = //q_1, q_2, \ldots, q_n - 1, 1//$?

7.3-3. Keressünk olyan 100-nál kisebb nevezőjű törtet, amelynek az eltérése $\sqrt{2}$-től kisebb, mint $0,001$.

7.3-4. Bizonyítsuk be, hogy $Q_n > F_n$ minden ($n \in \mathbb{N}$) esetén, ahol F_n az n-edik FIBONACCI-szám.

Megjegyzések a fejezethez

A tökéletes számok problémáját az ókori görögök vetették fel. Különös jelentőséget tulajdonítottak azoknak a számoknak, amelyek „részeikből visszanyerhetők", azaz részeinek összege éppen az eredeti számmal egyenlő. Ezen harmóniát testesítik meg a tökéletes számok, melyek közül négyet a régi görögök is ismertek: $6, 28, 496, 8128$. Euklidész így ír az Elemek IX. könyvének 36. tételében[1]: „Ha az egységtől kezdve kétszeres arányban képezünk egy mértani sorozatot, amíg a sorösszeg prím nem lesz, és az összeggel megszorozzuk az utolsó tagot, akkor a szorzat tökéletes szám lesz."

Ebben az áll, hogy ha $1+2+2^2+\cdots+2^n$ prímszám, akkor ezt 2^n-nel szorozva tökéletes számot kapunk. Jó kétezer évvel később Euler, majd Mersenne ennél az állításnál lényegesen többet bizonyítottak. A témakörben rajtuk kívül Lucas, majd Lehmer alkottak jelentőset:

7.70. tétel (Lucas). *Tekintsük az alábbi sorozatot:* $r_1 := 3$, *majd* $n > 1$ *esetén* $r_n := r_{n-1}^2 - 2$. *Ha a* p *prím* $4k+3$ *alakú, akkor* M_p *pontosan akkor prím, ha* M_p *osztója* r_{p-1}*-nek.*

7.71. tétel (Lehmer). *A* Lucas*-tételben lévő sorozat első elemét változtassuk* 4*-re, és a képzési szabály maradjon változatlan. Ekkor* M_p *pontosan akkor prím, ha* M_p *osztója* r_{p-1}*-nek.*

Ezek a tesztek egyszerűségük miatt könnyen alkalmazhatók prímszámkeresésre, így a legnagyobb ismert prímek továbbra is várhatóan Mersenne-prímek lesznek.

Ha a természetes számok különböző felbontásait vizsgáljuk, a legismertebb probléma az $x^2+y^2=z^2$ egyenlet pozitív egész megoldásainak vizsgálata. Nem nehéz meggondolni, hogy elegendő olyan megoldásokat keresni, amikor $(x,y,z)=1$. Ezeket primitív megoldásoknak nevezzük.

7.72. tétel. *Az* $x^2+y^2=z^2$ *egyenlet primitív megoldásai*

$$\begin{aligned} x &= 2mn \\ y &= m^2-n^2 \\ z &= m^2+n^2 \end{aligned}$$

alakúak, ahol $(m,n)=1$, *különböző paritásúak, és* $m>n>0$.

Az általános eset Fermat nevéhez fűződik, aki 1637 körül azt állította, hogy az $x^n+y^n=z^n$ egyenletnek, amelynek egész megoldásait keressük, $n>2$ esetén csak triviális megoldásai vannak. A tételt csak nemrég sikerült bizonyítani, ami az elliptikus görbék és moduláris formák elméletének mély meggondolásain alapszik.

A kínai csillagász Tsu Csung-Chih (430–501) már ismerte a π 6 tizedes jegyre pontos $355/113$ közelítését. A π irracionalitását Lambert bizonyította 1761-ben, transzcendens mivoltát Lindemann 1882-ben . Megoldatlan probléma, hogy a π decimális jegyeinek eloszlása egyenletes-e. Még azt sem tudjuk, hogy például az 1 jegy végtelen sokszor fordul-e elő benne.

[1] Mayer Gyula fordítása

Ajánlott irodalom: Cormen, Leiserson, Rivest, Stein [4], Dringó és Kátai [6], Freud, Gyarmati [8], Fuchs [11], Iványi [19], Kalmár [21], Láng [23], Megyesi [27], Niven és Zuckerman [29], Sárközy [35], Sierpiński [37], Szalay [38], valamint Vinogradov [43].

Irodalomjegyzék

[1] Aho, A.V., Hopcroft, J.E., Ullman, J.D., *Számítógép-algoritmusok tervezése és analízise.* Műszaki Könyvkiadó, Budapest, 1982.

[2] Bálintné, Sz.M., Czédli G., Szendrei, Á., *Absztrakt algebrai feladatok.* Tankönyvkiadó, Budapest, 1988.

[3] Birkhoff, G., Bartee, T.C., *A modern algebra a számítógéptudományban.* Műszaki Könyvkiadó, Budapest, 1974.

[4] Cormen, T.H., Leiserson, C.E., Rivest, R.L., Stein, C., *Új algoritmusok.* Scolar Kiadó, 2003.

[5] Demetrovics, J., Denev, J., Pavlov, R., *A számítástudomány matematikai alapjai.* Tankönyvkiadó, Budapest, 1989.

[6] Dringó, L., Kátai, I., *Bevezetés a matematikába.* Egyetemi jegyzet (ELTE), Tankönyvkiadó, Budapest, 1996.

[7] Euklidész, *Elemek, Szabó Árpád előszavával.* Gondolat Kiadó, Budapest, 1983.

[8] Freud, R., Gyarmati, E., *Számelmélet.* Tankönyvkiadó, Budapest, 2000.

[9] Fried, E., *Klasszikus és lineáris algebra.* Tankönyvkiadó, Budapest, 1977.

[10] Fried, E., *Általános algebra.* Tankönyvkiadó, Budapest, 1981.

[11] Fuchs L., *Bevezetés az algebrába és a számelméletbe. Kézirat.* Tankönyvkiadó, Budapest, 1977.

[12] Fuchs, L., *Algebra.* Egyetemi jegyzet (ELTE), Tankönyvkiadó, Budapest, 1970.

[13] von zur Gathen, J., Gerhard, J., *Modern computer algebra.* Cambridge University Press, 1999.

[14] Gavrilov, G.P., Szapozsenko, A.A., *Diszkrét matematikai feladatgyűjtemény.* Műszaki Könyvkiadó, Budapest, 1981.

[15] Graham, R.L., Knuth, D.E., Patashnik, O., *Konkrét matematika.* Műszaki Könyvkiadó, Budapest, 1998.

[16] Hajnal, A., Hamburger, P., *Halmazelmélet.* Tankönyvkiadó, Budapest, 1983.

[17] Hajnal, P., *Elemi kombinatorikai feladatok.* Polygon Kiadó, Szeged, 1997.

[18] Halmos, P.R., *Elemi halmazelmélet.* Siegler, L., E., *Halmazelméleti feladatok.* Műszaki Könyvkiadó, Budapest, 1981.

[19] Iványi, A., (ed.) *Informatikai Algoritmusok I.–II.* Eötvös Kiadó (ELTE), Budapest, 2004, 2005.

[20] Járai, A., (ed.) *Bevezetés a matematikába.* Eötvös Kiadó (ELTE), Budapest, 2005.

[21] Kalmár, L., *A matematika alapjai, I./I., I./II., II./I., II./II. Kézirat.* Tankönyvkiadó, Budapest, 1978, 1969, 1969, 1971.

[22] Knuth, D.E., *The art of computer programming. Vol. 1, 2, 3. Third edition.* Addison Wesley, 1998.

[23] Láng, Cs., *Bevezető fejezetek a matematikába. I.–II.* Egyetemi jegyzet (ELTE), Budapest, 2000.

[24] Láng, Cs., *Komplex számok – Példák és feladatok.* Egyetemi jegyzet (ELTE), Eötvös Kiadó, 2003.

[25] Láng, Cs., *Számelmélet – Példák és feladatok.* Egyetemi jegyzet (ELTE), Eötvös Kiadó, 2005.

[26] Lavrov, I.A., Makszimova, L.L., *Halmazelméleti, matematikai logikai és algoritmuselméleti feladatok.* Műszaki Könyvkiadó, 1987.

[27] Megyesi, L., *Bevezetés a számelméletbe.* Polygon Kiadó, Szeged, 1997.

[28] Mendelson, E., *Introduction to mathematical logic.* D. van Nostrand Company Inc., Princeton, New Jersey, 1964.

[29] Niven, I., Zuckerman, H.S., *Bevezetés a számelméletbe.* Műszaki Könyvkiadó, 1978.

[30] Pásztorné, V.K., *A matematikai logika és alkalmazásai.* Egyetemi jegyzet (ELTE), Tankönyvkiadó, Budapest, 1991.

[31] Penrose, R., *A császár új elméje. Számítógépek, gondolkodás és a fizika törvényei.* Akadémiai Kiadó, Budapest, 1993.

[32] Quine, W.V.O., *A logika módszerei*, Akadémiai Kiadó, Budapest, 1968.

[33] Rudin, W., *A matematikai analízis alapjai.* Műszaki Könyvkiadó, Budapest, 1978.

[34] Sain, M., *Nincs királyi út! – Matematikatörténet.* Gondolat kiadó, Budapest, 1986.

[35] Sárközy, A., *Számelmélet és alkalmazásai.* Műszaki Könyvkiadó, Budapest, 1978.

[36] Sárközy, A., Surányi, J., *Számelmélet – feladatgyűjtemény. Kézirat.* Tankönyvkiadó, Budapest, 1964.

[37] Sierpiński, W., *200 feladat az elemi számelmélet köréből.* Tankönyvkiadó, Budapest, 1964.

[38] Szalay, M., *Számelmélet.* Tankönyvkiadó, 1998.

[39] Szendrei, Á., *Diszkrét matematika; logika, algebra, kombinatorika.* Polygon Kiadó, Szeged, 2000.

[40] Totik, V., *Halmazelméleti feladatok és tételek.* Polygon Kiadó, Szeged, 1997.

[41] Tremblay, J., Mahonar, R., *Discrete Mathematical Structures with Applications to Computer Science.* McGraw-Hill Inc., New York, 1975.

[42] Vilenkin, N.J., *Kombinatorika.* Műszaki Könyvkiadó, Budapest, 1971.

[43] Vinogradov, I.M., *A számelmélet alapjai.* Tankönyvkiadó, Budapest, 1968.

Tárgymutató