

Az informatika matematikai alapjai

Kovács Attila

2015

Tartalomjegyzék

I. Alapok

1.	A matematikai logika alapjai	3
1.1.	Az ítéletlogika	3
1.1.1.	Kijelentések és igazságértékük	3
1.1.2.	Kijelentések összekapcsolása, kijelentéslogikai formulák	4
1.1.3.	Az ítéletlogika tételei, következtetési szabályok	6
1.2.	Az elsőrendű logika	9
1.2.1.	Predikátumok, kvantorok	9
1.2.2.	Az elsőrendű logika tételei	11
1.3.	Axiómák és a bizonyítások formái	13
2.	Halmazok, relációk, függvények	17
2.1.	Naiv halmazelmélet	17
2.1.1.	Bevezető fogalmak	17
2.1.2.	Részszíntér és hatványhalmaz	18
2.1.3.	Halmazműveletek	19
2.2.	Relációk	22
2.2.1.	Descartes-féle direkt szorzat	22
2.2.2.	Binér relációk	23
2.2.3.	Homogén binér relációk tulajdonságai	25
2.2.4.	Ekvivalenciareláció, hányadoshalmaz	26
2.3.	Függvények	29
2.3.1.	A függvény definíciója	29
2.3.2.	Függvények típusai, leszűkítés, kiterjesztés, indexelés	31
2.3.3.	Logikai függvények	33
2.3.4.	Függvények kompozíciója, inverze, műveletei halmazokkal	34
2.4.	Axiomatikus halmazelmélet	36
3.	Struktúrák	41
3.1.	Rendezési struktúrák	41
3.1.1.	Részbenrendezés	41
3.1.2.	Teljes rendezés, jólrendezés	44
3.2.	Algebrai struktúrák	47
3.2.1.	Belső művelet	47
3.2.2.	Külső művelet	52

Tartalomjegyzék

3.3.	Többszörös és származtatott struktúrák	53
3.3.1.	Rendezett integritási tartomány	53
3.3.2.	Lexikografikus rendezés	54
3.3.3.	Kapcsolat struktúrák között	54
3.4.	Speciális struktúrák	55
3.4.1.	Polinomok	55
3.4.2.	Mátrixok	56
4.	A számfogalom felépítése	61
4.1.	Természetes számok	61
4.1.1.	A Peano-axiómák	61
4.1.2.	Műveletek természetes számokkal	64
4.2.	Egész számok	71
4.2.1.	Konstrukció	71
4.2.2.	Műveletek, rendezésük	72
4.3.	Racionális számok	74
4.3.1.	Konstrukció	74
4.3.2.	Műveletek, rendezésük	74
4.4.	Valós számok	76
4.4.1.	Konstrukció	76
4.4.2.	Műveletek, rendezésük	77
4.5.	Komplex számok	86
4.5.1.	Konstrukció	86
4.5.2.	Szemléltetésük és műveleteik	87
4.5.3.	Komplex számok gyökei	90
4.5.4.	\mathbb{C} algebrai zártsgája és rendezési struktúrája	93
4.5.5.	Miért is lesz $i^2 = -1$?	94
4.6.	Algebrai és transzcendens számok	97
4.7.	Kvaterniák	98
4.7.1.	Konstrukció, tulajdonságok	98
4.7.2.	A kvaterniák és a háromdimenziós euklideszi tér	100
4.8.	Oktávok (Cayley-számok)	104
4.8.1.	Konstrukció, tulajdonságok	104
5.	Kombinatorika	109
5.1.	Véges halmazok	109
5.2.	Permutáció, variáció, kombináció	110
5.2.1.	Az ismétlés nélküli esetek	110
5.2.2.	Az ismétléses esetek	112
5.3.	Kapcsolat a klasszikus valószínűsséggel	116
5.3.1.	Eseményalgebra	116
5.3.2.	A valószínűség	120
5.3.3.	A születésnap-paradoxon	122
5.4.	Binomiális és polinomiális téTEL	125

5.5.	A skatulya-elv	127
5.6.	A logikai szita formula	128
5.7.	Speciális sorozatok	129
5.7.1.	Fibonacci	130
5.7.2.	Puskás, avagy a szubfaktoriális	132
5.7.3.	Pascal és a binomiális együtthatók	134
5.7.4.	Catalan	136
5.7.5.	Stirling és Bell	138
6.	Halmazok számosága	145
6.1.	Számosság	145
6.2.	Végtelen halmazok	145
6.3.	Megszámlálható és nem megszámlálható halmazok	147
6.4.	Bizonyítási módszerek jórendezett halmazokon	151
7.	Elemi számelmélet	155
7.1.	Alapvető fogalmak	155
7.1.1.	Oszthatóság	155
7.1.2.	Prímek, felbonthatatlanok	157
7.1.3.	Legnagyobb közös osztó, legkisebb közös többszörös	157
7.2.	Aritmetika \mathbb{Z}-ben	159
7.2.1.	Számrendszerök	159
7.2.2.	Euklideszi algoritmus	165
7.2.3.	A számelmélet alaptétele	170
7.2.4.	A prímszámok problémaköre	175
7.2.5.	Pithagoraszi számhármasok	178
7.3.	Kongruenciák	179
7.3.1.	Műveletek maradékosztályokkal	184
7.3.2.	Lineáris kongruenciák	185
7.3.3.	Szimultán kongruenciák	187
7.4.	Számelméleti függvények	192
7.5.	Racionális és valós számok ábrázolása	195
7.5.1.	q -adikus törtek	195
7.5.2.	Intervallum-aritmetika	197
7.5.3.	Lánctörtek	199
Névmutató		209

Előszó

Az informatika¹ az információ rögzítésével, kezelésével, rendszerezésével, és továbbításával foglalkozik. Az informatika a matematika, az információtudomány és számos mérnöki tudomány elegye. Ez a kézikönyv az informatika matematikai alapjairól szól.

A matematika olyan tudomány, amely részben más tudományok által vizsgált, részben pedig a matematika önálló fejlődéséből, differenciálódásából adódóan létrejött (felfedezett vagy feltalált) rendszereket, struktúrákat, azok absztrakt, közösen meglévő tulajdonságait vizsgálja. A matematika szó a görög nyelvből származik, a *μαθημα* (máthema) szó jelentése „tudomány, tudás”, a *μαθηματικωσ* (máthemátirosz) pedig azt jelenti, „tudásra vágyik”. A matematika gyakran olyan fogalmakkal és módszerekkel dolgozik, amelyek a minden nap életben és más tudományokban csak áttekelesen fordulnak elő. Úgy is mondhatjuk, hogy a matematika egy tömör, a köznyelv kétértelműségeitől mentes szimbólumrendszer. Ebben a könyvben egyrészt bemutatjuk ezt a nyelvezetet, másrészt a nyelv segítségével rávilágítunk a matematikai gondolkodás tiszta-ságára, szépségére, egyszóval mindenre, ami a modern számítástudományhoz és informatikához nélkülözhetetlen.

Az időszámításunk előtt 2000 körüli babiloni ékírásos szövegek azt mutatják, hogy elődeink már akkortájt meg tudtak oldani bizonyos matematikai problémákat: másodfokú egyenleteket, nemcsak egy, hanem két ismeretlennel, sőt, előfordultak harmad- és negyedfokú egyenletekre vezető feladatok is. Az ékírásnak köszönhetően Mezopotámia matematikájában határozottan jelentkezett valamiféle egységes jelölésrendszer és gondolkodásmód.

Az egyiptomi Rhind-papiruszon (Kr.e. 1750 táján) is felfedezhetők a gyakorlatból eredő matematikai ismeretek nyomai: olyan feladatokra adtak megoldást, amelyek elsőfokú és tiszta másodfokú egyenletekre vezetnek. Kínában ekkortájt már ismerték az efféle egyenletek megoldási módját, s erre a korra nyúlik vissza az irracionális és a negatív számok megismérése is.

A görög civilizáció felemelkedésével a matematika hatalmas léptékű fejlődésén ment keresztül anélkül, hogy a gyakorlati alkalmazásoktól elfordult volna. PITHAGORASZ számelméleti és THALÉSZ geometriai felfedezései után (Kr.e. VI. század) ARKHIMÉDÉSZ minden reneszánsz előtti európai matematikus kreativitását felülmúltva. A folyamat végül EUKLIDÉSZ híres tankönyvéhez, az *Elemekhez* vezetett. A korszak (vagy annak vége) fontos és híres, megoldhatatlannak bizonyult problémái a kockakettőzés és a kör-négyszögesítés, de lényeges eredmény még a kúpszeletek felfedezése is. DIOPHANTOSZ (kb. Kr.e. 250) volt az első görög matematikus, aki szisztematikusan vizsgálta az első- és másodfokú egyenleteket, az egyenletrendezés alapvető törvényeit. Olyan feladványokat kedvelt, amelyek megoldása egész szám, tiszteletére az ilyeneket mindmáig diofantikus problémáknak nevezzük.

A matematika ezen tündöklőként számon tartott korszaka azzal ért véget, hogy a római civilizáció rátelepedett a görögök, és megszerezte az akkori művelt világ feletti

¹A kifejezés legközelebbi angol megfelelője az *information technology*, IT

Előszó

uralmat. A matematika szempontjából a mediterrán római és az azt követő kontinentális korai kereszteny civilizációt (kb. a reneszánsz idejéig) a stagnálás, vagy még inkább a hanyatlás korszakának szokás tekinteni. Az éra leglényegesebb momentumaként megkezdődött a negatív számok felfedezése és alkalmazása, illetve a római helyett az arab számírás sok vitát kiváltó bevezetése.

Kelet felé tekintve a helyzet kevésbé volt szélsőséges: az arab, indiai és kínai matematika ebben az időben is virágzott, noha új felfedezések tekintetében egyik sem mérhető a görögökéhez. Az arabokat a geometrizáló görögökkel ellentétben inkább az algebra érdekelte, e tudományt magas szinten művelték. A hindu matematikát az arabok ismertették meg Európával. Az arab vagy iszlám korszak legnagyobb matematikusa AL-HVARIZMI (820 körül) egyik művében („Hisab al-dzsabr walmuquabala”, magyarul: „A rövidítés és törlés tudománya”) az első- és másodfokú egyenletek diszkussziójával foglalkozik. E műve latin fordításban vált ismertté, és a címben szereplő „al-dzsabr” szó latinos alakja, az algebra lett a szóban forgó matematikai tudományág neve. Az arab matematika hatása rányomta békelyegét a középkori Európa matematikájára is. A XII-XIII. században FIBONACCI már elérte az arabok színvonalát, sőt, felül is múulta azzal, hogy bizonyos harmadfokú egyenlet gyökeiről még az egyenlet megoldása előtt kimutatta, hogy sem racionális, sem speciális alakú irracionális számok nem lehetnek.

Az európaiak igazán önálló új eredményeket csak a reneszánsz idején értek el ismét. A középkori titokzatosság hatása kezdetben még érezhető volt, de hamarosan új felfedezések születtek. Jellemző példa a harmadfokú egyenlet megoldásának felfedezése a XVI. század első felében (FERRO, TARTAGLIA, CARDANO), majd az általános negyedfokú egyenlet harmadfokúra való visszavezetése (FERRARI). A korszakban az ókori eredmények egy részét és általában az egész ókori kultúrát újra felfedezték. Az európai matematika virágzásnak indult, a legfontosabb és legismertebb tudósok — FERMAT, DESCARTES, PASCAL, LEIBNIZ, NEWTON, EULER, GAUSS, ABEL, GALOIS és mások — közreműködése által egészen a legújabb korig. A tizenkilencedik században óriási áttörést jelentett CANTOR halmazelmélete, amely alapjaiban változtatta meg a matematika arculatát.

A huszadik században több évezredes, évszázados probléma oldódott meg: nemcsak az ókori kockakettőzés, körnégyyszögesítés, és szögharmadolás, de például a Fermat-sejtés kérdése, vagy a valószínűség fogalmának matematikai megalapozása is. A huszadik századi matematika legfontosabb felfedezésének mégis a számítástechnika elméleti alapjainak kialakulását tarthatjuk, amiben kulcsszerepe volt a magyar származású NEUMANN JÁNOSNAK. Az informatika egy új civilizációtípus, az információs társadalom kialakulásának alapjait vetette meg.

Köszönetnyilvánítás

Mindenekelőtt szeretnék köszönetet mondani a családom tagjainak, amiért beletörődtek a hétvégeken elvesztegett időbe, amelyet együtt tölthettünk volna, miközben a könyvon dolgoztam.

Köszönnett tartozom mindenkinél, akik lehetővé tették számomra, hogy ez a munka megszülethessen.

Nagy köszönet illeti az ELTE Komputeralgebra Tanszék azon mukatársait, akik bátorítottak a könyv megírására, hatással voltak gondolataimra, ők a következők: Burcsi Péter, Czirbusz Sándor, Járai Antal, Méri László, Nagy Gábor, Tihanyi Norbert, Vatai Emil.

Hálás köszönet illeti hallgatóimat, akik észrevételeikkel, javaslataikkal érdemben hozzájárultak a könyvben lévő gondolatok könnyebb megértését célzó javításokhoz, nagyban javítva ezzel a könyv minőségét, ők: Bán Róbert, Donkó István, Jaksov Anton, ...

Külön köszönet illeti a könyv megjelenését támogató XXX-t, támogatásuk nélkül ez a kiadás nem születhetett volna meg.

Végül, de nem utolsósorban köszönet illeti a szakmai lektor kiváló munkáját.

Információk

Ha az Olvasó a könyvben hibákat talál, egy-egy részlet tisztázására javaslatai vannak, szívesen várom az ötleteket. A honlapomon szándékomban áll javításokkal, lehetséges helyreigazításokkal és új információkkal bővíteni a könyv tartalmát. Elérhetőség:
<http://compalg.inf.elte.hu/~attila>

Budapest, 2014. október 20.
Kovács Attila, alkotó szerkesztő

Jelölések

A görög abc:

Kisbetű	Nagybetű	Elnevezés
α	A	alfa
β	B	béta
γ	Γ	gamma
δ	Δ	delta
ϵ vagy ε	E	epszilon
ζ	Z	záta
η	H	éta
θ vagy ϑ	Θ	théta
ι	I	ióta
κ vagy \varkappa	K	kappa
λ	Λ	lambda
μ	M	mű
ν	N	nű
ξ	Ξ	kszí
o	O	omikron
π vagy ϖ	Π	pí
ρ vagy ϱ	P	ró
σ vagy ς	Σ	szigma
τ	T	tau
υ	Υ	üpszilon
ϕ vagy φ	Φ	phi vagy phí
χ	X	khí
ψ	Ψ	pszí
ω	Ω	omega

I.

Alapok

1. A matematikai logika alapjai

A matematikai logika a gondolkodás és következtetés formális szabályaival foglalkozik. A „formális” szó azt jelenti, hogy a vizsgálatok tárgya a gondolatok, kijelentések szerkezetének, igazságuk leírásának formalizmusa. A logikát és részeit a(z emberi) nyelv-vagy gondolkodás egyes jelenségei szemantikai leírásának is tekinthetjük. Másféle, gyakorlatorientált interpretációk is léteznek, például az ismertetendő ítéletlogika az áram-körök, speciális algebrai rendszerek, programnyelvek, vagy általában a formális nyelvek vizsgálatának is az alapja. A matematikai logikát a számítástudomány más területein is széleskörűen alkalmazzák, például szakértői rendszereknél, mesterséges intelligenciában. Mindemellett a logikus gondolkodás törvényszerűségeinek ismerete a minden nap életben is elengedhetetlen.

1.1. Az ítéletlogika

Először egy egyszerű logikát, az **ítéletlogikát** (*ítéletkalkulus, kijelentéskalkulus, nulladrendű logika*) mutatjuk be. Az ítéletlogika a formális logika azon ága, ami az egyértelműen IGAZ vagy HAMIS kijelentő mondatokkal, az ítéletekkel (vagy más szóhasználattal kijelentésekkel) foglalkozik. A cél a kijelentések között értelmezhető műveletek (logikai műveletek), illetve a különféle levezetések tanulmányozása.

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. A matematikában olyan kijelentések is léteznek, amelyek 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-sejtés). Jegyezzük meg, hogy jelek vagy betűk nem minden sorozata kijelentés:

A matematikai logika alapjai

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.

A_5 : Bárcsak ötösöm lenne a lottón!

A_6 : Miért szeretjük a gyerekeket?

Ellenőrző kérdés. A formális logikában kijelentések-e az alábbi mondatok: (i) A kettő több. (ii) Az autó gyors. (iii) Létezik páros prímszám.

1.1.2. Kijelentések összekapcsolása, kijelentéslogikai formulák

A kijelentések összekapcsolásával *kijelentéslogikai formulákat* kaphatunk. Az összekapcsolás jelölésére különleges szimbólumokat, *logikai összekötőjeleket* (*logikai műveleti jeleket*) 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 *implikációt*nak és *ekvivalenciának* nevezzük. Az ítéletlogikában 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 minden IGAZ, minden HAMIS állításhoz eljuthatunk, ha az A kijelentés HAMIS, akkor $A \Rightarrow B$ igazságértékét minden célszerű IGAZ-nak rögzíteni.

A matematikai logika alapfokon nem foglalkozik a kijelentések tartalmával (intenzív), csak annak igazságértekkel (extenzió). Így az összekapcsolások igazságértéke is független attól, hogy a részkifejezések között tartalmilag van-e logikai összefüggés vagy nincs.

1.2. példa. Tekintsük az alábbi kijelentést:

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

Ekkor A_7 IGAZ kijelentés, mert a 7 páratlan szám.

Ellenőrző kérdés. A formális logikában igaz-e az alábbi kijelentés: Ha $1 = 2$, akkor én vagyok a római pápa.

A minden nap életben a „vagy” kétféle értelemben is előfordul.

1.3. példa. Tekintsük az alábbiakat:

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 (antivalencia, exclusive or, XOR), a két lehetőség közül valamelyik teljesülhet, de a kettő egyszerre nem.

AND	OR	NAND	NOR	NOT	XOR	XNOR
$A \wedge B$	$A \vee B$	$\neg(A \wedge B)$	$\neg(A \vee B)$	$\neg A$	$(\neg A \wedge B) \vee (A \wedge \neg B)$	$\neg(\neg A \wedge B) \vee (\neg A \wedge \neg B)$

1.1. táblázat. Logikai kapuk

A továbbiakban a „vagy” mindenkor a „megengedő vagy”-ot jelenti. Ennek felel meg a diszjunkció oszlopa az iménti 1.1. ábrában.

Ellenőrző feladat. Vizsgáljuk meg, hogy a „kizárt vagy” művelet megadható-e a negáció, a konjunkció és a diszjunkció segítségével. Mi lesz az $(A \vee B) \wedge \neg(A \wedge B)$, valamint a $(A \wedge \neg B) \vee (\neg A \wedge B)$ kifejezések logikai igazságítáblázata?

Jegyezzük meg, hogy a köznyelvben az „és”, „vagy” kötőszavakat nemcsak a konjunkció illetve diszjunkció értelemben használjuk.

1.4. példa. Tekintsük az alábbiakat:

- A_{10} : És mégis mozog a föld!
- A_{11} : Jancsi és Juliska testvérek.
- A_{12} : Móriczka vicceket mesél és hazament.
- A_{13} : Vagy huszonötözer szurkoló lehetett a mérkőzésen.

De vigyázat, a

- A_{14} : Jancsi és Juliska szeretik a mézeskalácsot.

már kijelentések konjunkciója, hiszen A_{14} jelentése: Jancsi szereti a mézeskalácsot és Juliska szereti a mézeskalácsot.

Ellenőrző feladat. Írjuk le formálisan az alábbi kijelentést: Jancsi vagy Juliska otthon van, de nincs otthon mind a kettő.

1.5. példa. A digitális áramkörök alapvető építőelemei a logikai kapuk. Egy kapu komplex áramköröket tartalmaz a lehető legnagyobb sebesség, kis fogyasztás és a nagy terhelhetőség érdekében. A kapuknak megfelelő kapcsolási szimbólumok az 1.1. táblázatban láthatók (IE-EE Std. 91:1984). Természetesen minden kapunak tápfeszültséget kell adni, ezt nem szokták feltüntetni a kapcsolási rajzon. A kapuk működése a bemenetek és kimenetek közötti igazságítáblázattal írható le.

A fizikai megvalósítás valamelyen tényleges feszültségtartományhoz fog logikai 1-ét és 0-t rendelni, ami alapján szabványos áramköri családok jöttek létre. Ezek a családok az áramkörök illesztése (a feszültségszintek), a gyártástechnológia, a fogyasztás és a különböző eltérő fejlesztési irányok következtében kaptak létjogosultságot. A legismertebb családok a TTL (Transistor-Transistor-Logic), a CMOS (Complementary Metal-Oxide-Semiconductor) és az ECL (Emitter-Coupled-Logic).

Az áramkörök tervezése szempontjából nagyon hasznos a kimenetek csoportba foglalása, mert így azok be- és kimenetként egyszerre több, párhuzamosan futó vezetéket is használhatnak. Ezeket *busznak* nevezzük. A vezetékek száma a buszvonal sávszélességét (4, 8, 16, 32, 64, stb.) adja meg. Egy buszon így egyszerre 4, 8, 16, 32, 64 bitból álló információ vihető át. Ennek a mérete a *gépi szó*. Általában pusztán csak igazságítáblák felhasználásával nem valósítható meg hatékony áramköri rendszer. Gyakran szükséges még valamilyen optimalizációs eljárás használata, ami minimalizálja a felhasznált kapuk számát, egyszerűsít egy adott bonyolult logikai kifejezést. Ilyen például a kifejtési módszer, a Karnaugh-tábla, a Quine-McCluskey-algoritmus. Nagyobb változószám esetére pedig heurisztikus algoritmusok léteznek.

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.

1.1.3. Az ítéletlogika tételei, következtetési szabályok

Valamely kijelentéslogikai formulát **kielégíthetőnek** nevezünk, ha alkalmas behelyettesítéssel (*interpretáció*) igazságérteke IGAZ lesz. Nagyon fontosak az **általános érvényű kijelentéslogikai formulák**, amelyek minden behelyettesítés esetén igazak. Ezeket az **ítéletlogika tételeinek** vagy **tautológiáknak** nevezzük. Az alábbiakban felsoroljuk az ítéletlogika fontosabb tételeit. Az írásmódot a zárójelek elhagyásával egyszerűsítettük annak figyelembevételével, hogy a $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$ logikai összekötőjelek közül a sorrendben előbbi erősebbet kapcsol, mint az utána következő. Úgy is mondjuk, hogy a sorrendben előbbinek nagyobb a **precedenciája**.

1.1.1. állítás. Az ítéletlogika fontosabb tételei.

- (1) $A \vee B \Leftrightarrow B \vee A, A \wedge B \Leftrightarrow B \wedge A$ (kommutativitás)
- (2) $A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C, A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$ (asszociativitás)
- (3) $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$ (a disztributivitás egyik tétele)
- (4) $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$ (a disztributivitás másik tétele)
- (5) $A \wedge (A \vee B) \Leftrightarrow A, A \vee (A \wedge B) \Leftrightarrow A$ (elnyelés, abszorbció)
- (6) $A \vee A \Leftrightarrow A, A \wedge A \Leftrightarrow A$ (idempotencia)
- (7) $A \vee \neg A$ (a harmadik kizárásnak tétele)
- (8) $\neg(A \wedge \neg A)$ (az ellentmondás tétele)
- (9) $\neg(\neg A) \Leftrightarrow A$ (a kettős tagadás tétele)
- (10) $A \vee \text{IGAZ} \Leftrightarrow \text{IGAZ}$
- (11) $A \wedge \text{IGAZ} \Leftrightarrow A$
- (12) $A \vee \text{HAMIS} \Leftrightarrow A$
- (13) $A \wedge \text{HAMIS} \Leftrightarrow \text{HAMIS}$
- (14) $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$ (DE MORGAN egyik tétele)
- (15) $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$ (DE MORGAN másik tétele)
- (16) $A \Rightarrow B \Leftrightarrow \neg B \Rightarrow \neg A$ (a kontrapozíció tétele)
- (17) $(A \Rightarrow B) \wedge A \Rightarrow B$
- (18) $(A \Rightarrow B) \wedge \neg B \Rightarrow \neg A$
- (19) $(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$ (szillogizmus)
- (20) $((A \Rightarrow B) \wedge (B \Rightarrow A)) \Leftrightarrow (A \Leftrightarrow B)$

A felsorolt tételek érvényességei az 1.1. logikai igazságtáblázat segítségével ellenőrizhetők. □

A kontrapozíció esetét az 1.2. ábra mutatja.

Ha egy kijelentéslogikai formula bármely behelyettesítés esetén HAMIS, akkor azt **ellentmondásnak** vagy **abszurditásnak** nevezzük. Két formula **logikailag ekvivalens**, ha logikai értékük minden interpretációjuknál megegyezik.

Ellenőrző kérdés. Igaz-e, hogy $A \wedge \neg A$ ellentmondás?

Ellenőrző feladat. Döntsük el, hogy az alábbi kijelentések az ítéletlogika tételei-e:

- (1) $A \Rightarrow B \Leftrightarrow \neg A \vee B$,
- (2) $(A \Rightarrow B) \vee (B \Rightarrow A)$.

1.6. példa. Igazoljuk az alábbi ekvivalenciát: $((\neg A \vee \neg B) \Rightarrow ((A \vee \neg B) \wedge B)) \Leftrightarrow A \wedge B$.

$$\begin{aligned} (\neg A \vee \neg B) \Rightarrow ((A \vee \neg B) \wedge B) &\Leftrightarrow \text{az iménti ellenőrző feladat első pontja miatt} \\ \neg(\neg A \vee \neg B) \vee ((A \vee \neg B) \wedge B) &\Leftrightarrow \text{a De Morgan szabály miatt} \\ (A \wedge B) \vee ((A \vee \neg B) \wedge B) &\Leftrightarrow \text{a disztributivitás miatt} \\ (A \wedge B) \vee ((A \wedge B) \vee (\neg B \wedge B)) &\Leftrightarrow \text{az alaptulajdonságok miatt} \\ (A \wedge B) \vee (A \wedge B) &\Leftrightarrow (A \wedge B). \end{aligned}$$

Az ítéletlogika tételeiből **következtetési szabályok** adódnak, amelyek segítségével IGAZ kijelentésekből újabb IGAZ kijelentéseket kaphatunk. A logika alapfeladata, hogy olyan formai kritériumokat tárjon fel, amelyek szerint egy adott IGAZ, vagy IGAZ-nak feltételezett p_1, p_2, \dots, p_n állítások (azaz a premisszák, előfeltételek) esetén helyesen következtethetünk egy q kijelentés (konklúzió, következmény) igazságára. Szimbolikusan a következtetés

$$\frac{p_1, p_2, \dots, p_n}{q}$$

alakú, amit az alábbi módon olvashatunk: „Tudjuk, hogy p_1, p_2, \dots, p_n fennáll. Ekkor q is teljesül”. Gyakran használjuk a

$$\{p_1, p_2, \dots, p_n\} \vdash q$$

jelölést is. Az ítéletlogika (17)–(19) tételeiből a következtetés alábbi szabályai származtathatók:

- $\{(A \Rightarrow B), A\} \vdash B$ (*modus ponens* vagy *leválasztási szabály*).
- $\{(A \Rightarrow B), \neg B\} \vdash \neg A$ (*modus tollens* vagy *indirekt következtetés*).
- $\{(A \Rightarrow B), (B \Rightarrow C)\} \vdash (A \Rightarrow C)$ (*modus barbara* vagy *lánckövetkeztetés szabálya*).

Igaz továbbá az alábbi szabály:

- $\{(A \Rightarrow B), (A \Rightarrow \neg B)\} \vdash \neg A$ (*reductio ad absurdum* vagy *lehetetlenre történő visszavezetés*)

Meg lehet tehát adni kijelentéslogikai formulák és következtetési szabályok egy rendszerét, amellyel az ítéletlogika újabb tételeihez juthatunk. Ezt az eljárást **levezetésnek** nevezzük.

1.7. példa. Tegyük fel, hogy az alábbi állítások IGAZAK.

p_1 : Ha János jól sakközök, akkor jól érti a mateket vagy számítástechnikai zseni.

p_2 : János nem érti a mateket.

p_3 : János a sakk, a matek és a számítástechnika közül legalább az egyikhez jól ért.

Igaz-e, hogy

q : János számítástechnikai zseni?

Vizsgáljuk meg az alábbi kijelentést:

p_4 : János jól sakközök.

Amennyiben p_4 teljesül, akkor p_1 és p_2 miatt János számítástechnikai zseni, $\{p_1, p_2, p_4\} \vdash q$. Ha pedig p_4 nem teljesül, akkor p_2 és p_3 miatt lesz János számítástechnikához értő, $\{p_2, p_3, \neg p_4\} \vdash q$. Összességében tehát $\{p_1, p_2, p_3, p_4\} \vdash q$ és $\{p_1, p_2, p_3, \neg p_4\} \vdash q$, ezért $\{p_1, p_2, p_3\} \vdash q$.

Az iménti levezetést az alábbi módon is megfogalmazhatjuk: Amennyiben János jól sakközök, p_1 és p_2 miatt János számítástechnikai zseni, amennyiben pedig János nem jól sakközök, p_2 és p_3 miatt lesz számítástechnikához értő.

A továbbiakban levezetéseinket az egyszerűség kedvéért mindig ezen utóbbi módon fogalmazzuk meg.

Gyakorlatok

1.1-1. Igazoljuk, hogy az alábbi kijelentéslogikai formulák kielégíthetőek:

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

1.1-2. Bizonyítsuk be, hogy az alábbi kijelentéslogikai formulák az ítéletlogika tételei:

- a) $(A \wedge B) \Rightarrow A$
- b) $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$
- c) $((A \wedge B) \Rightarrow C) \Leftrightarrow (A \Rightarrow (B \Rightarrow C))$
- d) $A \Rightarrow (B \Rightarrow C) \Leftrightarrow B \Rightarrow (A \Rightarrow C)$.

1.1-3. Állapítsuk meg, hogy logikailag igaz-e az alábbi következtetés:

Ha hideg van, akkor bekapcsolom a fűtést és nem megyek ki a szobából. Nem kapcsolom be a fűtést vagy nem fázom. Ha nem vacsorázom vagy nem alszik ki a villany, akkor bennmaradok a szobában vagy nem fázom. Ha bekapcsolom a fűtést, akkor hideg van és vacsorázom. Tehát ha bekapcsolom a fűtést, akkor kialszik a villany.

1.1-4. A király szabadulni akar miniszterelnökétől. Két cédulát tesz egy kalapba, és magához hívja őt: Az egyik cédrulán az áll, hogy „Menjen”, a másikon, hogy „Maradjon”. Amelyiket húzza, az lesz a sorsa. A miniszterelnök meg van győződve arról, hogy minden cédrulán a „Menjen” áll. Hogy sikerül mégis maradnia?

1.1-5. A kalózok szigetén a kincskeresők 3 látót ástak ki a homokból. A sorszámozott látákon az alábbi feliratok voltak:

1. : Ebben a látában van a kincs.
2. : Ebben a látában nincs kincs.
3. : A második látá felirata IGAZ.

A kincskeresők tudják, hogy a kalózok pontosan egy látába rejtték a kincset, továbbá a másik két látában mérgeskígyók tanyáznak. Hol lehet a kincs, ha

- (a) minden látában felirata IGAZ?
- (b) pontosan egy felirat HAMIS?
- (c) legalább két felirat HAMIS?

1.1-6. Indokoljuk meg a levelezés számozott lépésein (a, b valós számok).

$$|a + b|^2 = (a + b)^2 \quad (1)$$

$$= a^2 + 2ab + b^2$$

$$\leq a^2 + 2|a||b| + b^2 \quad (2)$$

$$= |a|^2 + 2|a||b| + |b|^2 \quad (3)$$

$$= (|a| + |b|)^2$$

$$|a + b| \leq |a| + |b| \quad (4)$$

1.1-7. Egy tolvaj egy régiségboltból sikeresen elcsent egy régi érmét. A felirata szereint Kr. e. 42-ben verték. Nagyon megörült neki a tolvaj, és elkezdte számolgatni, mennyit kaphat érte a feketepiacon, ha minden Krisztus előtti év 10 000 forintot ér. Vajon mennyit kaphatott érte?

1.1-8. Egy kis faluban 100 házaspár lakik. Nagyon vallásos a község, és papnak minden megtesznek. A pap egy vasárnap kihirdeti, hogy a faluban vannak olyan feleségek, akik megcsalják a férjüket, és felszólítja a férjeket, hogy ezeket a feleségeket hozzák el a templomba vasárnapig, hogy meggyónhassák bűneiket. minden hűtlen feleséget csakis a

saját férje viheti el a templomba. minden férfi tudja a másik feleségéről, hogy az hűtlen-e, de a sajátjáról nem. Nem tudja senkitől megkérdezni, magának kell kitalálnia, hogy mi a helyzet. Csütörtök délután már négy feleség várt gyónásra a templomban, és a pap nagyon elégedett volt. Hogyan jöttek rá a férjek, hogy kit kell elvinni a templomba?

1.1-9. 9 darab formára teljesen azonos pénzérme közül kell kiválasztani azt az egyetlen, amelyik hamis, ennél fogva a többinél valamivel könnyebb. Egy kétkarú mérleg áll a rendelkezésünkre. Minimálisan hány mérésre van szükség? A választ és az érvelést írjuk le!

1.1-10. Igazmondó Mackóéknál áramszünet van. A család (Mackó papa, Mackó mama és Mackó Lackó) éppen megéhezett, szerencsére lent a pincében még maradt a téli félretett mézből 10 csuporral. Lement hát először Mackó papa, a sötét pincében kitapogatott néhány mézes bődönt, megtömte a hasát, majd visszament. Így tett Mackó mama és Mackó Lackó is. minden szokás szerint történt: jól nevelt mackó módjára, ha valamelyikük megkezdett egy csuprot, akkor azt az utolsó cseppig ki is ürítette, és mindenki jóllakottan tért vissza. Tudják még egymásról, hogy Mackó papa ette a legtöbb mézet, Mackó mama kevesebbet evett, mint Mackó papa, de többet, mint Mackó Lackó. Egyszer csak beállít a Mackó családhoz Mackó nagybácsi:

- Jaj, elfogyott a mézem, Mackó papa, nektek van még?
- Nem tudom - felelte Mackó papa. – Mackó mama, te talán tudod?
- Én sem tudom. És te, Mackó Lackó?
- Én sem tudom.
- De én már tudom – mosolygott Mackó papa.

Honnan tudta? És mi is tudjuk? Írjuk le a választ és az érvelést!



1.1. Programozási feladat. Írunk olyan programot, melynek bemenete egy ítéletlogikai kifejezés legfeljebb 10 változóval, és a program eldönti, hogy a formula kielégíthető, tautológia vagy ellentmondás.

1.2. Az elsőrendű logika

1.2.1. Predikátumok, kvantorok

A valóság leírásához annak részeit is meg kell tudni nevezni. A matematikai elméletekben általában olyan fogalmak, kijelentések is 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 helyettesítve (interpretáció) a predikátumok igazságértéke egyértelműen eldönthető. Egy adott logikai rendszer esetén a **logikai konstansok** rögzített jelentéssel (rögzített szemantikai értékkel) rendelkeznek, jelentésük (szemantikai értékük) minden értelmezésben megegyezik.

1.8. példa. Az egész számok világában legyen P a „páros szám” predikátum, vagyis $P(\alpha)$ pontosan akkor legyen IGAZ, ha α páros. Ekkor például $P(2)$ és $P(100)$ IGAZ, míg $P(1)$ és $P(121)$ HAMIS kijelentések.

A síkbeli objektumok világában jelentse $Q(x, y)$ azt, hogy „az x pont illeszkedik az y egyenesre”. Ekkor az x változó helyébe egy konkrét síkbeli pontot, az y változó helyébe egy konkrét síkbeli egyenest helyettesítve $Q(x, y)$ igazságértéke egyértelműen eldönthető. Ha az origó konstanst O jelenti, akkor $Q(O, y)$ jelentése az, hogy az y egyenes az origóra illeszkedik.

A matematikai logika alapjai

A számok világában jelentse $S(a, b, c)$ azt, hogy sorrendben az első és a második bemenet összege a harmadikkal egyenlő. Ekkor $S(3, 4, 7)$ és $S(\frac{1}{2}, \frac{1}{3}, \frac{5}{6})$ igazságértéke IGAZ, míg $S(1, 1, 1)$ igazságértéke HAMIS.

Az 1.8. példa arra is rávilágít, hogy a predikátumok változói közötti sorrendiség lényeges.

A matematikai problémák formalizálására az ítéletlogika még nem elég. A kijelentések további vizsgálatánál olyan kifejezésekbe ütközünk, mint a „minden” és „létezik”. Ez azt jelenti, hogy ha egyszer létrehoztunk egy objektumokat is tartalmazó logikát, gyakran az objektumok egész gyűjteményére vonatkozó tulajdonságokat is ki szeretnénk fejezni az objektumok felsorolása nélkül. Ezekre a kifejezésekre **kvantorokat** vezetünk be: a \exists („van olyan”, „létezik”) egzisztenciális kvantort és a \forall („ minden”) univerzális kvantort.

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

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

alakban írhatjuk.

1.10. példa. A természetes számok $(0, 1, 2, \dots)$ világában jelentse a $NVE(x, y)$ predikátum azt, hogy „ x nagyobb vagy egyenlő mint y ”. Mit jelentenek ekkor a

- (1) $\forall x \exists y NVE(x, y)$,
- (2) $\exists x \forall y NVE(x, y)$

Kijelentések természetes nyelven (magyarul)? Határozzuk meg igazságértéküket!

Az első kijelentés lehetséges megfogalmazásai:

- minden x természetes számhoz található (létezik olyan) y természetes szám, hogy x nagyobb vagy egyenlő az y számnál.
- minden természetes számnál van kisebb, vagy vele egyenlő.

A második kijelentés lehetséges megfogalmazásai:

- létezik olyan x természetes szám, hogy valamennyi (minden) y természetes szám esetén x nagyobb vagy egyenlő mint y .
- létezik olyan természetes szám, ami minden természetes számnál nagyobb vagy egyenlő vele.

Az első kijelentés IGAZ, hiszen az $y = 0$ választás megfelelő, a második állítás ellenben HAMIS, hiszen nem található olyan természetes szám, ami minden természetes számnál nagyobb vagy akár azzal egyenlő lenne.

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. Ha egy kijelentésformulának nincs szabad változója, akkor a formulát **zárt formulának**, egyébként **nyitott formulának** nevezzük.

Ellenőrző kérdés. Soroljuk fel a $\forall x \forall y \exists z (P(x, y) \wedge (Q(x)) \Rightarrow ((R(z) \vee S(w)))$ formula kötött és szabad változóit. A formula nyílt vagy zárt?

1.11. példa. Az emberek világában jelentse az $A(x, y)$ kétbemenetű predikátum azt, hogy „az x ember édesanya y ”. Ekkor az a kijelentés, hogy „ mindenkinek van édesanya” az alábbi módon formalizálható:

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

Ha hangsúlyozni akarjuk azt, hogy mindenkinél pontosan egy édesanya van, akkor ezt az \exists („egyértelműen létezik” vagy „pontosan egy létezik”) szokásos jelölés segítségével tehetjük meg:

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

Figyeljük meg, hogy a kvantifikálás mindenkorra változókra vonatkozik, ami a matematika széles területének leírásához elegendő. Az ilyen tulajdonsággal bíró logikát nevezzük **elsőrendű logikának**. Esetenként azonban felléphet a predikátumok kvantifikálásának szükségesége, amivel magasabb rendű logikákhoz juthatunk. Ezekkel mi nem foglalkozunk.

1.2.2. Az elsőrendű logika tételei

Az elsőrendű logika tételeihez hasonló módon juthatunk el, mint a ítéletlogikában.

1.2.1. állítás. Az elsőrendű logika fontosabb tételei.

- (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) $\exists x \forall y A(x, y) \Rightarrow \forall y \exists x A(x, y)$

A tételek helyességének átgondolását az Olvasóra bizzuk. □

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

1.12. példa. Az emberek világában 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 szószerezzel is kifejezhetők. A „minden”, „az összes”, „tetszőleges”, „bármely” szavak az univerzális kvantort jelzik, a „létezik”, „van olyan”, „található”, „néhány”, „valamely”, „alkalmas”, „bizonyos”, stb. szavak az egzisztenciális kvantorra utalnak.

Egy kijelentés általában többféleképpen is formalizálható, ilyenkor a logikai tételek segítségével ezek egymásba alakíthatók. Törekedjünk mindenkorra, hogy formalizáláskor először a kvantorok, majd a vonatkozó predikátumok szerepeljenek, ellenkező esetben a formula nehezen lesz olvasható.

1.13. 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) $\exists x \exists y \forall z ((S(z, x) \wedge E(z, y)) \Rightarrow G(z))$ vagy $\exists x \exists y (G(z) \vee \neg S(z, x) \vee \neg E(z, y))$.

A matematikai logika alapjai

Az elsőrendű logika alkalmazhatósága céljából általában még néhány kiegészítést szokás tenni. Ezek közül mi az *azonosság* jelölésére szolgáló „=” *egyenlőségjelet* említi jük (*elsőrendű logika az azonossággal*). Az azonosságot a logikai műveleti jelek közé lehet sorolni.

Jegyezzük meg, hogy nem lehet bármely kifejezésről véges számú lépésekben eldöntení, hogy a predikátumkalkulus egy tételeről van-e szó, vagy sem (Church *eldönthetetlenségi tétele*).

Gyakorlatok

1.2-1. Formalizáljuk az ítéletlogika nyelvén az alábbi kijelentéseket:

- a) Kolumbus 1492-ben felfedezte Amerikát.
- b) Nem Kolumbus fedezte fel 1492-ben Amerikát.
- c) Kolumbus nem 1492-ben fedezte fel Amerikát.
- d) Kolumbus 1492-ben nem Amerikát fedezte fel.

1.2-2. Formalizáljuk, majd tagadjuk az alábbi bölcsességeket:

- a) minden szentnek maga felé hajlik a keze.
- b) aki nem tud arabusul, ne beszéljen arabusul.
- c) nem mind barátod, aki rád mosolyog.
- d) nem zörög a haraszt, ha a szél nem fújja.
- e) egy fecske nem csinál nyarat.
- f) nem mind arany, ami fénylik.
- g) ki korán kel, aranyat lel.
- h) senki sem lehet próféta a saját hazájában.

1.2-3. Az emberek világában 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.

1.2-4. Az emberek világában jelölje a $\Gamma(x, y)$ predikátum azt, hogy „ x gyermeké 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.

1.2-5. Jelentese $F(x)$, $I(x)$ és $H(x, y)$ rendre a következőket: x fiatal, x idős, x barátkozik y -nal, míg az B konstans jelölje Bendegúzt. Formalizáljuk az alábbiakat:

- a) Bendegúz fiatal.
- b) Bendegúz nem barátkozik senkivel.
- c) Bendegúz barátkozik fiatalokkal.
- d) Bendegúz csak fiatalokkal barátkozik.
- e) Bendegúz fiatal, vagy van fiatal barátja.
- f) Az idősek nem barátznak Bendegúzzal.
- g) Bendegúz mindenivel barátkozik, aki fiatal.
- h) A fiatalok nem barátznak idősekkel.
- i) Nincs olyan idős, aki nem barátkozik fiatallal.
- j) Aki fiatal, nem barátkozik Bendegúzzal, aki öreg, azzal pedig Bendegúz nem barátkozik.

1.2-6. Formalizáljuk az alábbi kijelentéseket:

- Ki nem szolt, csak bégetett, az kapott dicséretet.
- Nem minden fajta szarka farka tarka, csak a tarka farkú szarka farka tarka.

1.3. Axiómák és a bizonyítások formái

Már az ókorban törekedtek a matematikai ismeretek deduktív módon való felépítésére, vagyis arra, hogy minden állítást **bizonyítani** kell. Bizonyításon egy állításnak más állításokból meghatározott logikai következtetési szabályokkal való vezetését értjük. Az egyes állítások igazolásánál csak már korábban bizonyított tételek szabad felhasználni. Ez az út elvezetett a legegyszerűbb elemi állításokhoz, az **axiómákhoz**, amelyek bizonyítása már nem lehetséges. Így végső soron minden bizonyítást axiómákra lehet visszavezetni. Az, hogy mit lehet egy axiómarendszerből vezetni, attól függ, hogy melyik logikai rendszer mellett döntünk, és milyen következtetési szabályokat engedünk meg.

Az axiomatikus gondolkodásmód megalapozása vitathatatlanul EUKLIDÉSZ ókori görög matematikus érdeme, akinek síkgeometriai felépítése évezredeken keresztül szolgált mintául. Az *Elemek* című művében megfogalmazott euklideszi axiómák ma is érvényesek. Mindössze 9 axiómából és 5 posztulátumból (ma ezeket is axiómáknak mondjuk) álló rendszere hosszú időn át jelentette a matematika legfontosabb építőkövét. Csak a XIX. században született meg az első nem-euklideszi geometria, a Bolyai–Lobacsevszkij-féle hiperbolikus geometria. Ez egyetlen euklideszi axióma megváltoztatásából, a párhuzamossági axióma tagadásából született, ami egyben az axiómarendszerek fontosságára is rávilágított.

1882-ben az olasz PEANO megfogalmazta a természetes számok axiómáit. A geometria ma használt axiómarendszerét 1899-ben HILBERT a „Grundlagen der Geometrie” (A geometria alapjai) című művében fogalmazta meg, általánosítva az euklideszi axiómarendszert. Ugyancsak HILBERT volt az, aki megválaszolta azt a kérdést, hogy mikor megfelelő egy axiómarendszer.

- Legyenek az egyes axiómák egymástól *függetlenek*, azaz egyiket se lehessen iga-zolni a másik segítségével.
- Legyen az axiómarendszer *ellentmondásmentes*, vagyis ne fordulhasson elő olyan állítás, ami az axiómák alapján igazolható és cáfolható is egyben.
- Legyen az axiómarendszer *teljes*, azaz az adott tudományág minden problémája vagy igazolható vagy, cáfolható lehessen.

1908-ban kialakult a halmaelmélet axiómarendszere, majd 1933-ban a valósínűségszá-mításé is. Az előbbi ZERMELO német és FRAENKEL izraeli matematikusok, az utóbbi az orosz KOLMOGOROV érdeme. 1931-ben GÖDEL cseh-osztrák matematikus megmutatta, hogy valamely ellentmondás nélküli axiómarendszer sohasem lehet teljes, azaz bármelyik axiómarendszeren belül megfogalmazható olyan állítás, amelyik nem bizonyítható, de nem is cáfolható (nemteljességi téTEL). Egy vélegesen megfogalmazott axiómarendszerben pedig az ellentmondásmentesség nem bizonyítható, tehát az adott axiómarendszer nem képes igazolni saját maga IGAZ voltát. Mindez azt jelenti, hogy nem lehet egy adott tudományág axiómarendszerét vélegesen megfogalmazni. Új kérdések esetleg újabb axiómákat kívának.

A matematikai tételek, állítások jelentős része $A \Rightarrow B$ típusú implikáció. Korábban említettük, hogy A a téTEL feltételeit jelöli, amelyeket *premisszáknak* nevezünk („az, amit

A matematikai logika alapjai

tudunk”), B pedig a tételek állítását jelöli, amelyet *konklúziónak* is mondunk („amit tudni szeretnénk”). Az ilyen típusú tételek bizonyításának legismertebb 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 $\sqrt{2}$ irrationális voltának bizonyítása.

Ha egy állítás $A \Rightarrow B$ alakú, akkor néha a $\neg B \Rightarrow \neg A$ kontrapozíciót bizonyítjuk. Fontos még, hogy egy állítás hamis voltának bizonyításához mindenleges 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 elégséges 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 megfogalmazott tulajdonságára épül. Ennek az eljárásnak az általánosítása a **transzfinnit indukció**.

Definición egy fogalom pontos leírását értjük, esetleg más fogalmak felhasználásával. Itt hasonló problémák adódnak, mint a bizonyításnál. Sok fogalmat nem explicit módon ($A := B$), hanem implicit módon, kölcsönös összefüggések alapján definiálunk (ahogy például a síkgeometriában az egyenest, a távolságot, a területet stb.). A későbbiekben hasznos lesz annak ismerete, hogy egy reláció vagy függvény minden, az elsőrendű logika eszközeivel leírt implicit definícióját explicit alakban is meg lehet adni (Beth tétele).

Lényegesen eltérő körülmények adódhatnak akkor, ha feladjuk a kétértékűség elvét, és kettőnél több igazságértéket is megengedünk. Példaként említhetők a szimbolikus programozási nyelvek (pl. MAPLE, MATHEMATICA) 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.

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, ami a rendszer keretein belül sem nem bizonyítható, sem nem cáfolható.

Említettük, hogy az első fennmaradt axiómarendszert EUKLIDÉSZ Elemek [7] című munkája tartalmazza. EUKLIDÉSZ arra törekedett, hogy minél kevesebb axiómát mondjon ki, és tételekért bizonyított minden, amit csak lehet. A későbbiekben látni fogjuk, hogy az axiómák kiválasztása meglehetősen önkényes, egy adott téma köröz több különböző axiómarendzszer is megalkotható. Egy axiómarendzszer „erőssége” lényegében az adja, hogy „mennyi minden” lehet bizonyítani belőle.

A logika a természeti nyelvben szereplő nem-klasszikus logikai viszonyokkal is foglalkozik. Például a változó kontextusú terminusok és kijelentések logikája (dinamikus logika), az időviszonyok logikája (temporális logika), a lehetséges és biztos állítások logikája (modális logika), vagy az elmosódott igazság-tartományú tulajdonságok logikája (fuzzy logika).

A logika különböző szintjei jelen vannak a számítástudományban, adatbázis-elméletben és a mesterséges intelligencia területén. A számítógéppel történő tételebzonyítás napjaink kiemelkedően fontos kutatási területe.

2. Halmazok, relációk, függvények

A *halmaz* fogalma a modern matematikában alapvető szerepet játszik. A halmazelmélet alapjait CANTOR fektette le, de az általa alkotott ún. *naiv 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. Naiv halmazelmélet

Az elsőrendű predikátumkalkulusnál bizonyos tulajdonságú objektumokra érvényes logikai formulákkal foglalkoztunk. A naiv halmazelmélet kiindulópontja az, hogy ha T valamelyen tulajdonság, akkor gondolhatunk minden dolgok összességére, melyekre a T tulajdonság teljesül. Ezt az összességet a T tulajdonság *igazságtartományának* nevezzük.

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 valamelyen 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, \dots betűket, a halmazokra az A, B, C, \dots 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. 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 az elválasztójel zavaró, akkor az $\{x \in H : T(x)\}$ is használatos. Ha a H halmaz nyilvánvaló, kiírása elhagyható.

2.1. példa. Példák halmazokra:

$$H_1 = \{2, 3, 5, 7\},$$

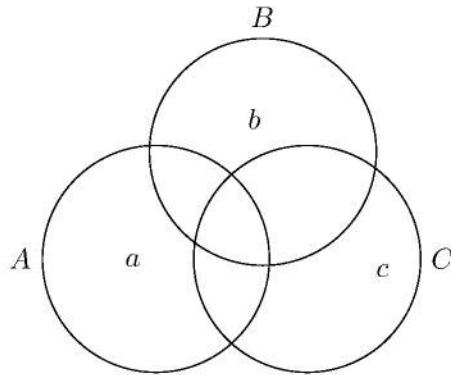
$$\mathbb{N} = \{0, 1, 2, \dots\},$$

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\},$$

$$H_2 = \{x \in \mathbb{N} \mid x^4 - 17x^3 + 101x^2 - 247x + 210 = 0\},$$

H_3 legyen a négy legkisebb pozitív prímból álló halmaz,

$$H_4 = \{x \in \mathbb{N} \mid x \text{ prím}\}.$$



2.1. ábra. Halmazok és elemeik Venn-diagramos szemléltetése.

Ekkor H_1, H_2, H_3 véges halmazok, és ahogy később bebizonyítjuk, H_4 végletes halmaz. Az \mathbb{N} -nel jelölt halmazt a **természetes számok halmazának** nevezzük. Ez a halmaz olyan lényeges szerepet játszik a matematikában, hogy axiomatikus felépítésére később visszatérünk. Addig \mathbb{N} -et mint a számlálás eszközét használjuk. Szokásosan, \mathbb{Z} az **egész számok halmazát** jelöli.

2.1.1. definíció. *Halmazokat akkor nevezünk egyenlőknek, ha ugyanazokból az elemekből állnak, vagyis*

$$A = B := \forall x (x \in A \Leftrightarrow x \in B).$$

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

2.1.2. definíció. *Azt a halmazt, amelynek nincs eleme, üres halmaznak nevezzük és \emptyset -zel 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 körül fogunk (Venn-diagram, 2.1. ábra). A Venn-diagrammal való ábrázolás csak vizuális szemléletet ad, állítások bizonyítására nem alkalmas.

2.1.2. Rész halmaz és hatvány halmaz

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

2.1.3. definíció. $A \subseteq B := \forall x (x \in A \Rightarrow x \in B)$.

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

2.1.4. definíció. $A \subset B := A \subseteq B \wedge A \neq B$.

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

2.2. példa. Fehívjuk a figyelmet az \in és \subset különbözésére. 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.

Ellenőrző kérdés. Igazak-e az alábbi állítások: $\emptyset \in \emptyset$, $\emptyset \subseteq \emptyset$?

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

2.1.5. definíció. $\wp(A) := \{x \mid x \subseteq A\}$.

Megjegyezzük, hogy a hatványhalmaz létezését axiómával kell biztosítani.

Ellenőrző feladat. Írjuk fel a $\wp(\wp(\wp(\emptyset)))$ halmazt.

A későbbiekben belátjuk, 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 kijelentés-kalkulus műveleteivel.

2.1.6. definíció. $A \setminus B := \{x \mid x \in A \wedge x \notin B\}$.

$A \setminus B$ -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 összefüggésekben világos, hogy mely H **alaphalmazról** (univerzum) van szó, akkor az \overline{A} jelölés használatos. Felhívjuk a figyelmet, hogy a komplementerképzésnél minden tisztában kell lennünk, hogy mely H halmazról is van szó.

Ellenőrző kérdés. Mi lesz $\overline{\emptyset}$?

A komplementerképzésnek a negációval való összefüggése nyilvánvaló:

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

A halmazok közötti legfontosabb művelet a metszet és az unió.

2.1.7. definíció. $A \cap B := \{x \mid x \in A \wedge x \in B\}$.

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

2.1.8. definíció. $A \cup B := \{x \mid x \in A \vee x \in B\}$.

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

Ellenőrző kérdés. Mi történne, ha az unió definíciójában a „kizáró vagy” műveletet alkalmaznánk? Szemléltessük Venn-diagramon!

2.1.9. állítás. 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) $A \cup A = A$. |

□

Bizonyítás. Az állítások a műveletek definícióiból következnek. ■

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. Példaképpen belátjuk az (5) disztributivitást. Az $(A \cap B) \cup C$ halmaznak x pontosan akkor eleme, ha $x \in A \cap B$ vagy $x \in C$. Első esetben $x \in A$ és $x \in B$, így $x \in A \cup C$ és $x \in B \cup C$ is teljesül, ezért $x \in (A \cup C) \cap (B \cup C)$. Második esetben, ha $x \in C$, akkor $x \in A \cup C$ és $x \in B \cup C$ is igaz, így ismét csak $x \in (A \cup C) \cap (B \cup C)$.

2.1.10. állítás. Az üres halmazra és a H alaphalmazra a következő tulajdonságok érvényesek:

$$\begin{aligned} A \cap \emptyset &= \emptyset & A \cup \emptyset &= A \\ A \cap H &= A & A \cup H &= H \\ A \cap \overline{A} &= \emptyset & A \cup \overline{A} &= H. \end{aligned}$$

Érvényesek továbbá a De Morgan-törvények:

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

Bizonyítás. Az állítások a műveletek definícióiból következnek. Például az első De Morgan szabály teljesülése az alábbi módon bizonyítható: amennyiben egy tetszőleges $x \in \overline{A \cap B}$, akkor $x \notin A \cap B$, vagyis $x \notin A$ vagy $x \notin B$ (esetleg mindkettő). Ez pedig azt jelenti, hogy $x \in \overline{A} \cup \overline{B}$. ■

A 2.2. ábrán néhány elemi halmazművelet Venn-diagrammos szemléltetése látható.

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 $A \cup B = \{a, c, e, f, g, h\}$, $A \cap B = \{e, g\}$, $A \setminus B = \{a, c\}$ és $\overline{A} = \{b, d, f, h\}$.

Ellenőrző feladat. Mutassuk meg, hogy $A \setminus B = A \cap \overline{B}$.

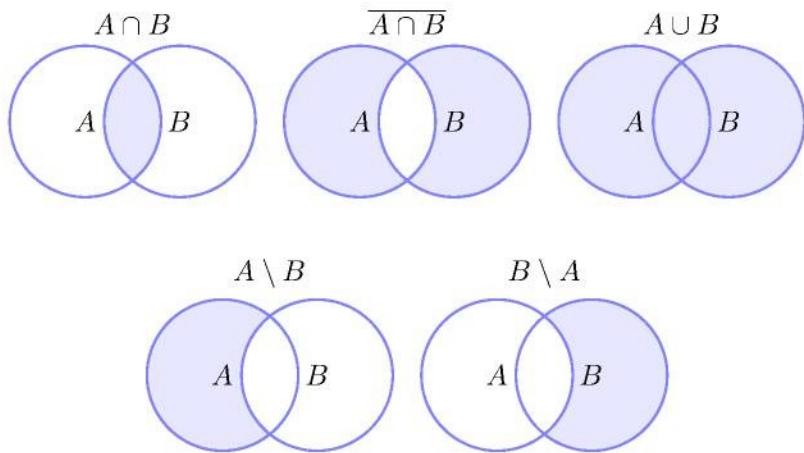
A metszetet és az uniót nem csak két halmazra lehet definiálni. A műveletek asszociativitása miatt a kettőnél több halmazból álló metszetet és uniót zárójelek nélkül írhatjuk, a kommutativitás miatt pedig a tagok sorrendje is lényegtelen.

2.1.1. megjegyzés. A továbbiakban a $\forall x(x \in A)$ és $\exists x(x \in A)$ jelöléseket egyszerűen $\forall x \in A$ és $\exists x \in A$ módon írjuk.

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

2.1.11. definíció. $\cap \mathcal{H} := \{x \mid \forall A \in \mathcal{H} \text{ esetén } x \in A\}$

2.1.12. definíció. $\cup \mathcal{H} := \{x \mid \exists A \in \mathcal{H} \text{ olyan, hogy } x \in A\}$



2.2. ábra. Halmazműveletek Venn-diagramos szemléltetése.

Így tehát a $\cap \mathcal{H}$ elemei a halmazcsalád minden halmazához hozzá tartoznak, $\cup \mathcal{H}$ pedig mindenazon elemekből áll, amelyek a halmazcsalád valamely halmazának elemei.

Ellenőrző feladat. Legyen $\mathcal{H} = \{\{a, b, c\}, \{a, d, e\}, \{a, f\}\}$. Mi lesz $\cap \mathcal{H}$ és $\cup \mathcal{H}$?

2.1.13. definíció. Amennyiben $\cap \mathcal{H} = \emptyset$, a halmazcsaládot diszjunktak nevezzük.

Ellenőrző kérdés. Létezik-e olyan halmazcsalád, amely diszjunkt, de nem páronként diszjunkt?

A halmazcsaládra is érvényes számos halmazelméleti azonosság, például kommutativitás, asszociativitás, disztributivitás, vagy a De Morgan-szabályok.

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

X osztályfelbontása tehát X olyan páronként diszjunkt, nem-üres részhalmazaira való bontása, ahol a részhalmazok uniója a teljes X halmaz. A definíció szerint az $\{X\}$ halmaz önmaga is egy osztályfelbontást alkot (triviális osztályfelbontás).

2.4. példa. Az emberek halmaza úgy (is) osztályozható, hogy azok, akik már jártak a Holdon, és azok, akik még nem.

2.5. példa. Az $\{a, b\}$ halmaz osztályfelbontásai az $\{\{a\}, \{b\}\}$ és az $\{\{a, b\}\}$.

Ellenőrző feladat. Készítsük el az $\{1, 2, 3\}$ halmaz összes különböző osztályfelbontását.

A halmazalgebra műveletei a matematika csaknem minden területén előbukkanak. 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. Bizonyítsuk be, hogy minden A, B, C halmaz esetén

- a) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
- b) $A \setminus (B \cup C) = (A \setminus B) \setminus C$
- c) $A \subseteq B \Rightarrow A \setminus C \subseteq B \setminus C$.

2.1-3. Bizonyítsuk be a De Morgan-törvényeket.

2.1-4. Bizonyítsuk be, hogy tetszőleges A, B halmazokra

- a) $A \cap B \subseteq A, B \subseteq A \cup B$,
- b) $A \subseteq B \Leftrightarrow A \cup B = B \Leftrightarrow A \cap B = A \Leftrightarrow A \cap \bar{B} = \emptyset$,
- c) $\wp(A) \cap \wp(B) = \wp(A \cap B)$,
- d) $\wp(A) \cup \wp(B) \subseteq \wp(A \cup B)$. Egyenlőség mikor teljesül?

2.1-5. Definiálunk 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 különbségnak* vagy *szimmetrikus differenciának* nevezzük.

- c) Mutassuk meg, hogy \triangle asszociatív.

2.1-6. Igazoljuk, hogy tetszőleges A, B halmazokhoz pontosan akkor létezik olyan C halmaz, amelyre $A \setminus C = B$, ha $A \triangle B \subseteq A$.

2.1-7. Az alábbi állítások közül melyik teljesül minden $A, B, C \subseteq H$ -ra:

- a) Ha $A \in B$ és $B \in C$ akkor $A \in C$.
- b) Ha $A \subseteq B$ és $B \in C$ akkor $A \in C$.
- c) Ha $A \cap B \subseteq \bar{C}$ és $A \cup C \subseteq B$ akkor $A \cap C = \emptyset$.

2.1-8. Milyen összefüggés van $(A \setminus B) \cup (A \setminus C) \cup (A \setminus D)$ és $B \cap C \cap D$ között?

2.1-9. Bizonyítsuk be, hogy ha tetszőleges A, B, C halmazokra $A \cup B = A \cup C$ és $A \cap B = A \cap C$, akkor $B = C$.

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

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

2.2.1. definíció. $(a_1, a_2) := \{\{a_1\}, \{a_1, a_2\}\}$.

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 egyenlők, 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.

2.2.2. definíció. $(a_1, a_2, \dots, a_n) := ((a_1, a_2, \dots, a_{n-1}), a_n)$.

2.2.3. definíció. Legyenek A_1, A_2, \dots, A_n halmazok. Az

$$A_1 \times A_2 \times \cdots \times A_n := \{(a_1, \dots, a_n) \mid a_i \in A_i\}$$

halmazt az A_1, A_2, \dots, A_n halmazok Descartes-féle **direkt szorzatának** nevezzük.
A $= A_1 = A_2 = \dots = A_n$ esetén az A^n jelölés használatos.

Két rendezett n -es egyenlősége ugyancsak a komponensenkénti egyenlőségből adódik. A rendezett pár definíciója miatt amennyiben valamelyik (akár több) A_i halmaz üres, akkor $A_1 \times A_2 \times \cdots \times A_n = \emptyset$, továbbá $A^0 = \{\emptyset\}$.

2.6. példa. Legyen az A halmaz a magyar keresztnévek halmaza. Ekkor a $\varrho = \{(Antal), (Imre), (József)\}$ egy *unér (unáris)* reláció A -n.

Ellenőrző kérdés. Milyen A, B halmazokra teljesül, hogy $A \times B = B \times A$?

2.2.4. definíció. $A \varrho \subseteq A_1 \times A_2 \times \cdots \times A_n$ részhalmazt **n -változós relációt** nevezzük. Az $n = 2$ esetben **binér relációról**, a $\varrho \subseteq A^n$ esetben **homogén relációról** beszélünk.

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

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

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

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

A predikátumok tehát a relációk leírásai a logika nyelvén.

2.2.2. Binér relációk

A $\varrho \subseteq A \times B$ binér relációt úgy is értelmezhetjük, hogy B elemeit meghatározott módon „hözzárendeljük” A elemeihez. Az $(a, b) \in \varrho$ helyett gyakran szokás $a \varrho b$ -t írni. Véges halmazok esetén ez a hozzárendelés „nyíldiagrammal” (a reláció irányított gráfjával) szemléltethető (2.3. ábra).

Ellenőrző kérdés. Legyen $A = \{(x, y) \mid x \in X, y \in Y\}$, $B = \{1, 3\}$. Igazak-e az alábbi állítások, ha $a \in X$ és $b \in Y$: $((a, b), 1) \subseteq A \times B$, $\{(a, b), 3\} \subseteq A \times B$, $\{((a, b), 3)\} \subseteq A \times B$?

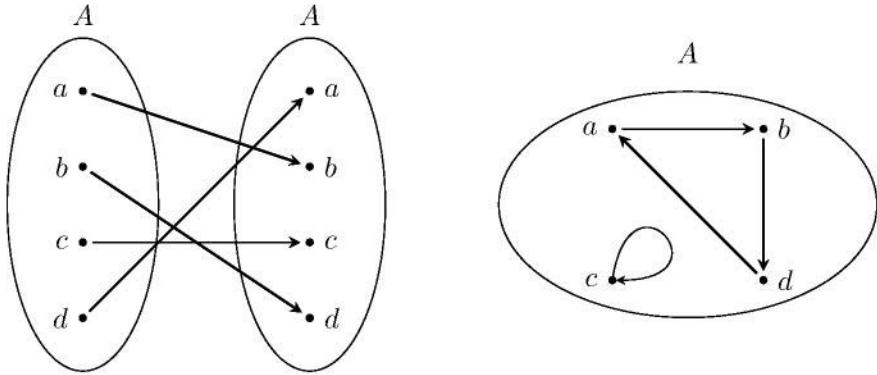
Ellenőrző feladat. Adjunk példát binér relációkra az emberek és az autók halmaza között.

2.8. példa. Binér relációra példa a „ \subseteq ” tartalmazás a halmazrendszerben, vagy a „ \perp ” merőlegesség az egyenesek egy halmazában.

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

2.2.5. definíció. $A \varrho \subseteq A \times B$ reláció **értelmezési tartománya**

$$\text{dmn}(\varrho) (= D_\varrho) := \{a \in A \mid \exists b \in B : (a, b) \in \varrho\},$$



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

értékkészlete pedig

$$\text{rng}(\varrho) (= R_\varrho) := \{b \in B \mid \exists a \in A : (a, b) \in \varrho\}.$$

2.2.1. megjegyzés. Az értelmezési tartományt néhány szerző $\text{dom}(\varrho)$ -ként jelöli.

2.10. példa. Az $A = \{a, b\}$, $B = \{c, d, e\}$, $\varrho = \{(a, d), (a, e)\} \subset A \times B$ reláció esetén $\text{dmn}(\varrho) = D_\varrho = \{a\}$, $\text{rng}(\varrho) = R_\varrho = \{d, e\}$.

Ellenőrző kérdés. Az iménti példában $A \times B$ -n hány relációt tudnánk megadni összesen? Lehetne ezt általánosítani véges n és m elemszámú A és B halmazokra?

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

$$\varrho|_H := \{(a, b) \in \varrho, a \in H\}$$

relációt értjük.

2.2.7. definíció. A $\varrho \subseteq A \times B$ reláció **inverzének** a

$$\varrho^{-1} := \{(b, a) \in B \times A \mid (a, b) \in \varrho\}$$

relációt nevezünk.

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

Ellenőrző kérdés. Mi lesz a 2.3. ábrán látható reláció inverze?

2.2.8. definíció. Ha $\varrho \subseteq A \times B$ és $\sigma \subseteq B \times C$, akkor a

$$\sigma \circ \varrho := \{(x, z) \in A \times C \mid \exists y \in B (x \varrho y \wedge y \sigma z)\}$$

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

Figyeljük meg, hogy relációk kompozíciója lehet üres reláció is.

2.2.9. tételel (relációsorozat asszociativitása). Legyen $\varrho \subseteq A \times B, \sigma \subseteq B \times C$ és $\tau \subseteq C \times D$. Ekkor a relációsorozat asszociatív, vagyis $(\tau \circ \sigma) \circ \varrho = \tau \circ (\sigma \circ \varrho)$.

Bizonyítás. A két halmaz egyenlőségét kölcsönös tartalmazással bizonyítjuk. Először a $(\tau \circ \sigma) \circ \varrho \subseteq \tau \circ (\sigma \circ \varrho)$ tartalmazást látjuk be. Ha $(a, d) \in (\tau \circ \sigma) \circ \varrho$, akkor létezik olyan $b \in B$, amelyre $(a, b) \in \varrho$ 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 $(a, c) \in \sigma \circ \varrho$ és $(c, d) \in \tau$. Így pedig $(a, d) \in \tau \circ (\sigma \circ \varrho)$ is teljesül. Hasonlóképpen bizonyítható a $\tau \circ (\sigma \circ \varrho) \subseteq (\tau \circ \sigma) \circ \varrho$ összefüggés is, amiből a két reláció egyenlősége következik. ■

2.11. példa. Legyenek egy garázscég alkalmazottai

$$A = \{\text{András, Béla, Cili, Dénes, Elemés, Flóra, Géza, Hugó}\},$$

a beosztások

$$B = \{\text{menedzser, fejlesztő, tesztelő, üzleti elemző, asszisztens}\},$$

feladatspecifikus projektjei

$$F = \{\text{bank, telko}\}.$$

Legyen az S (szerep) reláció

$$\begin{aligned} S &= \{(\text{András, menedzser}), (\text{Béla, fejlesztő}), (\text{Cili, tesztelő}), (\text{Dénes, fejlesztő}), \\ &\quad (\text{Elemér, üzleti elemző}), (\text{Flóra, asszisztens}), (\text{Géza, fejlesztő}), \\ &\quad (\text{Hugó, tesztelő})\} \subseteq A \times B, \end{aligned}$$

a P projekt reláció

$$\begin{aligned} P &= \{(\text{András, bank}), (\text{András, telko}), (\text{Béla, bank}), (\text{Cili, bank}), (\text{Dénes, telko}), \\ &\quad (\text{Elemér, bank}), (\text{Elemér, telko}), (\text{Flóra, bank}), (\text{Flóra, telko}), (\text{Géza, telko}), \\ &\quad (\text{Hugó, telko})\} \subseteq A \times F, \end{aligned}$$

a projektekhez tartozó határidők pedig

$$H = \{(\text{bank, 2013. december 31.}), (\text{telko, 2014. június 30.})\}.$$

- Milyen projektben dolgozik Elemér? Válasz: a banki és a telko-s projektben is, mert $(\text{Elemér, bank}), (\text{Elemér, telko}) \in P$.
- Kik a tesztelők? Válasz: Cili és Hugó, mert $\text{rng}(S^{-1}|_{\{\text{tesztelő}\}}) = \{\text{Cili, Hugó}\}$.
- Kik dolgoznak banki projekten?
Válasz: $\text{rng}(P^{-1}|_{\{\text{bank}\}}) = \{\text{András, Béla, Cili, Elemér, Flóra}\}$.
- Van-e olyan kollégá, aki nem dolgozik feladaton? Válasz: nincs, mert $\text{dmn}(P) = A$.
- Van-e minden projektnek menedzsere? Válasz: igen, mert $\text{rng}(P \circ (S^{-1}|_{\{\text{menedzser}\}})) = F$.
- A december 31.-i átadási határidejű projekten dolgozó tesztelőknek karácsony és szilveszter között is dolgozniuk kell. Kiknek is?
Válasz: $\text{rng}(P^{-1} \circ (H^{-1}|_{\{2013. \text{december } 31.\}})) \cap \text{rng}(S^{-1}|_{\{\text{tesztelő}\}}) = \{\text{Cili}\}$.

2.2.3. Homogén binér relációk tulajdonságai

2.2.10. definíció. Tekintsük a $\varrho \subseteq A \times A$ alakú (homogén binér) relációkat. Ekkor

(1) ρ reflexív	$:= \forall a \in A (a\varrho a)$
(2) ρ irreflexív	$:= \forall a \in A \neg(a\varrho a)$
(3) ρ szimmetrikus	$:= \forall a, b \in A (a\varrho b \Rightarrow b\varrho a)$
(4) ρ antiszimmetrikus	$:= \forall a, b \in A (a\varrho b \wedge b\varrho a \Rightarrow a = b)$
(5) ρ szigorúan antiszimm.	$:= \forall a, b \in A (a\varrho b \Rightarrow \neg(b\varrho a))$
(6) ρ tranzitív	$:= \forall a, b, c \in A (a\varrho b \wedge b\varrho c \Rightarrow a\varrho c)$
(7) ρ intranzitív	$:= \forall a, b, c \in A (a\varrho b \wedge b\varrho c \Rightarrow \neg(a\varrho c))$
(8) ρ trichotom	$:= \forall a, b \in A \left(\begin{array}{l} a\varrho b \vee b\varrho a \vee a = b \\ \text{és pontosan az egyik} \end{array} \right)$
(9) ρ gyengén trichotom	$:= \forall a, b \in A (a\varrho b \vee b\varrho a, \text{ esetleg mindkettő})$

A gyengén trichotom relációt gyakran **dichotomnak**, lineárisnak vagy konnexnek mondjuk. A gyengén trichotómia jelentősége abban áll, hogy teljesülése esetén az A halmaz bármely két eleme „összehasonlítható”, mégpedig önmagával is. Ezek a tulajdonságok a rendezési struktúrákhoz és a hányadoshalmazok konstrukciójához lesznek lényegesek.

2.12. példa. Az emberek halmazán tekintsük az ismertség relációt, vagyis A akkor ismeri B -t, ha egyszer már kezet fogtak. Ez a reláció reflexív, hiszen mindenki ismeri önmagát (most tekintsünk el a skizofrénektől); szimmetrikus, hiszen ha A ismeri B -t akkor B ismeri A -t; nem tranzitív, hiszen ha B ismeri az USA elnökét, attól még a haverja A nem biztos, hogy ismeri; sem a dichotomia, sem a trichotomia nem teljesül, hiszen könnyen találhatunk két vagy három olyan embert, akik egyáltalán nem ismerik egymást.

Ellenőrző kérdés. A 2.3. ábrán látható homogén binér reláció esetében a 2.2.10. definícióban megfogalmazottak közül két tulajdonság teljesül. Melyek ezek?

Ellenőrző kérdés. Lehet-e dichotom egy nem reflexív reláció?

Ellenőrző feladat. Legyen $A = \{a, b\}$. Adjuk meg az összes A -beli binér homogén relációt. Vizsgáljuk meg a kapott relációk közül kettőnek a tulajdonságait.

Ellenőrző feladat. Milyen tulajdonságokkal rendelkezik az emberek halmazán értelmezett „szülője” reláció?

2.2.2. megjegyzés. Ha egy ρ relációt a gráfjával adunk meg, akkor

- ρ pontosan akkor reflexív, ha minden pontjában van hurokél;
- ρ irreflexív, ha egyetlen hurokél sincs;
- ρ szimmetrikus, ha a gráf minden éle kétirányú;
- ρ tranzitív, ha teljesül rá az, hogy amennyiben létezik út tetszőleges a, b pontja között, akkor létezik él is a és b között;
- ρ antiszimmetrikus, ha bármely két különböző pontjára teljesül, hogy közöttük egyáltalán nem, vagy pontosan egy irányban megy él;
- ρ dichotom, ha reflexív és a gráf bármely két pontja között megy él.

2.13. példa. Bizonyítsuk be, hogy egy $\rho \subseteq A \times A$ reláció pontosan akkor tranzitív, ha $\rho \circ \rho \subseteq \rho$. Először tételezzük fel, hogy ρ tranzitív. Ha valamely a és b elemekre $a(\rho \circ \rho)b$, akkor a relációk szorzatának értelmezése alapján van olyan c amelyre apb és apc teljesülnek. A reláció tranzitivitása miatt ekkor apb is teljesül, vagyis $\rho \circ \rho \subseteq \rho$. Megfordítva, most tételezzük fel, hogy $\rho \circ \rho \subseteq \rho$. Tegyük fel továbbá, hogy valamely $a, b, c \in A$ -ra apb és apc . A relációszorzás értelmezése miatt ekkor apc is teljesül. Ez pontosan ρ tranzitivitását jelenti.

2.2.4. Ekvivalenciareláció, hányadoshalmaz

Kiemelkedően fontos szerepet játszanak az alábbi tulajdonságokkal rendelkező relációk:

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

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

Ellenőrző feladat. Ekvivalenciareláció-e az alábbi reláció: $\{(a, b) \in \mathbb{N} \times \mathbb{N} : a - b \text{ páros}\}$?

2.2.12. definíció. Adott $\varrho \subseteq A \times A$ ekvivalenciareláció esetén az A halmaz minden elemének halmazát, amelyek egy $a \in A$ elemmel ϱ relációban állnak, az a által meghatározott $[a]$ **ekvivalenciaosztálynak** nevezzük:

$$[a] := \{b \in A \mid a\varrho b\} \subseteq A.$$

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

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

Bizonyítás. Legyen adott az A halmazon egy ϱ ekvivalenciareláció. Megmutatjuk, hogy $\{[a] \mid a \in A\}$ egy osztályozása A -nak. Nyilván

$$\bigcup_{a \in A} [a] = A,$$

továbbá 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 $a\varrho c$ és $b\varrho c$, amiből a tranzitivitás és a szimmetria miatt $a\varrho b$ és $b\varrho a$. Ha most $d \in [a]$, akkor a szimmetria és a tranzitivitás miatt $d \in [b]$. Ugyanígy, ha $d \in [b]$, akkor $d \in [a]$. Végéredményben 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 adott az A halmaz egy osztályfelbontása, akkor a

$$\varrho = \{(a, b) \in A \times A \mid a \text{ és } b \text{ egyazon osztály elemei}\}$$

reláció reflexív, szimmetrikus és tranzitív, vagyis ekvivalenciareláció. ■

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

2.15. példa. Tekintsük az emberek halmazán azt az osztályfelbontást, amit a hajuk színei alapján teszünk. Az osztályfelbontáshoz tartozó ekvivalenciareláció ekkor azt írja le, hogy két ember pontosan akkor lesz relációban, ha a hajuk színe azonos.

2.2.14. definíció. Az

$$A/\varrho := \{[a] \mid a \in A\}$$

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 hánymoshalmaz egy absztraktiós folyamat eredménye: az ekvivalencia-osztályt létrehozó tulajdonságot az osztályfelbontással lehet azonosítani. Ha az A halmaz ϱ ekvivalenciareláció szerinti hánymoshalmazából 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 hánymoshalmazt, az eredeti osztályozást kapjuk.

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

Gyakorlatok

2.2-1. Legyen adott egy $\varrho \subseteq A \times B$ reláció, és legyen $A_1, A_2 \subseteq A$. Bizonyítsuk be az alábbiakat:

- a) Ha $A_1 \subseteq A_2$, akkor $R_{\varrho|_{A_1}} \subseteq R_{\varrho|_{A_2}}$,
- b) $R_{\varrho|_{A_1 \cup A_2}} = R_{\varrho|_{A_1}} \cup R_{\varrho|_{A_2}}$,
- c) $R_{\varrho|_{A_1 \cap A_2}} \subseteq R_{\varrho|_{A_1}} \cap R_{\varrho|_{A_2}}$.

2.2-2. Adjunk példát a homogén binér relációk 2.2.10. definícióban látott tulajdonságai közül mindegyikre.

2.2-3. Legyen A tetszőleges halmaz. Létezik-e olyan reláció A -n, amely egyidejűleg

- a) szimmetrikus és antiszimmetrikus;
- b) dichotom és szimmetrikus?

Ha a válasz igenlő, adjuk meg az összes szóban forgó relációt.

2.2-4. Adjunk példát olyan relációra, amely

- a) reflexív és szimmetrikus, de nem tranzitív;
- b) reflexív és tranzitív, de nem szimmetrikus;
- c) szimmetrikus és tranzitív, de nem reflexív.

2.2-5. Írjuk le a kő-papír-olló játék relációs modelljét és elemezzük tulajdonságait.

2.2-6. Legyen $E = \{\text{sík egyenesei}\}$. Az alábbi $E \times E$ -n értelmezett relációkról állapít-suk meg, hogy ekvivalenciarelációk-e:

- a) $\varrho = \{(a, b) \mid a \text{ egy pontban metszi } b\text{-t}\}$,
- b) $\sigma = \{(a, b) \mid a\text{-nak és } b\text{-nek van közös pontja}\}$.

2.2-7. Elemei felsorolásával határozzuk meg azt az ekvivalenciarelációt, amelyhez a megfelelő alaphalmazon az alábbi osztályfelbontás tartozik: $\{a, d, g\}$, $\{b\}$, $\{e\}$, $\{c, f\}$.

2.2-8. Az $\{1, 2, 3\}$ halmazon keressünk két olyan homogén binér relációt, amelyek szimmetrikusak, de a szorzatuk nem szimmetrikus.

2.2-9. Legyen $\varrho \subseteq A \times A$. Vizsgáljuk meg $\varrho \circ \varrho^{-1}$ reflexivitását, szimmetriáját és tranzitivitását.

2.2-10. Mutassuk meg, hogy minden $A \subseteq X$ halmazra és $\varrho \subseteq X \times X$ relációra

$$A \subseteq \varrho(\varrho^{-1}(A)) \Leftrightarrow A \subseteq \text{rng}(\varrho).$$

2.2-11. Legyen $\varrho \subseteq A \times A$. Bizonyítsuk be, hogy a

$$\hat{\varrho} = \varrho \cup \varrho^2 \cup \dots = \bigcup_{n=1}^{\infty} \varrho^n$$

reláció tranzitív. $\hat{\varrho}$ -t a ϱ reláció **tranzitív lezártjának** nevezzük.

($\varrho^n = \underbrace{\varrho \circ \varrho \circ \dots \circ \varrho}_{n\text{-szer}}$, ami a relációsorozat asszociativitása miatt egyértelmű.)

2.2-12. Mi az emberek közötti „gyermek” illetve „szülője” reláció tranzitív lezártja?



2.1. Programozási feladat. Írunk olyan programot, amely egy inputként megadott binér homogén reláció esetén megadja a reláció értékkészletét, értelmezési tartományát, eldönti, hogy milyen tulajdonságok teljesülnek rá, és amennyiben lehetséges, megadott tulajdonságokkal kiegészíti azt.



2.2. Programozási feladat. Készítsünk olyan programot, amely egy adott ekvivalenciareláció esetén elkészíti az osztályfelbontást.

2.3. Függvények

A binér relációk általában nem állítanak elő egyértelmű összefüggést halmazok között, vagyis egy elemmel több elem is relációban állhat. Egy halmaznak egy másik halmazra történő leképezésénél gyakran kívánatos, hogy a halmazt *egyértelműen* képezze le a másik halmazra. Effajta leképezések alkotják szinte az összes matematikai elmélet alapját. Az alábbiakban ilyen speciális relációkkal foglalkozunk.

2.3.1. A függvény definíciója

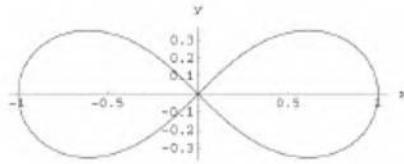
2.3.1. definíció. Legyenek A, B halmazok, továbbá $f \subseteq A \times B$. Az f relációt A -ból B -be képező **parciális függvénynek** nevezzük, ha bármely $x \in D_f$ esetén az $\{y \in B \mid (x, y) \in f\}$ halmaz egyetlen elemből áll. Ezt az egyetlen elemet az x -hez rendelt **függvényértéknek**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

Ha A vagy B üres halmaz, akkor $f = \emptyset$. Az $f(x)$ -et úgy olvassuk: „ x függ f ”, vagy f értéke az x helyen. Azt a tényt, hogy az x -hez rendelt függvényérték y , úgy jelöljük, hogy $x \mapsto y$, $f : x \mapsto y$, $f : x \xrightarrow{f} y$, $x \mapsto f(x)$ vagy $y = f(x)$. Az x -et gyakran **argumentumnak** (vagy független változónak), y -t pedig az f függvény x -beli **helyettesítési értékének** is nevezzük. 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 **hozzárendeléseknek** vagy **leképezéseknek** is szokás nevezni. Bizonyos speciális esetekben találkozhatunk a *transzformáció*, *operáció*, *operátor*, *funkcionál* elnevezésekkel is. Bizonyos számhalmazoknál a $\{(x, f(x)) \mid x \in D_f\} \subseteq A \times B$ relációt koordináta-rendszerben lehet ábrázolni (hogy ez miért tehető meg, a 3. és a 4. fejezetből kiderül).

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

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

A parciális függvényeket teljessé tehetjük oly módon, hogy értelmezési tartományukat a teljes A halmazon vesszük.



2.4. ábra. A Bernoulli-féle lemniszka.

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

$$B^A := \{f \mid f : A \rightarrow B\}.$$

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

Ellenőrző feladat. Határozzuk meg B^A összes elemét, ha az A és B halmazok 0, 1 illetve 2 eleműek.

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

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

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

Ellenőrző kérdés. Milyen A, B halmazok esetén lesz $A \times B$ biztosan függvény?

Ellenőrző feladat. Adjuk meg azt a függvényt, ami megadja Anna, Béla és Csilla nemét.

2.3.1. megjegyzés. A számítógépes programok legtöbbje nem fogad el mindenféle inputot. Például egy numerikus műveleteket kiértékelő program valószínűleg nem fogad el stringet bemenetként. Így ezek a programok parciális függvényeknek tekinthetők. Ez egy elég erős motíváció, hogy miért értelmezünk parciális függvényeket.

2.18. példa. Felmérülhet a kérdés, miért nem úgy értelmeztük az $f \in A \rightarrow B$ függvényeket, hogy $R_f = B$ legyen. Gyakorlati okokból. Nem minden egyszerű megmondani, hogy mi is lesz R_f valójában. Tekintsük például azt az $f \in \mathbb{R} \rightarrow \mathbb{R}$ függvényt, amelyre $t \mapsto (x(t), y(t))$ és $x(t) = \frac{t(1+t^2)}{1+t^4}$, $y(t) = \frac{t(1-t^2)}{1+t^4}$. Ekkor a függvény képe a Bernoulli-féle lemniszka (2.4. ábra).

2.3.3. definíció. Legyen $f \in A \rightarrow B$, továbbá $H \subseteq A$. Az

$$f[H] := \{f(x) \mid x \in H \cap D_f\} \subseteq R_f \subseteq B$$

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 $H \cap D_f = \emptyset$ esetén $f[H] = \emptyset$, speciálisan $f[\emptyset] = \emptyset$.

2.3.4. definíció. Legyen $f \in A \rightarrow B$, továbbá $H \subseteq B$. Az

$$f^{-1}[H] := \{x \in D_f \mid f(x) \in H\} \subseteq D_f \subseteq A$$

halmazt a H (f által létesített) **ösképének** (inverz képének) nevezünk.

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

Ellenőrző feladat. Adjuk meg a $\rho = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y^2 = 2 + x - x^2\}$ reláció esetén a $\{0\}$ halmaz képét és ösképét (\mathbb{R} a valós számok halmazát jelenti).

2.3.5. definíció. Legyenek A_1, \dots, A_n halmazok. Ha egy $f \in A \rightarrow B$ függvény esetén $D_f \subseteq A_1 \times \dots \times A_n$, akkor n -változós függvényről beszélünk.

Jelölésben $f((a_1, \dots, a_n))$ helyett általában $f(a_1, \dots, a_n)$ -et írunk. Az itt szereplő minden egyes a_i -t argumentumnak nevezünk, dacára annak, hogy formálisan az (a_1, a_2, \dots, a_n) rendezett n -es az argumentum.

2.19. példa. Legyen B a színek halmaza. Tekintsük az alábbi $f \in \mathbb{N} \times \mathbb{N} \times \mathbb{N} \rightarrow B$ háromváltozós függvényt:

$$\begin{aligned} (255, 255, 0) &\mapsto \text{sárga} \\ (160, 32, 240) &\mapsto \text{bíbor} \\ (0, 191, 255) &\mapsto \text{égszínkék} \end{aligned}$$

Az első koordináta a vörös, a második a zöld, a harmadik a kék szín erősséget jelzi (RGB skála).

2.3.2. Függvények típusai, leszűkítés, kiterjesztés, indexelés

2.3.6. definíció. Legyen adott egy $f \in A \rightarrow B$ függvény. Az f függvény **szürjektív**, ha $R_f = B$, **injektív**, ha $\forall x_1, x_2 \in D_f$ esetén $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. A leképezést **bijektívnek** nevezzük, ha $D_f = A$, valamint **szürjektív is** és **injektív is**.

Ellenőrző feladat. Legyen az $f \in A \rightarrow B$ függvény esetén A és B is véges elemszámú ($|A|, |B| < \infty$). Melyik igaz az alábbiak közül (indokuljuk állításunkat)?

- (a) Ha f injektív, akkor $|A| = |B|$,
- (b) Ha f injektív, akkor $|D_f| = |R_f|$,
- (c) Ha f szürjektív, akkor $|A| \geq |B|$,
- (d) Ha f szürjektív, akkor $|D_f| > |R_f|$,
- (e) Ha f bijektív, akkor $|D_f| = |R_f|$,
- (f) Ha $|D_f| = |R_f|$, akkor f bijektív.

2.20. példa. (1) Legyenek A_1, \dots, A_n halmazok és $i \in \{1, \dots, n\}$. A $p_i \in A_1 \times \dots \times A_n \rightarrow A_i$, $(x_1, \dots, x_n) \mapsto x_i$ függvényt **i -edik projekciónak** vagy **vetítésnek** nevezzük.

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

(3) Az $A \rightarrow A$, $a \mapsto a$ leképezés bijektív, amit **identikus leképezésnek**, **identitásnak** vagy **azonosságnak** nevezünk, és id_A -val vagy \mathbb{I}_A -val jelölünk.

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

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

Ezeket a függvényeket **permutáció-függvényeknek** nevezzük.

(5) Az $f \in A \rightarrow B$ leképezést **konstansfüggvénynek** nevezzük, ha $f(x) = f(y)$ minden $x, y \in D_f$ esetén. Ha $0 \in B$ és $f(x) = 0$ minden $x \in D_f$ esetén, akkor a konstansfüggvényt **nullfüggvénynek** nevezzük.

(6) Az $A \subseteq H \neq \emptyset$ halmaz **karakterisztikus függvényének** 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 $\chi_A^{(H)}(x)$.

(7) A $\delta : A \times A \rightarrow \{0, 1\}$ függvényt **Kronecker-féle δ -függvénynek** nevezzük, ha

$$\delta(i, j) = \delta_{ij} = \begin{cases} 1, & \text{ha } i = j \\ 0, & \text{ha } i \neq j \end{cases}.$$

A Kronecker-delta az id_A identikus leképezés karakterisztikus függvénye.

(8) Legyen $B = \{\text{IGAZ}, \text{HAMIS}\}$. Ekkor a $B^n \rightarrow B^m$ függvényeket **logikai függvényeknek** vagy **Boole-függvényeknek** nevezzük ($n, m \geq 1$ egész). A Boole-függvényeknek a logikai áramkörök tervezésében van nagy szerepük.

2.21. példa. Legyen A_1 a vezetéknévök, A_2 a keresztnévök, A_3 a foglalkozások, A_4 pedig az évszámok halmaza. Tekintsük azt a projekciót, ami egy vállalat $A_1 \times A_2 \times A_3 \times A_4$ relációs adattáblájához, ami a munkatársak adatait tartalmazza, hozzárendeli a megfelelő vezetéknévöket. Ekkor a projekció például az alábbi lehet:

$$\begin{aligned} (\text{Szabó, István, tesztelő, 1953}) &\mapsto \text{Szabó} \\ (\text{Kiss, Péter, tervező, 1960}) &\mapsto \text{Kiss} \\ (\text{Nagy, László, üzletkötő, 1971}) &\mapsto \text{Nagy} \end{aligned}$$

2.22. példa. Az $A = \{1, 2, 3\}$ halmazon értelmezett permutáció-függvények az alábbiak lesznek:

$$\begin{aligned} \text{id}_A &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \\ f_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}. \end{aligned}$$

2.23. példa. Legyen $A, B \subseteq H$, f és g pedig sorban a karakterisztikus függvényei. Ekkor \bar{A} karakterisztikus függvénye $1 - f$, $A \cap B$ karakterisztikus függvénye $f \cdot g$, $A \cup B$ karakterisztikus függvénye pedig $f + g - f \cdot g$. (A függvények közötti műveleteket a későbbiekben pontosan definiáljuk.)

2.3.7. definíció. *A $g \in C \rightarrow B$ függvényt az $f \in A \rightarrow B$ függvény (C-re való) leszűkítésének (vagy megsorításának) nevezzük, ha $\emptyset \neq C \subseteq D_f$, és $f(x) = g(x)$ minden $x \in C$ esetén. g helyett gyakran $f|_{C-t}$ írunk (olvasd: f leszűkítése C-re).*

2.3.8. definíció. *A $g \in C \rightarrow B$ függvényt az $f \in A \rightarrow B$ 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 „rendszeré” kap hangsúlyt. A „rendszer” valami olyant jelent, hogy az értékkészlet elemeit az értelmezési tartomány elemeinek segítségével adjuk meg, azaz „megindexeljük”.

2.3.9. definíció. *Legyen $I \neq \emptyset$ és $A \neq \emptyset$. Az $a : I \rightarrow A$ 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: $\langle a_i, i \in I \rangle$, $(a_i, i \in I)$, $(a_i)_{i \in I}$, $a_i \in A$ ($i \in I$). Az $\langle a_i, i \in I \rangle$ 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 $a : I \rightarrow A$ leképezés injektivitását. A 2.3.2. definíció alapján így az A -beli indexelt rendszerek halmazát A^I jelöli.

Ha A elemei minden halmazok, akkor *indexelt halmazcsaládról* beszélünk.

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

Legyen $A = \{\{\text{red, rouge, rot}\}, \{\text{white, blanc, weiß}\}, \{\text{green, vert, grün}\}\}$. Az $a : I \rightarrow A$, $a_{\text{piros}} = \{\text{red, rouge, rot}\}$, $a_{\text{fehér}} = \{\text{white, blanc, weiß}\}$, $a_{\text{zöld}} = \{\text{green, vert, grün}\}$ függvény egy indexelt halmazcsalád.

2.25. példa. Számos szimbolikus programozási nyelvben az indexelt rendszerek kezelése beépített. Szinte az összes programozási nyelv ismeri a **vector** struktúrát, ami a természetes számok egy részhalmazán, mint indexhalmazon értelmezett és valamilyen elemi informatikai adattípusra (**char**, **int**, **long**) képező indexelt rendszer. Például C-ben az **int v[MAX]** jelentése egy olyan **v** vektor deklarálása, ami MAX darab egészet tartalmaz, és **v[0]**, **v[1]**, ..., **v[MAX-1]**-gyel címezhető.

2.3.3. Logikai függvények

Legyen $B = \{\text{IGAZ, HAMIS}\}$. Az alábbiakban B -be képező logikai függvényeket vizsgálunk.

2.3.10. téTEL (Diszjunktív normálformára hozás). *Bármely $f : B^n \rightarrow B$ függvény megadható $f(x_1, x_2, \dots, x_n) = \mathcal{A}_1 \vee \mathcal{A}_2 \vee \dots \vee \mathcal{A}_m$ alakban ($m \in \mathbb{N}$), ahol az összes \mathcal{A}_i $\mathcal{B}_1 \wedge \mathcal{B}_2 \wedge \dots \wedge \mathcal{B}_k$ alakú, továbbá minden \mathcal{B}_j vagy x_{i_j} vagy $\neg x_{i_j}$ lehet ($1 \leq k \leq n$).*

A diszjunktív normálformák tehát olyan $\bigvee_i \bigwedge_j (\neg)x_{ij}$ alakú nulladrendű logikai formulák, amelyekben csak változók és a \neg , \vee , \wedge logikai műveleti jelek fordulnak elő. A téTEL szerint tetszőleges ítéletlogikai formulát elő lehet állítani diszjunktív normálformában. Azonban néha többféleképpen is, azaz az előállítás nem egyértelmű.

2.26. példa. Az $n = 4$ esetben az $f(x_1, x_2, x_3, x_4) = (\neg x_1 \wedge \neg x_2) \vee (x_2 \wedge x_3 \wedge \neg x_4)$ egy diszjunktív normálformában leírt logikai függvény.

Az x_1, x_2, \dots, x_n változókat a (normál)forma **atomjainak** nevezzük. Az iménti példában x_1, x_2, x_3, x_4 atomok. A változók vagy negáltjaik a (normál)forma **literáljai**. A példában $\neg x_1, \neg x_2, x_2, x_3, \neg x_4$ a literálok. A literálok konjunkciójait **elemi konjunkcióknak** nevezzük, a példában ezek: $\neg x_1 \wedge \neg x_2$ és $x_2 \wedge x_3 \wedge \neg x_4$.

Bizonyítás. Megkonstruálunk egy lehetséges megfelelő normálalakot. Tekintsük azokat az $\alpha = (x_1, x_2, \dots, x_n)$ n -eseket, amelyekre $f(\alpha)$ kielégíthető, és írjuk fel ezekből az $\mathcal{A}_i = \mathcal{B}_1 \wedge \mathcal{B}_2 \wedge \dots \wedge \mathcal{B}_n$ elemi konjunkciót úgy, hogy legyen $\mathcal{B}_j = x_j$ ha α -ban $x_j = \text{IGAZ}$, és $\mathcal{B}_j = \neg x_j$, ha α -ban $x_j = \text{HAMIS}$. Az összes így adódó (legfeljebb 2^n elemű) kifejezést kapcsoljuk össze diszjunkcióval. ■

Az így konstruált normálalakot **teljes diszjunktív normálformának** nevezzük, mert $k = n$ minden i -re.

2.27. példa. Tekintsük azt az $f : B^3 \rightarrow B$ logikai függvényt, melynek igazságátáblája:

Halmazok, relációk, függvények

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

A táblázatban az IGAZ = 1, HAMIS = 0 jelölést használtuk. Ekkor az elemi konjunkciók az alábbiak lesznek: $\mathcal{A}_1 = \neg x_1 \wedge x_2 \wedge x_3$, $\mathcal{A}_2 = x_1 \wedge \neg x_2 \wedge x_3$, $\mathcal{A}_3 = x_1 \wedge x_2 \wedge x_3$. A teljes diszjunktív normálforma pedig

$$\mathcal{A}_1 \vee \mathcal{A}_2 \vee \mathcal{A}_3 = (\neg x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge x_3).$$

A diszjunktív normálformák egyszerűsítésére különféle technikák léteznek (algebrai, Karnaugh-tábla, stb.).

2.28. példa. [folytatás] Az iménti példát folytatva a normálformára a disztributív szabályt egymás után többször alkalmazzuk. Először x_3 -ra, $((\neg x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2) \vee (x_1 \wedge x_2)) \wedge x_3$, majd a konjunkció első tagjának második és harmadik elemére, $((\neg x_1 \wedge x_2) \vee (x_1 \wedge (\neg x_2 \vee x_2))) \wedge x_3$, majd összevonás után újra alkalmazva kapjuk, hogy $(x_1 \vee x_2) \wedge x_3$.

Ha a diszjunktív normálformára alakítást az $f(x_1, x_2, \dots, x_n)$ függvény helyett annak negáltjára alkalmazzuk, majd az eredményt negáljuk, az alábbi eredményt kapjuk:

2.3.11. téTEL (Konjunktív normálformára hozás). *Bármely $f : B^n \rightarrow B$ függvény megadható $f(x_1, x_2, \dots, x_n) = \mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \dots \wedge \mathcal{A}_m$ alakban ($m \in \mathbb{N}$), ahol az összes \mathcal{A}_i $\mathcal{B}_1 \vee \mathcal{B}_2 \vee \dots \vee \mathcal{B}_k$ alakú, továbbá minden \mathcal{B}_j vagy x_{i_j} vagy $\neg x_{i_j}$ lehet ($1 \leq k \leq n$).*

2.3.4. Függvények kompozíciója, inverze, műveletei halmazokkal

Ha $g \in A \rightarrow B$ és $f \in B \rightarrow C$ függvények, akkor $f \circ g$ analóg a relációk kompozíciójával. Ekkor $f \circ g \in A \rightarrow C$ szintén függvény, hiszen ha van olyan α, β , amelyre $(f \circ g)(x) = \alpha$ és $(f \circ g)(x) = \beta$ valamely x -re, akkor vagy a g nem függvény (mert ekkor $g(x) = y_1$, $g(x) = y_2$, $f(y_1) = \alpha$, $f(y_2) = \beta$ valamely $y_1, y_2 \in B$ -re), vagy ha g függvény, akkor f nem az (mert ekkor $g(x) = y$, $f(y) = \alpha$, $f(y) = \beta$ valamely $y \in B$ -re).

Kapjuk tehát, hogy $f \circ g \in A \rightarrow C$ az a függvény, amelyre a

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

halmaz nem-üres, és ekkor a kompozíció

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

A felírásban szereplő g -t *belső függvénynek*, f -et *külső függvénynek* nevezzük. Az $f \circ g$ függvényt néha röviden fg -ként jelöljük.

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

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

2.29. 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.

2.3.12. téTEL. Az $f \in A \rightarrow B$ függvény inverze pontosan akkor függvény, ha f injektív. Ekkor f^{-1} maga is injektív, továbbá $f^{-1} \circ f = \text{id}_{D_f}$ és $f \circ f^{-1} = \text{id}_{R_f}$.

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.

2.30. példa. Számítsuk ki a 2.22. példa f_4 függvényének inverzét és az $f_3 \circ f_2$ függvénykompozíciót.

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

Gyakorlatok

2.3-1. Bizonyítsuk be, hogy tetszőleges $R \subseteq A \times A$ esetén R pontosan akkor

- a) reflexív, ha $\mathbb{I}_A \subseteq R$,
- b) irreflexív, ha $\mathbb{I}_A \cap R = \emptyset$,
- c) szimmetrikus, ha $R^{-1} = R$,
- d) antiszimmetrikus, ha $R \cap R^{-1} \subseteq \mathbb{I}_A$,
- e) szigorúan antiszimmetrikus, ha $R \cap R^{-1} = \emptyset$,
- f) tranzitív, ha $R \circ R \subseteq R$,
- g) dichotom, ha $R \cup R^{-1} = A \times A$,
- h) trichotom, ha R, R^{-1} és \mathbb{I}_A páronként diszjunktak, és egyesítésük $A \times A$.

2.3-2. Legyen $R \subseteq A \times B$. Mi mondható el R -ről, ha

- minden $Y \subseteq B$ esetén $R \circ R^{-1}(Y) \subseteq Y$,
- minden $X, Y \subseteq B$ esetén $R^{-1}(X \cap Y) = R^{-1}(X) \cap R^{-1}(Y)$.

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

$$\begin{aligned}\varrho &= \{(1, a), (1, c), (2, b), (2, d), (3, a)\}, \\ \varrho &= \{(1, d), (2, a), (3, c)\}, \\ \varrho &= \{(1, a), (2, a), (3, d)\}.\end{aligned}$$

2.3-4. Egy képernyőn a lehetséges pointer-pozíciókat az alábbi módon definiáljuk: $(oszlopindex, sorindex) \in X \times Y$, ahol $X = \{x \in \mathbb{Z} \mid 1 \leq x \leq 1080\}$ és $Y = \{y \in \mathbb{Z} \mid 1 \leq y \leq 1920\}$. A képernyő bal felső sarka az $(1, 1)$ pozíció. Határozzuk meg azt a függvényt, amely a képernyő pontjait egy tetszőleges lehetséges pozícióból

- a) a jobb alsó sarokba helyezi át;
- b) 1-gyel felfelé eltolja;
- c) 2-vel jobbra és 15-tel lefelé eltolja;
- d) a függőleges szimmetriatengelyre tükrözi;
- e) az $y = x$ egyenesre tükrözi;
- f) a $(20, 10)$ pontból háromszorosára nagyítja;

Minden esetben adjuk meg azokat az (x, y) koordinátákat, amelyeken az adott funkció nem hajtható végre. Feltéve hogy a vizsgált leképezéseket az $X \times Y$ halmazon értelmezzük, válasszuk ki a parciális függvényeket.

2.3-5. Adott $f, g \in A \rightarrow B$ függvények esetén függvény lesz-e $f \cup g$, $f \cap g$, $f \setminus g$, $f \triangle g$? A válaszokat indokoljuk!

2.3-6. Bizonyítsuk be, hogy tetszőleges $\phi : A \rightarrow B$ függvény esetén a $\text{Ker}(\phi) \subseteq A \times A$, $a_1 \text{Ker}(\phi) a_2 \Leftrightarrow \phi(a_1) = \phi(a_2)$ reláció ekvivalenciareláció. A $\text{Ker}(\phi)$ relációt a ϕ függvény *magjának* nevezzük.

2.3-7. Legyen $A, B \subseteq H$, χ_A és χ_B pedig sorban a karakterisztikus függvényeik. Mi lesz ekkor \bar{A} , $A \cup B$ és $A \cap B$ karakterisztikus függvénye?

2.3-8. Tekintsük az alábbi függvényeket: $\varphi, \psi : \mathbb{N} \rightarrow \mathbb{N}$,

$$\varphi(n) = \begin{cases} 3n + 1 & \text{ha } n \text{ páros,} \\ 3n - 1 & \text{egyébként,} \end{cases} \quad \psi(n) = \begin{cases} n - 20 & \text{ha } n > 20, \\ 1 & \text{egyébként.} \end{cases}$$

Vizsgáljuk meg, hogy injektív-e, szürjektív-e, és adjuk meg a $\varphi^2, \psi^2, \varphi\psi, \psi\varphi$ leképezéseket.

2.3-9. A $\varphi_0, \varphi_1, \varphi_2 : \mathbb{Z} \rightarrow \mathbb{Z}$, $\varphi_0(n) = 3n$, $\varphi_1(n) = 3n + 1$, $\varphi_2(n) = 3n + 2$, függvényekhez keressünk olyan $\psi : \mathbb{Z} \rightarrow \mathbb{Z}$ leképezést, amelyre $\psi\varphi_0 = \text{id}$, $\psi\varphi_1 = \text{id}$, $\psi\varphi_2 = \text{id}$ egyidejűleg teljesül.

2.3-10. Bizonyítsuk be, hogy injektív függvények kompozíciója injektív, szürjektív függvények kompozíciója szürjektív függvény.

2.3-11. Hozzuk diszjunktív normálformára az alábbi logikai függvényt:

$$f(p, q, r) = ((p \wedge q) \Rightarrow r) \wedge (\neg(p \vee q) \Rightarrow r).$$

2.3-12. Legyen $f : A \rightarrow B$ és $g : B \rightarrow C$ invertálható függvények. Bizonyítsuk be, hogy ekkor $g \circ f$ is invertálható, továbbá $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

2.3-13. Legyen $X \rightarrow Y$ függvény. Mutassuk meg, hogy az alábbi feltételek ekvivalenek:

- a) f injektív;
- b) minden $A \subseteq X$ -re $f^{-1}(f(A)) = A$;
- c) minden $A, B \subseteq X$ -re $f(A \cap B) = f(A) \cap f(B)$;
- d) Bármely $A \subseteq B \subseteq X$ esetén $f(B \setminus A) = f(B) \setminus f(A)$.

2.3-14. Legyenek $f : X \rightarrow Y$ és $g : Y \rightarrow Z$ függvények. Bizonyítsuk be a függvényekre és halmazműveletekre vonatkozó alábbi összefüggéseket:

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



2.3. Programozási feladat. Írunk olyan programot, amely egy logikai függvényt diszjunktív normálformára hoz.



2.4. Programozási feladat. Tervezzünk olyan programot, amely egy diszjunktív normálformában adott logikai függvényt egyszerűsít.

2.4. Axiomatikus halmazelmélet

A naiv halmazelméletben, mint látni fogjuk, ellentmondásokat lehet konstruálni. Az ilyen ellentmondásokhoz vezető megmondásokat **antinómiákknak** nevezzük. Ezeknek az elemzése a halmazelmélet új felépítéséhez vezetett.

(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) PROKLO SZ (Kr.e. 450 körül)

PRÓTAGORASZ 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, PRÓTAGORASZ végül beperelte a tandíj meg nem fizetése miatt. Így érveld: „Ha megnyerem a pert, akkor megkapom a pénzemet az ítélet alapján, ha elveszítem, akkor a korábbi megállapodás alapján kapom meg.” A tanítvány fordítva érveld: „A tandíjat egyik esetben sem kell megfizetnem, vagy a megállapodás vagy a bírói ítélet miatt.”

(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 következetetésre vezet, hogy saját magát nem tartalmazza, és az a feltevés, hogy H saját magát tartalmazza, arra vezet, hogy H önmagát nem tartalmazza. Formalizálva, legyen $H = \{x \mid x \notin x\}$. Ekkor $H \in H \Leftrightarrow H \notin H$.

(4) KARINTHY FRIGYES (Őrült sikerem a tébolydában)

„Ohó álljunk csak meg. Ön azt mondja, a rögeszmém, hogy őrült vagyok. De hiszen tényleg az vagyok, az imént mondta. De hiszen akkor ez nem rögeszme, akkor az egy logikus gondolat. Tehát nincs rögeszmém. Tehát mégse vagyok őrült. Tehát csak rögeszme, hogy őrült vagyok, tehát rögeszmém van, tehát őrült vagyok, tehát igazam van, tehát nem vagyok őrült. Mégiscsak gyönyörű dolog a tudomány!”

EPIMENDÉSZ és PRÓTAGORASZ állításai logikai értelemben tehát nem kijelentések.

Ellenőrző feladat. Képzeljük el, hogy megadunk egy webcímét, majd a szabályosan letöltődött oldalon az alábbi üzenet jelenik meg: „Az Ön által kért webcím nem létezik”. Elemezzük az oldal logikai tartalmát.

A Russel-paradoxon szerint minden halmaz halmaza ellentmondásos fogalom. Az antinomiák 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, melynek elemei minden halmazok, akkor van olyan halmaz, amely pontosan azokat a dolgokat tartalmazza, amelyek A valamely elemeinek az elemei. Vagyis minden A és B halmazhoz van olyan C halmaz, amely elemei pontosan azok az elemek, amelyek A -nak vagy B -nek elemei.

(6) *A hatványhalmaz axiómája.* minden A halmazhoz létezik egy olyan halmazsalád, amelynek elemei pontosan A részhalmazai.

Halmazok, relációk, függvények

(7) *A végtelenségi axióma.* Van olyan A halmaz, amelynek \emptyset 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 létezik kiválasztási függvény.

Kiválasztási függvény alatt olyan leképezést értünk, amelynek az értelmezési tartománya tetszőleges nem-üres halmazokból áll és minden egyes nem-üres halmazhoz hozzárendel egy elemet az adott halmazból, azaz minden halmazból kiválaszt egy elemet. A kiválasztási függvény értékkészlete tehát az értelmezési tartományban lévő halmazok uniójának egy részhalmaza. Kicsit precízebben: az $X_i, i \in I$ halmazrendszerhez tartozó kiválasztási függvénynek nevezzük azokat az $f : I \rightarrow \bigcup_{i \in I} X_i$ függvényeket, amelyekre $f_i \in X_i$ minden $i \in I$ -re. Még másik fogalmazva: nem-üres halmazok bármely indexelt családjának Descartes-szorzata nem-üres.

2.4.1. megjegyzés. *A kiválasztási axióma hétköznapi nyelven megfogalmazva azt állítja, hogy végtelen elemszámú halmaz mindegyikéből kiválasztható egyetlen szempillantás alatt egy-egy elem.*

Az imént megadott nyolc axiómát tartalmazó axiómarendszerből FRAENKEL kihagyta a kiválasztási axiómát, és kizárt minden 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 az $\{y : \mathcal{F}(x, y)\}$ halmaz egyelemű, akkor létezik az A halmazon értelmezett olyan f függvény, amelyre az $f(x) = y$ fennáll minden $x \in A$ esetén.

Azaz, legyen az $\mathcal{F}(x, y)$ formula „függvényeszerű” abban az értelemben, hogy minden x -hez egyetlen y létezik, amellyel $\mathcal{F}(x, y)$ teljesül. Ekkor tekinthetjük azt az $f(x) = y$ függvényt, mely minden x -hez azt az egyetlen y -t rendeli, melyre $\mathcal{F}(x, y)$ fennáll. A pótlás axiómája azt mondja, hogy ekkor minden H halmaz f általi $f(H)$ képe szintén halmaz.

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

A Zermelo-féle axiómarendzszer 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 mesebeli várat egy félelmetes sárkány őrzi. A sárkány arról híres, hogy minden állításról el tudja döntení, hogy igaz vagy hamis. Ha igaz az állítás, akkor megégeti az illetőt, ha hamis (vagy nem állítás), akkor megeszi. Arra jár egy vándor, odamegy a sárkányhoz, mond neki valamit, mire a sárkány beengedi a várba. Milyen kijelentést

tett a vándor?

2.4-2. Egy politikus elhatározza, hogy minden napos hazudozásait ezentúl néha igazmondással fűszerezí, azaz hétfőn, szerdán és pénteken mindenig igazat mond, más napokon mindenig hazudik. Egyszer azt mondta: „Holnap igazat fogok mondani!”. A hét melyik napján történt ez?

2.4-3. A borbély azt a parancsot kapja a katonaságban, hogy csak azokat kell megorotálnia, akik nem borotválják saját magukat. Szabad-e a parancs értelmében a borbélynak megorotálnia saját magát?

2.4-4. 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

Az **antinómia** a filozófiában két egymást kizáró, de egyformán bizonyítható, elfogadható téTEL ellentmondását jelenti. Az ókori filozófusok (PLATÓN, ARISZTOTELÉSZ) alkották meg, majd a skolasztikus logikában volt jelentős szerepe. Nagy figyelmet fordított az antinomiákra KANT, aki az ész önmagával való ellentmondásosságának bebizonításakor négy antinómiát állított föl: a) a világ végesége és végtelensége; b) az anyag végtelen oszthatósága és elemeinek oszthatatlansága; c) szükségszerűség és szabadság; d) a világ okának létezése és ennek lehetetlensége.

A **paradoxon** állítások egy olyan halmaza, amelyek ellentmondásra vezetnek, vagy a józan észnek ellentmondó következtetés vonható le belőlük. A legősibb paradoxon egyike Zénón paradoxonja, amelyeket az eleai ZÉNÓN ötlött ki PARMENIDÉSZ elméletének alátámasztására, miszerint az érzékek által alkotott kép félrevezető, konkrétaban, hogy a mozgás csak illúzió, valójában nem létezik. ZÉNÓN nyolc fennmaradt (és ARISZTOTELÉSZ *Fizika* című művében leírt) paradoxonja mind nagyjából ugyanarra az alapgondolatra épül, és a legtöbbet már az ókorban is könnyen cáfolhatónak tartották. A három leghíresebb és legjobban védhető Akhilleusz és a teknős, a fának hajított kő, és a nyílvessző paradoxonja. Ez a három paradoxon sok fejtörést okozott számos ókori és középkori filozófusnak. NEWTON és LEIBNIZ az analízis területén (elsősorban a végtelen sorozatok kezelésében) elért áttöréseinek köszönhetően váltak feloldhatóvá a 17. században.

Az első említett paradoxon így szól: Képzeljük el Akhilleuszt, a leggyorsabb görögöt, amint versenyt fut egy teknőssel. Mivel Akhilleusz szélvész gyors, nagyvonalúan száz láb előnyt ad a hüllőnek. Alighogy elindul a verseny, Akhilleusz pár ugrással ott terem, ahol a teknős kezdett. Ezalatt az idő alatt azonban a teknős is haladt egy keveset, talán egy lábnyit. Akhilleusz egy újabb lépéssel ott terem, ám ezalatt a teknős ismét halad egy kicsit, és még mindenig vezet. Akármilyen gyorsan is ér Akhilleusz oda, ahol a teknős egy pillanattal korábban volt, amaz mindenig egy kicsit előrébb lesz. ZÉNÓN érvelése azt látszik igazolni, hogy Akhilleusz sohasem fogja megelőzni, de még csak utolérni sem a teknőst.

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

Halmazok, relációk, függvények

problémaköre a kontinuumhipotézis köré csoportosul. A problémát az 5. fejezet végén ismertetjük. Fontos még megemlíteni, hogy a kiválasztási axiómának léteznek egyéb ekvivalens megfogalmazásai. Az egyik ezek közül a jórendezési tételel, mely szerint minden halmaz jórendezhető.

Az általunk tárgyalt rendezett pár fogalmát KURATOWSKI vezette be 1921-ben. A függvényfogalom LEIBNIZ-nek tulajdonítható, aki a függvényeket különböző formulák leírásra használta. Az általa adott definíciót később nagymértékben általánosították.

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. 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

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

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

Az irreflexivitásból és a tranzitivitásból a szigorú antiszimmetria nyilvánvalóan következik, hiszen ha egy a elem relációban áll egy b elemmel, és ekkor b is relációban állna a -val, az a elem önmagával is relációban állna a tranzitivitás miatt, így a reláció nem lehetne irreflexív.

3.1.3. téTEL (részbenrendezés és szigorú részbenrendezés kapcsolata). Ha ϱ részbenrendezés és σ szigorú részbenrendezés egy A halmazon, akkor

- (1) $\varrho \setminus \mathbb{I}_A$ szigorú részbenrendezés,
- (2) $\sigma \cup \mathbb{I}_A$ részbenrendezés, és
- (3) $\sigma = \varrho \setminus \mathbb{I}_A$ pontosan akkor, ha $\sigma \cup \mathbb{I}_A = \varrho$.

Bizonyítás.

(1) $\varrho \setminus \mathbb{I}_A$ nyilván irreflexív. Ha $(a, b) \in \varrho \setminus \mathbb{I}_A$, akkor $a \neq b$, amiből ϱ antiszimmetriája miatt $(b, a) \notin \varrho$. Ezért $(b, a) \notin \varrho \setminus \mathbb{I}_A$, amiből a szigorú antiszimmetria adódik. Tegyük most fel, hogy $(a, b), (b, c) \in \varrho \setminus \mathbb{I}_A$. Ekkor ϱ tranzitivitásából $(a, c) \in \varrho$. Mivel $\varrho \setminus \mathbb{I}_A$ szigorúan antiszimmetrikus, ezért $c \neq a$, így $(a, c) \in \varrho \setminus \mathbb{I}_A$. Ezzel $\varrho \setminus \mathbb{I}_A$ tranzitivitását is bebizonyítottuk.

(2) $\sigma \cup \mathbb{I}_A$ reflexivitása az identitás-függvény definíciójából következik. Ha $(a, b) \in \sigma$,

akkor $(b, a) \notin \sigma$. Vagyis $(a, b), (b, a) \in \sigma \cup \mathbb{I}_A$ csak akkor lehetséges, ha $(a, b), (b, a) \in \mathbb{I}_A$. Ez pedig $\sigma \cup \mathbb{I}_A$ antiszimmetriáját jelenti. Tegyük fel, hogy $(a, b), (b, c) \in \sigma \cup \mathbb{I}_A$. Ha $(a, b), (b, c) \in \sigma$, akkor a tranzitivitás miatt $(a, c) \in \sigma$. Ha egyikük σ -nak eleme, a másik pedig \mathbb{I}_A -beli, akkor (a, c) megegyezik (a, b) és (b, c) valamelyikével, és így ugyancsak σ -beli. Amennyiben pedig $(a, b), (b, c) \in \mathbb{I}_A$, akkor (a, c) is az. Vagyis (a, c) minden eleme $\sigma \cup \mathbb{I}_A$ -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.

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

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

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

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

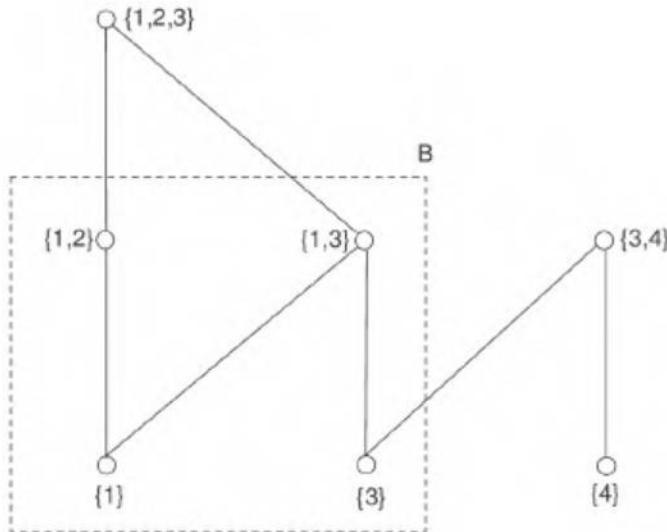
Analóg módon definiálhatjuk egy részhalmaz **maximális elemeit**, illetve **legnagyobb elemét**. A definícióból világos, hogy egy tetszőleges részbenrendezett halmaz bármely véges részhalmazának van minimális eleme. Ezzel szemben legkisebb elem még véges részbenrendezett halmazok esetében sem minden létezik. Ha viszont legkisebb elem létezik, akkor az 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.

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

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

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



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 $\{1\}, \{3\}, \{4\}$, 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 szuprénuma az $\{1, 2, 3\}$ elem, alsó korlátja és infimuma nincs.

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).

3.1. példa. Legyen adott egy SMP (symmetric multiprocessor) architektúrával rendelkező többmagos számítógép, amelyben tehát minden processzor egyetlen közös memóriában tárolja az adatokat. Legyen adott az alábbi program:

```

a[1] = 1; a[2] = 4; a[3] = 9; a[4] = 16; a[5]=25
for i=1 to 4 do
    b[i] = a[i+1] - a[i]
enddo
for i=1 to 3 do
    if b[i+1] - b[i] ≠ 2 then
        print "Megtörtént a lehetetlen..."
    endif
enddo

```

Tegyük fel, hogy a program minden utasítását a processzor egységnyi idő alatt hajtja végre (a valóságban nem egészen így van). Vajon ideális esetben mennyi idő alatt hajtódiik végre az iménti program (a ciklusszámláló inkrementálását nem számoljuk)? Vizsgáljuk meg először azt az esetet, amikor egyetlen mag áll rendelkezésre. Ekkor az utasítások egymás után hajtódnak végre, összesen 9 értékadás, 7 kivonás, 3 összehasonlítás, minden összesen 19 időegységre van tehát szükség. Több mag esetén bevezetjük a „megelőzési relációt”. Ez azt jelenti, hogy egy utasítás csak akkor hajtható végre, ha hozzá minden szükséges adat megtalálható a memóriában, így bizonyos utasítások végrehajtásának meg kell előznie másokét. A megelőzési reláció alapján felépíthetjük a Hasse-diagramot. Kis számolás után azt kapjuk, hogy 2 mag esetén 10 időegységre, 4 mag esetén 6 időegységre, 8 vagy több mag esetén 5 időegységre van szükség.

3.1.9. definíció. Legyen (A, \leq_1) és $(B; \leq_2)$ részbenrendezett struktúra. Az $f \in A \rightarrow B$ 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.

3.2. példa. Tekintsük a 3.2. ábra a) és b-1) részbenrendezéseit, amelyek az $A = \{a, b, c, d, e, f\}$ halmazon vannak értelmezve. Jelölje az elsőt \leq , a másodikat \preceq . Ekkor az

$$F = \begin{pmatrix} a & d & f & b & e & c \\ b & e & f & a & d & a \end{pmatrix}$$

függvény monoton növő. Például $e < f \Rightarrow d \preceq f$, etc. Figyeljük meg, hogy F sem nem injektív, sem nem szürjektív.

3.1.10. definíció. Az $(A; \leq)$ részbenrendezés esetén $[x, y]$ -nal jelöljük minden $z \in A$ elemek halmazát, amelyekre $x \leq z$ és $z \leq y$, vagy rövidebben $x \leq z \leq y$. Hasonlóan, $]x, y[$ -nal jelöljük minden 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.

Ellenőrző kérdés. Melyek lesznek a zárt intervallumok a 3.2. a) ábrán?

3.1.2. Teljes rendezés, jórendezés

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

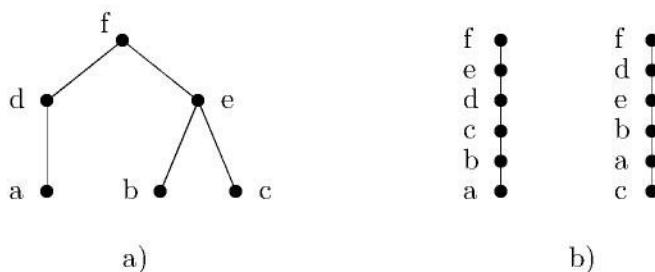
Ha $(A; \leq)$ teljes rendezés, akkor a legkisebb és minimális elem, valamint a legnagyobb és maximális elem fogalma egybeesik, továbbá az indukált részbenrendezésnél egy teljesen rendezett halmaz minden részhalmaza is teljesen rendezett.

3.3. példa. A későbbiekben bizonyítjuk, hogy a természetes számok $\mathbb{N} = \{0, 1, 2, \dots\}$, az egész számok $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$, a racionális számok $\mathbb{Q} = \{a/b, a, b \in \mathbb{Z}, b \neq 0\}$, és a valós számok $\mathbb{R} = \mathbb{Q} \cup \{x : x \text{ iracionális}\}$ halmaza is rendezett. Ekkor a valós számokon

- (1) $\sup \{1, 2, 3, \dots, n\} = n$,
- (2) $\sup \{x \in \mathbb{R} : 0 < x < 1\} = \sup \{x \in \mathbb{R} : 0 \leq x \leq 1\} = 1$,
- (3) $\inf \{(-1)^n + \frac{1}{n} : n \in \mathbb{N} \setminus \{0\}\} = -1$,
- (4) $\sup \{x \in \mathbb{Q} : x^2 < 2\} = \sqrt{2}$.

3.1.12. téTEL. Véges halmazon minden részbenrendezés kiterjeszhető rendezéssé.

BIZONYÍTÁS. Legyen $(A; \leq)$ egy véges részbenrendezett halmaz. Tekintsük az összes olyan kiterjesztésnek H halmazát, ami szintén részbenrendezés (H elemei tehát részbenrendezések, $A \in H$). H a kiterjesztés mentén szintén részbenrendezés és mivel véges, van maximális eleme. Legyen ez a maximális elem (A, \preceq) . Ha ebben a részbenrendezésben volnának $a, b \in A$ összehasonlíthatatlan elemek, akkor $\preceq \cup \{(a, b)\}$ tranzitív lezártja egy valódi részbenrendezett kiterjesztése lenne \preceq -nak, ami ellentmond a maximalitásának. ■



3.2. ábra. Az a) ábrán egy részben rendezés Hasse-diagramját láthatjuk. A b) ábra az előbbinek két lehetséges topologikus rendezését mutatja.

3.1.13. definíció. Legyen adott egy $(A; \leq)$ részbenrendezés. minden olyan, ehhez a részbenrendezéshez tartozó $(A; \preceq)$ (teljes) rendezést, amelyre tetszőleges $a \leq b$, $a, b \in A$ esetén teljesül, hogy $a \preceq b$ **topologikus rendezésnek** nevezzük.

A topologikus rendezés általában nem egyértelmű (3.2. ábra).

3.1.14. definíció. Egy részben rendezett halmaz valamely részhalmazát **láncnak** nevezik, ha az indukált részben rendezésnél teljesen rendezett.

A későbbiekben látni fogjuk, hogy a „tradicionális számhalmazok” és véges részhalmazai teljesen rendezhetőek, ezért a rendezéssel kapcsolatos összefüggéseket jól lehet írni, *számegevenesen* ábrázolni.

Ha (A, \leq_1) és (B, \leq_2) rendezett, akkor az $f \in A \rightarrow B$ szigorúan monoton növekvő (csökkenő) függvény kölcsönösen egyértelmű, és az inverze is az.

A teljesen rendezett halmazok további specializálását adja az alábbi definíció:

3.1.15. definíció. Az $(A; \leq)$ részbenrendezsnél az A halmaz **jólrendezett**, ha minden nem-üres részhalmazának van leküisebb eleme.

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

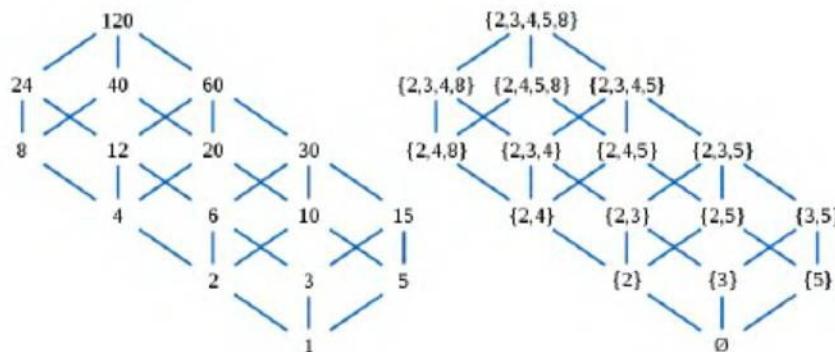
3.1.16. Tétel (biz. nélkül) (jólrendezési tétele). *Minden halmaz jólrendezhető.*

Megjegyezzük, hogy a jólrendezési téTEL következik a kiválasztási axiómát is tartalmazó axiomatikus halmazelméletből. Megfordítva, a jólrendezési téTELből le lehet vezetni a kiválasztási axiómát. A jólrendezési téTEL alkalmazásánál a probléma az, hogy a jólrendezésnek csak a létezése van biztosítva. A jólrendezési téTELLEL EKVIVALENS A

3.1.17. Tétel (biz. nélkül) (Zorn-féle lemma). *Ha egy részben rendezett halmaz minden lánca felülről korlátos, akkor a halmaznak van maximális eleme.*

Gyakorlatok

3.1-1. Adjuk meg a 2, 3, 4-elemű halmazok összes (lényegesen különböző) részbenre-



3.3. ábra. Példák Hasse-digramokra.

dezéseit.

3.1-2. Definiálunk $\mathbb{N} \times \mathbb{N}$ -en egy R relációt az alábbi módon: $(n_1, m_1)R(n_2, m_2)$ ha $m_1 \leq m_2$ és $n_1 \leq n_2$. Mutassuk meg, hogy R részbenrendezés.

3.1-3. Határozzuk meg azokat a relációkat, amelyek egyidejűleg részbenrendezések és ekvivalenciák.

3.1-4. Mutassuk meg, hogy az alábbi, \leq -vel jelölt relációk mindegyike részbenrendezés:

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

b) az $\{a, b, c, d\}$ halmaz legfeljebb kételemű 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.

3.1-5. Bizonyítsuk be, hogy egy részbenrendezett halmaz bármely nem-üres véges részhalmazának van maximális és minimális eleme.

3.1-6. Adjuk meg azokat a részbenrendezéseket, melyeknek Hasse-diagramjai a 3.3. ábrán láthatók. Mi a kapcsolat közöttük?

3.1-7. Bizonyítsuk be, hogy ha $\varrho \subseteq A \times A$ részbenrendezés, akkor ϱ^{-1} is az. Mi a kapcsolat a két reláció Hasse-diagramja között? Mutassuk meg, hogy ha $(A; \varrho)$ -n az $a \in A$ elem maximális, akkor (A, ϱ^{-1}) -en a minimális és fordítva.

3.1-8. Írjuk fel egy családi ház építésének 20 legfontosabb (diszjunkt) folyamatát, és rendeljük hozzájuk a megvalósításukhoz szükséges becsült időket. A folyamatok megelőzési relációja alapján írjuk fel a Hasse-diagramot, mely alapján számítsuk ki az építkezés lehetséges leggyorsabb befejezését.

3.1-9. Mutassuk meg, hogy jólrendezett halmaz bármely részhalmaza is jólrendezett.

3.1-10. Mutassuk meg, hogy ha A és B teljesen rendezettek, akkor minden $f : A \rightarrow B$ szigorúan monoton növő (illetve csökkenő) függvény injektív. Állíthatunk-e hasonlót f inverzéről?

3.1-11.* Legyen $A \neq \emptyset$, és ϱ egy A -n értelmezett reláció. Bizonyítsuk be, hogy ϱ pontosan akkor terjeszthető ki részbenrendezéssé, ha a $\tilde{\varrho} = \mathbb{I}_A \cup \hat{\varrho}$ reláció részbenrendezés A -n ($\hat{\varrho}$ a ϱ reláció tranzitív lezártját jelenti.) Ekkor $\tilde{\varrho}$ a ϱ reláció **reflexív-tranzitív lezártja**.



3.1. Programozási feladat. Írunk olyan programot, amely egy adott binér homogén reláció esetén megkonstruálja annak reflexív tranzitív lezártját.



3.2. Programozási feladat. Íjunk olyan programot, amely egy adott rendezésről eldönti, hogy részbenrendezés-e, és ha igen, kirajzolja a Hasse-diagramot, meghatározza a minimális, maximális, legkisebb, legnagyobb eleme(ke)t.

3.2. Algebrai struktúrák

Az absztrakt algebra a matematika azon területe, ami a matematikai struktúrák szerkezetét vizsgálja. Egy halmazhoz **algebrai struktúrát** rendelünk, ha benne egy vagy több műveletet értelmezünk. Ilyen művelet például számhalmazokon a „hagyományos” összeadás vagy szorzás. Az „absztrakt” szó arra utal, hogy az érdeklődésünk középpontjában nem a halmaz elemei, hanem a közöttük lévő műveletek szerkezete áll. Műveleteket persze nem csak számhalmazokon definiálhatunk. Kézenfekvő, hogy a definíciót általánosan fogalmazzuk meg.

3.2.1. Belső művelet

3.2.1. definíció. *Tetszőleges A nem-üres halmaz és n nemnegatív egész esetén A -n értelmezett n -változós (belő) műveletén egy $A^n \rightarrow A$ függvényt értünk, ahol n -et a művelet változószámának vagy aritásának nevezünk.*

Az $n = 0$ eset különleges. Mivel A^0 egyelemű halmaz, ezért egy A -n értelmezett null-változós 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 „közé írást” (infix írásmódot) alkalmazunk. Ha tehát \oplus kétváltozós művelet A -n, akkor tetszőleges $a, b \in A$ -ra a művelet eredményét $a \oplus b$ -vel jelöljük, továbbá 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 gyakran ab -t írunk.

Ellenőrző kérdés. Művelet-e a természetes számokon az $x \rightarrow -x$ ellentétképzés? És az egész számokon?

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

A műveletek megadása a függvények megadásához hasonlóan történhet. Véges halmazokra a műveleteket **műveleti táblázattal** lehet ábrázolni (3.3. ábra).

3.2.2. definíció. *Az $(A; \Omega)$ párt, ahol A nem-üres halmaz, Ω pedig A -n értelmezett műveletek egy rendezett halmaza, **algebrai struktúrának**, vagy röviden **algebrának** nevezünk. Az A halmazt alaphalmaznak, vagy **tartóhalmaznak** hívjuk.*

3.2.3. definíció. *Ha Ω n_0 darab nullváltozós, n_1 darab egyváltozós, és rendre n_i darab i -változós műveletből áll, akkor azt mondjuk, hogy $(n_0, n_1, \dots, n_i, \dots)$ az $(A; \Omega)$ struktúra típusa.*

Szokás továbbá megállapodni a műveletek végrehajtási sorrendjében, idegen szóval **precedenciájában**. Például először a nullváltozós, majd az egyváltozós (unér), azután a

\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

3.4. ábra. Az $A = \{a, b, c, d\}$ halmazon értelmezett kétváltozós \oplus művelet műveleti táblázata (más néven **Cayley-táblázata**). A struktúra a Klein-féle csoport.

kétváltozós (binér) műveleteket végezzük el, stb. Ha az $(A; \Omega)$ algebrai struktúrában Ω véges, mondjuk $\Omega = (\oplus, \otimes)$, akkor az algebrát $(A; \oplus, \otimes)$ módon is jelölhetjük.

3.5. példa. Kétváltozós műveletek infix írásmódja esetén ha egy művelet eredményére újabb műveletet alkalmazunk, akkor valamilyen módon (például zárójelekkel) jelölni kell azok végrehajtási sorrendjét. A zárójelek teljesen el is hagyhatók, ha a műveleti jeleket minden az operandusok előtt írjuk. Ezt a jelölésmódot ŁUKASIEWICZ tiszteletére *lengyel jelölésnek* szokás nevezni. Az informatikában még elterjedtebb a *fordított lengyel jelölés* (RPN, Reversed Polish Notation), ahol a műveleti jelek az operandusok után következnek. Néhány zsebszámológép mellett a PostScript nyomtatővezérlő nyelv és a fordítóprogramok is ezt használják. Például a helyesen zárójelezett $5 + ((1 + 2) * 4)/3$ kifejezés RPN alakja $5 \ 1 \ 2 \ + \ 4 \ * \ 3 \ / \ +$. Az alak helyességének ellenőrzéséhez egy informatikában használt speciális adatstruktúra, egy verem (stack) szükséges. A verem olyan adatszerkezet, amely több elemet is tartalmazhat, de minden csak az utolsónak belerakott (legfelső) eleme érhető el. Nevét is erről kapta, vagyis egy földebe ásott veremhez hasonlóan minden csak a legutolsónak belerakott eleme használható, és az alsóbb elemek minden csak az utánuk a verembe rakott elemek eltávolítását követően válnak elérhetővé. A veremből az elemek a behelyezéssel (push) ellentétes sorrendben emelhetők ki (pop). Így tehát a legelsőnek belehelyezett elem csak az összes utána belerakott elem kifejtése után válik elérhetővé. A példánkban

Input	Művelet	Stack
5	push	5
1	push	5 1
2	push	5 1 2
+	add	5 3
4	push	5 3 4
*	multiply	5 12
3	push	5 12 3
/	divide	5 4
+	add	9

A eredmény tehát 9. A műveletek elvégzését úgy kell értelmezni, hogy a verem felső két elemének kivétele (pop) után a művelet eredménye visszakerül a verem tetejére (push).

A továbbiakban az *egyetlen* kétváltozós művelettel rendelkező – vagyis $(0, 0, 1, 0, \dots)$ típusú – struktúrák, az ún. **grupoidok** tulajdonságait vizsgáljuk.

3.2.4. definíció. Az $(S; \oplus)$ grupoid s_b elemét **bal oldali illetve** s_j elemét **jobb oldali semleges elemnek** nevezzük, ha $s_b \oplus a = a$ illetve $a \oplus s_j = a$ minden $a \in S$ elemre.

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

Ellenőrző kérdés. Létezik-e semleges elem a $(\mathbb{Z}; +)$ és a $(\mathbb{Q} \setminus \{0\}; \cdot)$ grupoidokban?

3.2.5. 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.

3.2.6. definíció. Az $(S; \oplus)$ grupoidot **félcsoporthnak** nevezzük, ha a művelete asszociatív.

Ellenőrző kérdés. Tetszőleges H halmazra félcsoportok-e a $(\wp(H); \cap)$ és a $(\wp(H); \cup)$ grupoidok?

Ha az asszociativitás érvényes, akkor háromnál több tényező esetén sem függ az eredmény a zárójelezéstől (4.1.15. tétel), így a zárójeleket bárhová lehet tenni, vagy akár el is hagyhatóak.

3.2.7. definíció. A semleges elemet tartalmazó félcsoportot **egységelemes félcsoporthnak** nevezzük.

3.2.8. definíció. Ha egy $(S; \oplus)$ egységelemes félcsoporthoz 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 elemek ugyanaz az elem bal és jobb oldali inverze, 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 félcsoporthoz egy elemnek létezik bal és jobb oldali inverze, akkor azok megegyeznek, így az inverz egyértelmű.

3.2.9. definíció. A $(G; \oplus)$ egységelemes félcsoportot **csoportnak** nevezzük, ha minden elemnek létezik inverze.

A $(G; \oplus)$ algebrai struktúra tehát pontosan akkor csoport, ha

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

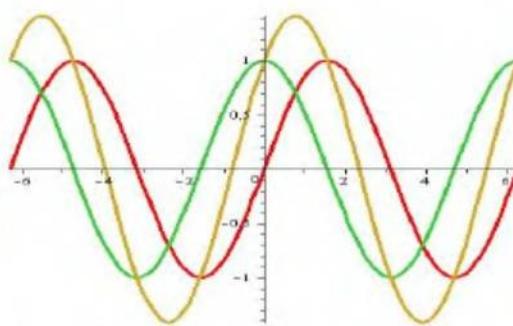
3.2.10. definíció. Az $(A; \oplus)$ grupoidban az $a \in A$ és $b \in A$ elemek felcserélhetők, ha $a \oplus b = b \oplus a$.

3.2.11. definíció. Az $(A; \oplus)$ grupoidban a művelet **kommutatív**, ha minden elem felcserélhető.

Kommutatív félcsoporthoz a többtényezős szorzatok függetlenek a tényezők sorrendjétől.

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

3.6. példa. (1) Tetszőleges H halmazra a $(\wp(H); \cap)$ és az $(\{\text{IGAZ}, \text{HAMIS}\}; \wedge)$ algebrai struktúrák kommutatív egységelemes félcsoporthoz. (2) A 3.3. ábrán látható algebrai struktúra kommutatív csoport, az ún. Klein-féle csoport. (3) $(\mathbb{Z}; +)$ Abel-csoport. (4) $(\mathbb{Z}; \cdot)$ egységelemes félcsoporthoz az 1 egységelemmel.



3.5. ábra. A $\sin(x)$ és $\cos(x)$ valós függvények pontonkénti összege a $[-2\pi, 2\pi]$ intervallumban.

Függvények között is értelmezhetünk műveleteket.

3.2.13. definíció. Legyen A_1, A_2 tetszőleges halmaz és $(B; \oplus)$ egy algebrai struktúra. Ekkor az $f \in A_1 \rightarrow B$ és $g \in A_2 \rightarrow B$ függvények közötti („pontonkénti”) műveletet azt a $h \in A_1 \cap A_2 \rightarrow B$ függvényt értjük, melyre minden $x \in A_1 \cap A_2$ -re

$$h(x) = f(x) \oplus g(x).$$

3.7. példa. Tekintsük a $f = \sin(x)$ és $g = \cos(x)$ valós függvényeket. Ekkor pontonkénti összegük a $[-2\pi, 2\pi]$ intervallumban a 3.5. ábrán látható.

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.

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

$$\begin{aligned} a \otimes (b \oplus c) &= (a \otimes b) \oplus (a \otimes c), \quad \text{illetve} \\ (a \oplus b) \otimes c &= (a \otimes c) \oplus (b \otimes c), \end{aligned}$$

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

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

3.2.15. 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** nevezzük, és 0-val jelöljük. Ha létezik a \otimes műveletre semleges elem, akkor ezt az elemet **egységelemnek**, a gyűrűt **egységelementes gyűrűnek** nevezzük. Az egységelementet 1-gyel vagy e-vel jelöljük.

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

A későbbiekben bebizonyítjuk, hogy $(\mathbb{Z}; +, \cdot)$ a szokásos műveletekkel kommutatív gyűrű.

Ellenőrző kérdés. Gyűrű-e a páros egészek $(2\mathbb{Z}; +, \cdot)$ struktúrája a szokásos műveletekkel?

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 **zérogyűrüknek** nevezzük. Észrevehetjük, hogy a zérogyűrű tetszőleges sok elemet tartalmazhat.

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 minden oldalhoz hozzáadva az $a \otimes 0$ elem \oplus műveletre vett inverzét, adódik, hogy $a \otimes 0 = 0$. Bizonyos esetekben ennek megfordítása is igaz:

3.2.17. definíció. Ha egy gyűrű bármely a, b elemére $a \otimes b = 0 \Rightarrow (a = 0 \text{ vagy } b = 0)$, akkor a gyűrűt **nulosztómentesnek** 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 **nulosztónak**, az a, b párt **nulosztópárnak** nevezzük. Nulosztómentes 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.

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

3.8. példa. Legyen H legalább kételemű halmaz. Ekkor a $(\wp(H); \Delta, \cap)$ struktúra kommutatív egységelemes gyűrű a \emptyset nullemmel (Δ a szimmetrikus differencia művelete). Figyeljük meg, hogy ekkor két nem-nulla elem „szorzata” (metszete) lehet nulla, vagyis a struktúra nem integritási tartomány.

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

3.2.19. 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.

3.9. példa. Később bebizonyítjuk, hogy a racionális és valós számok testet alkotnak a szokásos összeadás és szorzás műveleteire nézve.

3.10. példa. Láttuk, hogy tetszőleges $H \neq \emptyset$ halmazra a $(\wp(H); \Delta, \cap)$ struktúra gyűrű. Amennyiben H egyetlen elemet tartalmaz, akkor a struktúra test.

3.11. példa. minden $n \geq 2$ egészre legyen $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$. Ezen a halmazon definiálunk két műveletet: $a +_n b$ legyen az a \mathbb{Z}_n -beli elem, amit úgy kapunk, hogy az $a + b$ összeget elosztjuk n -el, és vesszük a maradékot. Hasonlóan, $a \cdot_n b$ legyen az a \mathbb{Z}_n -beli elem, amit úgy kapunk, hogy az $a \cdot b$ szorzatot elosztjuk n -el, és vesszük a maradékot. Ekkor $(\mathbb{Z}_2; +_2, \cdot_2)$ és $(\mathbb{Z}_3; +_3, \cdot_3)$ test, ahol utóbbi műveleti táblái

$+_3$	0	1	2	\cdot_3	1	2
0	0	1	2	1	1	2
1	1	2	0	2	2	1
2	2	0	1			

$(\mathbb{Z}_4; +_4, \cdot_4)$ azonban nem test, sőt, nem is integritási tartomány, hiszen nulosztópárt tartalmaz: $2 \cdot_4 2 = 0$.

3.2.2. Külső művelet

A belső műveletek mellett az ún. **külső műveletek** is fontos struktúrákat eredményeznek. A nem-üres A halmazhoz itt egy további nem-üres 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.

3.2.20. definíció. Az A halmazon és az Ω operátortartományon ($A \cap \Omega = \emptyset$) értelmezett $\circ : \Omega^n \times A \rightarrow A$, $(\omega_1, \dots, \omega_n, a) \mapsto b$ ($\omega_i \in \Omega, a, b \in A$) függvényt **n -változós külső műveletnek** nevezzük ($n \in \mathbb{N}$). Azt a struktúrát, melyre külső összekapcsolás definiálva van, (Ω^n, A, \circ) -rel jelöljük.

Az $n = 0$ esetben egyváltozós belső műveletet kapunk. Az $n = 1$ eset kiemelt fontosságú a lineáris algebra felépítésében, így most csak ezzel foglalkozunk. Általában gyűrűket és testeket alkalmazunk mint operátortartományokat, és gyakran A -ra vonatkozó külső műveletről beszélünk.

3.2.21. definíció. Legyen $(A; +)$ kommutatív csoport, $(\Omega; \oplus, \otimes)$ gyűrű, és legyen értelmezve rajtuk egy (Ω, A, \circ) külső összekapcsolás. Ekkor A -t (bal oldali) **Ω -modulusnak** nevezzük, ha minden $\omega, \mu \in \Omega$ és $a, b \in A$ esetén

- I. $\omega \circ (a + b) = (\omega \circ a) + (\omega \circ b)$
- II. $(\omega \oplus \mu) \circ a = (\omega \circ a) + (\mu \circ a)$
- III. $(\omega \otimes \mu) \circ a = \omega \circ (\mu \circ a)$.

Ha a gyűrű egységelemes, akkor minden $a \in A$ esetén teljesülni kell az alábbinak:

$$\text{IV. } 1 \circ a = a.$$

Az I–III. tulajdonságok szabályozzák az összekapcsolások összeférhetőségét.

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

3.2.22. 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.

3.12. példa. A sík és a tér vektorai a szokásos összeadásra és számmal való szorzásra nézve vektorteret alkotnak a valós (racionális) számok teste felett.

Gyakorlatok

3.2-1. Hány nullér, unér, illetve binér művelet definiálható 1, 2, illetve háromelemű halmazokon?

3.2-2. Hányféleképpen lehet műveletet definiálni egy 3 és egy 4 elemű halmazon úgy, hogy

- (1) egységelemes félcsoport legyen,
- (2) csoport legyen,
- (3) Abel-csoport legyen?

3.2-3. A *latin négyzet* egy $n \times n$ -es táblázat, amelynek soraiban és oszlopaiban n különböző elem (szimbólum) szerepel oly módon, hogy ezek mindenike minden sorban és minden oszlopban pontosan egyszer fordul elő. Az elnevezés EULER-től származik, aki latin betűket használt szimbólumokként. Mutassuk meg, hogy bármely csoport Cayleytáblázata latin négyzet.

3.2-4. Bizonyítsuk be, hogy tetszőleges A halmaz esetén a

- (1) $(\wp(A); \cup)$ struktúra kommutatív egységelemes félcsoport,
- (2) $(\{\text{IGAZ}, \text{HAMIS}\}; \vee)$ struktúra kommutatív egységelemes félcsoport,
- (3) $(\wp(A); \Delta)$ struktúra kommutatív csoport,
- (4) $(\{\text{IGAZ}, \text{HAMIS}\}; \Leftrightarrow)$ struktúra kommutatív csoport.

3.2-5. Tetszőleges A nem-üres halmaz esetén a $(\wp(A); \setminus)$ struktúrában milyen tulajdonságok érvényesek?

3.2-6. Bizonyítsuk be, hogy az $(\{\text{IGAZ}, \text{HAMIS}\}; \Leftrightarrow, \vee)$ struktúra test.

3.3. Többszörös 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.

3.3.1. Rendezett integritási tartomány

3.3.1. 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.

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

Az alapstruktúrból új struktúrák konstruálhatók. Ennek három lényegesen különböző módoszata 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 strukturált halmazok Descartes-szorzatát tekintjük, az alapstruktúrákat komponensenként rendelve egymás-hoz.

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:

3.3.3. 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

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

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

Tanulmányaink során bőven látunk példákat mindenekkel említett konstrukcióra. Íze-lítőül tekintsünk egy szorzatstruktúrát a rendezési struktúrák közül.

3.13. példa. Legyen $(A; \leq_1)$ 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 részben-rendezett 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:

$$(a_1, b_1) \leq_4 (a_2, b_2), \quad := \quad (a_1 <_1 a_2) \vee (a_1 = a_2 \wedge b_1 \leq_2 b_2).$$

Ekkor $(A \times B; \leq_4)$ újra egy részbenrendezés. Viszont most ha A és B teljesen rendezett, illetve jólrendezett, akkor $A \times B$ is teljesen illetve jólrendezett.

Az iménti példában látott rendezési konstrukciónak (\leq_4) különlegesen fontos szerepe van az informatikában.

3.3.2. Lexikografikus rendezés

3.3.4. definíció. Legyen $n \in \mathbb{N}$, $(A_1; \leq_1), \dots, (A_n; \leq_n)$ pedig tetszőleges rendezett halmazok. Az $A_1 \times \dots \times A_n$ halmaz **lexikografikus rendezése** az alábbi \leq reláció:

$$(a_1, \dots, a_n) \leq (b_1, \dots, b_n) \Leftrightarrow \begin{aligned} &(a_1, \dots, a_n) = (b_1, \dots, b_n), \text{ vagy} \\ &\text{van olyan } i \ (1 \leq i \leq n), \text{ amelyre} \\ &a_1 = b_1, \dots, a_{i-1} = b_{i-1} \text{ és } a_i <_i b_i. \end{aligned}$$

3.14. példa. Legyen A a magyar ábécé betűinek halmaza, $<$ pedig a szokásos ábécésorrend ($a < \text{\'a} < b < \dots$). Ekkor A^n -en a lexikografikus rendezés az n -betűs „szavak” ábécérendbe szedését adja.

Ellenőrző kérdés. Legyen adott egy A ábécé, és legyenek X elemei az A betűiből álló szavak (stringek). X elemein készítsünk egy \leq relációt úgy, hogy legyen $x \leq y$, ha x rövidebb, mint y (kevesebb betűből áll), ha pedig egyenlő hosszúak, akkor x lexikografikus rendezés szerint kisebb, mint y . Mit kaptunk?

3.3.3. Kapcsolat struktúrák között

Függvények segítségével strukturált halmazok között is létesíthetünk összefüggéseket. Lényeges szempont ugyanakkor, hogy a függvény mindenekkel struktúrával összeférjen. Ilyen, a struktúra szempontjából összeférő leképezéseket **homomorfizmusoknak** vagy **művelettartó leképezéseknek** nevezzük. A struktúra lényeges jellegzetességei ekkor megőrződnek (például a csoport tulajdonság csoport-homomorfizmusoknál). Kiemelten

fontos homomorfizmusok azok, amelyek bijektívek. Ezeket **izomorfizmusoknak** nevezzük. Izomorfizmus esetén a struktúrák a műveletek szempontjából megkülönböztethetetlenek. A számfogalom felépítésekor (kétnyelvű algebrai struktúrák között) az alábbi fogalmat fogjuk felhasználni.

3.3.5. definíció. Az $(A; +, \cdot)$ algebrai struktúrát **beágyazzuk** a $(B; \oplus, \otimes)$ algebrai struktúrába, ha megadható olyan $C \subset B$ halmaz és $\varphi : A \rightarrow C$ 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 típusú algebrai struktúrák között is értelmezhető.

Gyakorlatok

3.3-1. Adjunk példát az informatika világából a lexikografikus rendezésre.

3.3-2. Legyen $(F; \oplus, \otimes)$ test és $(F; \leq)$ rendezett integritási tartomány az alábbi tulajdonsággal: létezik $F_1 \subset F$, melyre

- (1) $(F_1; \oplus, \otimes)$ test (F részteste),
- (2) $F_1 \cup (-F_1) = F$,
- (3) $F_1 \cap (-F_1) = \{0\}$.

Bizonyítsuk be, hogy ekkor $(F; \oplus, \otimes; \leq)$ rendezett test.

3.3-3. Legyen A egy rendezett test valamely nem-üres részhalmaza. Mutassuk meg, hogy A pontosan akkor felülről korlátos, ha $-A$ alulról korlátos, és ekkor $\inf(-A) = -\sup(A)$.

3.4. Speciális struktúrák

3.4.1. Polinomok

A polinomok kiemelkedő szerepet játszanak a matematikában. A ???. fejezetben részletesen foglalkozunk velük, most csak a polinomstruktúrák lényegesebb fogalmait emeljük ki. Szemléletesen, polinomnak nevezünk egy olyan kifejezést, amely valamilyen számkörből vett számokból és valamilyen szimbólum(ok)ból készül véges sok ismételt összeadás, kivonás és szorzás segítségével.

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

$$f = a_0 + a_1x + \cdots + a_nx^n \quad (a_i \in R, n \in \mathbb{N}) \quad (3.1)$$

alakú formális kifejezések azzal a megállapodással, hogy $n \leq m$ esetén az $a_0 + a_1x + \cdots + a_nx^n$ és a $b_0 + b_1x + \cdots + b_mx^m$ ($a_i, b_j \in R$) kifejezések pontosan akkor jelölik ugyanazt a polinomot, ha $a_0 = b_0, a_1 = b_1, \dots, a_n = b_n$ és $b_{n+1} = \cdots = b_m = 0$.

(3.1)-ben az $a_0, a_1, \dots, a_n \in R$ értékeket **együttthatóknak** 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.

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

3.15. példa. Tekintsük az $f(x) = x^4 - 17x^3 + 101x^2 - 247x + 210 \in \mathbb{Z}[x]$ polinomot. Ekkor $f(x)$ negyedfokú ($\deg(f) = 4$), főpolinom, hiszen főegyütthatója 1, a polinom gyökei a $2, 3, 5, 7 \in \mathbb{Z}$, mert $f(2) = f(3) = f(5) = f(7) = 0$. A $g(x) = x^2 + 1 \in \mathbb{Z}[x]$ polinomnak nincs sem egész, sem racionális, sőt, még valós gyöke sem. Mindez könnyen ellenőrizhető a másodfokú egyenlet megoldóképletét alkalmazva, a diszkrimináns negatív lesz.

A későbbiekbén definiálni fogjuk polinomok \oplus összegét és \otimes szorzatát. Bebizonyítjuk, hogy tetszőleges R gyűrű esetén $(R[x]; \oplus, \otimes)$ szintén gyűrűt alkot. Sőt, ha R kommutatív, egységelemes, vagy nulosztómentes, akkor $R[x]$ is teljesíti ugyanazokat a tulajdon-ságokat.

3.4.3. definíció. Legyen R gyűrű és $f \in R[x]$. Ekkor azt az $R \rightarrow R$ függvényt, ami minden $c \in R$ -hez $f(c)$ -t rendeli, az f polinomhoz tartozó **polinomfüggvénynek** nevezzük.

Tetszőleges f és g $R[x]$ -beli polinomokhoz tartozó polinomfüggvényt akkor tekintünk egyenlőnek, ha $f(c) = g(c)$ minden $c \in R$ esetén teljesül.

3.16. példa. Az $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ ($a_i \in R$) polinomfüggvények közül azokat, melyeknek foka legfeljebb egy, **lineáris függvényeknek** nevezzük. Beszélhetünk másodfokú, harmadfokú, stb., n -edfokú polinomfüggvényekről. A **racionális függvények** két polinomfüggvény hárnyadosaként kaphatók:

$$f(x) = \frac{g(x)}{h(x)},$$

ahol a függvény értelmezési tartománya azon x -ek halmaza, ahol $h(x) \neq 0$.

3.4.2. Mátrixok

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

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

$$A : \{1, \dots, m\} \times \{1, \dots, n\} \rightarrow R$$

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.

A mátrix tehát egy olyan R -beli indexelt rendszer, amelynek indexhalmaza az $I = \{1, \dots, m\} \times \{1, \dots, n\}$ Descartes-szorzat. Egy mátrixot táblázattal is megadhatunk:

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

Ekkor az $(i, j) \in \{1, \dots, m\} \times \{1, \dots, n\}$ helyen felvett $A(i, j) \in R$ függvényérték szokással 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 (vagy a j -edik oszlop i -edik elemének) nevezzük.

Mátrixok között műveleteket értelmezhetünk.

3.4.5. 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

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

3.17. példa. Legyen A, B valamely $(R; +, \cdot)$ gyűrű feletti mátrix,

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \quad \text{és} \quad B = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}.$$

Ekkor

$$C = A \oplus B = \begin{bmatrix} 1+a & 2+b & 3+c \\ 4+d & 5+e & 6+f \end{bmatrix}.$$

Az $(R^{m \times n}; \oplus)$ struktúra neutrális eleme a **zérusmátrix** (vagy nullmátrix), amelynek 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 mivel $(R; +)$ Abel-csoport, $(R^{m \times n}; \oplus)$ is az.

3.4.6. definíció. Azt mondjuk, hogy az $A \in R^{m \times n}$ és $B \in R^{k \times l}$ mátrixok **kompatibilisek**, ha $n = k$, vagyis ha A oszlopainak száma megegyezik B sorainak számával.

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

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

minden $1 \leq i \leq m$ és $1 \leq k \leq p$ esetén.

3.18. példa. Legyen A, B valamely $(R; +, \cdot)$ gyűrű feletti mátrix,

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \quad \text{és} \quad B = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}.$$

Ekkor

$$C = A \otimes B = \begin{bmatrix} a+2d+3g & b+2e+3h & c+2f+3i \\ 4a+5d+6g & 4b+5e+6h & 4c+5f+6i \\ 7a+8d+9g & 7b+8e+9h & 7c+8f+9i \end{bmatrix}.$$

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

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

Struktúrák

Belátható, hogy a mátrixszorzás disztributív. Kommutatívak természetesen csak az (n, n) -es mátrixok lehetnének, de az $n = 1$ esettől eltekintve általában nem azok. (Az $n = 1$ eset is csak akkor, ha az alapgyűrű kommutatív.)

3.19. példa. Legyen

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

Ekkor

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

3.4.8. definíció. Az $n \times n$ -es mátrixokat **négyzetes** (gyakran kvadratikus vagy n -edrendű) **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 tételeket bizonyítottuk.

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

A struktúrák tulajdonságainak származtatott struktúrára történő örököltése nem automatikus.

3.20. 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).

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

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

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

Gyakorlatok

3.4-1. Adjunk példát egy 2×2 -es egész mátrixok feletti harmadfokú polinomra, és egy másodfokú egész polinomok feletti 3×3 -as mátrixra.

3.4-2. 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

Láttuk, hogy 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 műveettel rendelkező) algebrai struktúrává válik.

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

4. A számfogalom felépítése

Ha a minden napjai életben használt számokkal való számolást szeretnénk megalapozni, akkor kiindulhatunk a legátfogóbb számtartományból, és részstruktúrák vizsgálatára szorítkozhatunk, vagy mint az alábbiakban, a természetes számok axiomatikus felépítése után egyre bővebb struktúrákba ágyazzuk a keletkezetteket.

4.1. Természetes számok

4.1.1. A 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 **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-t 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 nevezik.

4.1.1. tétele. *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 $M = \mathbb{N}$. ■

4.1.2. tétele. *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

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

A számfogalom felépítése

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

A 4.1.1. és 4.1.2. tételek miatt a rákövetkezési relációval a 0 alapfogalomból a többi természetes számot explicit módon lehet definiálni:

4.1.3. definíció. $1 := 0'$, $2 := 1'$, $3 := 2'$

Az így konstruált halmazt a **természetes számok halmazának** nevezik és \mathbb{N} -nel jelöljük. Megmutatható, hogy az axiomatikus halmazelmélet végtelenségi axiómája (lásd 2.4 rész (7) axióma) által definiált halmaz, azaz a

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

halmaz teljesíti a Peano-axiómákat, ilyen halmaz tehát létezik.

Az alábbi tétel \mathbb{N} -en értelmezett függvények **rekurzióval** való megadásának módszert tárgyalja.

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

A rekurziótétel segítségével belátható, hogy \mathbb{N} létezése egyértelmű.

Ellenőrző feladat. Adjunk példát, amikor g nem szürjektív.

A teljes indukció kitüntetett szerepet játszik a matematikában, a bizonyítási technikák egy kiemelkedően fontos esete.

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

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

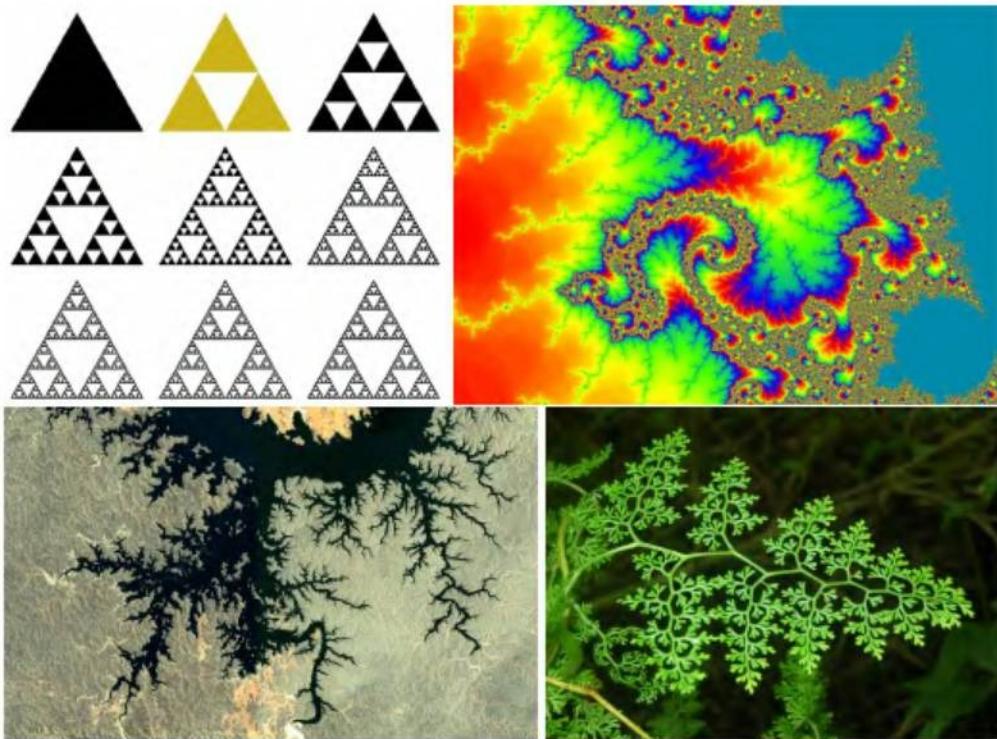
Teljes indukcióval bizonyítunk. Az $n = 2$ eset a már látott De Morgan szabály. Tegyük fel, hogy $2 \leq k < n$ -re igaz az állítás (indukciós feltétel). Bebizonyítjuk, hogy ekkor $k + 1$ -re is igaz:

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

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

A rekurzió a matematikában gyakran előkerül függvényeknél, halmazoknál, önhasonló matematikai és természeti struktúrák (fraktálok) esetében (4.1. ábra).

Ellenőrző kérdés. Jellemezzük azokat a természetes számokon értelmezett függvényeket, amelyek rekurzív megadásai



4.1. ábra. A bal felső ábra az ún. Sierpinski-szönyeg. Jobb felül a Mandelbrot-halmaz egy részlete található (bővebben a komplex számoknál olvashatunk róla). Bal alul Egyiptom egy részének műholdfelvétele, jobb alul egy erdei páfrányfélé fotója látható.

- (1) $\text{fakt}(n) := n \cdot \text{fakt}(n - 1)$, $\text{fakt}(0) = 1$,
- (2) $\text{hanoi}(n) := 2 \cdot \text{hanoi}(n - 1) + 1$, $\text{hanoi}(1) = 1$.

Ezen utóbbiti függvény a Hanoi tornyai néven ismert probléma megoldásának lépésszámát írja le, ahol n a kezdeti állapot egyik rúdján lévő korongok száma. (A feladvány az alábbi: 3 rúd egyikre n darab korong van fűzve, a másik kettő üres. Az egymáson lévő korongok egyre kisebbek. Mennyi a legkevesebb szükséges lépés amivel az első rúdról a harmadik rúdra lehet juttatni a korongokat, úgy, hogy nagyobb korongot kisebb korongra tilos mozgatni?)

4.2. példa. Tekintsük az alábbi, rekurzív módon adott formulát:

- (1) minden változó (x, y, z, \dots stb.) egyben formula, amelyeket **atomi formuláknak** nevezünk.
- (2) Ha A egy formula, akkor $\neg A$ is az.
- (3) Ha A és B formulák és \circ binér logikai összekötőjel, akkor $A \circ B$ is formula.
- (4) minden formula az (1–3). szabályok véges sokszori alkalmazásával áll elő.

Az így definiált halmaz minden eleme ítéletlogikai formula, sőt, a halmaz a legszűkebb ilyen halmaz.

4.3. példa. Rekurzív megadási módot használunk a programozási nyelvek kifejezései és utasításai struktúrájához is. Például

```

<number> ::= 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
<expr> ::= <number>
          | (<expr> * <expr>)
          | (<expr> + <expr>)
  
```

Ekkor a $(7 * ((3 * 6) + 8))$ kifejezés levezethető a definícióból. A legismertebb ilyen nyelvi szintaxis megadási forma a Backus–Naur forma.

A számfogalom felépítése

4.4. példa. A rekurziókat a legtöbb programozási nyelv támogatja. Egy algoritmust akkor hívunk rekurzívnak, ha a feladatot ugyanannak a feladatnak egymást követően egyre kisebb méretű bemenetet használó példányait alkalmazva oldja meg. Az egyik legszemléletesebb példa a faktoriális számító függvény, melynek C nyelvű implementációja az alábbi:

```
int faktorialis(int n)
{
    if(n <= 1)
        return 1;
    return n * faktorialis(n-1);
}
```

A függvény tehát egy egész értékkel tér vissza, ami a bemeneti egész számtól függ, mégpedig úgy, hogy a függvény számítás közben meghívja saját magát, de egyel kisebb bemeneti paraméterrel, míg nem n el nem éri az 1-et, és a számítás véget ér. minden rekurzió ciklussá alakítható (hívási verem – angolul *call stack* – segítségével) és minden ciklus megadható rekurzív módon. Egy algoritmus implementálásának a stílusát érthetőségi és hatékonysági szempontok alapján szokták megválasztani. Vannak olyan programozási nyelvek (funkcionális nyelvek), ahol a rekurzió megvalósítása a nyelv alapvető építőköve.

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 $s_m : \mathbb{N} \rightarrow \mathbb{N}$ függvény, amelyre $s_m(0) = m$, és minden $n \in \mathbb{N}$ -re $s_m(n') = (s_m(n))'$. Az $s_m(n)$ számot $m + n$ -nel fogjuk jelölni, és az m és n természetes számok **összegének** nevezzük. Megjegyezzük, hogy az összeadásból visszakapjuk a rákövetkezést, hiszen $m' = (s_m(0))' = s_m(0') = s_m(1) = m + 1$. A továbbiakban az összeadás műveletének tulajdonságait vizsgáljuk.

4.1.5. 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 ekkor $n' \in \mathbb{N}$ -re is igaz.

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

(2) bizonyítása n szerinti indukcióval történik. $0 + n = n + 0 = n$ 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. (3) 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 $m' + n = (m + n)'$ valamelyen $n \in \mathbb{N}$ -re. Ekkor

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

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 valamelyen $n \in \mathbb{N}$ -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 $m \in \mathbb{N}$ -re létezik olyan $p_m : \mathbb{N} \rightarrow \mathbb{N}$ 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.

4.5. példa. A szorzat definíciója miatt $1 \cdot 1 = p_1(1) = p_1(0') = p_1(0) + 1 = 1$, továbbá $5 \cdot 3 = p_5(3) = p_5(2') = p_5(2) + 5 = p_5(1') + 5 = p_5(1) + 5 + 5 = p_5(0') + 10 = p_5(0) + 5 + 10 = 0 + 15 = 15$.

4.1.6. téTEL. Ha $k, m, n \in \mathbb{N}$, akkor

- (1) $k \cdot (m + n) = k \cdot m + k \cdot n$ (bal oldali disztributivitás)
- (2) $0 \cdot n = n \cdot 0 = 0$
- (3) $1 \cdot n = n \cdot 1 = n$
- (4) $(k \cdot m) \cdot n = k \cdot (m \cdot n)$ (asszociativitás)
- (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

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

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

(3) bizonyításához először megmutatjuk az alábbi állítás teljesülését:

$$m' \cdot n = m \cdot n + n \quad (4.1)$$

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 valamelyen $n \in \mathbb{N}$ -re igaz az állítás. Ekkor

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

(3) bizonyítása n szerinti indukcióval történik. Az $n = 0$ eset (2) 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 $n \cdot 1 = n$ valamelyen $n \in \mathbb{N}$ -re. Ekkor (4.1) miatt

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

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

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

(5) Az $m \cdot n = n \cdot m$ kommutativitás bizonyítása n szerinti indukcióval történik. Az $n = 0$ eset (2) miatt teljesül. Tegyük fel, hogy $n \in \mathbb{N}$ -re igaz az állítás. Ekkor (4.1)-et felhasználva

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

A jobb oldali disztributivitás a kommutativitásból adódik. ■

Az előző két téTEL következménye az alábbi

4.1.7. téTEL. $(\mathbb{N}; +)$ kommutatív félcsoport a 0 nullelemmel. $(\mathbb{N}; \cdot)$ kommutatív félcsoport az 1 egységelemmel.

A természetes számok rendezési struktúrája

4.1.8. definíció. $n \leq m := \exists k \in \mathbb{N} : n + k = m$.

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

4.1.9. tételel (monotonia tételei). *Minden $m, n, k \in \mathbb{N}$ -re*

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

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 4.1.8. 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 tételel egyenlőségre vonatkozó állításai az alábbi

4.1.10. tételel (egyszerűsítési szabályok).

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

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

Sorozatok, összegek, szorzatok

4.1.11. definíció. Legyen H egy nem-üres halmaz. A természetes számok \mathbb{N} halma-zán értelmezett H -ba képező függvényeket **H -beli sorozatoknak** nevezik. Az $n \in \mathbb{N}$ számhoz rendelt elemet a sorozat n -edik tagjának hívjuk.

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 tagja, csak első, második, stb.

4.1.12. definíció. Egy n hosszúságú (véges) sorozaton olyan f függvényt értünk, amelynek az értelmezési tartománya a $\{0, 1, \dots, n-1\}$ halmaz.

Ezeket a sorozatokat gyakran értékeik felsorolásával jelöljük:

$$\langle f(0), f(1), \dots, f(n-1) \rangle.$$

4.1.1. megjegyzés. Véges sorozatok $\{1, \dots, n\}$ -en is értelmezhetők.

4.6. példa. A véges sorozat fogalma nagyon lényeges a számítástudományban, ahol 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 (általában) $V[n]$ jelöli.

A számfogalom felépítése

4.7. példa. Legyen A egy tetszőleges, legalább kételemű halmaz, amit ábécének fogunk nevezni. Az összes, A elemeiből képezhető véges sorozatok (amelyeket szavaknak nevezünk) egységelemes félcsoportot alkotnak a konkatenáció (egymás után írás) műveletére nézve, ahol az üres szó az egységelem. Ha tehát $a = a_1 a_2 \dots a_n$ és $b = b_1 b_2 \dots b_m$ szavak (a betűket elválasztó vesszőket nem szokás jelezni), akkor $ab = a_1 a_2 \dots a_n b_1 b_2 \dots b_m$. Az így definiált félcsoport nem kommutatív.

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

4.1.13. definíció.

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

4.8. példa. Tekintsük az $(\mathbb{Z}; +)$ csoportot. Ekkor $\sum_{i=6}^2 i = -12$, $\sum_{i=0}^5 (i+1) = 21$.

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

4.1.14. definíció.

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

Ha az összeg minden **tagja** ugyanaz az $a \in G$ elem, a szokásos jelölés szerint

$$\sum_{i=m}^{m+n-1} a = na,$$

ahol n ekkor az $a \in G$ elem együtthatója. Hasonlóan, ha a szorzat minden **tényezője** ugyanaz az $a \in G$ szám, akkor ezt úgy jelöljük, hogy

$$\prod_{i=m}^{m+n-1} a = a^n,$$

ahol a az alap, n a kitevő, míg a^n a hatvány. Az összegek esetében **additív írásmód-ról**, a szorzatok esetében **multiplikatív írásmód ról** 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 tételek a lehető legáltalánosabban fogalmazzuk meg.

4.1.15. 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 $a_1, \dots, a_m, b_1, \dots, b_n, \dots, z_1, \dots, z_t \in R$ eleme-

ire

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

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

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

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

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

Ha $i = k - 1$, akkor a második lépés szükségtelen, így az első sor jobb oldala és a harmadik sor azonos. Azt kaptuk, hogy bármely félcsoportban 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 általános asszociativitást teljes mértékben kihasználtuk.

(3) Csak a 2 tényezős esetet bizonyítjuk, a több tényezős eset bizonyítása indukcióval történik, amit 4.1-6. gyakorlatra hagyunk. Ha tehát 2 tényezőnk van, akkor n szerinti indukcióval

$$\begin{aligned} \left(\sum_{i=1}^m a_i \right) \left(\sum_{j=1}^n b_j \right) &= \left(\sum_{i=1}^m a_i \right) \left(\sum_{j=1}^{n-1} b_j + b_n \right) \\ &= \left(\sum_{i=1}^m a_i \right) \left(\sum_{j=1}^{n-1} b_j \right) + \left(\sum_{i=1}^m a_i \right) b_n \\ &= \sum_{i=1}^m \sum_{j=1}^{n-1} a_i b_j + \sum_{i=1}^m a_i b_n \\ &= \sum_{i=1}^m \sum_{j=1}^n a_i b_j. \end{aligned}$$

A bizonyítást befejeztük. ■

A számfogalom felépítése

4.9. példa. *Számtoni sorozatoknak* nevezzük azokat a sorozatokat, amelyekben (a második-tól kezdve) bármelyik tag és az azt megelőző tag különbsége állandó, vagyis $a_n - a_{n-1} = d$, ha $n > 1$. A sorozat d -vel jelölt különbségét **differenciának** nevezzük. A sorozat n -edik elemére nem csak rekurzív, hanem explicit képlet is adható:

$$a_n = a_1 + (n-1) \cdot d.$$

A számtoni sorozat első n tagjának

$$S_n = \frac{(2a_1 + (n-1)d) \cdot n}{2}$$

összegét már Leonardo Pisano (ismertebb nevén Fibonacci) is ismerte (Liber Abaci; 1202, II/12).

Gyakorlatok

4.1-1. Mutassuk meg, hogy minden $n \in \mathbb{N}$ -re

- a) $\sum_{k=1}^n k = \frac{n(n+1)}{2},$
- b) $\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6},$
- c) $\sum_{k=1}^n k^3 = \left(\frac{n(n+1)}{2}\right)^2,$
- d) $\sum_{k=1}^n (2k-1) = n^2,$
- e) $\sum_{k=1}^n (2k-1)^2 = \frac{n(4n^2-1)}{3},$
- f) $\sum_{k=1}^n k(k+1) = \frac{n(n+1)(n+2)}{3},$
- g) $\sum_{k=1}^n k(3k+1) = n(n+1)^2,$
- h) $\sum_{k=1}^n \frac{1}{k(k-1)} = \frac{n-1}{n},$
- i) $\sum_{k=1}^n \frac{1}{k^2} < \frac{2n-1}{n} \quad (k \geq 1),$
- j) $\sum_{k=1}^n \frac{1}{4k^2-1} = \frac{1}{2} \left(1 - \frac{1}{2n+1}\right),$
- k) $\sum_{k=1}^n (k-1)^2 < \frac{n^3}{3},$
- l) $\sum_{k=0}^n q^k = \frac{q^{n+1}-1}{q-1} \quad (q \neq 1),$
- m) $\sum_{k=1}^n \frac{1}{n+k} > \frac{13}{24} \quad (n > 1),$
- n) $\prod_{k=1}^n \left(1 + \frac{1}{k}\right) = n + 1.$

4.1-2. Hozzuk egyszerűbb alakra az alábbi összeget:

$$\sum_{k=1}^n k^4.$$

4.1-3. Mutassuk meg, hogy minden $a_k \in \mathbb{N}^+$ sorozatra

$$\sum_{k=1}^n a_k \cdot \sum_{k=1}^n \frac{1}{a_k} \geq n^2.$$

4.1-4. Mutassuk meg, hogy

- a) minden $n \geq 9$ esetén $2^{2n} \leq n \cdot (n-1) \cdots 2 \cdot 1$,
- b) minden $n \geq 4$ esetén $3^n > n^3$,
- c) minden $n \geq 5$ esetén $2^n > n^2$,
- d) minden $n \geq 4$ esetén $3^n > 2^n + 7n$,
- e) minden $n \geq 3$ esetén $\left(1 + \frac{1}{n}\right)^n > 2$,
- f) minden $n \geq 2$ esetén $\frac{(n+1)^n}{n^n} > 2$.

4.1-5. Bizonyítsuk be, hogy $(\mathbb{N}; \leq)$

- (1) gyengén trichotom,
- (2) teljes rendezés,
- (3) jólrendezés.

4.1-6. Bizonyítsuk be az általános disztributivitás tételeit.

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:

$$(n_1, m_1) \varrho (n_2, m_2) := n_1 + m_2 = n_2 + m_1.$$

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

4.10. példa. $(3, 8) \in [(1, 6)]$, mivel $(3, 8) \varrho (1, 6)$.

A számfogalom felépítése

4.2.1. definíció. $\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/\varrho = \{[(n, m)] \mid (n, m) \in \mathbb{N} \times \mathbb{N}\}$.

4.2.2. Műveletek, rendezésük

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

4.2.2. definíció.

$$\begin{aligned} [(n, m)] \oplus [(k, l)] &:= [(n + k, m + l)], \\ [(n, m)] \odot [(k, l)] &:= [(nk + ml, nl + mk)]. \end{aligned}$$

Az így definiált műveletek kommutativitása, asszociativitása és disztributivitása az \mathbb{N} -ben érvényes műveletek tulajdonságai alapján könnyen belátható. Ennél több is igaz: az $[(n, m)] \oplus x = [(k, l)]$ egyenlet tetszőleges $[(n, m)]$ és $[(k, l)]$ esetén egyértelműen megoldható, a megoldás a (4.2.2) definíció és ϱ definíciója, valamint a 4.1.10. 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. \mathbb{Z} -ben tehát az összeadást, kivonást és a szorzást korlátozás nélkül el lehet végezni. Fennmarad a kérdés, hogy \mathbb{N} -et valóban beágyaztuk-e \mathbb{Z} -be.

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

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

továbbá

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

Ha $\varphi(n) = \varphi(m)$, akkor $[(n, 0)] = [(m, 0)]$, így a 4.2.1. 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, továbbá $+t$ -t írunk \oplus helyett. Az $a+x = b$ egyenlet egyértelmű x megoldását $b-a$ -val jelöljük. 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 nullosztómentes, ezért \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.

4.2.3. definíció. $a \leq b := b - a \in \mathbb{N}$.

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 számegebenesen 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 beleírtjük, a szokásos jelölés \mathbb{Z}_0^- és \mathbb{Z}_0^+ . Az eddigiek alapján tehát kijelenthetjük, hogy $\mathbb{N} = \mathbb{Z}_0^+$.

Ellenőrző kérdés. Az előző fejezetben megmutattuk, hogy minden jólrendezett halmaz lánc. Igaz-e az állítás megfordítása?

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 minden természetes szám, ezt a **abszolút értéknek** nevezzük, és $|a|$ -kel jelöljük.

4.2.4. definíció.

$$|a| := \begin{cases} a & \text{ha } a \geq 0 \\ -a & \text{ha } a < 0. \end{cases}$$

4.2.5. téTEL. Számolási szabályok \mathbb{Z} -ben:

- (1) $a \in \mathbb{Z}_0^+ \wedge b \in \mathbb{Z}_0^- \wedge |a| \geq |b| \Rightarrow a + b = |a| - |b|$
- (2) $a \in \mathbb{Z}_0^+ \wedge b \in \mathbb{Z}_0^- \wedge |a| \leq |b| \Rightarrow a + b = -(|b| - |a|)$
- (3) $a \in \mathbb{Z}_0^- \wedge b \in \mathbb{Z}_0^- \Rightarrow a + b = -(|a| + |b|)$
- (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) $a \in \mathbb{Z}_0^- \wedge b \in \mathbb{Z}_0^- \Rightarrow ab = |a| \cdot |b|$
- (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) $a \neq 0 \Rightarrow a^2 \in \mathbb{Z}^+$.

Bizonyítás. Az (1)–(4) állítások bizonyítását az Olvasóra hagyjuk. (5) bizonyítása: $a = [(a, 0)]$ és $b = [(0, |b|)]$ miatt $ab = [(a, 0)] \cdot [(0, |b|)] = [(0, a \cdot |b|)] = -(a \cdot |b|) = -(|a| \cdot |b|)$. (6) abból következik, hogy $a = [(0, |a|)]$ és $b = [(0, |b|)]$, ezért $ab = [(0, |a|)] \cdot [(0, |b|)] = [(|a| \cdot |b|, 0)] = |a| \cdot |b|$. (7) bizonyítása egyszerű számolással adódik. (8) bizonyítása: $a = [(a, 0)]$, $b = [(b, 0)]$ miatt $ab = [(ab, 0)]$, amiből az állítás következik. (9)-et úgy bizonyíthatjuk, hogy észrevesszük, $b - a > b - b = 0$, amiből $(b - a)c > 0$, így $bc = (b - a)c + ac > 0 + ac = ac$. (10) bizonyítása (9)-hez hasonlóan megy. (11)-hez először feltesszük, hogy $a \in \mathbb{Z}^+$, vagyis $a = [(a, 0)]$. Ekkor $a^2 = a \cdot a = [(a \cdot a, 0)]$, így $a^2 \in \mathbb{Z}^+$. Ha pedig $a \in \mathbb{Z}^-$, akkor $a^2 = [(0, |a|)] \cdot [(0, |a|)] = [(|a| \cdot |a|, 0)] = [(a \cdot a, 0)]$, vagyis $a^2 \in \mathbb{Z}^+$. ■

A gyakorlat (7),(9),(10) állításai a \mathbb{Z} -beli műveletek monotonitását jelentik, ezért a 3.3.1. definíciónak megfelelően azt is mondhatjuk, hogy

4.2.6. téTEL. $(\mathbb{Z}; +, \cdot; \leq)$ rendezett integritási tartomány.

Gyakorlatok

4.2-1. Sokan ismerik az alábbi trükköt: „Gondolj egy egész számot, adj hozzá ötöt, az eredményt szorozd meg kettővel, a kapott számból vonj ki hatot, az eredményt oszd el kettővel, és végül vonj ki a kapott számból egyet. Mond meg mit kaptál és én megmondom, mely számra gondoltál.” A gondolt számot x -szel jelölve adjuk meg a végeredményt x függvényeként. Lebbentsük fel a fátylvat a varázslatról.

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 additív semleges elemek minden esetre kitüntetett szerepe van, hiszen $\forall c (c \in \mathbb{Z} \Rightarrow c \cdot 0 = 0)$. A $0x = a$ egyenletet $a \neq 0$ esetén egyáltalán nem lehet megoldani, míg $a = 0$ esetén a megoldás nem egyértelmű. 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 $a_1b_2 = a_2b_1$ következik.

$$(a_1, b_1)\vartheta(a_2, b_2) := a_1b_2 = a_2b_1.$$

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

4.3.1. definíció. $\mathbb{Q} := (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \vartheta = \{[(a, b)] \mid (a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\}$.

\mathbb{Q} elemeit *racionális számoknak* nevezzük¹.

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.

4.3.2. definíció.

$$\begin{aligned} [(a, b)] \oplus [(c, d)] &:= [(ad + bc, bd)], \\ [(a, b)] \odot [(c, d)] &:= [(ac, bd)]. \end{aligned}$$

Könnyű belátni, hogy $(\mathbb{Q}; \oplus)$ kommutatív csoport a $[(0, 1)]$ semleges elemmel, továbbá az $[(a, b)]$ -hez tartozó, az összeadásra vonatkozó inverz elem $\ominus[(a, b)] = [(-a, b)]$. Ekkor az $[(a, b)]$ és a $[(c, d)]$ elemek különbségén az $[(a, b)] \oplus (\ominus[(c, d)])$ elemet értjük. A $(\mathbb{Q} \setminus \{(0, 1)\}; \odot)$ 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 disztributív törvények is igazak, ezért $(\mathbb{Q}; \oplus, \odot)$ *test*.

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

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

¹A ratio latin kifejezés, arányt, hányadost jelent.

és

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

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, valamint $+t$ -t írhatunk \oplus és ‘·’-ot \odot helyett. minden $[(a, b)]$ racionális szám egy $b \cdot x = a$ alakú egyenlet megoldása, ezért egész számok hányadosaként írható. A szokásos jelölés szerint

$$\frac{a}{b} (= a/b) := [(a, b)].$$

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 beleérjük, akkor \mathbb{Q}_0^+ -t, illetve \mathbb{Q}_0^- -t írunk.

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

4.3.3. definíció. $p \leq q := q - p \in \mathbb{Q}_0^+$.

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 monotoníára vonatkozó törvények (4.2-1. gyakorlat (2),(4) pontjai) \mathbb{Q} -ban is érvényesek. Ezért a 3.3.2. definíciónak megfelelően

4.3.4. téTEL. $(\mathbb{Q}; +, \cdot, \leq)$ rendezett test.

De ennél több is igaz.

4.3.5. 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 $na \geq b$.

4.3.6. téTEL. $(\mathbb{Q}; +, \cdot, \leq)$ arkhimédeszi tulajdonságú.

Bizonyítás. A definíció jelöléseit alkalmazva, amennyiben $b \leq 0$, az $n = 0$ választás megfelelő. Ha pedig $0 < b = w/z$ és $a = x/y$, ahol $x, y, z, w \in \mathbb{N}^+$, akkor az $n \geq yw$ választás esetén $na \geq b$. ■

A \mathbb{Q} -beli rendezés számos fontos és érdekes tulajdonsággal rendelkezik. 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. Igaz továbbá az is, hogy

$$p \leq q \Rightarrow \frac{p}{r} \leq \frac{q}{r}, \quad (p, q, r \in \mathbb{Q}, r > 0).$$



Minden pozitív racionális szám felírható véges sok pozitív egész reciprokának összegeként. Például

$$\frac{5}{121} = \frac{1}{33} + \frac{1}{121} + \frac{1}{363}.$$

Sőt, minden pozitív racionális számnak végtelen sok ilyen formájú, különböző felírása lehetséges. Ezt az alakot **egyiptomi törtnek** is nevezik, mivel már az ókori Egyiptomban is használták. Adjunk hatékony algoritmust egy pozitív racionális szám legkevesebb tagot tartalmazó egyiptomi tört alakjának meghatározására. Adjunk algoritmust egy $4/n$ alakú tört

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$$

felírásának meghatározására ($n, x, y, z \in \mathbb{N}^+$). Ez utóbbi esetben még nem bizonyított, hogy minden van ilyen felírás (Erdős—Straus-sejtés), de $n < 10^{14}$ -ig számítógéppel ellenőrizték.

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 PITHAGORASZ szerint az egységnyi oldalú négyzet átlójának hossza nem racionális szám. Meg lehet adni közelítő értékek egy sorozatát ($1, 1.4, 1.41, 1.414, \dots$), mégis, az $\{x \in \mathbb{Q} \mid x^2 < 2\}$ halmaznak (\mathbb{Q} -ban) nincs felső határa.

4.4.1. 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.

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

4.4.3. definíció. *Legyen $\emptyset \neq \alpha \subset \mathbb{Q}$. 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” racionális szám.

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

A valós számokat tehát a racionális számok megfelelő részhalmazaiként (nyílt kezdetek) definiáljuk.

4.4.5. definíció. Azokat a valós számokat, amelyek nem nyílt kezdőszeletei racionális számok halmazainak, irracionális számoknak nevezzük.

4.4.2. Műveletek, rendezésük

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

4.4.6. definíció. $\alpha \leq \beta := \alpha \subseteq \beta$ ($\alpha, \beta \in \mathbb{R}$).

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

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

$$\begin{aligned}\alpha \oplus \beta &:= \{r + s \in \mathbb{Q} \mid r \in \alpha \text{ és } s \in \beta\} \subset \mathbb{Q}, \\ \alpha \odot \beta &:= \mathbb{Q}^- \cup \{rs \mid r \in \alpha \setminus \mathbb{Q}^- \text{ és } s \in \beta \setminus \mathbb{Q}^-\}, \text{ ha } \alpha, \beta \geq 0.\end{aligned}$$

Tetszőleges valós számok szorzatát az $\alpha \odot \beta = (\ominus \alpha) \odot (\ominus \beta) = \ominus((\ominus \alpha) \odot \beta) = \ominus(\alpha \odot (\ominus \beta))$ 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:

4.4.8. téTEL.

- $(\mathbb{R}; \oplus)$ 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.
- $(\mathbb{R} \setminus \{0\}; \odot)$ kommutatív csoport, amelynek 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 $\alpha \odot (\beta \oplus \gamma) = (\alpha \odot \beta) \oplus (\alpha \odot \gamma)$.
- minden $\alpha, \beta, \gamma \in \mathbb{R}$ esetén $\alpha \leq \beta \Rightarrow \alpha \oplus \gamma \leq \beta \oplus \gamma$.
- minden $\alpha, \beta, \gamma \in \mathbb{R}$, $\gamma \geq 0$ esetén $\alpha \leq \beta \Rightarrow \alpha \odot \gamma \leq \beta \odot \gamma$.

Azt kaptuk tehát, hogy

4.4.9. téTEL. $(\mathbb{R}; \oplus, \odot; \leq)$ felső határ tulajdonságú rendezett test.

Vajon hogy viszonyulnak egymáshoz a \mathbb{Q} és az \mathbb{R} rendezett testek? Tekintsük a $\varphi : \mathbb{Q} \rightarrow \mathbb{R}$, $\varphi(p) = \mathbb{Q}_p$ függvényt. Bebizonyítható, hogy φ injektív, valamint művelet- és

A számfogalom felépítése

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 műveleti jeleket mostantól $+$ -szal és \cdot -ral jelölhetjük. 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.

Ellenőrző kérdés. Mit mondhatunk egy racionális és egy irrationális szám összegéről?

Ellenőrző kérdés. Igaz-e, hogy irrationális számok összege minden irrationális?

Ellenőrző kérdés. Lehet-e irrationális szám reciproka racionális?

Ellenőrző kérdés. Lehet-e két irrationális szám szorzata racionális?

4.4.10. definíció. Legyen $x \in \mathbb{R}$. Ekkor x **abszolút értéke** az alábbi függvény:

$$|x| := \begin{cases} x & \text{ha } x \geq 0, \\ -x & \text{ha } x < 0 \end{cases}$$

Az abszolút érték definíciója a beágyazások miatt \mathbb{Z} -ben és \mathbb{Q} -ban hasonlóan értelmezhető. Megjegyezzük továbbá, hogy ha $a \in \mathbb{Z}^+$, akkor szintén a beágyazások tulajdonságai miatt $a \in \mathbb{Q}^+$ és $a \in \mathbb{R}^+$ is teljesül. Az abszolútérték-függvény legfontosabb tulajdonsága a **szubadditivitás**, azaz

$$|x + y| \leq |x| + |y|$$

minden $x, y \in \mathbb{R}$ esetén (a bizonyítást az Olvasóra bízzuk, az előjelekre vonatkozó esetszétválasztás alapján történhet). Ez szemléletesen a valós számokra vonatkozó háromszög-egyenlőtlenség.

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

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

(Kiejtésben „szignum függvény”.) A szignum függvényt **előjelfüggvénynek** is nevezünk. A szignum függvény segítségével az abszolút érték az $|x| = x \cdot \operatorname{sgn}(x)$ módon is megadható. A szignum függvény legfontosabb tulajdonsága a **multiplikativitás**, azaz

$$\operatorname{sgn}(x \cdot y) = \operatorname{sgn}(x) \cdot \operatorname{sgn}(y)$$

minden $x, y \in \mathbb{R}$ esetén.

Megmutatható, hogy \mathbb{R} arkhimédeszi tulajdonságú (lásd 4.4-21. gyakorlat), ami miatt definiálhatjuk $x \in \mathbb{R}$ „egészrészét”:

4.4.12. definíció.

$$\begin{aligned} \lfloor x \rfloor &:= \max\{n \in \mathbb{Z} : n \leq x\}, \\ \lceil x \rceil &:= \min\{n \in \mathbb{Z} : n \geq x\}. \end{aligned}$$

Az első esetben x **alsó egészrészéről**, a második esetben x **felső egészrészéről** beszélünk. Az alábbi összefüggések átgondolását az Olvasóra bízzuk:

4.4.13. téTEL. Az egészrész függvények elemi tulajdonságai:

$$\begin{aligned} \lfloor x \rfloor = n &\Leftrightarrow n \leq x < n + 1, \\ \lceil x \rceil = n &\Leftrightarrow n - 1 < x \leq n, \\ \lfloor x \rfloor = n &\Leftrightarrow x - 1 < n \leq x, \\ \lceil x \rceil = n &\Leftrightarrow x \leq n < x + 1. \end{aligned}$$

Ellenőrző feladat. Mi a kapcsolat $\lfloor a+b \rfloor$ és $\lfloor a \rfloor + \lfloor b \rfloor$ között?

Az egészrész függvény felhasználásával definiáljuk $x \in \mathbb{R}$ **törtrészét**²:

4.4.14. definíció. $\{x\} := x - \lfloor x \rfloor$.

Egy $x \in \mathbb{R}$ elem törtrészét néha $x \bmod 1$ -gyel jelöljük.

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

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

4.4.15. definíció. Egy $a \in \mathbb{R}$ szám $n \in \mathbb{N}^+$ kitevős hatványa alatt az $a \cdot a \cdots a = a^n$ valós számot értjük, ahol a szorzatban az a szám n -szer szerepel.

Legyen $a^0 := 1$ és ekkor rekurzívan $a^n = a^{n-1} \cdot a$ minden $n \in \mathbb{N}^+$ -ra. Elnevezése „a az n -ediken”. A definícióból könnyen beláthatóak az alábbi jól ismert számolási szabályok ($a, b \in \mathbb{R}, m, n \in \mathbb{N}_0^+$):

- $a^m \cdot a^n = a^{m+n}$,
- $a^n \cdot b^n = (a \cdot b)^n$,
- $(a^m)^n = a^{m \cdot n}$.

Nemnegatív valós számokra értelmezhető az egész kitevős **gyökvonás**, mint az iménti hatványozás (egyik) inverz művelete.

4.4.16. téTEL. Minden $a \in \mathbb{R}_0^+, n \in \mathbb{N}^+$ számhoz egyértelműen létezik olyan $x \in \mathbb{R}$, amelyre $x^n = a$.

Elnevezése „ n -edik gyök a”, jelölésben $\sqrt[n]{a}$ vagy $a^{1/n}$ ($n = 2$ esetén \sqrt{a}).

BIZONYÍTÁS. (Vázlat.) Az egyértelműség \mathbb{R} rendezettségből, a létezés pedig abból adódik, hogy $\mathbb{Q}^- \cup \{x \in \mathbb{Q}_0^+ \mid x^n \in a\}$ nyílt kezdet. ■

Analízisből látni fogjuk, hogy a gyökvonást (például intervallum skatulyázással) „tetszés szerinti pontossággal” el lehet végezni.

4.4.17. Következmény. Ha $a, b \in \mathbb{R}_0^+$ és $n \in \mathbb{N}^+$, akkor $\sqrt[n]{ab} = \sqrt[n]{a} \sqrt[n]{b}$.

A hatvány fogalmának negatív kitevőre való kiterjesztése az következőt jelenti (szokás szerint / jellel jelöljük a szorzás inverz műveletét):

²A törtrész jelölés könnyen összetéveszthető az egyedül az x -et tartalmazó halmazzal, mégis ez a jelölés terjedt el, ezért mi is ezt használjuk.

A számfogalom felépítése

4.4.18. definíció. Legyen $n \in \mathbb{N}, a \in \mathbb{R} \setminus \{0\}$. Ekkor $a^{-n} := 1/a^n$.

Az egész kitevős hatványozás és az egész kitevős gyökvonás segítségével definiálható a racionális kitevős hatványozás:

4.4.19. definíció. Legyen $a \in \mathbb{R}_0^+, m, n \in \mathbb{Z}, n > 0$. Ekkor $a^{\frac{m}{n}} := \sqrt[n]{a^m}$.

Tetszőleges valós kitevőre történő hatványozás is megadható ($a \in \mathbb{R}_0^+, b \in \mathbb{R}$):

4.4.20. definíció.

$$a^b := \begin{cases} \bigcup_{p \in \mathbb{Q}} a^p & (p \in \mathbb{Q}) \text{ ha } a \geq 1 \\ (a^{-1})^{-b} & \text{ha } 0 < a < 1 \\ 0 & \text{ha } a = 0 \text{ és } b \neq 0 \end{cases}$$

Az így definiált hatványok értékei minden \mathbb{R}_0^+ -ban vannak. Ha $a = b = 0$ akkor az egész hatványozásnál tett megállapítás miatt $0^0 = 1$. Ha eltekintünk a 0 alaptól, az egész kitevős hatványozásra adott számolási szabályok valós kitevős hatványokra is érvényesek.

4.12. példa. A matematikában az egyik legfontosabb függvény az **exponenciális függvény**. Szokásos jelölése e^x vagy $\exp(x)$, ahol e egy matematikai állandó, értéke 60 jegyre

$$\exp(1) \approx 2.71828182845904523536028747135266249775724709369995957496697,$$

és Euler-féle számnak is szokás nevezni. Alapvető jelentőséggel bír mind a matematika elméletében, mind a mérnöki, pénzügyi, közgazdaságtani stb. alkalmazásokban. Valós x változóra az $y = \exp(x)$ függvény értéke minden pozitív. Egyszerűen fogalmazva az exponenciális függvény által leírt mennyiség állandó mértékben többszöröződik. Például egy baktériumkultúra, amely „minden órában megduplázódik”, hozzávetőlegesen exponenciális függvénytel írható le. Hasonlóan ahhoz, ahogy egy autó értéke csökken, amely minden évben 10%-ot amortizálódik. Analitikusan, az exponenciális függvény végtelen hatványszor alakja

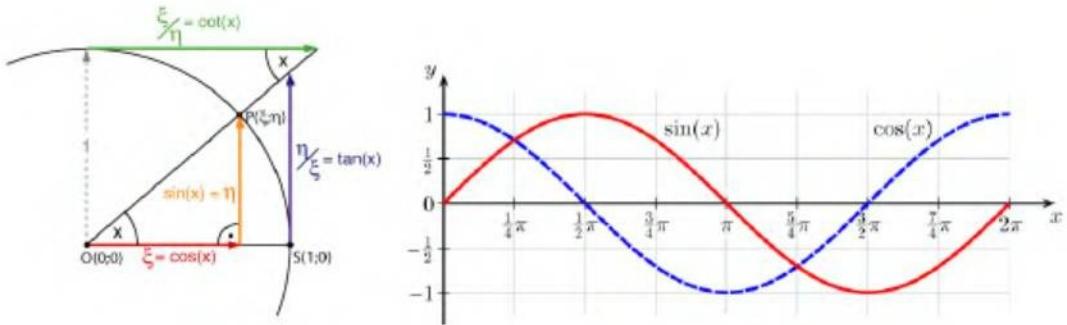
$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}. \quad (4.2)$$

A **logaritmusképzés** a hatványozás (másik) inverz művelete. Az $a^x = b$ egyenletnek $1 \neq a \in \mathbb{R}^+$ -ra és $b \in \mathbb{R}^+$ -ra a hatványozás monotonitása és a felső határ tulajdonság miatt minden pontosan egy megoldása van, amit $x = \log_a b$ alakban írunk.

4.4.21. definíció. A $b \in \mathbb{R}^+$ szám $a \in \mathbb{R}^+, a \neq 1$ alapú logaritmus a valós szám, amelyre a-t emelve b-t kapjuk.

Elnevezése „a alapú logaritmus b”. A logaritmusképzés értelmezési tartománya a pozitív valós számok halmaza, értékkészlete a valós számoké. A logaritmusképzés legfontosabb szabályai ($x, y, a, c \in \mathbb{R}^+, a \neq 1 \neq c$):

$$\begin{aligned} \log_a xy &= \log_a x + \log_a y, \\ \log_a \frac{x}{y} &= \log_a x - \log_a y, \\ \log_a x^y &= y \log_a x, \\ \log_a x &= \frac{\log_c x}{\log_c a}. \end{aligned}$$



4.2. ábra. A trigonometrikus függvények értelmezése.

A számításokban leggyakrabban a tízes ($\lg x$) és a kettes alapú logaritmust, valamint az e alapú természetes logaritmust ($\ln x$) használják („logarithmus naturalis”).

4.13. példa. A logaritmusfüggvény segítségével a szorzások összeadássá egyszerűsödnek. A kitévők összeadását a logaritmus értékeit skálájában tartalmazó logarléc használatakor egyszerű tologatással megoldhatjuk. A logaritmus használatával mennyiségek nagyságrendjeit egyetlen skálára sűríthetjük. Ennek hasznosságát gyakran a természet törvényszerűségei is alátámasztják. A különböző fizikai mennyiségek (hangerősség, hangmagasság, fényintenzitás stb.) által keltett, általunk érzékelt fisiológiai érzet a fizikai jel (teljesítményének) logaritmusával arányos. Ez indokolja a logaritmussal arányos decibel-skálák bevezetését. Logaritmikus továbbá a földrajz erősséget jelző Richter-skála is. A logaritmusfüggvény alapvető szerepet játszik a statisztikus fizikában használatos entrópia, illetve azzal gazdag analógiákat mutató információmennyiség és hírérték megadásában.

4.14. példa. minden bizonnal a matematika egyik legfontosabb konstansa a π , egy valós szám, amit egy $d = 2r$ átmérőjű és K kerületű kör $\pi = K/d$ arányaként értelmezünk. A π -ről könyveket írtak, módszerek sokaságával számították ki jegyeit, ami 60 jegyre közelítően

$$\pi \approx 3,14159265358979323846264338327950288419716939937510582097494 .$$

4.15. példa. Nagyon fontos valós függvények még a **trigonometrikus függvények**, amelyek eredetileg egy derékszögű háromszög egy szöge és oldalai közötti összefüggést írnak le (innen nyerték magyar és latin nevüket is). A trigonometrikus függvények fontosak többek között a geometriai számításoknál, különféle mozgások (harmonikus rezgőmozgás, körmozgás) és a periodikus jelenségek leírásánál, a műszaki élet számtalan területén. Hagyományosan hat fontos szögfüggvény alakult ki: szinusz (sin), koszinusz (cos), tangens (tg), kotangens (ctg), szekáns (sec) és koszekáns (csc). Legszemléletebb bevezetésük az egységsugarú kör segítségével történhet. Ez a definíció lehetővé teszi, hogy a szögfüggvényeket kiterjesszük a valós számokra. Az egységsugarú kör ugyanakkor könnyen használható vizuális segédeszköz is a szögfüggvényeket értelmező összes derékszögű háromszög megmutatására. Az 4.2. ábra a négy legfontosabb szögfüggvény értelmezését mutatja.

A sin és cos függvényekkel elemi síkgeometriai összefüggések bizonyíthatók. Legyenek a, b és c egy háromszög oldalai, az oldalakkal szemben lévő szögek rendre α, β, γ . Ekkor

$$\frac{\sin \alpha}{a} = \frac{\sin \beta}{b} = \frac{\sin \gamma}{c} \quad (\text{szinusztétel}),$$

$$c^2 = a^2 + b^2 - 2ab \cos \gamma \quad (\text{koszinusztétel, a Pithagorasz-tétel általánosítása}).$$

Továbbá

- $\sin^2 x + \cos^2 x = 1$ (Pithagoraszi azonosság),
- $\sin(x \pm y) = \sin x \cos y \pm \cos x \sin y$,
- $\cos(x \pm y) = \cos x \cos y \mp \sin x \sin y$,

A számfogalom felépítése

$$\bullet \sin x = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} x^{2n+1}, \quad (4.3)$$

$$\bullet \cos x = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} x^{2n}. \quad (4.4)$$

A szinuszra vonatkozó addíciós képlet a Ptolemaiosz-tételből következik, amennyiben a szóban forgó húrnégyszög egyik átlója egy egységnyi átmérőjű kör átmérője (a Ptolemaiosz-tétel azt állítja, hogy egy húrnégyszögben a szemközti oldalak hosszai szorzatainak összege megegyezik az átlók hosszának szorzatával). A végtelen hatványsor alakok a sin és cos függvények 0 körüli Taylor-sorfejései.

4.4.22. definíció. Az $f : H \rightarrow \mathbb{R}$ függvényt **periodikusnak** mondjuk, ha létezik olyan $0 < p \in \mathbb{R}$ konstans, hogy minden $x \in H$ -ra $x+p \in H$, és ekkor $f(x) = f(x+p)$. Ha p a legkisebb ilyen szám, amelyre ez teljesül, akkor p az f függvény **periódusa** vagy **alappériódusa**.

4.16. példa. A sin és cos függvények alappériódusa 2π .

4.4.23. definíció. Tegyük fel, hogy egy $f \in \mathbb{R} \rightarrow \mathbb{R}$ függvényre $x \in D_f \Rightarrow -x \in D_f$. Ekkor

- f páros, ha $f(-x) = f(x)$,
- f páratlan, ha $f(-x) = -f(x)$.

Pontosan azok a függvények párosak, amelyek függvénygörbéi szimmetrikusak az y tengelyre (azaz az y tengelyre való tükrözés helybenhagyja őket), és azok páratlanok, amelyek szimmetrikusak az origóra (azaz az origó körüli 180 fokos forgatás helybenhagyja őket).

Ellenőrző kérdés. Párosak vagy páratlanok az alábbi függvények: abszolút érték, $x \mapsto x$, $x \mapsto x^2$, $x \mapsto x^3$, sin, cos, exp?

A valós függvények egyik leggyakoribb informatikai alkalmazása a függvények növekedési ütemének jellemzésére szolgál.

4.4.24. definíció. Legyenek $f, g \in \mathbb{N} \rightarrow \mathbb{R}$ függvények. Azt mondjuk, hogy $f(x) = O(g(x))$ (kiejtése: $f(x)$ egyenlő nagy ordó $g(x)$), ha léteznek olyan c és n_0 pozitív számok, hogy minden $x > n_0$ esetén $|f(x)| \leq c \cdot |g(x)|$.

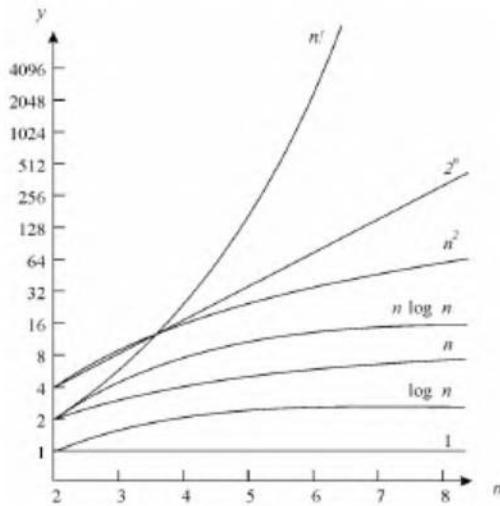
Intuitíven átfogalmazva: $f(x) = O(g(x))$, ha elegendően nagy x esetén $g(x)$ csak konszanszor nagyobb, mint $f(x)$, azaz ha $f(x)$ „nem nő gyorsabban” $g(x)$ -nél.

4.17. példa. A definíció szerint az $f(x) = 13x + 1$ függvény esetén $f(x) = O(x)$ és $f(x) = O(x^2)$ egyaránt teljesül, ezért gyakorlatban mindenkor a legkisebb lehetséges nagy ordót adjuk meg, így az már egyértelmű. A nagy ordó segítségével egy algoritmus futására jellemző: a vizsgált függvény a futáshoz szükséges időt adja meg a bemenet hosszának függvényében. Leegyszerűsítve, egy $O(x^2)$ futásidőjű algoritmus kétszer akkora méretű bemenetre négyeszer annyi ideig fog futni, háromszor akkora bemenetre kilencszer annyi ideig. Míg maga a futásidőt leíró függvény függ az implementáció részleteitől és a futtatáshoz használt architektúrától, az algoritmus nagy ordója csak az **algoritmus alapelveitől** függ. A nagy ordó két egyszerű szabály követésével megkapható:

(1) Egy összegből mindenkor a leggyorsabban növekedő tagot tartjuk meg. Polinomok esetén ez a legnagyobb kitevőjű tag.

(2) A szorzatokból eltávolítjuk a konstans tagokat.

4.18. példa. $12x^3 + 2x^2 + 3 = O(x^3)$.



4.3. ábra. Az alapfüggvények növekedési üteme. Elnevezései (alulról felfelé haladva): konstans, logaritmikus, lineáris, szemilineáris, polinomiális (az ábrán kvadratikus), exponenciális, hiperexponenciális.

4.19. példa. A nagy ordó korlátlanul növekedő változó esetén jellemzi a függvényt, kis változóértékekre kevés információt hordoz. Könnyen lehetséges például, hogy egy $O(x^2)$ függvény kisebb egy $O(x)$ függvénynél a gyakorlatban előforduló x -ekre, mert az $O(x)$ függvény nagy konstans szorzókat tartalmaz. Ezért fontos, hogy ha egy feladathoz algoritmust választunk, ne kizárolag a nagy ordós futásidőt vegyük figyelembe, hanem a konkrét adatokra várható futásidőt is. A függvények növekedésének ütemét szemlélteti az 4.3. ábra.

4.20. példa. Tegyük fel, hogy egy program az n méretű tesztseteken 6 másodpercig fut. Meddig fog futni $20n$ méretű bemeneten? Jelölje $f(x)$ az algoritmus maximális lépésszámát az x hosszú bemeneteken.

Logaritmikus függvény: $f(x) = \lg x = O(\lg x)$. A futási $6 \cdot \lg 20 \approx 25.9$, azaz kb. 26 másodperc lesz.

Lineáris függvény: $f(x) = x = O(x)$. A futási idő kb. 20-szorosára nő, azaz 2 percig is eltartható.

Másodfokú függvény: $f(x) = x^2 = O(x^2)$. A futási idő 20^2 -szeresére nő, azaz 400 perc körül idővel számolhatunk.

Exponenciális függvény: $f(x) = 2^x = O(2^x)$. A futási idő $6 \cdot 2^{20} \approx 6.3 \cdot 10^6$ másodperc lesz, ami közelítőleg 73 nap.

4.21. példa. A különféle matematikai modellekben gyakran használjuk a számtani és a mértani középre vonatkozó egyenlőtlenséget, amely szerint nemnegatív valós számok számtani középértéke nem lehet kisebb, mint a számok mértani középértéke; egyenlőség pedig csak akkor állhat fenn, ha a szóban forgó számok megegyeznek:

$$\frac{a_1 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 \cdots a_n},$$

ahol $0 \leq a_1, \dots, a_n \in \mathbb{R}$. Az állításnak többféle bizonyítása ismerete, mi most Riesz Frigyes bizonyítását közöljük. Ha $a_1 = a_2 = \cdots = a_n$, akkor az állítás egyenlőséggel teljesül. Legyenek tehát az a_i -k nem mind egyformák, és legyen

$$A_n = \frac{a_1 + \cdots + a_n}{n}.$$

Ha mondjuk $a_1 = \min\{a_i\}$ és $a_2 = \max\{a_i\}$, akkor nyilván $a_1 < A_n < a_2$ teljesül. Helyettesítsük a_1 -et A_n -nel, a_2 -t pedig $(a_1 + a_2 - A_n)$ -nel. Ekkor a számtani közép nem változik, hiszen

$$\frac{A_n + (a_1 + a_2 - A_n) + a_3 + \cdots + a_n}{n} = A_n,$$

A számfogalom felépítése

a mértani közép viszont nő, mert

$$A_n(a_1 + a_2 - A_n) - a_1 a_2 = (a_1 - A_n)(A_n - a_2) > 0.$$

Észrevehetjük még, hogy a számok között most már az A_n elem eggel többször szerepel. Ezzel az eljárással véges sok lépésben valamennyi elemet A_n -re cserélhetjük, miközben a számtani közép változatlan marad, a mértani közép pedig fokozatosan nő. Az eljárás végén elérjük a bizonyítás elején már tárgyalt egyenlőséget, és ezzel egyben az állítást is igazoltuk.

Gyakorlatok

4.4-1. Igazoljuk, hogy minden $1 < n \in \mathbb{N}$ -re

$$\sqrt{n} \leq \sum_{k=1}^n \frac{1}{\sqrt{k}} < 2\sqrt{n}.$$

4.4-2. Határozzuk meg az alábbi valós függvények értelmezési tartományát és érték-készletét: $y = x^2$, $y = 1/x$, $y = \sqrt{x}$, $y = \sqrt{4-x}$, $y = \sqrt{1-x^2}$.

4.4-3. Tekintsük az $f(x) = \sqrt{x}$ és $g(x) = x + 2$ valós függvényeket. Határozzuk meg az alábbi függvényeket és értelmezési tartományukat:

- a) $f \circ g$,
- b) $g \circ f$,
- c) $f \circ f$,
- d) $g \circ g \circ g$.

4.4-4. Bizonyítsuk be az általánosított **Bernoulli-egyenlőtlenséget**:

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

ahol x_1, x_2, \dots, x_n azonos előjelű és -1 -nél nagyobb valós számok. Így $x > -1, n \in \mathbb{N}^+$ esetén

$$(1 + x)^n \geq 1 + nx$$

is fennáll, és egyenlőség csak $n = 1$ vagy $x = 0$ esetén teljesül.

4.4-5. Bizonyítsuk be, hogy ha $a, b \in \mathbb{R}$, $a < b$, akkor az (a, b) intervallumban van racionális és iracionális szám is.

4.4-6. Ábrázoljuk a Fahrenheit-Celsius hőmérsékleti skálák fokokban mért kapcsolatát leíró

$$C = \frac{5}{9}(F - 32)$$

valós függvényt. Van-e olyan hőmérséklet, amelynek a Celsius-, illetve a Fahrenheit skálán ugyanaz az érték felel meg?

4.4-7. Határozzuk meg a feltételt kielégítő valós számok mértani helyét.

- (1) $|4x - 1| < |x - 1|$,
- (2) $||x + 1| - |x - 1|| < 1$.

4.4-8. Mikor igazak az alábbi összefüggések?

- (1) $\lfloor x + n \rfloor = \lfloor x \rfloor + n$,
- (2) $\lceil x + n \rceil = \lceil x \rceil + n$,
- (3) $\{x + n\} = \{x\}$.

4.4-9. Az IEEE 754 szabvány szerint a modern processzorokban négyféle egésszé kerekítési mód létezik: $+\infty$ felé, $-\infty$ felé, 0 felé, és a legközelebbi egészre (párosra, ha két ilyen van). Az ismert jelölésekkel írjuk le valamennyit. Megjegyzés: A legközelebbi egészre történő kerekítés során a törtrész szokásos jelölése

$$\|x\| = \min\{|n - x| : n \in \mathbb{Z}\} = \min\{\{x\}, 1 - \{x\}\}.$$

4.4-10. A $H(x) : \mathbb{R} \rightarrow \mathbb{R}$ Heaviside-függvényt a műszaki életben (elektronika, vezérléselmélet, stb.) gyakran alkalmazzák. A jelfeldolgozásban például olyan szignálok leírására, amelyek egy adott időponttól kezdve folyamatosan észlelhetőek. Az általános Heaviside-függvény az alábbi ($z \in \mathbb{R}$):

$$H_z(x) = \begin{cases} 1 & \text{ha } x > 0, \\ z & \text{ha } x = 0, \\ 0, & \text{ha } x < 0. \end{cases}$$

Per default, $H(x) = H_{0.5}(x)$. Adjuk meg a $\operatorname{sgn}(x)$ függvényt $H(x)$ segítségével.

4.4-11. A hidrosztatikai nyomást leíró valós függvény lineáris: a búvár által a víz alatt érzékelt nyomás a víz felszíne alatt d távolságban a $p = kd + 1$ egyenlettel írható le, ahol k egy állandó. Ábrázoljuk a függvényt, ha tudjuk, hogy 100 méter mélyen a nyomás 10.94 atmoszféra.

4.4-12. Bizonyítsuk be, hogy ha $a, b \in \mathbb{R}$, akkor

$$\max\{a, b\} = \frac{|a - b| + a + b}{2}, \quad \min\{a, b\} = \frac{-|a - b| + a + b}{2}.$$

4.4-13. Bizonyítsuk be, hogy $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ test a valós számok szokásos műveleteivel.

4.4-14. Legyen $m, n \in \mathbb{Z}$, $m > 0$. Bizonyítsuk be, hogy ekkor

$$\begin{aligned} \left\lceil \frac{n}{m} \right\rceil &= \left\lfloor \frac{n+m-1}{m} \right\rfloor = \left\lfloor \frac{n-1}{m} \right\rfloor + 1, \\ \left\lfloor \frac{n}{m} \right\rfloor &= \left\lceil \frac{n-m+1}{m} \right\rceil = \left\lceil \frac{n+1}{m} \right\rceil - 1. \end{aligned}$$

4.4-15. Legyen $m, n \in \mathbb{Z}$, $m > 0$. Bizonyítsuk be, hogy ekkor

$$n = \sum_{i=0}^{m-1} \left\lfloor \frac{n+i}{m} \right\rfloor = \sum_{i=0}^{m-1} \left\lceil \frac{n-i}{m} \right\rceil.$$

4.4-16. Legyen $m, x \in \mathbb{Z}$, $m > 0$. Bizonyítsuk be, hogy ekkor

$$\begin{aligned} \lfloor mx \rfloor &= \sum_{i=0}^{m-1} \left\lfloor x + \frac{i}{m} \right\rfloor, \\ \lceil mx \rceil &= \sum_{i=0}^{m-1} \left\lceil x - \frac{i}{m} \right\rceil. \end{aligned}$$

4.4-17. A számtani és mértani középre vonatkozó egyenlőtlenség segítségével bizonyítsuk be az alábbiakat:

a) Az $(1 + \frac{1}{n})^n$ sorozat szigorúan monoton növekvő ($n \in \mathbb{N}^+$);

b) Az azonos kerületű háromszögek között a szabályos háromszög területe a legnagyobb. Segítség: Alkalmazzuk Héron képletét.

4.4-18. Bizonyítsuk be, hogy $\sqrt{2} + \sqrt{p}$ minden p prím esetén irrationális.

4.4-19. Legyenek $A, B \subseteq \mathbb{R}$ nem-üres halmazok. Mutassuk meg, hogy ekkor $\sup(A + B) = \sup A + \sup B$, továbbá $\inf(A + B) = \inf A + \inf B$.

A számfogalom felépítése

4.4-20. Bizonyítsuk be, hogy egy rendezett test pontosan akkor felső határ tulajdon-ságú, ha alsó határ tulajdonságú, azaz ha minden nem-üres alulról korlátos részhalma-zának van legnagyobb eleme.

4.4-21. Mutassuk meg, hogy egy felső határ tulajdonságú test minden arkhimédeszi tulajdonságú is.

4.4-22. Mutassuk meg, hogy $\mathbb{R} \times \mathbb{R}$ a koordinátánkénti összeadással és szorzással kommutatív egységelemes gyűrű, de nem test.

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 egyenlet megoldásánál bukkant elő, ami a reneszánsz matematika egyik nagy felfedezése volt. CARDANO és FERRO észrevették, hogy bizonyos harmadfokú egyenletek megoldása során a négyzetgyökjel alatt negatív szám szerepel, és az összes megoldás a korábbi módon nem volt számolható („casus irreducibilis”). 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 a szorzat-konstrukció útját követjük.

4.5.1. definíció. $\mathbb{C} := \mathbb{R} \times \mathbb{R}$.

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

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

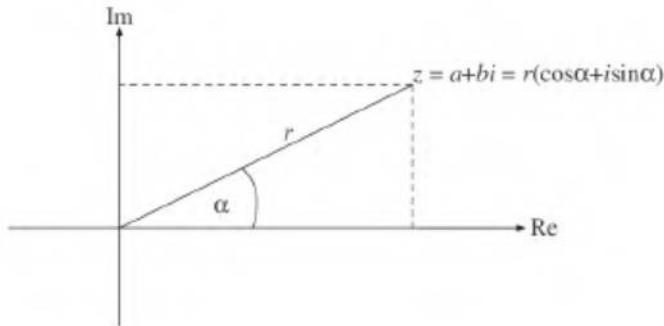
$$\begin{aligned}(a, b) \oplus (c, d) &:= (a + c, b + d), \\ (a, b) \odot (c, d) &:= (ac - bd, ad + bc).\end{aligned}$$

Belátható, hogy $(\mathbb{C}; \oplus)$ kommutatív csoport a $(0, 0)$ semleges elemmel, továbbá az (a, b) -hez tartozó, az összeadásra vonatkozó inverz elem $\ominus(a, b) = (-a, -b)$. Ezen kívül $(\mathbb{C} \setminus \{(0, 0)\}; \odot)$ kommutatív csoport az $(1, 0)$ semleges elemmel. Az (a, b) -hez tartozó, a szorzásra vonatkozó inverz elem $(a, b)^{-1} = (a/(a^2 + b^2), -b/(a^2 + b^2))$. A két műveletet összekapcsoló disztributív törvények is igazak, ezért

4.5.3. téTEL. $(\mathbb{C}; \oplus, \odot)$ test.

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

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

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

és

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

Mivel $\Phi(a) = \Phi(b) \Rightarrow a = b$, ezért Φ injektív. Vagyis \mathbb{R} -et valóban beágyaztuk \mathbb{C} -be, az $(a, 0)$, $a \in \mathbb{R}$ alakú komplex számok halmazát azonosítjuk \mathbb{R} -rel, a továbbiakban a műveleteket $+$ -szal és \cdot -tal jelöljük, i -t írunk $(0, 1)$ helyett, és általánosan, $a + bi$ -t írunk $(a, b) = (a, 0) \oplus (b, 0) \odot (0, 1)$ helyett.

4.5.2. Szemléltetésük és műveleteik

Ha $z = a + bi \in \mathbb{C}$, akkor megkülönböztetjük a z komplex szám **valós** (Re) és **képzetes** (imaginárius, Im) **részét**: $\text{Re}(z) = a$, $\text{Im}(z) = b$. 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.

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

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

4.5.5. téTEL. Ha $z = x + yi \in \mathbb{C}$, akkor $\max\{|x|, |y|\} \leq |z| \leq |x| + |y|$.

Bizonyítás. A bal oldali egyenlőtlenség abból következik, hogy

$$|x| = \sqrt{x^2} \leq \sqrt{x^2 + y^2} = |z| \text{ és } |y| = \sqrt{y^2} \leq \sqrt{x^2 + y^2} = |z|.$$

Másrészt

$$\begin{aligned} |z| &= \sqrt{x^2 + y^2} \\ &\leq \sqrt{x^2 + 2|x||y| + y^2} \\ &= \sqrt{|x|^2 + 2|x||y| + |y|^2} \\ &= \sqrt{(|x| + |y|)^2} \\ &= |x| + |y|. \end{aligned}$$

A számfogalom felépítése

A bizonyítás kész. ■

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

Egy komplex szám tehát pontosan akkor valós, ha megegyezik konjugáltjával. Ha egy nem-nulla komplex szám valós része nulla, akkor **képzetesnek** nevezzük.

Ellenőrző kérdés. A komplex számok előjelfüggvénye megegyezik a valós függvényeknél látottakkal, vagyis $\operatorname{sgn}(0) = 0$, egyébként pedig $\operatorname{sgn}(z) = z/|z|$. Igaz-e, hogy $\operatorname{sgn}(\bar{z}) = \overline{\operatorname{sgn}(z)}$?

Ha $z, w \in \mathbb{C}$, akkor az alábbi összefüggések igazolhatók:

4.5.7. téTEL. Minden $z, w \in \mathbb{C}$ -re

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

BIZONYÍTÁS. Az első 10 állítás közvetlenül következik a definíciókból, az utolsó pedig a komplex számok vektor alakjából, így a hosszukra vonatkozó állítás pontosan a jól ismert háromszög-egyenlőtlenség. ■

Az alábbiakban felhasználjuk a \sin , \cos függvények, valamint az e és a π számok definícióját és tulajdonságait. 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 (4.4. ábra).

Ellenőrző kérdés. Mi az argumentuma a $-x - ix$ alakú komplex számoknak ($x \in \mathbb{R}$)?

A (4.3), (4.4) és (4.12) egyenletekből következik, hogy $\cos \varphi + i \sin \varphi = e^{i\varphi}$, így a komplex számok $z = re^{i\varphi}$ alakjához jutunk. Az iménti jelölésekkel tehát

4.5.8. definíció. Egy $z \neq 0$ komplex számot többféle alakban is felírhatunk:

$$z = \begin{cases} a + bi & (\text{algebrai alak}), \\ r(\cos \varphi + i \sin \varphi) & (\text{trigonometrikus alak}), \\ re^{i\varphi} & (\text{Euler-féle alak}). \end{cases}$$

4.22. példa. A $\frac{3}{2+i}$ komplex szám algebrai alakja

$$\frac{3}{2+i} = \frac{3}{2+i} \cdot \frac{2-i}{2-i} = \frac{6-3i}{4-2i+2i-i^2} = \frac{6-3i}{5} = \frac{6}{5} - \frac{3}{5}i.$$

Az $n - \sqrt{3}ni$ komplex szám trigonometrikus alakja

$$n - \sqrt{3}ni = \sqrt{(n^2 + 3n^2)} \left(\frac{1}{2} - i \frac{\sqrt{3}}{2} \right) = 2n(\cos 5\pi/3 + i \sin 5\pi/3).$$

Az $5i$ komplex szám Euler-féle alakja

$$5i = 5e^{i\pi/2}.$$

4.23. példa. A komplex számok Euler-féle alakjának az $r = 1, \varphi = \pi$ helyettesítéssel kapott kimenete az $e^{\pi i} + 1 = 0$ formula, ami egyesek szerint a világ legszebb egyenlete, mert a lehető legtömörebben írja le a matematika 5 legfontosabb konstansa közti összefüggést.

Ellenőrző kérdés. Mely esetekben könnyű meghatározni egy komplex szám trigonometrikus vagy Euler-alakját?

A 4.5.7. téTELben megvizsgáltuk a komplex számok algebrai alakjával történő műveleteket. Most a trigonometrikus alakkal vett műveleteket vizsgáljuk.

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

$$z \cdot w = |zw|(\cos(\varphi + \psi) + i \sin(\varphi + \psi)),$$

továbbá $w \neq 0$ esetben

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

Bizonyítás. A sin és cos függvények addíciós képleteiből

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

a második állítás pedig a 4.5.7. téTEL (7) tulajdonságából következik. ■

Ha z, w nem-nulla komplex számok, akkor a sin és cos függvények periodicitása miatt $0 \leq \arg(z) + \arg(w) < 2\pi$ esetben $\arg(zw) = \arg(z) + \arg(w)$, ha pedig $\arg(z) + \arg(w) \geq 2\pi$, akkor $\arg(zw) = \arg(z) + \arg(w) - 2\pi$. Hasonlóan, a $0 \leq \arg(z) - \arg(w) < 2\pi$ esetben $\arg(z/w) = \arg(z) - \arg(w)$, az $\arg(z) - \arg(w) < 0$ 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 mindenkorban vesszük.

Ellenőrző kérdés. Mi a szükséges és elégéges feltétele annak, hogy két komplex szám összege, illetve szorzata valós legyen?

4.24. példa. A 4.5. ábra a sík egységsugarú köre néhány pontja koordinátáit mutatja a hozzájuk tartozó szögekkel.

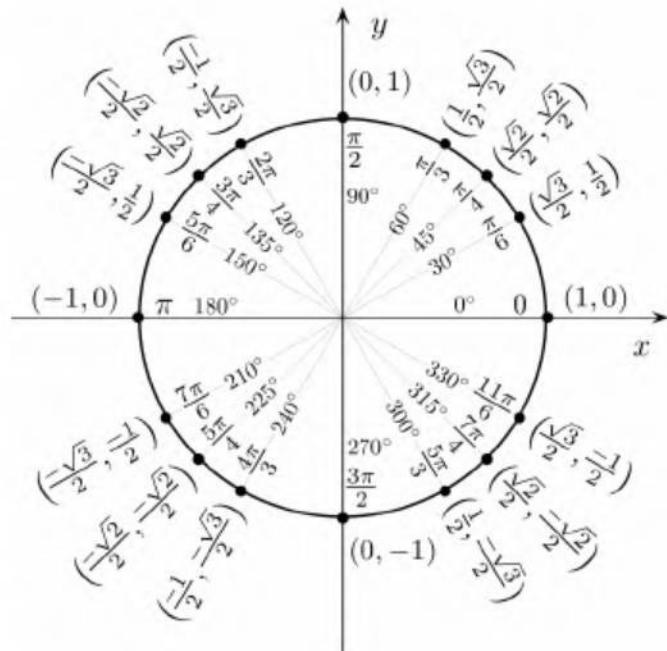
A komplex számok természetes ($n \in \mathbb{N}$) kitevős hatványozását a De Moivre-azonosság egymás utáni alkalmazásából kapjuk:

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

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

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

A számfogalom felépítése



4.5. ábra. Az egységkör néhány pontjának koordinátái.

4.26. példa. A $z = a + bi$ komplex szám ($a, b \in \mathbb{R}$) geometriai értelmezésben felfogható egy $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ alakú mátrixnak. Ekkor a komplex számok összeadása és szorzása a szokásos mátrixösszeadásnak és mátrixszorzásnak felel meg, egy $\lambda \in \mathbb{R}$ számmal való szorzás (nyújtás) eredménye $\begin{pmatrix} \lambda a & -\lambda b \\ \lambda b & \lambda a \end{pmatrix}$, továbbá z inverze $\frac{1}{a^2+b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. A $z = a + bi = (a, b)$ síkbeli pont φ szöggel történő elforgatása (negatív, vagyis az óramutató járásával ellentétes irányba) megfelel a $\begin{pmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{pmatrix}$ mátrixszal történő szorzásnak.

4.5.3. Komplex számok gyökei

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

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

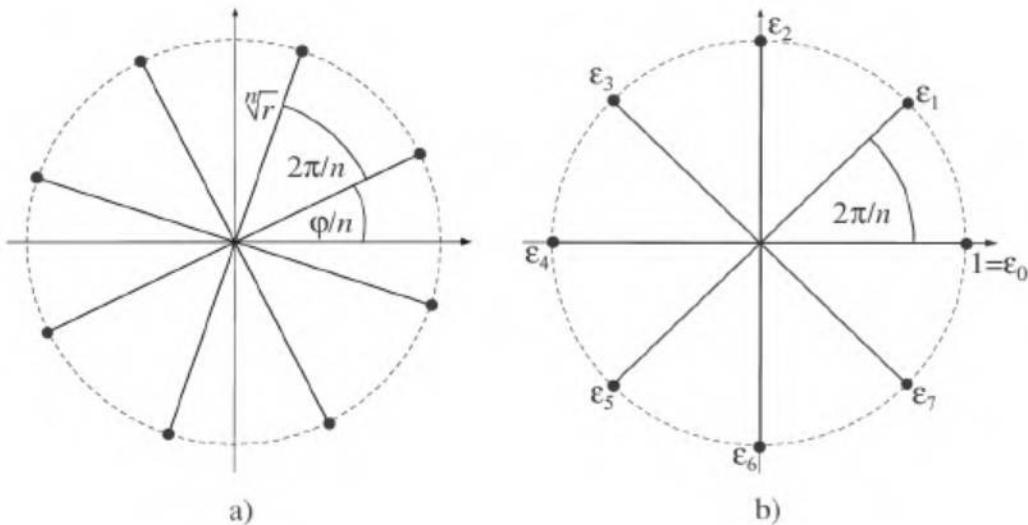
A $z = 0$ esetben nyilván $w = 0$.

4.5.11. téTEL (Komplex szám n -edik gyöke). Ha $0 \neq z = |z|(\cos \varphi + i \sin \varphi)$, akkor

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

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 (4.6. ábra).



4.6. 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 egységgökök. Mindkét ábrán $n = 8$.

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

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

továbbá

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

ezért

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

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

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

komplex számok tesznek eleget. Ezeket **n -edik komplex egységgököknek** nevezzük. Némely n -edik egységgöök természetes kitevős hatványai előállítják a többi n -edik egységgöököt, **primitív n -edik egységgööknek** nevezzük.

4.5.12. definíció. Azt az n -edik egységgöököt, amelynek különböző természetes kitevős hatványai előállítják a többi n -edik egységgöököt, **primitív n -edik egységgööknek** nevezzük.

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

A számfogalom felépítése

4.5.13. téTEL. Legyen $0 \neq z \in \mathbb{C}$, $n \in \mathbb{N}^+$ és $w_1^n = z$. Ekkor z többi n -edik gyöke $w_1\varepsilon_k$ ($1 \leq k \leq n - 1$), ahol ε_k n -edik egységgöök.

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 $w_1\varepsilon_k$ ($1 \leq k \leq n - 1$) minden különbözők, mert ha $w_1\varepsilon_k = w_1\varepsilon_s$, akkor $w_1 \neq 0$ miatt $\varepsilon_k = \varepsilon_s$. ■

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

Bizonyítás. Az előző téTEL jelöléseivel:

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

Az alábbiakban megvizsgáljuk a valós és komplex számok komplex hatványát. Legyen először $a, b, c \in \mathbb{R}$ és $z = b + ci$. Ekkor egyrészt

$$e^{b+ci} = e^b \cdot e^{ci} = e^b (\cos c + i \sin c),$$

másrészt felhasználva, hogy $a = e^{\ln a}$

$$\begin{aligned} a^{b+ci} &= e^{(\ln a)(b+ci)} = e^{b \ln a + i(c \ln a)} \\ &= e^{b \ln a} (\cos(c \ln a) + i \sin(c \ln a)) \\ &= a^b (\cos(c \ln a) + i \sin(c \ln a)). \end{aligned}$$

Amennyiben az alap komplex, a dolgok újragondolást igényelnek. Egy $z = |z| \cdot e^{i\varphi}$ komplex szám logaritmusát keresve ugyanis végtelen sok olyan $w \in \mathbb{C}$ szám van, amelyre $e^w = z$, hiszen $w = \ln|z| + (\varphi + 2k\pi)i$ minden k egészre megfelel. A komplex logaritmus az alábbi módon egyértelművé tehető:

4.5.15. definíció. Legyen $z = |z| \cdot e^{i\varphi} \in \mathbb{C}$. Ekkor

$$\text{Log } z := \ln|z| + i\varphi = \ln|z| + i\text{Arg } z,$$

ahol $-\pi < \text{Arg } z \leq \pi$ a **fő argumentum**.

A definíció miatt $e^{\text{Log } z} = z$ minden $z \neq 0$ komplex számra.

De vigyázat!! Az olyan megszokott, ártatlan dolgok, mint $\text{Log } z_1 z_2 = \text{Log } z_1 + \text{Log } z_2$ nem biztos, hogy igazak, mert a két oldal $2\pi i$ egész többszörösében különbözhet!

Vajon a valós alapnál nem volt ilyen probléma? De igen! Csakhogy a valós alap esetében a logaritmusra a(z egyetlen) valós w értéket használtuk.

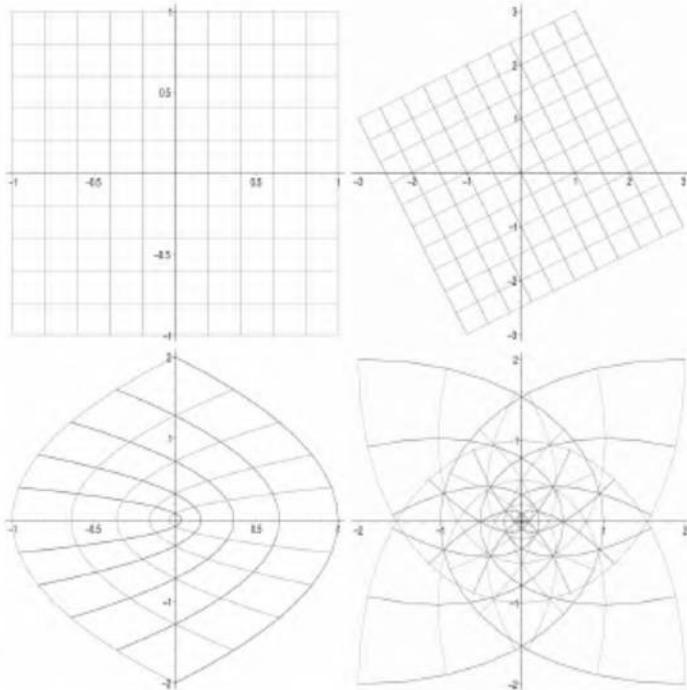
Ne felejtsük el: komplex szám komplex hatvanya általában nem függvény, csak az imént definiált Log függvény segítségével lehetőazzá.

4.28. példa. Megmutatjuk, hogy az i^i komplex szám valós. Az Euler-formulát a $\pi/2$ argumentummal véve $i = e^{i\pi/2}$ adódik, ezért

$$i^i = e^{i^2\pi/2} = e^{-\pi/2},$$

ami egy picike valós szám, közelítőleg

$$0.207879576350761908546955619834978770033877841631769608075136.$$



4.7. ábra. Példa komplex függvényekre. A bal felső ábrán az A alaprácsot láthatjuk. A jobb felső ábra az A pontjaira végrehajtott $z \rightarrow z(2 + i)$, a bal alsó ábra a $z \rightarrow z^2$, a jobb alsó ábra pedig a $z \rightarrow z^3$ függvényeket mutatja.

4.29. példa. A 4.7. ábrán komplex függvényekre láthatunk példát.

4.30. példa. A komplex számok és függvények alkalmazása igen széleskörű, alkalmazzák őket repülőgépek szárnyprofiljának tervezésékor (Zsukovszkij-profil) vagy a komplex impedanciák számításakor a mérnöki gyakorlatban.

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

4.5.16. téTEL (algebra alaptétele). *Minden $\mathbb{C}[x]$ -beli, legalább elsőfokú polinomnak létezik zérushelye \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 **algebraileg zártnak** nevezzük.

A számfogalom felépítése

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.

4.5.17. téTEL. *Nem létezik olyan rendezés, 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) teljesülne 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. ■

A **bázis** a lineáris algebrában egy olyan vektorhalmazt jelent, mely elemeinek lineáris kombinációi előállítják a megadott vektortér valamennyi vektorát, valamint ezen vektorhalmaz egyik eleme sem fejezhető ki a többi elem lineáris kombinációjával. Tehát bázison lineárisan független generátorrendszert értünk. Vektortér **dimenzióján** egy bázisának elemszámát, számoságát értjük. Ha a vektortérnek nincs véges generátorrendszere, akkor dimenziója végtelen. Az üres tér dimenziója 0.

4.5.18. téTEL. *\mathbb{C} vektortér \mathbb{R} felett az $\{1, i\}$ bázissal.*

BIZONYÍTÁS. minden $z, z_1, z_2 \in \mathbb{C}$ és $\lambda, \mu \in \mathbb{R}$ esetén teljesül, hogy

- (1) $\lambda(z_1 + z_2) = \lambda z_1 + \lambda z_2$,
- (2) $(\lambda + \mu)z = \lambda z + \mu z$,
- (3) $(\lambda\mu)z = \lambda(\mu z)$,
- (4) $1z = z$ (itt \mathbb{R} egységeleme). ■

4.5.5. Miért is lesz $i^2 = -1$?

Az 4.4-22. gyakorlatban láttuk, hogy $\mathbb{R} \times \mathbb{R}$ -en a koordinátánkénti összeadással és szorzással definiált műveletekre „csak” egységelemes gyűrű konstruálható. Amennyiben az $A = \{a + bi \mid a, b \in \mathbb{R}\}$ halmazon valamilyen más egyéb szorzást szeretnénk bevezetni, az a kérdés merül fel, hogy mi legyen két A -beli elem szorzata. A belső művelet elvárásai szerint a szorzás eredménye A -beli, tehát $i^2 = p + qi$ valamilyen $p, q \in \mathbb{R}$ -re. Ez pontosan azt jelenti, hogy $i^2 - qi = p$, vagy másképp

$$\left(i - \frac{q}{2}\right)^2 = p + \frac{q^2}{4} \tag{4.5}$$

adódik. Jelöljük (4.5) jobb oldalát K -val. Hárrom eset lehetséges.

K negatív. Ekkor valamilyen nem nulla $k \in \mathbb{R}$ -re $p + q^2/4 = -k^2$, vagy másként

$$\left(i - \frac{q}{2}\right)^2 = -k^2.$$

Az egyenletet átalakítva

$$\left(-\frac{q}{2k} + \frac{1}{k}i \right)^2 = -1.$$

Ha a zárójelben lévő számot Θ -val jelöljük, azt kapjuk, hogy $\Theta^2 = -1$, és ekkor $i = q/2 + k\Theta$. Tetszőleges $a + bi$ szám esetén

$$a + bi = a + b\left(\frac{q}{2} + k\Theta\right) = \left(a + \frac{b}{2}q\right) + bk\Theta$$

alakban írható. Más szóval minden $a + bi$ számról feltehető, hogy $a_1 + b_1\Theta$ alakú, ahol $a_1, b_1 \in \mathbb{R}$ és $\Theta^2 = -1$. Ez pontosan a már látott komplex számokkal egyezik meg.

K pozitív. Az iméntihez hasonlóan valamelyen nem-nulla $k \in \mathbb{R}$ esetén

$$\left(-\frac{q}{2k} + \frac{1}{k}i \right)^2 = 1.$$

A zárójelben lévő számot jelöljük most Υ -nal. Ekkor $\Upsilon^2 = 1$, és az $a + bi$ számokat felírhatjuk $a_1 + b_1\Upsilon$ alakban, ahol $a_1, b_1 \in \mathbb{R}$ és $\Upsilon^2 = 1$. Nézzük meg, hogy néz ki most az elemek szorzata:

$$(\alpha + \beta\Upsilon)(\gamma + \delta\Upsilon) = (\alpha\gamma + \beta\delta) + (\alpha\delta + \beta\gamma)\Upsilon.$$

Ezeket a rendszereket **hiperbolikus komplex rendszereknek** nevezzük.

K = 0. Jelöljük most az $i - q/2$ számot Ω -val. Ekkor tehát $\Omega^2 = 0$, és tetszőleges szám $(a + b/2q) + b\Omega$, vagyis $a_1 + b_1\Omega$ alakban írható, ahol $a_1, b_1 \in \mathbb{R}$ és $\Omega^2 = 0$. A szorzási szabály esetén

$$(\alpha + \beta\Omega)(\gamma + \delta\Omega) = \alpha\gamma + (\alpha\delta + \beta\gamma)\Omega.$$

Ezeket a rendszereket **Study-féle rendszereknek** nevezzük.

4.5.19. téTEL. Sem a hiperbolikus komplex, sem a Study-féle rendszerben nem teljesül, hogy minden elemnek létezik multiplikatív inverze.

BIZONYÍTÁS. Ha a hiperbolikus rendszerben lenne megoldása az $(1 + \Upsilon)x = 1$ egyenletnek, akkor $(1 - \Upsilon)$ -val szorozva azt kapnánk, hogy $(1 - \Upsilon^2)x = 1 - \Upsilon$, azaz $\Upsilon = 1$, ami ellentmondás. A Study-féle rendszerben Ω nem invertálható, mert bármely $z = a + b\Omega$ esetén $z\Omega = a\Omega \neq 1$. ■

Gyakorlatok

4.5-1. Számítsuk ki i^n értékét, ahol $n \in \mathbb{Z}$.

4.5-2. Legyen $z_1 = 3 + 4i$ és $z_2 = 2 - 3i$. Mennyi lesz ekkor $z_1 + z_2, z_1 + \bar{z}_2, z_1 \cdot z_2, z_1 \cdot \bar{z}_2, z_1^{-1}, \bar{z}_2/z_1, \sqrt{z_1}, z_2^2 + z_2^3$?

4.5-3. Adjuk meg az alábbi komplex számok algebrai alakját:

- (1) $z_1 = 2(\cos \pi/6 + i \sin \pi/6)$
- (2) $z_2 = 17(\cos 3\pi/2 + i \sin 3\pi/2)$.

4.5-4. Adjuk meg az alábbi komplex számok trigonometrikus alakját:

- (1) $\cos \phi - i \sin \phi$,
- (2) $-\cos \phi - i \sin \phi$,
- (3) $-1 - i\sqrt{3}$,
- (4) $4i$.

4.5-5. Mi a geometriai jelentése az alábbiaknak:

- (1) $|z_1 - z_2|$, ahol $z_1, z_2 \in \mathbb{C}$,

A számfogalom felépítése

(2) i -vel történő szorzás,

(3) $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$ -vel történő szorzás?

4.5-6. Bizonyítsuk be, hogy tetszőleges z_1, z_2, \dots, z_n komplex számok esetén

$$|z_1 + z_2 + \dots + z_n| \leq |z_1| + |z_2| + \dots + |z_n|.$$

4.5-7. Bizonyítsuk be, hogy tetszőleges $z, w \in \mathbb{C}$ esetén teljesül a *parallelogramma-azonosság*:

$$|z + w|^2 + |z - w|^2 = 2|z|^2 + 2|w|^2.$$

4.5-8. Határozzuk meg az

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

polinom gyökeit.

4.5-9. Mennyi $\sin 3\alpha$ és $\cos 3\alpha$ pontos értéke, ha $\sin \alpha$ és $\cos \alpha$ ismert?

4.5-10. Mely z komplex számok elégítik ki a $\bar{z} = z^3$ egyenletet?

4.5-11. Hol helyezkednek el a komplex síkon azok pontok, amelyekre teljesül, hogy

- a) $\arg z = \pi/6$,
- b) $|z| = 2 \operatorname{Re}(z)$,
- c) $|z| = iz$,
- d) $\left| \frac{z - 3i}{z + i} \right| \geq 1$.

4.5-12. Adjuk meg az n -edik komplex egységgökök szorzatát ($n > 1$).

4.5-13. Mutassuk meg, hogy ha ε hatodik egységgökre $\varepsilon^{2013} = -1$, akkor ε primitív egységgöök.

4.5-14. Számoljuk ki a) $\sqrt[6]{1}$,

b) $\sqrt{-8i}$, és

c) $\sqrt[4]{-4}$ értékét.

4.5-15. Írjuk fel a $\sqrt{2+2i}$ komplex számot trigonometrikus és algebrai alakban is.

4.5-16. Igazoljuk, hogy egy m -edik és egy n -edik egységgöök szorzata mn -edik egységgöök.



A Mandelbrot-halmaz a komplex számoknak olyan részhalmaza, amelyre a $z_0 = c$, $z_{n+1} = z_n^2 + c$ rekurzív sorozat adott $z_0 \in \mathbb{C}$ kezdőpontból indulva korlátos. Rajzoljuk ki különböző tartományokban a halmazt! Az algoritmus működése: minden egyes kiinduló érték esetében megnézzük, hogy a rekurzióval előállított pontsorozat hogyan viselkedik. Lehetőségek: 1) Egy adott értékhez tartanak (konvergencia); 2) Két, vagy több érték között ingadoznak (határ-ciklus); 3) Korlátosak maradnak, de elemeik soha nem ismétlődnek (kaotikus dinamikai rendszer); 4) Végtelenbe tartanak. Azok a komplex számok alkotják a Mandelbrot-halmaz pontjait, amelyek az első három kategória valamelyikébe tartoznak. Attól függően lehet színezni egy kezdőpontot, hogy az iterációsorozat hány lépés alatt alatt hagyja el az előre kijelölt korlátos tartományt. A halmaz szélén az egyes részeket újra és újra kinagyítva visszatérő, egymáshoz hasonló motívumokat, indákat, spirálok fedezhetünk fel. A Mandelbrot-halmaz a matematika egyik legbonyolultabb képződménye. Ahhoz, hogy egyre beljebb és beljebb zoom-olhassunk, nagyobb pontosságot kínáló aritmetikai csomag hasz-

nálata javasolt. A halmazt BENOIT B. MANDELBROT amerikai tudósról nevezték el.



A Julia-halmazokat úgy kapjuk, hogy a Mandelbrot-halmaznál látott leképezésnél rögzített $c \in \mathbb{C}$ érték esetén a z kezdőértékét pásztázzuk a komplex számsík egy területén, és vizsgáljuk az iteráció során z végtelenbe menekülését. A halmazok GASTON JULIA francia matematikusról kapták a nevüket. Rajzunk Julia-halmazokat!

4.6. Algebrai és transzcendens számok

Vizsgáljuk meg a racionális együtthatós polinomok gyökeit.

4.6.1. definíció. Egy $\mathbb{Q}[x]$ -beli nem-nulla polinom komplex 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 .

4.6.2. definíció. A \mathbb{Q} felett nem algebrai komplex számokat **transzcendens számnak** nevezzük.

Ezek közé tartozik két fontos szám, az e és a π . Az e transzcendens mivoltát 1873-ban HERMITE, a π -ét 1882-ben LINDEMANN bizonyította. Utóbbiból már következik a körnégyzetes megoldhatatlansága, azaz hogy nem lehet körzövel és vonalzóval adott négyzettel egyenlő területű kört szerkeszteni.

Egyéb, bizonyítottan transzcendens számok:

- e^a , ahol a nem-nulla algebrai szám (Lindemann–Weierstrass-tétel),
- e^π , a Gelfond-konstans,
- i^i (Gelfond–Schneider-tétel),
- a^b , ahol a algebrai (de nem 0 vagy 1), b iracionális algebrai (Gelfond–Schneider-tétel), speciálisan
- $2^{\sqrt{2}}$, a Gelfond–Schneider-konstans (néha Hilbert-szám),
- $\sin(a)$, $\cos(a)$ és $\tan(a)$, továbbá multiplikatív inverzeik: $\csc(a)$, $\sec(a)$ és $\cot(a)$ tetszőleges nem-nulla algebrai a esetén (Lindemann–Weierstrass-tétel),
- $\ln(a)$, ha a algebrai és nem 0 vagy 1 (Lindemann–Weierstrass-tétel).

4.6.3. definíció. Egy $y = f(x)$ függvényt **algebrai függvénynek** nevezzük, ha megoldása valamelyen

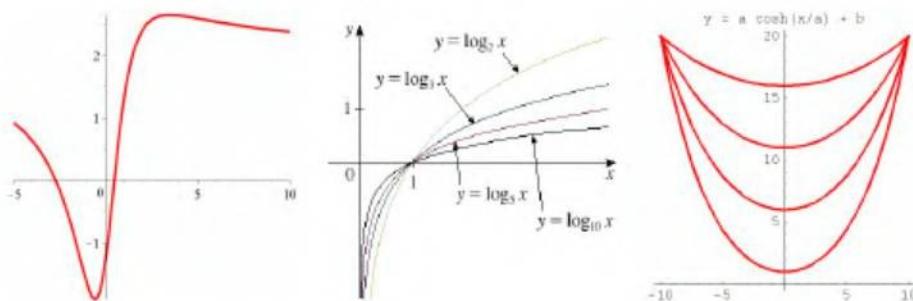
$$a_n(x)y^n + a_{n-1}(x)y^{n-1} + \cdots + a_0(x) = 0$$

alakú polinomegyenletnek, ahol minden $a_i(x) \in \mathbb{Q}[x]$. A nem-algebrai függvényeket **transzcendens függvényeknek** nevezzük.

4.31. példa. Az algebrai függvények polinomfüggvényekből tetszőleges számú algebrai műveettel (összeadás, kivonás, szorzás, osztás, gyökvonás) származtathatók. Például az

$$f(x) = \frac{4x^2 + 9x - 5}{2x^2 + 4}$$

A számfogalom felépítése



4.8. ábra. Az első ábra a 4.31. példa $f(x)$ algebrai függvénye. A második ábra a transzcendens log függvény. A harmadik ábra a láncgörbe (a koszinusz hiperbolikusz függvény speciálisan transzformált alakja), a két végénél felfüggesztett lánc vagy kötél saját súlya alatt felvett formája. Jegyezzük meg, hogy a függőhídak (pl. a budapesti Erzsébet-híd) alakja nem láncgörbe, hanem parabola.

függvény algebrai. Transzcendens függvények az $\exp(x)$, $\ln(x)$, $\sin(x)$, $\cos(x)$, $\tan(x)$ és a **láncgörbe** (4.8. ábra).

4.7. Kvaterniák

4.7.1. Konstrukció, tulajdonságok

A komplex számok konstrukciójánál látott $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ „megkettőzési eljárás” továbbvihető, az eredmény a $\mathbb{H} = \mathbb{C} \times \mathbb{C}$ kvaterniák halmaza. Ha báziselemként az $1, i, j, k$ szimbólumokat választjuk, akkor \mathbb{H} minden eleme

$$a + bi + cj + dk \quad (a, b, c, d \in \mathbb{R}) \quad (4.6)$$

alakban írható. A kvaterniák felfedezése HAMILTON ír matematikus nevéhez fűződik. A kvaterniokat precízen a már megszokott beágyazással kaphatjuk:

$$\begin{aligned} (z_1, w_1) \oplus (z_2, w_2) &= (z_1 + z_2, w_1 + w_2), \\ (z_1, w_1) \odot (z_2, w_2) &= (z_1 z_2 - w_1 \bar{w}_2, z_1 w_2 + \bar{z}_2 w_1). \end{aligned}$$

Ámbár a szorzás kísértetiesen hasonlít a komplex számok bevezetésekor alkalmazottal, de itt konjugáltak is szerepelnek.

4.7.1. tétele. $(\mathbb{H}; \oplus, \odot)$ ferdetest.

A struktúra nulleleme $(0, 0)$, egy (z, w) elem additív inverze $(-z, -w)$, a struktúra egységeleme $(1, 0)$, egy nem-nulla (z, w) multiplikatív inverze $(\bar{z}/(z\bar{z}+w\bar{w}), -w/(z\bar{z}+w\bar{w}))$. A $\Phi : \mathbb{C} \rightarrow \mathbb{H}$, $\Phi(z) = (z, 0)$ függvény injektív homomorfizmus, így a $(z, 0)$ alakú kvaterniokat \mathbb{C} -vel azonosíthatjuk. Összességében azt kapjuk, hogy $\mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$. Ha j jelöli a $(0, 1)$ kvaterniót, és k a $(0, i)$ kvaterniót, akkor minden (z, w) kvaterniós egyértelműen írható (4.6.) alakban.

Vagyis a \mathbb{H} -beli elemek összeadása koordinátánként, míg szorzása a 4.9. ábrán látható szorzótábla szerint történik.

.	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

4.9. ábra. A kvaterniók szorzási táblázata.

4.32. példa.

$$(1 + 2i + 3j + 4k) + (4 - 3i - 2j - k) = 5 - i + j + 3k, \text{ és}$$

$$(1 + 2i + 3j + 4k)(4 - 3i - 2j - k) = 20 + 10i + 20k.$$

4.33. példa. A kvaterniók halmaza megfelel a

$$\left\{ \begin{pmatrix} w & z \\ -\bar{z} & \bar{w} \end{pmatrix} \mid w, z \in \mathbb{C} \right\}$$

mátrixok halmazának. Ezeknek a mátrixoknak a determinánsa mindenkorban $|w|^2 + |z|^2$, amiből már következik a nullosztómentesség, hiszen a mátrixok gyűrűjében a nullosztók determinánsa nulla, itt pedig az összes nem-nulla mátrix determinánsa pozitív. A műveletek asszociativitása a mátrixműveletek asszociativitásából következik. A műveletekre vonatkozó szabályok egyszerű számolással igazolhatók.

4.7.2. definíció. Egy $z = a + bi + cj + dk$ kvaternió **skalár része** vagy **valós része** $\Re(z) = a$, **vektor része** vagy **képzetes része** $\Im(z) = bi + cj + dk$, **konjugáltja** $\bar{z} = a - bi - cj - dk$, abszolút értéke $|z| = \sqrt{a^2 + b^2 + c^2 + d^2}$.

Ha egy kvaternió skalár része nulla, akkor képzetes kvaterniónak nevezzük. A definíció jelöléseivel az alábbi téTEL igazolható:

4.7.3. téTEL. Minden $z, w \in \mathbb{H}$ -ra

- (1) $\bar{\bar{z}} = z$,
- (2) $\bar{z + w} = \bar{z} + \bar{w}$,
- (3) $\bar{z \cdot w} = \bar{w} \cdot \bar{z}$, (figyelem, a sorrend számít!)
- (4) $z + \bar{z} = 2\Re(z)$,
- (5) $z - \bar{z} = 2\Im(z)$,
- (6) $z\bar{z} = |z|^2$,
- (7) $z \neq 0$ esetén $z^{-1} = \bar{z}/|z|^2$,
- (8) $|0| = 0$, és $z \neq 0$ esetén $|z| > 0$,
- (9) $|z| = |\bar{z}|$,
- (10) $|z \cdot w| = |z| \cdot |w|$,
- (11) $|z + w| \leq |z| + |w|$ (háromszög-egyenlőtlenség).

Bizonyítás. (10) bizonyítása:

$$|zw|^2 = zw \bar{z}\bar{w} = zw \bar{w}\bar{z} = z |w|^2 \bar{z} = |w|^2 z\bar{z} = |w|^2 |z|^2 = |z|^2 |w|^2.$$

Figyelemre méltó, hogy a (3)-ban rejlő sorrendiség az egyetlen, amiben a téTEL összes állítása különbözik a komplex számoknál látottaktól. ■

4.7.4. Következmény. minden kvaternió felírható $z = \Re(z) + \Im(z)$ alakban.

4.7.5. definíció. Legyen V vektortér a \mathbb{K} test felett kiegészítve egy $\otimes : V \times V \rightarrow V$ művelettel. Ha tetszőleges $x, y, z \in V$ és $\alpha, \beta \in \mathbb{K}$ elemekre teljesül, hogy

- (1) $(x + y) \otimes z = x \otimes z + y \otimes z$ (jobb oldali disztributivitás),
- (2) $x \otimes (y + z) = x \otimes y + x \otimes z$ (bal oldali disztributivitás),
- (3) $(\alpha x) \otimes (\beta y) = (\alpha\beta)(x \otimes y)$ (műveleti kompatibilitás),

akkor V -t a \mathbb{K} test feletti **algebrának** (\mathbb{K} -algebrának) nevezzük.

4.7.6. téTEL (Frobenius, 1880). Ha \mathcal{A} olyan véges dimenziós \mathbb{R} -algebra, amely ferde-test, akkor \mathcal{A} izomorf a valós számok, a komplex számok, vagy a kvaterniók algebrájával.

A téTEL lezárja a számfogalom bővítésének folyamatát abban az értelemben, hogy nem kapunk jól használható struktúrát. Már a kvaterniók esetén is fel kellett adni a szorzás kommutativitását, más konstrukció pedig a téTEL szerint nem lehetséges.

4.7.2. A kvaterniók és a háromdimenziós euklideszi tér

Általános fogalmak

A skaláris és a vektoriális szorzás a vektoralgebra alapja, amelynek számtalan alkalmazása van mind a matematikában, mind a fizikában. A mechanika alapfogalmai, mint a test pozíóját megadó helyvektor, az elmozdulás, sebesség, gyorsulás, impulzus (vagy lendület), erő – minden vektormennyiségek.

4.7.7. definíció. Egy n -dimenziós vektortér $\mathbf{a} = (a_1, \dots, a_n)$ és $\mathbf{b} = (b_1, \dots, b_n)$ elemeinek **skaláris szorzatán** (vagy belső szorzatán) az

$$\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=1}^n a_i b_i$$

összeget (skalárt) értjük.

Többféle jelölés is adható, mi a fejezetben a definícióban megadottat használjuk. Speciálisan, a háromdimenziós térben két geometriai vektor skaláris szorzatát megkapjuk, ha összeszorozzuk abszolútértéküket (hosszukat) és az általuk közbezárt szög koszinuszát.

$$\langle \mathbf{a}, \mathbf{b} \rangle = |\mathbf{a}| |\mathbf{b}| \cos \theta.$$

Két vektor skaláris szorzatának előjelét meghatározza a közbezárt szögük. Ha ez hegyesszög, akkor a szorzat pozitív, ha tompaszög, akkor negatív. Ha két vektor merőleges egymásra, akkor skaláris szorzatuk 0. Az állítás megfordítható, ha a skalárszorzat nulla, akkor a két vektor merőleges (a zérusvektort minden vektorra merőlegesnek tekintjük). Belátjuk, hogy a kétféle felírási forma megegyezik. Egy tetszőleges $0 \neq \mathbf{v} = (v_1, \dots, v_n)$ vektorra

$$\langle \mathbf{v}, \mathbf{v} \rangle = v_1^2 + \dots + v_n^2 = |\mathbf{v}|^2 = |\mathbf{v}| |\mathbf{v}| \cos 0. \quad (4.7)$$

Két különböző, az origóból induló \mathbf{a} és \mathbf{b} vektorok esetén pedig ha $\mathbf{c} = \mathbf{a} - \mathbf{b}$, akkor egrészt a koszinusz-tétel miatt $|\mathbf{c}|^2 = |\mathbf{a}|^2 + |\mathbf{b}|^2 - 2|\mathbf{a}||\mathbf{b}| \cos \theta$, másrészt $|\mathbf{c}|^2 = \langle \mathbf{c}, \mathbf{c} \rangle =$

$\langle \mathbf{a} - \mathbf{b}, \mathbf{a} - \mathbf{b} \rangle$, és a disztributivitást alkalmazva kapjuk, hogy $|\mathbf{c}|^2 = \langle \mathbf{a}, \mathbf{a} \rangle + \langle \mathbf{b}, \mathbf{b} \rangle - 2\langle \mathbf{a}, \mathbf{b} \rangle$. A két egyenletből (4.7) miatt kapjuk az állítást.

A *vektoriális szorzást* csak 3-dimenziós (térbeli) vektorokra értelmezzük.

4.7.8. definíció. Két térbeli \mathbf{a}, \mathbf{b} vektor vektoriális (más néven külső- vagy keresztszorzata) a vektorokkal végzett olyan művelet, amelynek eredménye egy \mathbf{c} vektor az alábbi tulajdonságokkal:

- (1) \mathbf{c} nagysága (abszolút értéke) a két vektor hosszának és a közbezárt szögük szinusának szorzata ($0 \leq \theta \leq \pi$),
- (2) \mathbf{c} iránya merőleges mind \mathbf{a} -ra, mind \mathbf{b} -re (az \mathbf{ab} síkra),
- (3) \mathbf{c} iránya olyan, hogy $\mathbf{a}, \mathbf{b}, \mathbf{c}$ jobbsodrású vektorrendszer alkot.

Az $\mathbf{a}, \mathbf{b}, \mathbf{c}$ vektorrendszer akkor hívjuk jobbsodrásúnak, ha a jobb kezünk hüvelykujja \mathbf{a} -val, mutatóujja \mathbf{b} -vel, középső ujja pedig (tenyerünkre merőlegesen) \mathbf{c} -vel párhuzamosan áll. Jelölése: $\mathbf{a} \times \mathbf{b}$ (szóban: a kereszt b), tehát

$$|\mathbf{c}| = |\mathbf{a} \times \mathbf{b}| = |\mathbf{a}| |\mathbf{b}| \sin(\theta).$$

Ha elképzelünk egy paralelogrammát, aminek szomszédos oldalait az \mathbf{a} és \mathbf{b} vektorok alkotják, akkor $\mathbf{a} \times \mathbf{b}$ nagysága (tehát az eredményvektor hossza) megegyezik a két vektor által kifeszített paralelogramma területével. Két vektor vektoriális szorzata akkor és csak akkor nullvektor, ha párhuzamos állásúak, hiszen ekkor a bezárt szögük 0 vagy π , amiknek szinusza 0. Akkor lesz leghosszabb az eredményvektor, ha az összeszorzandó vektorok derékszögen állnak egymáshoz képest (mert $\pi/2$ szinusza 1). A vektoriális szorzat legegyszerűbb kiszámítási módja a

$$\mathbf{a} \times \mathbf{b} = \begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix}$$

determináns kiszámításával történhet (ahol \mathbf{i}, \mathbf{j} és \mathbf{k} az egységvektorok), vagyis egy derékszögű koordináta-rendszerben a \mathbf{c} eredményvektor koordinátáit a következőképp kaphatjuk meg \mathbf{a} és \mathbf{b} koordinátáiból: $c_1 = a_2b_3 - a_3b_2$, $c_2 = a_3b_1 - a_1b_3$, $c_3 = a_1b_2 - a_2b_1$.

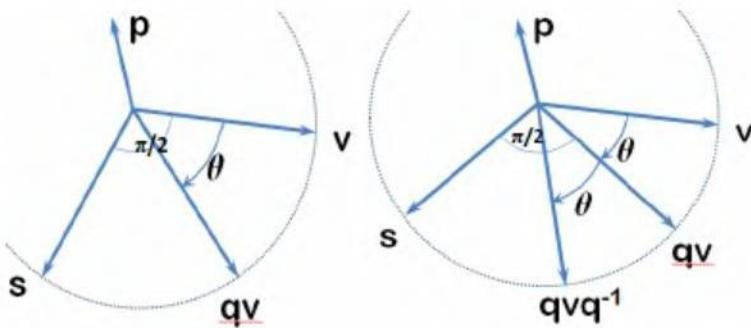
Képzetes kvaterniók szorzata

A továbbiakban azonosítjuk a kvaternióknál használt i, j, k szimbólumokat \mathbb{R}^3 standard ortonormált bázisával, azaz legyen $i = (1, 0, 0)$, $j = (0, 1, 0)$, $k = (0, 0, 1)$. Először megvizsgáljuk a tisztán képzetes kvaterniók szorzatát, amelyek felfoghatók a 3-dimenziós tér pontjaiként. Legyen $p = 0 + p_1i + p_2j + p_3k$, és $q = 0 + q_1i + q_2j + q_3k$. Ekkor

$$\begin{aligned} pq &= (-p_1q_1 - p_2q_2 - p_3q_3, p_2q_3 - p_3q_2, p_3q_1 - p_1q_3, p_1q_2 - p_2q_1) \\ &= -\langle p, q \rangle + p \times q. \end{aligned}$$

Ha tehát p, q merőleges vektorok, akkor skaláris szorzatuk 0, így szorzatuk tisztán képzetes. A skaláris és vektoriális szorzat tehát bizonyos értelemben a kvaterníoszorzat „része”.

A számfogalom felépítése



4.10. ábra. Bal oldali ábra: Ha a $q = \cos \theta + p \sin \theta$ egységnyi hosszú kvaterniót szorozzuk balról a v vektoriális kvaternióval, ahol p és v merőlegesek, a szorzat a v vektornak a p tengely körüli θ szögű elforgatását adja. Jobb oldali ábra: a $v \mapsto qvq^{-1}$ leképezés.

Egy tetszőleges és egy vektoriális kvaternió szorzata

Vizsgáljuk most meg egy tetszőleges és egy tiszta vektoriális kvaternió szorzatának geometriai jelentését. Legyen $q = q_1 + q_2i + q_3j + q_4k$ tetszőleges, de 1 abszolút értékű kvaternió, azaz $q_1^2 + q_2^2 + q_3^2 + q_4^2 = 1$. Legyen $q = q_1 + r$, ahol $r = q_2i + q_3j + q_4k$. Mivel $|q_1|^2 + |r|^2 = 1$, ezért létezik olyan θ szög, amelyre $q_1 = \cos \theta$ és $|r| = \sin \theta$. Teljesül továbbá, hogy $r = |r|p$, ahol p egységvektor. Következésképp

$$q = \cos \theta + p \sin \theta.$$

Hangsúlyozzuk, hogy minden 1 abszolút értékű kvaternió előállítható a fenti alakban. Most szorozzuk meg q -t valamelyen v vektoriális kvaternióval, de szorítkozzunk arra az esetre, amelyben v és p merőlegesek:

$$qv = (\cos \theta + p \sin \theta)v = v \cos \theta + pv \sin \theta.$$

Mivel p és v merőlegesek, $\Re(pv) = 0$, $\Im(pv) = p \times v = |p||v| \sin \pi/2 = |v|$, és $p \times v$ iránya olyan, hogy $p \times v$ -nek p -hez és v -hez viszonyított irányítása megegyezik k -nak i -hez és j -hez viszonyított irányával. Jelölje ezt a vektort s . Azt mondhatjuk, hogy s a v -ból a p vektor körüli $\pi/2$ nagyságú elforgatással adódik (4.10.bal oldali ábra). Összefoglalva tehát megmutattuk, hogy a $v \mapsto qv$ leképezés, ahol q egységnyi abszolút értékű $\cos \theta + p \sin \theta$ kvaternió, a v vektornak θ szöggel való elforgatása a p tengely körül, éspedig a p vége felől nézve olyan irányba, mint a k vektor felől nézve i -nek j -be való forgatása.

Tetszőleges térfelvételi forgatás kvaterniókkal

Tekintsük a $v \mapsto qvq^{-1}$ leképezést ($q = \cos \theta + p \sin \theta$). Megmutatjuk, hogy ez tetszőleges v vektorra pontosan a p tengely körüli 2θ szöggel történő elforgatás. Nyilván $q^{-1} = \bar{q} = \cos \theta - p \sin \theta$. Jelöljük a qv szorzatot (vektort) s -sel.

Először vizsgáljuk azt az esetet, amikor p merőleges v -re. Ekkor

$$qvq^{-1} = sq^{-1} = s(\cos \theta - p \sin \theta) = s \cos \theta - s' \sin \theta,$$

ahol $s' = (qv)p$. A korábbiakban láttuk, hogy ha v merőleges p -re, akkor qv is, így

$$qvq^{-1} = qv \cos \theta - s \times p \sin \theta = qv \cos \theta + p \times s \sin \theta.$$

A jobb oldalon egy olyan vektor áll, amit $s = qv$ -ből p körüli θ szögű elforgatásból kapunk. Ha még számításba vesszük, hogy magát a qv vektort is ugyanilyen elforgatással kaptuk v -ből, akkor már meg is bizonyosodtunk afelől, hogy qvq^{-1} a v vektor p körüli 2θ szögű elforgatásával áll elő.

A tetszőleges eset vizsgálata előtt megjegyezzük, hogy ha v számszorosa p -nek (azaz $v = \lambda p$), akkor $qv = vq$ és $qvq^{-1} = vqq^{-1} = v$.

Legyen most v tetszőleges. Bontsuk fel két összetevőre, legyen $v = v_1 + v_2$, ahol v_1 a v -re merőleges vektor, v_2 pedig p számszorosa. Ekkor

$$qvq^{-1} = qv_1q^{-1} + qv_2q^{-1} = qv_1q^{-1} + v_2.$$

Azt kaptuk, hogy a v_1 összetevő 2θ szöggel fordul el p közül, míg a v_2 összetevő változatlan marad. Összegezve eredményeinket azt kaptuk, hogy a p tengely körüli 2θ szögű elforgatással egy tetszőlegesen választott v vektor a qvq^{-1} vektorba megy át, ahol $q = \cos \theta + p \sin \theta$.

Elforgatások kompozíciója

Hajtsunk végre egy 2θ szögű elforgatást a p_1 egységvektorral megadott tengely körül, majd ezt követően hajtsunk végre egy másik, 2ϕ szögű elforgatást a p_2 tengely körül. Megmutatjuk, hogy az eredő (kompozíció) szintén egy elforgatás lesz (ez távolról sem nyilvánvaló). A kérdés az eredő elforgatás tengelye és szöge.

Az első elforgatással tetszőleges v vektor a $v_1 = q_1 v q_1^{-1}$ vektorba megy át, ahol $q_1 = \cos \theta + p_1 \sin \theta$. A második elforgatással v_1 a

$$v_2 = q_2 v q_2^{-1} = q_2 (q_1 v q_1^{-1}) q_2^{-1} = (q_2 q_1) v (q_2 q_1)^{-1}$$

vektorba jut ($q_2 = \cos \phi + p_2 \sin \phi$). Az eredő elforgatás tehát egy olyan elforgatás, ami a $q_2 q_1$ kvaterniós megfelelője. A szorzás elvégzése után elő kell állítani az eredménynek megfelelő $q_2 q_1 = \cos \psi + p \sin \psi$ alakot, ahol p egységnyi hosszúságú vektor. Az eredő elforgatás tengelye p , szöge 2ψ lesz.

4.34. példa. Az első elforgatás legyen egy x -tengelyű $\pi/3$ szögű elforgatás, a második pedig egy y -tengelyű, ugyancsak $\pi/3$ szögű elforgatás. Az első elforgatás megfelelője a $q_1 = \cos \pi/6 + i \sin \pi/6 = \sqrt{3}/2 + i/2$ kvaterniós, a másodiké a $q_2 = \cos \pi/6 + j \sin \pi/6 = \sqrt{3}/2 + j/2$ kvaterniós. Ekkor

$$q_2 q_1 = \frac{3}{4} + \frac{\sqrt{3}}{4}i + \frac{\sqrt{3}}{4}j - \frac{k}{4}.$$

Ennek a kvaterniónak a valós része $3/4$, amiből $\psi = \arccos 3/4$, így $\sin \psi = \sqrt{7}/4$. Azt kapjuk, hogy

$$q_2 q_1 = \cos \psi + p \sin \psi,$$

ahol

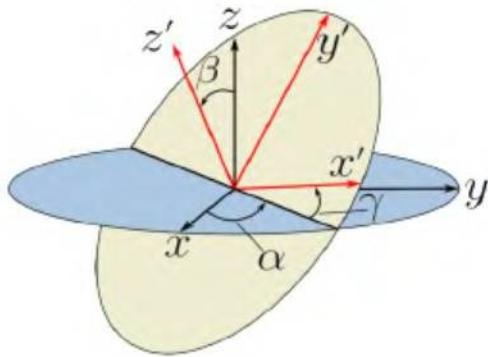
$$p = \sqrt{\frac{3}{7}}i + \sqrt{\frac{3}{7}}j - \frac{\sqrt{7}}{7}k.$$

Az eredő elforgatás tengelye tehát p , és az elforgatás szöge 2ψ .

Gyakorlatok

4.7-1. Ha $z = 1 + i + j + k$ és $w = j - k$ kvaterniós, határozzuk meg összegüket, szorzatukat, konjugáltjukat, négyzetüket, inverzüket, hányadosukat.

4.7-2. Mutassuk meg, hogy tetszőleges z kvaterniósra $z - izi - jzj - kzj = 4\Re(z)$.



4.11. ábra. A kvaternióknak számos elméleti alkalmazásuk mellett (kvantummechanika, stb.) a gyakorlatban a merev testek forgatásánál, a robotikában, 3D grafikában, a távközlési műholdak vezérlésében van nagy jelentőségük.



Tervezzünk olyan algoritmust, amelyben a kvaterníoszorzás 16 szorzás helyett 8 szorzással is megvalósítható (természetesen az összeadások rovására).



Írunk olyan programot, amely megvalósítja a kvaterniók elforgatásainak kompozícióját.

4.8. Oktávok (Cayley-számok)

A Frobenius-tétel szerint a számfogalom olyan további bővítése, amelyben testet vagy ferde testet kapunk nem lehetséges. Mégis furdalhat minket a kíváncsiság, hogy a komplex számoknál és a kvaternióknál is látott „duplázási eljárás” vajon hogyan folytatható.

4.8.1. Konstrukció, tulajdonságok

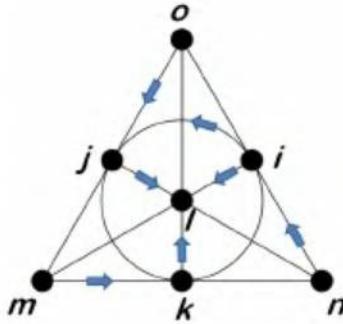
Az oktávokat a kvaterniókból kaphatjuk, $\mathbb{O} = \mathbb{H} \times \mathbb{H}$. A műveletek pedig

$$\begin{aligned}(z_1, w_1) \oplus (z_2, w_2) &= (z_1 + z_2, w_1 + w_2), \\ (z_1, w_1) \odot (z_2, w_2) &= (z_1 z_2 - \overline{w_2} w_1, w_2 z_1 + w_1 \overline{z_2}),\end{aligned}$$

ahol $z_1, w_1, z_2, w_2 \in \mathbb{H}$. A műveletek megadása teljesen megegyezik a kvaternióknál látottakkal, de most már a szorzások sorrendje is fontos, mert a kvaterníoszorzás nem kommutatív. Megfigyelhetjük, hogy

$$x \cdot (z, w) = (z, w) \cdot x = (xz, xw)$$

minden $x \in \mathbb{R}$ esetén teljesül. Ennek felhasználásával vezessük be az alábbi jelöléseket: legyen $l = (0, 1)$, $m = (0, i) = il$, $n = (0, j) = jl$, $o = (0, k) = kl$. Ekkor az i, j, k, l, m, n, o elemek mindegyikének négyzete -1 , a szorzataikra vonatkozó szabályok pedig a 4.12. ábráról olvashatók le: az egyeneseken, illetve a körön a megjelölt irányban az egyik elemtől a másikig (ciklikusan) haladva a szorzat a harmadik elem lesz, míg ellenkező irányban haladva annak ellentettje.



4.12. ábra. Az oktávok szorzása.

4.35. példa. $ij = k, jl = n, on = i, mn = -k$.

Azt kapjuk, hogy minden $u \in \mathbb{O}$ egyértelműen írható fel

$$u = a + bi + cj + dk + el + fm + gn + ho \quad (a, b, c, d, e, f, g, h \in \mathbb{R})$$

alakban.

4.8.1. definíció. Egy $u = a + bi + cj + dk + el + fm + gn + ho$ oktáv **valós része** $\Re(u) = a$, **képzetes része** $\Im(u) = u - \Re(u)$, konjugáltja $\bar{u} = \Re(u) - \Im(u)$, **abszolút értéke** $|z| = \sqrt{a^2 + b^2 + c^2 + d^2 + e^2 + f^2 + g^2 + h^2}$.

4.8.2. téTEL.

- (1) $(\mathbb{O}; \oplus)$ Abel-csoport,
- (2) $(\mathbb{O}; \odot)$ nem kommutatív, nem asszociatív,
- (3) $(\mathbb{O}; \odot)$ egységelemes, és minden nem-nulla elemnek létezik inverze,
- (4) $(\mathbb{O}; \oplus, \odot)$ -ban teljesül minden oldali disztributivitás,
- (5) $\Phi : \mathbb{H} \rightarrow \mathbb{O}$, $\Phi(z) = (z, 0)$ beágyazás, ezért $\mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O}$.

Továbbá minden $u, v \in \mathbb{O}$ esetén

- (6) $\bar{\bar{u}} = u$,
- (7) $\overline{u+v} = \bar{u} + \bar{v}$,
- (8) $\overline{u \cdot v} = \bar{v} \cdot \bar{u}$, (figyelem, a sorrend számít!)
- (9) $u + \bar{u} = 2\Re(u)$,
- (10) $u - \bar{u} = 2\Im(u)$,
- (11) $u\bar{u} = \bar{u}u = |u|^2$,
- (12) $|0| = 0$, és $u \neq 0$ esetén $|u| > 0$,
- (13) $|u| = |\bar{u}|$,
- (14) $|u \cdot v| = |u| \cdot |v|$,
- (15) $|u + v| \leq |u| + |v|$ (háromszög-egyenlőtlenség).

BIZONYÍTÁS. (1) Triviális, a nullelem a 0. (2) A szorzás nyilván nem kommutatív, de nem is asszociatív, mert például $(ij)l = kl = o \neq -o = in = i(jl)$. (3) A szorzás egységeleme az 1 és egy $u \neq 0$ oktáv inverze $u^{-1} = \bar{u}/|u|^2$. (4)–(5) A disztributivitások és a beágyazás nyilvánvalóak. (6)–(13) A definíciók következményei. (14) Hasonlóan igazolható, mint a kvaternióknál. ■

Az igazán megdöbbentő az, hogy minden tulajdonság ugyanúgy működik, mint a kvaternióknál, kivéve, hogy a szorzás nem asszociatív. Vajon meddig lehetne megkettőzéssel

A számfogalom felépítése

további azt az irányt, melyben lemondunk az asszociativitásról, de megőrizzük az invertálhatóságot? HURWITZ 1898-ban megmutatta, hogy a Cayley-számokon túl már sok jóra nem számíthatunk.

4.8.3. definíció. A \mathbb{K} test feletti V lineáris teret **normált térnak** nevezzük, ha létezik rajta egy valós értékű $\|\cdot\|$ függvény az alábbi tulajdonsággal:

- (1) $\|x\| \geq 0$ és pontosan akkor nulla, ha $x = 0$ (a távolság nemnegatív),
- (2) $\|x + y\| \leq \|x\| + \|y\|$ (háromszög egyenlőtlenség),
- (3) $\|\lambda x\| = |\lambda| \|x\|$

minden $x, y \in V$ és $\lambda \in \mathbb{K}$ esetén.

4.8.4. definíció. Egy normált vektorteret **normált algebrának** nevezünk, ha létezik rajta egy olyan $|\cdot|$ függvény, amelyre a norma-tulajdonságokon kívül teljesül még egy szorzási szabály is:

$$|z_1 z_2| = |z_1| |z_2| \quad (4.8)$$

minden z_1, z_2 elemre.

4.36. példa. \mathbb{R} normált algebra az abszolútérték-függénnel. A komplex számoknál a konjugálással megadott abszolút érték megfelelő lesz, hiszen ha $|z| = z\bar{z}$ ($z \in \mathbb{C}$), akkor a norma-tulajdonságok és (4.8) nyilván teljesül. Ugyanez mondható el a kvaterniók és az oktárok esetére is.

4.8.5. téTEL (Hurwitz). Ha \mathcal{A} olyan valós számtest feletti nem-asszociatív normált algebra, amelyben minden nem-nulla elemnek létezik multiplikatív inverze, akkor \mathcal{A} izomorf a Cayley-számok algebrájával.

Összefoglalva, a valós számtestnek véges fokú bővítése tehát csak kettő van, maga a valós számtest és a komplex számtest. A valós számtestnek véges fokú ferdetest bővítése az előbbiekt mellett még a kvaterniók ferdeteste, és más bővítés nem is lehetséges.

Megjegyzések a fejezethez

PEANO öt axiómája egyértelműen meghatározza a természetes számokat, sőt, egyik axióma sem hagyható el anélkül, hogy ne sérülne 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 $N = \{0, 1, 2\}$, $0' = 1$, és $1' = 2$, de nem értelmezzük a $2'$ jelölést. Ekkor az 1, 3, 4, 5 axiómák teljesülnek, de a második nem.

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

(4) Legyen $N = \{0, 1\}$, 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 konstrukciójának léteznek egyéb megközelítései is.

CANTOR a valós számok rendezett testének az ún. intervallum-skatulyázással történő jellemzését adta: ha a_n, b_n ($n \in \mathbb{N}$) valós számsorozatok, $a_n < b_n$, $a_n < a_{n+1}$, és $b_n > b_{n+1}$ ($n = 1, 2, \dots$), akkor

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

CAUCHY a racionális számok topológiai struktúrájának nem teljes voltából indult ki és jutott el a valós számokhoz. Például a $\sqrt{2}$ tizedes törtekben kifejezett közelítő értékeinek sorozata nem konvergens Cauchy-féle sorozat \mathbb{Q} -ban. Ha a racionális számok halmazát oly módon bővítjük ki, hogy benne minden Cauchy-féle sorozat konvergens legyen, a valós számokhoz jutunk. Az ilyen tulajdonságú topologikus tereket **teljesnek** nevezzük. Vegyük észre, hogy ennél a megközelítésnél nem kell sem \mathbb{Q} algebrai sem rendezési struktúráját felhasználni.

4.8.6. definíció. *Valamely M halmazt **metrikus térrének** nevezünk, ha létezik egy $d : M \times M \rightarrow \mathbb{R}_0^+$ leképezés (**metrika**) az alábbi tulajdonságokkal:*

1. $d(x, y) = 0 \Leftrightarrow x = y$,
2. $d(x, y) = d(y, x)$,
3. $d(x, y) + d(y, z) \geq d(x, z)$.

Bebizonyítható, hogy \mathbb{Q} és \mathbb{R} metrikus terek. A részleteket könyvünk harmadik részében tárgyaljuk.

DEDEKIND a valós számok axiomatikus felépítéséhez az algebrai és rendezési axiómákon kívül a teljességi axiómát (Dedekind-axióma vagy szétválasztási axióma) vezette be: legyen A és B a valós számok két nem-üres részhalmaza. Ha minden $a \in A$ és minden $b \in B$ elemre $a \leq b$, akkor létezik olyan c valós szám, amelyre

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

A természetes, egész, racionális és valós számkörök úgy is felépíthetőek lettek volna, hogy axiomatizáljuk a valós számokat, majd különböző megszorítások révén jutunk el a racionális, egész és természetes számokhoz.

A transzcendens számok létezését CANTOR és LIOUVILLE mutatta meg. 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 irrationális algebrai szám, állítható-e, hogy minden transzcendens. HILBERT a problémát igen nehéznek gondolta, de GELFOND és SCHNEIDER 1934-ben megoldották. Később a megoldási módszert még élesíteni is sikerült (BAKER, 1966).

A π -ről első írott emlékünk Kr. e. 1650 körüli, a számtannal és mértannal foglalkozó egyiptomi RHIND-papiruszban található, ahol JAHMESZ, az írnok, az alábbi számítási modellt fogalmazta meg: „A 9 egység átmérőjű kör területe ugyanakkora, mint a 8 egység oldalú négyzet területe.” Mindez mai jelölésekkel:

$$\left(\frac{9}{2}\right)^2 \pi = 8^2.$$

A számfogalom felépítése

Ebből π -re a $\frac{256}{81}$ racionális közelítését kapjuk, ami megközelítőleg 3,1605. Ugyanekkor Mezopotámiában a lényegesen rosszabb $\pi \approx 3\frac{1}{8} = 3,125$ közelítő értéket használták. A π megtalálható az Ószövetségben is³, ahol a nagyon durva $\pi \approx 3$ becslés szerepel. Kínában a földmérők akkortájt ugyanezzel az értékkel számoltak, majd ugyanott LIU CI csillagász munkássága nyomán (időszámításunk kezdete körül) törvény szabta meg a $\pi \approx 3,1547$ értékét. Az V-VI. században a hinduk már 9 tizedes jegyig ismerték a π jegyeit, amely a kor matematikai hátteréhez képest nagyon jó eredménynek számított. A XVIII. századig senki sem tudta, hogy a π racionális vagy irracionális. 1761-ben LAMBERT bizonyította, hogy a π irracionális szám, majd 1882-ben LINDEMANN bizonyította, hogy transzcendens. A π szimbólumot először JONES használta 1706-ban a *Synopsis Palmariorum Matheseos* című munkájában, majd EULER kezdte következetesen használni az *Introductio in analysin infinitorum*-tól kezdve, valószínűleg a görög $\pi\rho\nu\phi\rho\epsilon\iota\alpha$ (periféria, kerület) szó alapján. Azóta ez a jelölés vált elfogadottá.

GIBBS a kvaterniókra támaszkodva magyarázta a fizikai mennyiségek (például mágneses és elektromos jelenségek) dinamikáját. Szerinte mindegyik rendelkezik nagysággal és irányjal a háromdimenziós térben, ezért azt javasolta, hogy a kvaterniók szorzatát célszerű felbontani két részre: egy egydimenziós skaláris mennyiségre, és egy háromdimenziós vektorra. Mi is ezt az utat követtük.

Érdekes történet a Cayley-számok megszületése. Ezekre a „számokra” egymástól függetlenül CAYLEY, ARTHUR (1821–1895), illetve HAMILTON, SIR WILLIAM ROWAN (1805–1865) egyik főiskolai barátja, GRAVES bukkant rá. GRAVES-t ugyanúgy érdekeltek a háromdimenziós struktúrák kutatási eredményei, mint HAMILTON-t. Éppen ezért, a kvaterniók felfedezésének másnapján HAMILTON egy levelet írt barátjának, amelyben leírja eredményeit. GRAVES azon gondolkozott, vajon meddig lehet elmeni a képzetes számok hozzá vételében. Hamarosan meg is találta a nyolc dimenziós struktúrát, amelyeket oktávoknak (octaves) nevezett el. 1844-ben három levelet is írt HAMILTONNAK a kvaterniók és az oktávok általánosításáról. Úgy gondolta, hogy vannak minden n -re $2n$ -iök, és ebben a reményben kereste a 16 dimenziós változatot. Azonban nem volt biztos abban, hogy a sejtése igaz, és valóban létezik ilyen struktúra. HAMILTON megígérte barátjának, hogy publikálja eredményeit, de túlságosan elfoglalt volt, így folyton csak halogatta. Nem sokkal később HAMILTON egy levelében rámutatott arra, hogy GRAVES struktúrája nem asszociatív, bár a kvaterniók azok. HAMILTON tulajdonképpen ekkor fogalmazta meg az asszociativitás fogalmát, így ebben nagy szerepe volt GRAVES oktávjainak. Eközben CAYLEY, egy Cambridge-i friss diplomás, HAMILTON korábbi publikációja hatására szintén foglalkozott a kvaterniókkal. Ámbár ő elsősorban a kvaterniók és a hiperelliptikus függvények kapcsolatára volt kíváncsi. 1845-ben publikált is egy cikket a témaáról a Philosophical Magazine-ban. Az írás végén van egy rész a GRAVES által is felfedezett 8 dimenziós struktúráról. GRAVES írt az újságnak egy levelet, amelyben közli, hogy az ő hasonló eredményei korábbiak. HAMILTON is írt egy rövid megjegyzést az Ír Királyi Akadémiának, megerősítve GRAVES elsőbbségét. Azonban elkészett: a világ számára az új struktúra Cayley-számok néven maradt meg.

A vektoralgebra megalkotójának a matematikai közvélemény GRASSMAN-t tekinti, akinek ezzel foglalkozó könyve 1844-ben jelent meg. Nehézkes, spekulációkkal átszölt stílusa miatt nem kapott érdemleges figyelmet. 1878-ban CLIFFORD irányította rá a tudományos körök figyelmét – erről szóló cikke az American Journal of Mathematics első számában jelent meg.

³Királyok Könyve, 7.23

5. 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, a véges halmazok pontos megfogalmazása után megkíséreljük a leszámlálási problémákat alapmintákra visszavezetni, és általános módszereket kifejleszteni. Ismertetni fogjuk a klasszikus valószínűség fogalomrendszerét is. 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, sorozatokkal, és kombinatorikai összefüggésekkel foglalkozunk.

5.1. Véges halmazok

Könyvünk eddigi részében intuitíven használtuk a halmazok végességének fogalmát. Egy A halmazt akkor tekintettünk végesnek, ha megadható volt egy $\{1, 2, \dots, n\} \rightarrow A$ bijekció valamely $n \in \mathbb{N}$ -re. Azokat a halmazokat, amelyek nem végesek, végtelennek vettük. Ezzel az intuitív fogalommal az a baj, hogy a természetes számok fogalmára épül. A véges halmazoknak van azonban olyan jellemzésük is, amely csak elemi halmazelméletet használ.

5.1.1. definíció. *Egy A halmazt végesnek nevezzünk, ha nem létezik A -nak valamely valódi részhalmazára való bijektív leképezése.*

5.1.2. téTEL. *Ha $n \in \mathbb{N}$, akkor nem létezik bijekció $\{1, 2, \dots, n\}$ és egy valódi részhalmaza között.*

Bizonyítás. Indukcióval bizonyítunk. $n = 0$ -ra az állítás igaz, mert az üres halmaznak nincs valódi részhalmaza. Az indukciós feltevés szerint n -re teljesül az állítás, vagyis nem létezik bijekció $H_n = \{1, 2, \dots, n\}$ -nek egy valódi A részhalmazára. Vizsgáljuk meg az $n + 1$ -elemű H_{n+1} halmazt. Tegyük fel indirekt, hogy létezik egy ϕ bijekció H_{n+1} -nek egy valódi A részhalmazára. Három esetet fogunk megkülönböztetni:

- $n + 1 \notin A$. Ekkor léteznie kell egy bijekciónak H_n -ről A egy valódi részhalmazára, mert $\phi(n+1) \in A$, és ϕ megszorítása H_n -re A valódi részhalmazára képez. Ez ellentmond az indukciós feltevésnek.
- $n + 1 \in A$ és $\phi(n+1) = n + 1$. Ekkor $H_n \rightarrow A \setminus \{n + 1\}$ bijekció, ami szintén ellentmondás.
- $n + 1 \in A$ és $\phi(n+1) \neq n + 1$. Ekkor a $(k, n+1)$, $(n+1, l)$ reláció párokat kihagyva ϕ -ből, és hozzávéve a (k, l) , $(n+1, n+1)$ párokat, visszavezetünk a feladatot b)-re, vagyis ismét ellentmondást kaptunk. ■

5.1.3. Következmény. Az $\{1, 2, \dots, n\}$ és $\{1, 2, \dots, m\}$ halmazok között pontosan akkor létezik bijekció, ha $n = m$.

5.1.4. definíció. Azt az $n \in \mathbb{N}$ természetes számot, amelyre az $\{1, 2, \dots, n\}$ halmaz bijektíven képezhető le A -ra, az A halmaz **elemszámának**, vagy **számossgának** nevezzük. Jelölésben $\sharp(A)$, $\text{card}(A)$ vagy leggyakrabban $|A|$ használatos.

A $\text{card}(A)$ jelölés a *cardinal number* rövidítése.

5.1. példa. $\sharp(\emptyset) = 0$, $|\{a\}| = 1$, $\text{card}(\{a, b\}) = 2$ tetszőleges $a \neq b$ -re.

Ezzel megmutattuk, hogy korábban valóban helyesen használtunk az n -elemű halmaz kifejezést.

5.1.5. téTEL. Legyenek A és B halmazok. Ekkor

- (1) ha A véges és $B \subseteq A$, akkor B is véges és $|B| \leq |A|$;
- (2) ha A véges és $B \subset A$, akkor $|B| < |A|$;
- (3) ha A, B végesek és diszjunktak, akkor $A \cup B$ is véges, és $|A \cup B| = |A| + |B|$;
- (4) ha A, B végesek, akkor $|A \cup B| + |A \cap B| = |A| + |B|$;
- (5) ha A, B végesek, akkor $A \times B$ is az, és $|A \times B| = |A| \cdot |B|$;

BIZONYÍTÁS. Legyen $|A| = n, |B| = m$. (1) nyilvánvaló, ha $A = B$. Ha $B \subset A$, akkor B bijektíven képezhető le $\{1, 2, \dots, n\}$ egy valódi részhalmazára, ami valamely $m < n$ -re szintén bijektív $\{1, 2, \dots, m\}$ -mel. Ezzel (2)-t is beláttuk. (3) Mivel az $\{1, 2, \dots, m\}$ és $\{1+n, 2+n, \dots, m+n\}$ halmazok között létezik bijekció, ezért az $A \cup B$ és $\{1, 2, \dots, m+n\}$ között is. (4) következménye (3)-nak azzal az észrevételellet, hogy $|A \cup B| = |A \setminus B| + |A \cap B| + |B \setminus A|$. (5)-öt B elemszáma szerinti indukcióval kapjuk. A $|B| = 1$ eset nyilvánvaló. Tegyük fel, hogy $|B| = n$ -re az állítás teljesül. Ekkor az indukciós feltételből, és abból, hogy $A \times \{1, 2, \dots, n+1\} = A \times \{1, 2, \dots, n\} \cup A \times \{n+1\}$ kapjuk az állítást. ■

5.2. Permutáció, variáció, kombináció

5.2.1. Az ismétlés nélküli esetek

5.2.1. 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 permutációjának számát. Jelöljük ezt a számot P_n -nel. A problémát máshogyan megfogalmazva, ha $S_n = \{\varphi \mid \varphi : A \rightarrow A, \text{bijektív}\}$, akkor $P_n = |S_n|$ keresett. Láthatjuk, hogy P_n az A halmazon értelmezett permutációfüggvények száma. Bevezetjük az $n!$ (olvasd „n faktoriális”) jelölést az első n pozitív természetes szám szorzatára, tehát $n! = 1 \cdot 2 \cdot \dots \cdot n$. Meggondolható, hogy $0! = 1$.

5.2.2. 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

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

5.1. ábra. A faktoriális függvény első néhány értéke.

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 $P_n = n \cdot (n-1)! = n!$. ■

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

5.3. példa. A háromelemű halmazon értelmezett permutáció-függvények száma $3! = 6$, a konkret függvényeket a 2.22. példa mutatja.

A 5.1. ábra a faktoriális függvény értékeit mutatja az első néhány helyen. Hasznos megjegyezni 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 ($n-2$ darab szorzás egyre nagyobb és nagyobb számokon), ilyenkor a Stirling-formula ad jól használható becslést:

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

5.4. példa. Vajon milyen számra végződik $n!$ ha $n \geq 5$? Mivel a 2 és az 5 is tényezők $n!$ -ban, szorzatuk 10, tehát biztosan 0-ra. Na jó, de hányra? Nyilván annyira, ahány 10-es tényező felírható $n!$ -ban. Ez pedig pontosan annyi, ahány 5-ös tényező szerepel $n!$ törzstényezőkre bontásában (a 2-es tényezőből jóval több van, hiszen minden második szám páros és csak minden ötödik lesz 5 többszöröse). A keresett érték tehát

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{5^k} \right\rfloor,$$

hiszen minden ötödik szám osztható 5-tel, minden huszonötödik 5²-tel, etc. Például a 127! a tízes számrendszerben 31 nullára végződik.

Permutációkkal kapcsolatban időnként felmerül a **ciklikus permutálás** fogalma. Egy adott permutációban lévő elemeket ciklikusan permútálunk, 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. Ahelett, hogy n számú elemből n -elemű sorozatokat képeznénk, képehetünk k -elemű sorozatokat is, ahol $k \leq n$.

5.2.3. 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** nevezzük.

Jelölje V_n^k az n elem összes k -ad osztályú (ismétlés nélküli) variációi számát.

5.2.4. téTEL. $V_n^k = P_n / P_{n-k} = n(n-1) \cdots (n-k+1)$.

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, ahányféléképpen 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, ahányféléképpen 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. ■

5.5. példa. Arra, hogy 6 ember 10 különböző 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.

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

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

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

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

5.2.6. 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 sorba rendezés 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. ■

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

5.2.2. Az ismétléses esetek

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

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

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

5.2.8. 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 $V_n^{k,i} = V_n^{k-1,i} \cdot n = n^{k-1} \cdot n = n^k$. ■

5.7. példa. Egy totószelvényt (ahol 13+1 helyre 1,x vagy 2 kerülhet) $3^{14} = 4\,782\,969$ -féleképpen lehet kitölteni.

5.8. példa. Adjuk meg egy n -elemű A halmaz összes részhalmazainak számát. Mivel minden elem A valamely részhalmazához való tartozása a karakteristikus függvénytel egyértelműen jellemzhető, így az összes részhalmaz száma megegyezik az n -hosszú, 0, 1 jegykból álló különböző sorozatok számával, ami $V_2^{n,i} = 2^n$.

5.9. 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. Ekkor hányfélé azonosítót képezhetünk? Az első betűt $\binom{7}{1}$ -féleképpen választhatjuk, a többöt pedig 62^6 -féleképpen ($62 = 2 \cdot 26 + 10$). Ez összesen 397 601 649 088 lehetőség.

5.2.9. 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.

5.2.10. téTEL. $C_n^{k,i} = C_{n+k-1}^k$.

Bizonyítás. Az $\{1, 2, \dots, n\}$ halmaz valamely 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, az $\{1, 2, \dots, n+k-1\}$ halmaz k -ad osztályú ismétlés nélküli kombinációi száma az $n+k-1$ elemből képezhető k elemű szigorúan monoton sorozatok számával egyezik meg. Ennek megfelelően definiálunk két halmazt:

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

Mivel $|A| = C_n^{k,i}$ és $|B| = C_{n+k-1}^k$, a tételek bizonyításához elegendő egy bijekciót létesíteni a két halmaz között. Legyen $f : A \rightarrow B$ az alábbi: $a = (a_1, a_2, \dots, a_k)$ és $b = (b_1, b_2, \dots, b_k)$ esetén $f(a) = b$, ahol

$$\begin{aligned} b_1 &= a_1, \\ b_2 &= a_2 + 1, \\ &\dots \\ b_k &= a_k + (k-1). \end{aligned}$$

f nyilvánvalóan függvény. Mivel adott $b = (b_1, b_2, \dots, b_k) \in B$ ponthoz az f függvény képzési szabálya miatt egyetlen $a = (a_1, a_2, \dots, a_k)$ pont tartozik, ezért f injektív. De

f szürjektív is, hiszen tetszőleges $b \in B$ pontoz tartozó a pont minden eleme A -nak. Eszerint f bijekció. ■

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

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

Jelölje ezen ismétléses permutációk számát $P_n^{n_1, n_2, \dots, n_k}$.

5.2.12. 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 adott k különböző elem n_1, n_2, \dots, n_k előfordulási gyakoriságokkal. Az ismétléses permutációk között készítsünk relációt: két permutáció akkor legyen relációban, ha elhagyva belőlük az n_k -szor előforduló elemeket, 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 sorba rakott tárgy között $s - 1$ darab helyre, valamint az első elő és az utolsó 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

$$P_n^{n_1, n_2, \dots, n_k} = P_{n-n_k}^{n_1, \dots, n_{k-1}} C_n^{n_k} = \frac{(n - n_k)!}{n_1! n_2! \cdots n_{k-1}!} \frac{n!}{n_k! (n - n_k)!} = \frac{n!}{n_1! n_2! \cdots n_k!}.$$

■

5.11. példa. Két piros, négy fehér, egy zöld, valamint egy sárga golyót $8!/(2!4!1!1!) = 840$ -féleképpen lehet sorba rakni.

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 akárhány-szor felhasználhatjuk.

A fejezetben látott alapesetek a gyakorlatban nem önállóan, hanem vegyesen fordulnak elő.

5.12. példa. Egy trafikban kapható k fajta képeslap közül $\binom{k}{2}^n$ -féleképpen küldhetünk n barátunknak 2-2 különbözőt.

5.13. példa. 5 lapot húzunk egy 52 lapos franciakártya-csomagból. 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 összeszámolni. 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 $\binom{48}{4}$ -féléképpen. 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

5.2-1. Valamelyik héten az ötös és a hatoslottó nyereményalapja megegyezik. Melyik játékot érdemesebb játszani, ha a szelvények ugyanannyiba kerülnek?

5.2-2. Egy 12 csapatos labdarúgó tornán hányfélé sorrend alakulhat ki a dobogón?

5.2-3. A Földön a beszélt nyelvek száma körülbelül 6000, de ezek felét kevesebb mint 3000 ember beszéli (a különféle dialektusok száma eléri a 20 ezret). Hány szótárra lenne szükség, hogy bármely nyelvről bármely nyelvre fordíthassunk? A beszélt nyelvek száma rohamosan csökken, a szakértők szerint a ma beszélt nyelvek fele eltűnik 50-150 éven belül. Hány szótárra lesz szükség akkor? Mekkora a csökkenés?

5.2-4. Egy n -elemű halmazon hány rendezés konstruálható?

5.2-5. Egy n -elemű halmazon hány homogén binér reláció konstruálható? Ebből hány reflexív, hány szimmetrikus, és hány reflexív és szimmetrikus?

5.2-6. Hányféléképpen lehet eljutni az origóból a (2, 3, 5) pontba, úgy, hogy csak egységes hosszú jobbra, fel és előre lépések lehetségesek?

5.2-7. Az oxigénnek három, a hidrogénnek két stabil izotópja van. Hány stabil vízmolekula képződhet ezekből?

5.2-8. Hányféléképp választhatunk ki az $\{1, 2, \dots, 100\}$ halmazból két elemet, hogy összegük páros legyen?

5.2-9. Egy szállodába 12 fős csoporthoz érkezik. Hányféléképpen lehet elhelyezni őket, ha egy 2 fős, egy 4 fős, és egy 6 fős szoba szabad?

5.2-10. Hány csupa különböző jegyből álló hatjegyű szám képezhető? Ezen számok közül hány olyan van, amelyikben pontosan 4 páratlan számjegy szerepel?

5.2-11. Hányféléképpen ültethet le Hófehérke egy hosszú asztal mellé a 7 törpe közül ötöt, ha Tudor és Kuka nem ülhet egymás mellé?

5.2-12. Artúr király kerekasztala körül 12 lovag ül. Mindegyikük hadilábon áll a szomszédjával (és csak velük). Hányféléképpen választhat a király a hercegnő kiszabadítására 5 lovagot úgy, hogy ne legyenek közöttük ellenségek? És n lovag közül k -t?

5.2-13. Hány részre osztja a síkot n egyenes, ha „általános helyzetűek”, azaz közülük semelyik kettő sem párhuzamos és semelyik kettő sem megy át egy ponton?

5.2-14. Hány részre osztja a síkot n általános helyzetű kör?

5.2-15. Igazoljuk, hogy minden $k \geq 1$ -re k egymás utáni egész szám szorzata osztható $k!$ -sal.

5.2-16. Hány dominóból áll egy szabályos dominókészlet? (A pöttyök száma a dominók két felén 0-tól 9-ig terjed.)

5.2-17. Egy terem memmeyezetén 5 sorban és 6 oszlopban összesen 30 lámpa van felszerelve. Közülük 4 nem világít. Nincs olyan sor és nincs olyan oszlop, amelyben egynél több lámpa nem égne. Hányféléképpen lehetséges ez?

5.2-18. Hány különböző rendszám adható ki, amely három betűből és azt követő három számból áll (az angol ábécé 25 betűt tartalmaz)?

5.2-19. Legyenek $n, k \geq 1$. Hány olyan megoldása van az $x_1 + x_2 + \dots + x_k = n$ egyenletnek, ahol

$$\text{a)} x_1, x_2, \dots, x_k \geq 0 \text{ egész számok}$$

$$\text{b)} x_1, x_2, \dots, x_k \geq 1 \text{ egész számok}$$

és tekintettel vagyunk a sorrendre is?

5.2-20. Hányféleképpen lehet 10 számot 5 párba rendezni?

5.2-21. Hányféleképpen lehet sorba rakni n darab nullát és k darab egyest, hogy két egyes ne kerüljön egymás mellé?

5.2-22. A vakok részére készített Braille-írás (ejtsd: bráj) a következőképpen készül. Kartonpapírra előrenyomott téglalaphálózat egyes téglalapjaiba lyukakat szúrnak. A lyukak száma egytől hatig terjedhet, mégpedig úgy, hogy minden téglalapban, egymás alatti háromszor két hely megfelelő pontjainak kiszírásával. Az így kapott jeleket a vakok ujjaiikkal kitapintva „olvassák”. Hányféle jel készülhet így?

5.2-23. Egy páncélszekrény hat egymás mögötti tárcsa megfelelő beállításakor nyitható ki. A tárcsák 9 számjegyet tartalmaznak, amelyekből egyet kell beállítanunk. Ha valaki nem ismeri a megfelelő számkombinációt, mennyi időt vesz igénybe, amíg biztosan ki tudja nyitni a szekrényt, ha egy beállítás öt másodpercig tart?

5.2-24. Oldjuk meg az alábbi egyenletet:

$$\frac{1}{C_4^n} - \frac{1}{C_5^n} = \frac{1}{C_6^n}.$$

5.2-25. Számítsuk ki az

$$S(n) = \sum_{k=1}^n k C_n^k$$

összeget.



Írunk olyan programot, amely megadja az $\{1, 2, \dots, n\}$ halmaz összes permutációját, k -ad osztályú variációját, k -ad osztályú kombinációját, k -ad osztályú ismétléses variációját, k -ad osztályú ismétléses kombinációját, illetve i_1, i_2, \dots, i_r ismétlődésű permutációját. Elemezzük az algoritmusok műveletigényét.



Adjunk hatékony implementációt az $n!$ pontos értékének kiszámítására nagy n esetére, és vizsgáljuk meg a Stirling-formula hibáját az alábbi képlet alapján:

$$\sqrt{2\pi n} \left(\frac{n}{e}\right)^n \leq n! \leq \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \exp\left(\frac{1}{12n} - c_n\right)$$

ahol $0 \leq c_n \leq 1/180n^3$.

5.3. Kapcsolat a klasszikus valószínűsséggel

A valószínűségszámítás a matematikának azon ága, amely számszerűsíti egy esemény bekövetkezésének vagy be nem következésének esélyét. Feladata olyan mérték bevezetése, amely a bizonytalanságot numerikusan méri, így az események lehetséges előfordulásainak esélyeit össze lehet hasonlítani.

5.3.1. Eseményalgebra

Esemény

Véletlen kísérleten olyan jelenség megfigyelését értjük, amely azonos körülmények között akárhányszor megismételhető, és amelynek kimenetele előre meg nem mondható, mert az a véletlentől függ.

5.3.1. definíció. Egy véletlen kísérlet egyes kimeneteleit **elemi eseményeknek** nevezzük, a lehetséges kimenetelek halmazát pedig **eseménytérnek**. Az eseménytér részhalmazai az **események**.

Az eseményeket nagybetűkkel, az eseményteret Ω -val jelöljük.

5.14. példa. Ha egy szabályos dobókockával dobunk, akkor $\Omega = \{1, 2, 3, 4, 5, 6\}$. Elemi esemény lehet például az, hogy hatost dobunk, vagy az, hogy prímszámot dobunk. Egy esemény lehet például $A_1 = \{6\}$, vagy $A_2 = \{2, 3, 5\}$.

Egy A esemény akkor következik be, ha a véletlen kísérlet kimeneteként kapott elemi esemény A -hoz tartozik.

5.15. példa. (folytatás) Ha a kockadobás eredménye 5, akkor az A_1 esemény biztosan nem következett be, míg az A_2 esemény biztosan bekövetkezett.

Speciálisan, \emptyset és Ω is események. Az elsőt **lehetetlen eseménynek** nevezzük, mert soha nem következik be, a másodikat **biztos eseménynek** nevezzük, mert minden bekövetkezik.

Műveletek eseményekkel

5.3.2. definíció (események láncolata). Az $A \subseteq \Omega$ esemény bekövetkezése maga után vonja a $B \subseteq \Omega$ esemény bekövetkezését, ha B minden bekövetkezik, valahányszor A bekövetkezik. Jelölésben $A \subseteq B$.

5.16. példa. Két szabályos dobókockával dobunk. Jelentse az A esemény azt, hogy mindenketővel hatost dobunk, továbbá a B esemény azt, hogy a dobott számok összege páros. Ekkor $A \subseteq B$.

5.3.3. lemma. Tetszőleges $A, B, C \subseteq \Omega$ eseményekre

- $\emptyset \subseteq A \subseteq \Omega$
- $A \subseteq A$,
- $A \subseteq B$ és $B \subseteq A$ esetén $A = B$,
- $A \subseteq B$ és $B \subseteq C$ esetén $A \subseteq C$,

vagyis az $(\Omega; \subseteq)$ struktúra részbenrendezés.

5.3.4. definíció (esemény ellentettje vagy komplementere). Az $A \subseteq \Omega$ esemény **ellentettje** vagy **komplementere** az \bar{A} esemény, amely pontosan akkor következik be, ha A nem következik be.

5.17. példa. Ha a kockadobásnál az A esemény azt jelenti, hogy prímszámot dobunk, akkor $A = \{2, 3, 5\}$ és $\bar{A} = \{1, 4, 6\}$.

Nyilvánvaló, hogy $\bar{\Omega} = \emptyset$, $\bar{\emptyset} = \Omega$, és tetszőleges A eseményre $\bar{\bar{A}} = A$.

5.3.5. definíció (események összege). Legyen $A, B \subseteq \Omega$ két esemény. Ezen események **összege** az az esemény, amely pontosan akkor következik be, ha A vagy B bekövetkezik. Jelölésben $A + B$.

5.3.6. lemma. Legyen $A, B, C \subseteq \Omega$ tetszőleges esemény. Ekkor

- $A + B = B + A$ (kommutativitás)
- $(A + B) + C = A + (B + C)$ (asszociativitás)
- $A + A = A$ (idempotencia)
- $A + \Omega = \Omega$ (elnyelési tulajdonság)
- $A + \emptyset = A$
- $A + \bar{A} = \Omega$.

5.3.7. definíció (események szorzata). Legyen $A, B \subseteq \Omega$ két esemény. Ezen események **szorzata** az az esemény, amely pontosan akkor következik be, ha A és B is bekövetkezik. Jelölésben $A \cdot B$ vagy AB .

5.3.8. lemma. Legyen $A, B, C \subseteq \Omega$ tetszőleges esemény. Ekkor

- $A \cdot B = B \cdot A$ (kommutativitás)
- $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ (asszociativitás)
- $A \cdot A = A$ (idempotencia)
- $A \cdot \Omega = A$
- $A \cdot \emptyset = \emptyset$
- $A \cdot \bar{A} = \emptyset$.

5.3.9. definíció (események különbsége, szimmetrikus differenciája). Legyen $A, B \subseteq \Omega$ két esemény. Ezen események **különbsége** az az esemény, amely pontosan akkor következik be, ha A bekövetkezik, de B nem. Jelölésben $A - B$. Az A és B események $A \circ B$ **szimmetrikus differenciáján** azt az eseményt értjük, amely pontosan akkor következik be, ha az A és B közül pontosan az egyik bekövetkezik.

5.18. példa. A kockadobásnál jelentse A azt az eseményt, hogy páros számot dobunk, B pedig azt az eseményt, hogy 2-nél nagyobb számot dobunk. Ekkor $A + B = \{2, 3, 4, 5, 6\}$, $A \cdot B = \{4, 6\}$, $A - B = \{2\}$, $A \circ B = \{2, 3, 5\}$.

A különbség és a szimmetrikus differencia felírható az összeadással és a szorzással: $A - B = A \cdot \bar{B}$, $A \circ B = A \cdot \bar{B} + B \cdot \bar{A}$. Teljesülnek továbbá a műveleteket összekapcsoló disztributivitások is:

5.3.10. lemma. Legyen $A, B, C \subseteq \Omega$ tetszőleges esemény. Ekkor

- $A + (B \cdot C) = (A + B) \cdot (A + C)$
- $A \cdot (B + C) = (A \cdot B) + (A \cdot C)$

Az események összegére és szorzatára vonatkozó tulajdonságok szembetűnő hasonlósága nem a véletlen műve, ez az úgynevezett **dualitás elve**, amely a De Morgan azonosságok következménye:

5.3.11. lemma. Legyen $A, B \subseteq \Omega$ tetszőleges esemény. Ekkor

- $\overline{A + B} = \bar{A} \cdot \bar{B}$
- $\overline{A \cdot B} = \bar{A} + \bar{B}$.

5.3.12. definíció. Legyen A_1, A_2, \dots véges vagy végtelen sok esemény. Ezen események összegén azt az eseményt értjük, amely pontosan akkor következik be, ha legalább az egyik A_i esemény bekövetkezik. Az iménti események szorzatán azt az eseményt értjük, amely pontosan akkor következik be, ha minden A_i esemény bekövetkezik.

5.3.13. definíció (egymást kizáró események). Az olyan eseményeket, amelyek egyidejűleg nem következhetnek be, **egymást kizáró eseményeknek** vagy **diszjunkt eseményeknek** nevezzük.

5.19. példa. A kockadobásnál jelentse A azt az eseményt, hogy páros számot dobunk, B pedig azt az eseményt, hogy páratlan számot dobunk. Ekkor $A \cdot B = \emptyset$, vagyis A és B egymást kizáró események.

5.3.14. definíció (eseményalgebra). Az Ω eseménytér bármely részhalmazaiból képzett \mathcal{E} nem-üres eseményrendszeret **eseményalgebrának** nevezzük, ha zárt az összeadásra és a komplementerképzésre, azaz

- (1) minden $A, B \in \mathcal{E}$ esetén $A + B \in \mathcal{E}$, és
- (2) minden $A \in \mathcal{E}$ esetén $\overline{A} \in \mathcal{E}$.^a

^aHa (1) helyett azt az erősebb követelményt állítjuk fel, hogy \mathcal{E} legyen zárt tetszőleges (akár végtelen, de megszámlálható) sok tagjának egyesítésére, akkor a **σ -algebra** fogalmát kapjuk. Ha további erősítést teszünk, nevezetesen az uniós legyen zárt akármilyen végtelen családokra is, és egyúttal a (2) tulajdonságot meggyengítjük a komplementerre zártsgához helyett a (véges) metszetre való zártsgággal, a **topologikus tér** fogalmához jutunk. Mindkét fogalom a modern analízis és valószínűségelmélet kulcséléme.

Az eseményalgebra fogalomrendszerére megegyezik a halmazalgebrával:

esemény	\leftrightarrow	halmaz
eseménytér	\leftrightarrow	alaphalmaz (univerzum)
elemi esemény	\leftrightarrow	alaphalmaz elemei
események láncolata	\leftrightarrow	részhalma
lehetetlen esemény	\leftrightarrow	üres halmaz
biztos esemény	\leftrightarrow	alaphalmaz
események összege	\leftrightarrow	halmazok uniójá
események különbsége	\leftrightarrow	halmazok különbsége
események szorzata	\leftrightarrow	halmazok metszete

5.20. példa. (1) Ω összes részhalmazai halmaza eseményalgebrát alkot. (2) $\Omega = \{1, 2, 3\}$ esetén $\mathcal{E} = \{\emptyset, \{1\}, \{2, 3\}, \Omega\}$ eseményalgebrát alkot.

A továbbiakban jelentse \mathcal{E} az Ω eseménytér feletti eseményalgebrát.

5.3.15. téTEL. Legyen $A, B \in \mathcal{E}$. Ekkor

- (1) $\Omega \in \mathcal{E}$,
- (2) $\emptyset \in \mathcal{E}$,
- (3) minden $A, B \in \mathcal{E}$ esetén $A \cdot B \in \mathcal{E}$,
- (4) minden $A, B \in \mathcal{E}$ esetén $A - B \in \mathcal{E}$.

Bizonyítás.

- (1) $A \in \mathcal{E} \Rightarrow \overline{A} \in \mathcal{E} \Rightarrow A + \overline{A} \in \mathcal{E} \Rightarrow \Omega \in \mathcal{E}$.
- (2) $\emptyset = \overline{\Omega}$.
- (3) $A \cdot B = \overline{\overline{A} + \overline{B}}$.
- (4) $A - B = A \cdot \overline{B}$. ■

5.3.16. definíció. Az A_1, A_2, \dots , véges vagy végtelen sok esemény teljes eseményrendszerét alkot, ha

- (1) egyik sem a lehetetlen esemény, azaz minden i -re $A_i \neq \emptyset$,
- (2) az események egymást kizárok, azaz minden $i \neq j$ -re $A_i A_j = \emptyset$,
- (3) összegük a biztos esemény, azaz $A_1 + A_2 + \dots = \Omega$.

5.21. példa. Egy tetszőleges esemény és a komplementere teljes eseményrendszeret alkot, csak úgy, mint egy eseménytér összes elemi eseményei.

5.3.17. definíció. Boole-algebrának nevezzük az olyan algebrai struktúrát, amelyben értelmezve van két darab kétváltozós művelet (egy „összeadás” és egy „szorzás”), továbbá egy unér művelet, az „ellenérték”, valamint két speciális elem, az \emptyset és az Ω úgy, hogy teljesülnek az 5.3.6., 5.3.8., 5.3.10. lemmák azonosságai.

5.22. példa.

- A legegyszerűbb Boole-algebra csak az 1 és a 0 elemeket tartalmazza. Ez megfelel a korábban látott \vee, \wedge, \neg igazságértékekkel végzett logikai műveletek algebrájának.
- Egy adott $H \neq \emptyset$ halmaz esetén $\wp(H)$ Boole-algebrát alkot az unió, metszet, komplementer műveletekkel.
- Egy adott Ω eseménytér feletti \mathcal{E} eseményalgebra Boole-algebra az események összege, szorzata, komplementere műveletekkel.

5.3.2. A valószínűség

Egy kísérletsorozat során az A esemény bekövetkezésének gyakoriságát jelölje k_A . Egy A esemény **relatív gyakorisága** az esemény bekövetkezéseinek gyakorisága az összes kísérlet n számához viszonyítva, számszerűen k_A/n . A relatív gyakoriság kellően nagy számú kísérlet során egy számérték körül ingadozik. Ez a szám az A esemény valószínűsége. Az egyes események valószínűségeinek létezésére és tulajdonságaira vonatkozóan feltételeket kell tennünk. Erre vonatkoznak a valószínűségszámítás KOLMOGOROV orosz matematikustól származó axiómái.

5.3.18. definíció. Legyen adott egy Ω eseménytér feletti \mathcal{E} eseményalgebra. Ekkor a $P : \mathcal{E} \rightarrow \mathbb{R}_0^+$ függvényt valószínűségnek nevezzük, ha

- (1) minden $A \in \mathcal{E}$ eseményhez tartozik egy 0 és 1 közé eső $P(A)$ szám, azaz

$$0 \leq P(A) \leq 1;$$

- (2) a biztos esemény valószínűsége 1, azaz

$$P(\Omega) = 1;$$

- (3) az egymást páronként kizáró események összegének valószínűsége az egyes események valószínűségével egyenlő, vagyis az A_1, A_2, \dots, A_n események esetén ha $A_i A_j = \emptyset$ ($i \neq j$), akkor

$$P\left(\sum_i^n A_i\right) = \sum_i^n P(A_i).$$

5.3.19. definíció. Az (Ω, \mathcal{E}, P) hármast valószínűségi mezőnek nevezzük.

5.3.1. megjegyzés. A valószínűségi mezőt eseményalgebra helyett σ -algebra felett szokás értelmezni. Ekkor (3) helyett azt tesszük fel, hogy A_1, A_2, \dots események esetén ha

$A_i A_j = \emptyset$ ($i \neq j$), akkor $P(\sum_i A_i) = \sum_i P(A_i)$.

A valószínűségszámítás axiómáiból levezetjük a valószínűségszámítás tételeit.

5.3.20. téTEL. Az A esemény ellentettjének valószínűsége $P(\overline{A}) = 1 - P(A)$.

BIZONYÍTÁS. A második és a harmadik axióma miatt $1 = P(\Omega) = P(\overline{A} + A) = P(\overline{A}) + P(A)$, amiből az állítás következik. ■

5.3.21. Következmény. A lehetetlen esemény valószínűsége $P(\emptyset) = 0$.

5.3.22. Következmény. Ha A_1, A_2, \dots, A_n teljes eseményrendszer alkot, akkor valószínűségük összege egy.

BIZONYÍTÁS. $1 = P(\Omega) = P(A_1 + \dots + A_n) = P(A_1) + \dots + P(A_n)$. ■

5.3.23. téTEL. $P(B - A) = P(B) - P(AB)$.

BIZONYÍTÁS. Mivel $B = (B - A) + AB$ és $(B - A) \cdot (AB) = \emptyset$, ezért azt kapjuk, hogy $P(B) = P(B - A) + P(AB)$. ■

5.3.24. Következmény. Ha $A \subseteq B$, akkor $A \cdot B = A$, így $P(B - A) = P(B) - P(A)$.

5.3.25. téTEL. A valószínűség monoton, azaz ha $A \subseteq B$, akkor $P(A) \leq P(B)$.

BIZONYÍTÁS. A 5.3.24. következmény miatt $0 \leq P(B - A) = P(B) - P(A)$, amiből $P(A) \leq P(B)$. ■

5.3.26. téTEL. Az A és B események összegének valószínűsége $P(A + B) = P(A) + P(B) - P(AB)$.

BIZONYÍTÁS. Mivel $A + B = A + (B - A)$ és $A \cdot (B - A) = \emptyset$, ezért $P(A + B) = P(A) + P(B - A) = P(A) + P(B) - P(AB)$. ■

A klasszikus valószínűségszámítás olyan eseményekkel foglalkozik, amelyeknél az elemi események száma véges, és valószínűségük megegyezik, azaz amennyiben $\Omega = \{A_1, A_2, \dots, A_n\}$, akkor

$$P(A_i) = P(A_j) = \frac{1}{n}$$

minden $i \neq j$ esetén ($1 \leq i, j \leq n$). Ilyen esetekben a k_A -féléképpen bekövetkező A esemény valószínűsége

$$P(A) = \frac{k_A}{n} = \frac{|A|}{|\Omega|},$$

vagyis az A esemény bekövetkezésének valószínűsége arányos azoknak az elemi eseményeknek a számával, amelyek maguk után vonják A bekövetkezését. A klasszikus valószínűség számítási szabálya tehát

$$P(A) = \frac{\text{kedvező elemi események száma}}{\text{összes elemi esemény száma}}.$$

Ebben az esetben (Ω, \mathcal{E}, P) -t **klasszikus valószínűségi mezőnek** nevezzük.

5.23. példa. (1) Egy szabályos dobókocka feldobásakor minden elemi esemény valószínűsége $1/6$. A páros dobás valószínűsége $P(A) = 3/6 = 1/2$. (2) Egy 32 lapos kártyacsomagból egyetlen lap húzásának valószínűsége $1/32$. Piros lap húzásának valószínűsége $P(A) = 8/32 = 1/4$.

5.24. példa. Egy urnában n darab fehér és m darab fekete golyó van. Véletlenszerűen választunk az urnából k darabot. Mi a valószínűsége annak, hogy a kihúzott golyók között pontosan r darab lesz fehér ($r \leq k$, n és $k - r \leq m$)?

Jelöljük a kérdéses eseményt A -val. Az összes esetek száma nyilván $C_{n+m}^k = \binom{n+m}{k}$. Ezek közül azok lesznek a kedvezők, amikor a választott k darab közül éppen r darab lesz fehér és $k - r$ darab lesz fekete, vagyis a kedvező esetek száma $\binom{n}{r} \cdot \binom{m}{k-r}$. Így a keresett valószínűség

$$P(A) = \frac{\binom{n}{r} \cdot \binom{m}{k-r}}{\binom{n+m}{k}}.$$

5.3.3. A születésnap-paradoxon

A születésnap-paradoxon alapkérdése az alábbi: „Mekkora a valószínűsége annak az eseménynek, hogy emberek egy véletlenszerűen választott k fős csoportjában van legalább két személy, akik azonos napon születtek?” A paradoxon az, hogy (a józan ész diktálta sejtéssel ellentétben) ahhoz, hogy a kérdéses valószínűség $1/2$ körül legyen, elegendő $k = 23$ személyből álló csoportot választani.

5.3.27. téTEL (Születésnap-paradoxon alaptétele). Legyen adott egy n elemű T halmaz, a tulajdonságok halmaza, és egy M elemű halmaz, az objektumok halmaza (M legyen sokkal nagyobb, mint n). minden objektum azonos valószínűsséggel rendelkezik a tulajdonságok közül pontosan eggyel. Jelölje A azt az eseményt, hogy véletlenszerűen választva k objektumot lesz legalább kettő, amelyik azonos tulajdonsággal rendelkezik. Ekkor

$$P(A) = 1 - \frac{V_n^k}{n^k}.$$

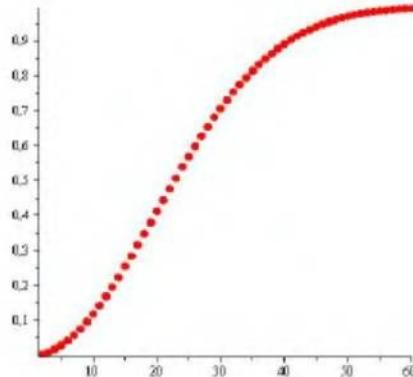
5.3.2. megjegyzés. A téTELben M konkrét értéke lényegtelen, a fontos az, hogy azonos valószínűsséggel tudunk az objektumok halmazából a különböző tulajdonságú elemek közül választani.

Bizonyítás. Tekintsünk egy

$$(t_1, t_2, \dots, t_k) \in \{1, 2, \dots, n\}^k \tag{5.1}$$

elemi eseményt, ahol az i -edik objektum a $t_i \in T$ tulajdonsággal rendelkezik ($1 \leq i \leq k$). Az összes elemi esemény száma nyilván n^k . A feltétel szerint az elemi események azonos valószínűsséggel következnek be, így az elemi események valószínűsége $1/n^k$. Annak az eseménynek a valószínűsége, hogy a választott k objektumból minden különböző tulajdonságú, nyilván $P(B) = 1 - P(A)$. Számoljuk ki $P(B)$ -t. A B -beli elemi események pontosan azok, amelyek esetén (5.1)-ben a koordináták minden különbözőek. Ezek száma V_n^k , a keresett valószínűség pedig

$$P(B) = \frac{1}{n^k} \prod_{i=0}^{k-1} (n-i) = \prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right).$$



5.2. ábra. Annak a valószínűsége, hogy k emberből kettőnek egy napra esik a születésnapja.

Mivel $1 + x \leq e^x$ minden x valós számra teljesül, ezért

$$P(B) \leq \prod_{i=1}^{k-1} e^{-i/n} = e^{-\sum_{i=1}^{k-1} i/n} = e^{-k(k-1)/(2n)}.$$

Jelöljük az iménti egyenlet jobb oldalát $1/\zeta$ -val, $1 \leq \zeta \in \mathbb{R}$. Könnyen ellenőrizhetjük, hogy amennyiben

$$k \geq (1 + \sqrt{1 + 8n \log \zeta})/2,$$

akkor $P(B) \leq 1/\zeta$, vagyis $P(A) \geq 1 - 1/\zeta$. ■

5.25. példa. Legyen $n = 365$. Egy $k = 23$ személyből álló csoport elegendő ahhoz, hogy legalább $1/2$ valószínűsséggel valamelyik két személynek egy napra essen a születésnapja. A 5.2. ábra mutatja azt a függvényt, amely leírja a valószínűség változását az emberek számának függvényében.

Amennyiben tehát van egy nagy méretű halmazunk, amelynek minden eleme azonos valószínűsséggel rendelkezik egy n elemű tulajdonsághalmazból választott tulajdonság valamelyikével, akkor n négyzetgyökének nagyságrendjébe eső méretű részhalmazt választva már nagy annak a valószínűsége, hogy a választott részhalmazban van legalább kettő azonos tulajdonságú elem.

A születésnapi paradoxon módosított formája az alábbi

5.3.28. tétele (Születésnap-paradoxon halmazokra). *Legyen adott egy n elemű T halmaz, a tulajdonságok halmaza, és egy M elemű halmaz, az objektumok halmaza (M legyen sokkal nagyobb, mint n). Minden objektum azonos valószínűsséggel rendelkezik a tulajdonságok közül pontosan eggyel. Jelölje A azt az eseményt, hogy véletlenszerűen választva két k elemű részhalmazt M -ből azok metszete nem üres. Ekkor*

$$P(A) = 1 - \frac{V_n^{2k}}{(V_n^k)^2}.$$

A bizonyítás teljesen hasonló a születésnapi paradoxon bizonyításához. A $k = \sqrt{n}$ választás esetén a $P(A) = 0.95$ közelítést kapjuk.

A lenyomatkészítő (vagy más néven: hash) függvények tetszőleges méretű bemenetből adott méretű kivonatot képeznek úgy, hogy magából a kivonatból a gyakorlatban

ne lehessen következtetni a kiindulási adatra, illetve nagyon nehéz legyen olyan másik adatsort készíteni, aminek ugyanaz lesz a kivonata. A lenyomatkészítő függvényeket több kriptográfiai protokoll is felhasználja, alapvető szerepe van például az üzenet sértetlenségét bizonyító eljárásokban, továbbá használják eredetiség ellenőrzésre is. A születésnap-paradoxon jelentőségét egy h hash függvény esetében az adja, hogy segítségével a $h(x_1) = h(x_2)$ ütközés valószínűsége becsülhető. Ha ugyanis h bemenete n bites, akkor a születésnapi paradoxon alapján $2^{n/2}$ véletlenül választott üzenet között $1/2$ -hez közeli valószínűsséggel lesz kettő, amelynek ugyanaz a hash értéke. Az ütközés-ellenállósághoz ezért a kimenetet úgy kell méretezni, hogy $2^{n/2}$ elég nagy legyen, így ütköző párok keresése véletlen választással ne legyen kivitelezhető. Ez manapság legalább $n = 160$ bites kimenetet jelent.

Gyakorlatok

5.3-1. Dobunk fel két (szabályos) dobókockát. Mennyi annak a valószínűsége annak, hogy a dobott pontok összege 8?

5.3-2. 10 darab modultesztet lefuttatunk abból a szempontból, hogy hány hibás modult találunk. Mik lesznek az eseménytér pontjai?

5.3-3. Bizonyítsuk be, hogy bármely eseményalgebrában érvényesek az alábbi azonosságok:

- a) $A = A \cap (A \cup B);$
- b) $A \cup B = A \cup (\overline{A} \cap B);$
- c) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C);$
- d) $(A - B) - C = (A - C) - (B - C);$
- e) $(A \cap B) - C = (A - C) \cap (B - C);$
- f) $A - (B \cup C) = (A - B) - C.$

5.3-4. Hány k hosszú infix van egy n hosszú szónak?

5.3-5. Egy pékségben három kemence működik. Jelentse A_i azt az eseményt, hogy az i -edik kemence szoftvere fél éven belül elromlik ($i = 1, 2, 3$). Fejezzük ki az A_i eseményekkel a következőket:

- a) csak az első romlik el;
- b) minden három elromlik;
- c) egyik sem romlik el;
- d) az első és második nem romlik el;
- e) az első és a második elromlik, a harmadik nem;
- f) pontosan az egyik kemence romlik el;
- g) legfeljebb egy kemence romlik el;
- h) legfeljebb két kemence romlik el;
- i) legalább egy kemence elromlik.

5.3-6. Egy dobozban 12 darab piros golyó van és még valamennyi fehér és zöld. Annak a valószínűsége, hogy pirosat vagy fehéröt veszünk ki találomra $2/3$. Annak, hogy fehéröt vagy zöldet választunk ki találomra $3/5$. Mennyi fehér és mennyi zöld golyó van a dobozban?

5.3-7. Legalább hányszor kell két kockát egyszerre feldobni, hogy 0, 9-nél nagyobb valószínűsséggel kapunk 6-t?

5.3-8. Négy pénzérmét dobunk fel egyszerre. Mennyi a valószínűsége annak, hogy

- a) mind a négy fej lesz;
- b) két fej és két írás lesz;
- c) legalább az egyik fej lesz?

5.3-9. Az 1, 2, 3, 4 számkártyákat összekeverjük, majd egymás után letesszük az asz-

talra. Mekkora a valószínűsége annak, hogy az így kirakott négyjegyű szám

- a) páratlan,
- b) hárommal osztható,
- c) négygyel osztható?

5.3-10. Mennyi a valószínűsége annak, hogy ha két egyforma kockával dobunk, 24 do-básból lesz egy dupla hatosunk?

5.3-11. Mekkora az esélye, hogy az ötlapos pókerben osztás után a kezünkben az alábbi leosztás található: royal flush, straight flush, póker, full house, flush, straight, drill, 2 pár, 1 pár, egyik sem?

5.4. Binomiális és polinomiális téTEL

Az alábbiakban két lényeges állítást vizsgálunk összegek hatványairól. Mindkét állítás bizonyításakor messzenenően kihasználjuk az általános asszociativitás, kommutativitás és disztributivitás tételét (4.1.15. téTEL).

5.4.1. téTEL (binomiális téTEL). *Legyen $(R; +, \cdot)$ egy kommutatív, egységelemes gyűrű, $x, y \in R$ 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 ($0 \leq k \leq n$). 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.

5.4.2. Következmény. *Legyen $n \in \mathbb{N}^+$. Az $x = y = 1$, illetve $x = 1, y = -1$ helyettesítéssel azt kapjuk, hogy*

$$\begin{aligned} \sum_{k=0}^n \binom{n}{k} &= 2^n, \\ \sum_{k=0}^n \binom{n}{k} (-1)^k &= 0. \end{aligned}$$

A következmény első állításával újabb bizonyítást adtunk arra, hogy egy n elemű halmaz összes részhalmazai száma 2^n . De vajon mi a helyzet akkor, ha kettő helyett többszöglű összeg n -edik hatványát szeretnénk kiszámítani?

5.4.3. téTEL (polinomiális téTEL). *Legyenek x_1, x_2, \dots, x_r egy kommutatív egységelemes gyűrű elemei és legyen $r, n \in \mathbb{N}^+$. Ekkor*

$$(x_1 + x_2 + \dots + x_r)^n = \sum_{i_1+i_2+\dots+i_r=n} P_n^{i_1, i_2, \dots, i_r} x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r}.$$

A „polinom” görög eredetű szó, jelentése „több tag”, ami esetünkben az $x_1 + \dots + x_r$ összegre vonatkozik.

Bizonyítás. Két különböző bizonyítást is adunk.

(1) Az n tényezős $(x_1 + x_2 + \dots + x_r)(x_1 + x_2 + \dots + x_r) \dots (x_1 + x_2 + \dots + x_r)$ szorzatból válasszuk ki x_1 -et i_1 -szer, ami $\binom{n}{i_1}$ -féleképpen lehetséges, a fennmaradó $n - i_1$ tényezőből x_2 -t i_2 -ször, ami $\binom{n-i_1}{i_2}$ -féleképpen lehetséges, és így tovább, az $n - i_1 - i_2 - \dots - i_{r-1}$ tényezőből x_r -t i_r -szer, ami $\binom{n-i_1-i_2-\dots-i_{r-1}}{i_r}$ -féleképpen lehetséges. Ekkor

$$\begin{aligned} & \binom{n}{i_1} \binom{n-i_1}{i_2} \dots \binom{n-i_1-i_2-\dots-i_{r-1}}{i_r} \\ &= \frac{n!}{(n-i_1)!i_1!} \frac{(n-i_1)!}{(n-i_1-i_2)!i_2!} \dots \frac{(n-i_1-i_2-\dots-i_{r-1})!}{(n-i_1-i_2-\dots-i_r)!i_r!} \\ &= \frac{n!}{i_1!i_2!\dots i_r!} = P_n^{i_1, i_2, \dots, i_r}, \end{aligned}$$

ami éppen az $x_1^{i_1} x_2^{i_2} \dots x_r^{i_r}$ tag együtthatója.

(2) 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 $x_2 + \dots + x_r = u$ helyettesítést, és tekintsük a binomiális tételelt. Ekkor

$$(x_1 + x_2 + \dots + x_r)^n = (x_1 + u)^n = \sum_{i_1=0}^n \binom{n}{i_1} x_1^{i_1} u^{n-i_1}.$$

Az indukciós feltevést u^{n-i_1} -re alkalmazva

$$\begin{aligned} & \sum_{i_1=0}^n \binom{n}{i_1} x_1^{i_1} \sum_{i_2+i_3+\dots+i_r=n-i_1} P_{n-i_1}^{i_2, i_3, \dots, i_r} x_2^{i_2} x_3^{i_3} \dots x_r^{i_r} \\ &= \sum_{i_1+i_2+\dots+i_r=n} \binom{n}{i_1} P_{n-i_1}^{i_2, i_3, \dots, i_r} x_1^{i_1} x_2^{i_2} \dots x_r^{i_r}. \end{aligned}$$

Felhasználva, hogy

$$\binom{n}{i_1} P_{n-i_1}^{i_2, i_3, \dots, i_r} = \frac{n!}{i_1!(n-i_1)!} \frac{(n-i_1)!}{i_2! \dots i_r!} = P_n^{i_1, \dots, i_r},$$

a bizonyítás kész. ■

A $P_n^{i_1, \dots, i_r}$ együtthatókat szokás *polinomiális együtthatóknak* is nevezni.

5.4.4. Következmény. Az iménti tételeben az $x_1 = \dots = x_r = 1$ helyettesítéssel

$$\sum_{i_1+i_2+\dots+i_r=n} P_n^{i_1, \dots, i_r} = r^n.$$

5.26. példa. Az $(x + y + z)^{100}$ kifejezésben az $x^{80}y^{15}z^5$ tag együtthatója

$$P_{100}^{80, 15, 5} = \frac{100!}{80! 15! 5!} = 8309886174740665324766880.$$

És mennyi lenne az $x^5y^{80}z^{15}$ tagé?

Gyakorlatok

- 5.4-1.** Határozzuk meg az $(1 + \sqrt[3]{5})^{2004}$ kifejtésének racionális tagjait.
- 5.4-2.** Hány nullára végződik $11^{100} - 1$?
- 5.4-3.** Mennyi lesz az $(3x + y + 5)^{2004}$ kifejtésében az együtthatók összege?
- 5.4-4.** Határozzuk meg az x^6 együtthatóját az $(1 + x)^n + (1 + x)^{n-1}$ kifejtésben, ha a tagok összevonása után a kifejtésben megjelenő binomiális együtthatók összege 1536.
- 5.4-5.** Bizonyítsuk be, hogy a $(2 + \sqrt{3})^n + (2 - \sqrt{3})^n$ kifejezés értéke minden $n \in \mathbb{N}$ -re egész.

5.5. A skatulya-elv

Egyszerű, de igen hasznos gondolatot fogalmazunk meg az alábbiakban.

5.5.1. téTEL (skatulya-elv). *Ha $n + 1$ darab dologot n skatulyába kell elhelyeznünk, akkor legalább egy skatulyába legalább két dolog kerül.*

Ez másként fogalmazva azt jelenti, hogy egy n -elemű halmaz n -elemű halmazra való leképezése akkor és csak akkor injektív, ha szürjektív.

5.27. példa. Megmutatjuk, hogy az $A = \{1, 2, \dots, 7, 8\}$ halmzból bárhogy is választunk ki ötöt, közülük valamelyik kettőnek az összege pontosan 9.

Konstruálunk 4 halmazt az alábbi módon: $A_1 = \{1, 8\}$, $A_2 = \{2, 7\}$, $A_3 = \{3, 6\}$, $A_4 = \{4, 5\}$. Az A halmzból kiválasztott öt szám mindegyike benne lesz A_1, \dots, A_4 valamelyikében. De mivel ez csak négy halmaz, valamelyik két szám ugyanabba a halmazba fog tartozni. Márpédig a halmazokon belüli számok összege mindig 9.

5.5.2. téTEL (Általános skatulya-elv). *Ha n darab dologot 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. ■

5.28. példa. Megmutatjuk, hogy 30 tetszőlegesen választott ember közül minden van legalább 5 olyan, akik a hétközött napján születtek.

A hétközött napjai lesznek a skatulyák, így az iménti tételek megfelelően $n = 30$ és $m = 7$. Ekkor $\lfloor(30-1)/7\rfloor + 1 = 5$ ember biztosan a hétközött napján ünnepli a születésnapját.

Gyakorlatok

- 5.5-1.** Mutassuk meg, hogy emberek bármely csoportjában van olyan 2 ember, akiknek a csoporton belül ugyanannyi ismerőse van.
- 5.5-2.** Mutassuk meg, hogy minden $m \in \mathbb{N}^+$ -hoz van olyan $n \in \mathbb{N}^+$, hogy az mn tízes számrendszerbeli alakjában minden jegy csupa 0 vagy 1.
- 5.5-3.** Bizonyítsuk be, hogy n darab tetszőlegesen választott egész közül minden kiválasztható néhány, hogy az összegük osztható legyen n -nel.
- 5.5-4.** Egy n elemű halmaznak legfeljebb hány részhalmaza adható meg úgy, hogy bármelyik kettő metszete nem-üres halmaz legyen?

5.5-5. Maximum hány olyan pontot lehet kijelölni egy 2 oldalú négyzetben, hogy bármely kettő távolsága $\sqrt{2}$ -nél nagyobb legyen?

5.6. A logikai szita formula

Legyen adott N objektum, amelyek közül bizonyosak rendelkeznek az előre megadott $\alpha_1, \alpha_2, \dots, \alpha_n$ tulajdonságok közül egyesekkel. Az N objektum bármelyikének lehet több tulajdonsága is, vagy akár egy sem. Jelölje $N(\alpha_i, \alpha_j, \dots, \alpha_k)$ azon objektumok számát, amelyek az $\alpha_i, \alpha_j, \dots, \alpha_k$ tulajdonságok mindegyikével (esetleg továbbiakkal is) rendelkeznek. Ha hangsúlyozni akarjuk, hogy olyan objektumot választunk ki, amelyik valamelyik tulajdonsággal nem rendelkezik, akkor azt fölülvonással jelöljük. Például $N(\alpha_1, \alpha_3, \bar{\alpha}_4)$ 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 $N(\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n)$ jelöli. Vezessük be az alábbi jelöléseket.

$$\begin{aligned} S_0 &= N, \\ S_1 &= N(\alpha_1) + N(\alpha_2) + \dots + N(\alpha_n), \\ S_2 &= N(\alpha_1, \alpha_2) + N(\alpha_1, \alpha_3) + \dots + N(\alpha_1, \alpha_n) + \dots + N(\alpha_{n-1}, \alpha_n), \\ S_3 &= N(\alpha_1, \alpha_2, \alpha_3) + \dots + N(\alpha_{n-2}, \alpha_{n-1}, \alpha_n), \\ &\vdots \\ S_n &= N(\alpha_1, \alpha_2, \dots, \alpha_n). \end{aligned}$$

Az összegzés az $\alpha_1, \dots, \alpha_n$ tulajdonságok minden lehetséges kombinációjára értendő a sorrend figyelembevétele nélkül.

5.6.1. téTEL. Az iménti jelölésekkel

$$N(\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n) = S_0 - S_1 + S_2 - S_3 + \dots + (-1)^n S_n.$$

Bizonyítás. Legyen P egy olyan objektum, amelyre az $\alpha_1, \alpha_2, \dots, \alpha_n$ 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, $\binom{k}{3}$ -ször a legalább három tulajdonsággal rendelkező objektumok számának felsorolásában, és így tovább, $\binom{k}{k}$ -ször a legalább k tulajdonsággal rendelkező objektumok számának felsorolásában. Így, ha $k \geq 1$, akkor a 5.4.2. következmény szerint a P objektum előfordulásainak száma az egyenlet jobb oldalán

$$1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \dots + (-1)^k \binom{k}{k} = (1 - 1)^k = 0.$$

Ha $k = 0$, akkor P egy olyan objektum, amely az $\alpha_1, \alpha_2, \dots, \alpha_n$ tulajdonságok közül egyikkel sem rendelkezik, így pontosan egyszer fordul elő az egyenlet jobb oldalán. Ezzel a tételett bebizonyítottuk. ■

A tételet általánosan is megfogalmazhatjuk: adott $A_1, A_2, \dots, A_n \subseteq H$ véges halmazok esetén hogyan számoljuk ki $\overline{A_1 \cup \dots \cup A_n}$ elemszámát, ha ismerjük az A_1, \dots, A_n halmazokból képzett összes egy, két, három, stb., n -tagú metszetek elemszámát.

5.6.2. téTEL (logikai szita formula). *Legyen H egy tetszőleges véges halmaz, A_1, A_2, \dots, A_n pedig H részhalmazai ($n \in \mathbb{N}$). Ekkor*

$$|\overline{A_1 \cup \dots \cup A_n}| = |H| + \sum_{r=1}^n (-1)^r \sum_{\substack{1 \leq i_1 < \dots < i_r \leq n}} |A_1 \cap \dots \cap A_{i_r}|.$$

A szita formulát gyakran szokták a **tartalmazás-kizáráS** elvének is nevezni. A szita formula az eratoszthenészi szita leszármazottja abban az értelemben, hogy az eratoszthenészi szita módszert ad azon számok meghatározására, amelyek prímszámok egy előre megadott véges halmazának egyik elemével sem oszthatók.

5.29. példa. Egy vállalatnál 67 ember dolgozik, közülük 47-en angolul, 35-en németül, 20-an franciaul, 23-an angolul és németül is, 12-en angolul és franciaul is, 11-en németül és franciaul is, végül mindenki nyelven 5-en beszélnek, akkor hány munkatárs nem beszéli a felsorolt nyelvek egyikét sem? A szita-formula szerint $67 - (47 + 35 + 20) + (23 + 12 + 11) - 5 = 6$.

5.30. 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 $X \rightarrow Y$ leképezések halmazát, ahol i nem képelem. Ekkor az $X \rightarrow Y$ 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 leképezésekbeli 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. Más szóval, ha S_r jelöli azon esetek számát, ahol legalább r darab képpont nem képelem, akkor $S_r = \binom{n}{r}(n-r)^k$. Így a szita formula alapján

$$|\overline{A_1 \cup \dots \cup A_n}| = \sum_{r=0}^n (-1)^r \binom{n}{r} (n-r)^k.$$

Gyakorlatok

5.6-1. Egy 100 hallgatóból álló évfolyamon 50 hallgató jár diszkrét matematika órára, 40 lineáris algebra órára, 35 programozás órára, 12 jár diszkrét matematika és lineáris algebra órára is, 10 diszkrét matematika és programozás órára is, 11 lineáris algebra és programozás órára is, 5 hallgató pedig minden a három órára jár. Hány hallgató jár legalább az egyik órára? Hány olyan hallgató van, aki nem jár az egyik órára sem?

5.6-2. 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.)

5.6-3. Egy toronyház legfelső emeletére 10 ember megy fel a rendelkezésre álló négy lift valamelyikével. Hányféleképpen történhet ez, ha egyik lift sem üres?

5.7. Speciális sorozatok

A rekurziótétel mintájára a természetes számok halmazán értelmezhetünk olyan függvényeket, amelyeknek az n helyen felvett értékei a $\{0, 1, \dots, n-1\}$ helyeken felvett értékeitől, vagy ezek közül néhányuktól függenek. Ezeket a függvényeket **rekurzív sorozatoknak** nevezzük. A sorozatok kezdőtagjait szintén meg kell adni, mert a következő tagok csak így lesznek egyértelműen meghatározottak. A kezdőtagok száma minden attól

Kombinatorika

függ, hogy a rekurzió a sorozat egy általános tagját hány előző tag függvényeként adja meg.

Ha egy rekurzív sorozat valamelyik elemére vagyunk kíváncsiak, akkor annak meg-határozásához az azt megelőző elemeket is ismernünk kell. Ez esetenként költséges. A gyakorlatban valamilyen „explicit formulát”, ún. zárt alakot próbálunk adni a sorozat általános tagjára. Az általános tag megadását a **rekurzió megoldásának** is nevezzük. Bizonyos lineáris rekurziók egyszerűen megoldhatók. *Generátorfüggvények* segítségével nem-lineáris rekurziókra is tudunk megoldást adni. Az ilyen vizsgálatokkal később fog-lalkozunk. Szerencsére egy sorozat különböző tulajdonságainak vizsgálata gyakran a rekurzió megoldása nélkül is lehetséges.

5.31. példa. Az informatikai algoritmusok elemzése során esetenként nagyon nehéz megsejteni a megoldást. Ilyenkor helyettesítő technikák, a rekurziós fa felrajzolása, vagy speciális esetekben a Mester Tétel segíthet bennünket. Ezekről bővebben algoritmusokkal foglalkozó könyvekben olvashatunk.

A rekurziók, különböző szempontokat figyelembe véve, többféleképpen osztályozhatók.

- Egy rekurzió lehet *első-, másod-, harmadrendű, stb.*, aszerint, hogy a rekurzió hány előző tag függvényében adja meg az új tagot. Például az $a_n = 5a_{n-1} + 4a_{n-2} + 3a_{n-3}$, $a_0 = 1, a_1 = 2, a_2 = 3$ harmadrendű rekurzió.
- Egy rekurzió lehet *lineáris vagy nem-lineáris* aszerint, hogy a tagot az előző tagok lineáris függvényeként adja-e meg. Például az iménti a_n rekurzió egy lineáris harmadrendű rekurzió, míg a $b_n = 5b_{n-1}^2 + 4$ egy nem-lineáris elsőrendű rekurzió.
- Egy rekurzió lehet *állandó vagy változó együtthatós* aszerint, hogy az a_n -et megadó függvényben az a_i -k együtthatói konstansok, vagy n -től függnek. Például az előző a_n és b_n rekurziók állandó együtthatósak, míg a $c_n = nc_{n-1} + 2$ egy változó együtthatós lineáris elsőrendű rekurzió.

Léteznak olyan sorozatok, amelyeknek a megoldása 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.

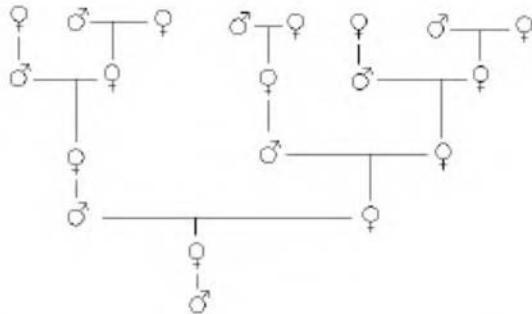
5.7.1. Fibonacci

A Fibonacci-sorozatot az alábbi lineáris másodrendű állandó együtthatós rekurzióval definiáljuk:

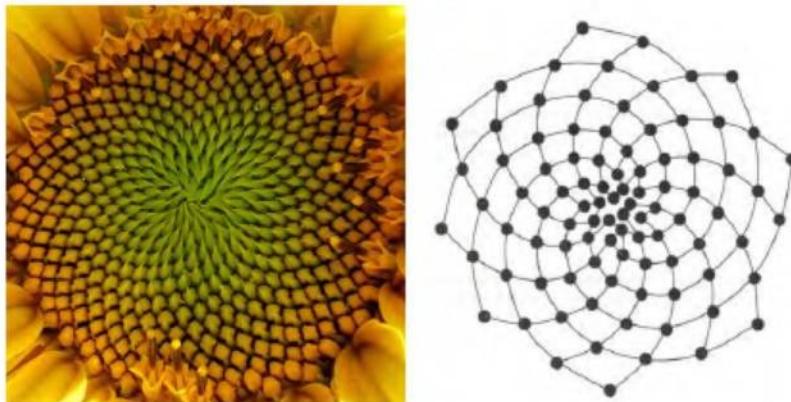
$$\begin{aligned} F_0 &= 0, \\ F_1 &= 1, \\ F_n &= F_{n-1} + F_{n-2} \quad (n > 1). \end{aligned}$$

Ez a legegyszerűbb olyan rekurziós szabály, amelyben a következő tag minden az előző kettőtől függ. Jegyezzük meg, hogy egy rekurziót a kezdeti értékek és a képzési szabály *együtt* határozza meg. A Fibonacci-rekurzióval a kezdeti értékek a lehető legegyszerűbbek.

5.32. példa. A „méhek családfája” jó példa arra, hogyan lehet a Fibonacci-sorozatot 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 (part-henogenetikus, szűznemzés). minden nónemű méhnek (dolgozó vagy királynő) azonban két szülője



5.3. ábra. A hímnemű méhek családfájának első öt szintje.



5.4. ábra. A napraforgó tányérján elhelyezkedő magok és modellje. A fotón is jól láthatók a spirálok, 21 spirál látszik az egyik, 34 a másik irányban. Ezek egymást követő Fibonacci-számok.

van, egy here és egy királynő. A 5.3. ábra a családfa első öt szintjét mutatja be. Egy herének tehát egy nagyapja és egy nagyanya, egy dédapja és két dédanya, két ükapja és három ükanya van. Általánosan, egy herének pontosan F_{n+1} „ n -edrendű nagyapja” és F_{n+2} „ n -edrendű nagyanya” van, ahol a nagyszülők esetén $n = 0$, a dédszülőknél $n = 1$, stb.

5.33. példa. Ahogy említettük, a Fibonacci-sorozat gyakran fordul 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 (5.4. ábra). Hasonló elrendezés figyelhető meg a fenyőtobozokon is.

A természetben számos példa akad még a Fibonacci-számok megjelenésére, de a számítástudományban is gyakran bukkannak elő. A 5.1. táblázat a Fibonacci-sorozat első néhány tagját mutatja.

5.7.1. tételel (Binet-formula). A Fibonacci-sorozat n -edik tagja

$$F_n = \frac{1}{\sqrt{5}} \left(\phi^n - \psi^n \right) \quad (n = 0, 1, 2, 3, \dots), \quad (5.2)$$

ahol

$$\phi = \frac{1 + \sqrt{5}}{2}, \quad \text{és} \quad \psi = \frac{1 - \sqrt{5}}{2}.$$

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

5.1. táblázat. A Fibonacci-sorozat első néhány tagja.

Bizonyítás. Mielőtt a (5.2) egyenletet bizonyítjuk, figyeljük meg az alábbi, ϕ -re és ψ -re vonatkozó azonosságokat:

$$\begin{aligned}\phi^2 &= \phi + 1, \\ \psi^2 &= \psi + 1, \\ \psi &= -1/\phi.\end{aligned}$$

A tételt n szerinti teljes indukcióval bizonyítjuk. $n = 0$ -ra és $n = 1$ -re az állítás nyilvánvaló. Csak a kíváncsiság kedvéért $n = 2$ -re $\phi^2 - \psi^2 = \phi - \psi = \sqrt{5}$, amire az állítás szintén teljesül. Tegyük fel, hogy az állítás $n - 1$ -ig igaz. Vizsgáljuk meg az n esetet.

$$\begin{aligned}F_n &= F_{n-1} + F_{n-2} = \frac{1}{\sqrt{5}}(\phi^{n-1} - \psi^{n-1}) + \frac{1}{\sqrt{5}}(\phi^{n-2} - \psi^{n-2}) = \\ &= \frac{1}{\sqrt{5}}(\phi^{n-1} + \phi^{n-2} - (\psi^{n-1} + \psi^{n-2})) = \\ &= \frac{1}{\sqrt{5}}(\phi^{n-2}(\phi + 1) - \psi^{n-2}(\psi + 1)) = \\ &= \frac{1}{\sqrt{5}}(\phi^n - \psi^n).\end{aligned}$$

■

Bármilyen meglepő, az (5.2) 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 képzőművészettel is, ahol **aranyometszés** néven ismert. A ϕ betű a görög PHEIDIAS tiszteletére utal, aki állítólag tudatosan használta ezt a számot a szobrászatban.

5.34. példa. Tapasztalati tény, hogy az emberek köldökmagasságának és teljes magasságának aránya kb. 1.618.

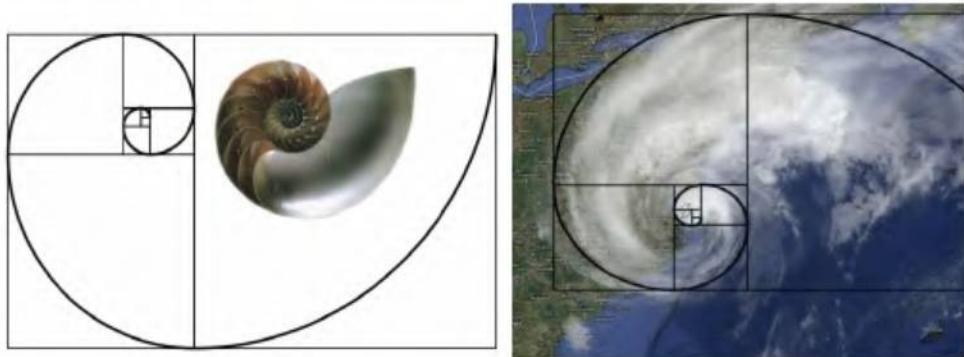
A téTELben szereplő állítást először EULER bizonyította 1765-ben.

5.7.2. Puskás, vagy a szubfaktoriális

Vajon hányféle módon lehet egy n számú különböző elemből álló sorozatot úgy átrendezni, hogy egyik elem se maradjon a helyén ($n \geq 2$)? Jelöljük ezeknek az ún. **fixpont nélküli permutációknak** a számát D_n -nel. Ezt az értéket az n elem **szubfaktoriálisanak** nevezzük. A probléma elemzését nézzük egy konkrét példán.

A legismertebb magyar a világon, akiről konkrétan tudják a származását, Puskás Ferenc. Tegyük fel, hogy egy csodálatos gólya után a nézőtéren ülő n ember örömeiben 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 sorszámról kalapot ($i \neq j$) kapja el $D_{n-1} + D_{n-2}$ esetben lehetséges, ugyanis A_j vagy az i sorszámról kalapot kapja el (D_{n-2} számú lehetőség), vagy egy másikat (D_{n-1} számú lehetőség). Mivel A_i egy i -től különböző sorszámról kalapot $n - 1$ -féleképpen kaphat el, az alábbi rekurzió adódik:

$$D_n = (n - 1)(D_{n-1} + D_{n-2}).$$



5.5. ábra. Ha veszünk két egymáshoz illeszkedő egység oldalú négyzetet, és e kettő mellé illesztünk egy dupla ilyen oldalhosszú négyzetet, majd ezt tovább folytatjuk, akkor az így keletkező négyzetek oldalhossza megegyezik a Fibonacci-számokkal. Az így keletkezett ábrába spirálist rajzolva az ún. Fibonacci-spirált kapjuk. A bal oldali ábrán a náutilus látható, ami egy, a Csendes-óceán nyugati részén élő, a puhatestűek törzsébe, a fejlábúak osztályába tartozó csigaházas polip, amelynek (szabályos) héja van. A jobb oldali ábra egy hurrikán műholdfelvételét mutatja az északi féltekén. (Vajon a déli féltekén képződő hurrikánok milyen „sodrásúak”?)

n	0	1	2	3	4	5	6	7	8	9	10
D_n	1	0	1	2	9	44	265	1854	14 833	133 496	1 334 961

5.2. táblázat. A szubfaktoriális-sorozat első néhány tagja.

A szubfaktoriális elnevezés a faktoriálisokkal vett hasonlóságból ered. Könnyen igazolható ugyanis, hogy

$$n! = (n-1)((n-1)! + (n-2)!).$$

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 (akár éppen a sajátját is), ez $(n-k)!$ lehetőség. Összesen tehát $S_k = \binom{n}{k}(n-k)!$. A szita formula szerint a minket érdeklő permutációk száma

$$D_n = \sum_{k=0}^n (-1)^k \binom{n}{k} (n-k)! = \sum_{k=0}^n (-1)^k \frac{n!}{k!} = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \dots + (-1)^n \frac{1}{n!} \right). \quad (5.3)$$

Az analízisben járatosak észrevehetik, hogy a szorzat második tényezője éppen e^{-1} hatványsorának kezdete. A formulából következik, hogy célszerű a $D_0 = 1$ megállapodás. Ekkor $D_1 = 0$, $D_2 = 1$, $D_3 = 2$, stb. A 5.2. táblázatban a szubfaktoriálisok sorozatának első néhány tagját láthatjuk.

A D_n szubfaktoriális értéke tehát (5.3) alapján nagy n -ekre is könnyen számolható:

$$D_n = \left\lfloor \frac{n!}{e} \right\rfloor,$$

ahol $\lfloor n \rfloor$ az n -hez legközelebbi egészet jelöli, a fél-egészknél a páros felé történő szokásos kerekítési szabály alkalmazásával ($\lfloor 3.5 \rfloor = 4$).

5.7.3. Pascal és a 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 (5.3. táblázat). Ha a táblázatot alaposan szemügyre vesszük, számtalan érdekes összefüggés tárul elénk. Az első a táblázat sorainak szimmetriája. Az

$$\binom{n}{k} = \binom{n}{n-k}$$

szimmetria-tulajdonság következik a definícióból, de abból is, hogy n elemből pontosan annyiféleképpen választhatunk ki k darabot, ahányféléképpen a fennmaradó $n - k$ darabot. További észrevétel, hogy a táblázat n -edik sorának ($n > 0$) k -adik eleme a fölötté lévő és a fölötté lévő bal oldali szomszédjainak összege, vagyis

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Az **addíciós képlet** 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

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-2}{k-1} + \cdots + \binom{k}{k-1} + \binom{k-1}{k-1}.$$

A kapott **felső összegzés** képlete azt jelenti, hogy a táblázatban egy elem a tőle balra lévő oszlopban a fölötté lévő elemek összege. Jól használható és elemi észrevétel még az **elnyelési tulajdonság**:

$$\binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1}.$$

A $0 \leq r$ és $r \leq n$, $r \leq m$ esetben az

$$\binom{m+n}{r} = \sum_{k=0}^r \binom{m}{k} \binom{n}{r-k}$$

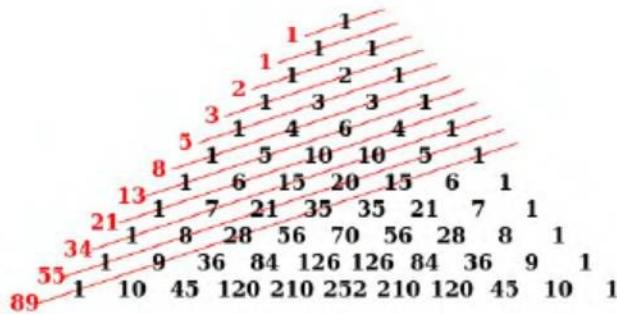
Vandermonde-azonosság az alábbi módon bizonyítható: Legyen A egy m elemű, B pedig egy n elemű halmaz úgy, hogy $A \cap B = \emptyset$. Ekkor $A \cup B$ elemszáma $m + n$. Hány r elemű részhalmaza van $A \cup B$ -nek? Egyszerűbb $\binom{m+n}{r}$, másrészt minden r elemű részhalmazt megkapunk úgy, hogy az összes lehetséges módon vesszük A -nak egy k elemű részhalmazát és B -nek egy $r - k$ elemű részhalmazát, majd képezzük ezek unióját, ahol $0 \leq k \leq r$. A lehetőségek száma éppen a képletben lévő jobb oldali összeg.

Ha a Vandermonde-azonosságban $n = m = r$, a szimmetria-tulajdonságot alkalmazva az alábbi **négyzetösszeg-tulajdonságot** kapjuk:

$$\sum_{j=0}^m \binom{m}{j}^2 = \binom{2m}{m}.$$

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

5.3. táblázat. A Pascal-háromszög első néhány sora.

5.6. ábra. A Pascal-háromszög és a Fibonacci-számok kapcsolata: $F_n = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-k-1}{k}$.

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 korlát kapható:

$$\begin{aligned} \binom{n}{k} &= \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1} \\ &\leq \frac{n^k}{k!} \\ &\leq \left(\frac{en}{k}\right)^k. \end{aligned}$$

5.7.4. Catalan

Bolyongási problémák a matematika és a fizika számos területén előbukkanak. Véletlen bolyongásra a legegyszerűbb példa egy egyenes mentén történő mozgás: a véletlen bolyongó lehet egy részeg bolha, aki nem tudván merre ugorjon (előre vagy hátra), minden ugrás előtt egy érme feldobásával dönt. Ha például fejet dob, akkor előre ugrik, ha az érme írást mutat, akkor hátra. Az így kapott modell általánosítható síkban vagy térben való mozgásra is, és nagyon sikeresen alkalmazható összetett fizikai rendszerek leírására. Például a tea anyagainak a filterből való kioldódását pontosan ennek a modellnek a térbeli, folytonos idejű általánosítása írja le.

5.35. példa. Az egész rácson csak jobbra vagy felfelé lépegetve egyet-egyet $\binom{n+m}{n} = \binom{n+m}{m}$ -féleképpen juthatunk el az origóból az (n, m) pontba ($n, m \geq 0$).

Tekintsük az alábbi feladatot: egy mozi pénztára előtt $m+n$ ember áll sorban. Közülük m -nek van kétezer forintos bankjegye, n -nek van ezer forintos. Nyitáskor nincs pénz a pénztárban és a mozigégy ára ezer forint. Hányféleképpen állhatnak sorba az emberek, hogy egyszer sem szakadjon meg a jegykiadás váltópénz hiánya miatt?

Nyilván $m \leq n$ (máshogy nincs megoldás). minden egyes sorban állásnak feleltessünk meg a koordináta-rendszerben egy olyan utat, amely az origóból indul és az (n, m) koordinátájú pontba vezet. Ha valaki ezressel áll sorban, a megfelelő egységnyi útszakasz legyen vízszintes, ha kétezessel, függőleges. Így minden út egyértelműen megfelel egy sorban állásnak. Az összes lehetséges sorban állások $((n, m)$ pontba vivő utak) száma $\binom{n+m}{n}$. Ezek között persze vannak nem megfelelők is, amikor megszakad a jegykiadás. Ez akkor fordul elő, ha valaki kétezessel akar fizetni, de a pénztárban nincs visszajáró ezres. Más szavakkal akkor, ha az út metszi az $y = x + 1$ egyenest. minden egyes rossz útnak keressük meg az $y = x + 1$ egyenettel való első metszéspontját, és az út hátralévő részét tükrözük az egyenesre. Így egy olyan úthoz jutunk, ami az origóból az $(m-1, n+1)$ pontba vezet csak jobbra, illetve felfelé történő haladással. Az ekképp definiált leképezés bijektív: szürjektív, mert ha egy tetszőleges $(m-1, n+1)$ pontba vivő utat nézünk, az metszi az $y = x + 1$ egyenest, és az első metszéspont utáni részt az egyenesre tükrözve kapjuk a (m, n) -ba vivő rossz utat; a leképezés injektív, mert ha két rossz út különbözik, akkor a tükrözéssel nyert változatok is különböznek. Ezért a rossz utak száma pontosan $\binom{n+m}{m-1}$, vagyis a megfelelő sorban állások száma

$$\binom{m+n}{n} - \binom{m+n}{m-1} = \frac{n-m+1}{n+1} \binom{m+n}{n}.$$

Amennyiben $m = n$, akkor

$$C_n = \frac{1}{n+1} \binom{2n}{n} \quad (n \geq 0) \tag{5.4}$$

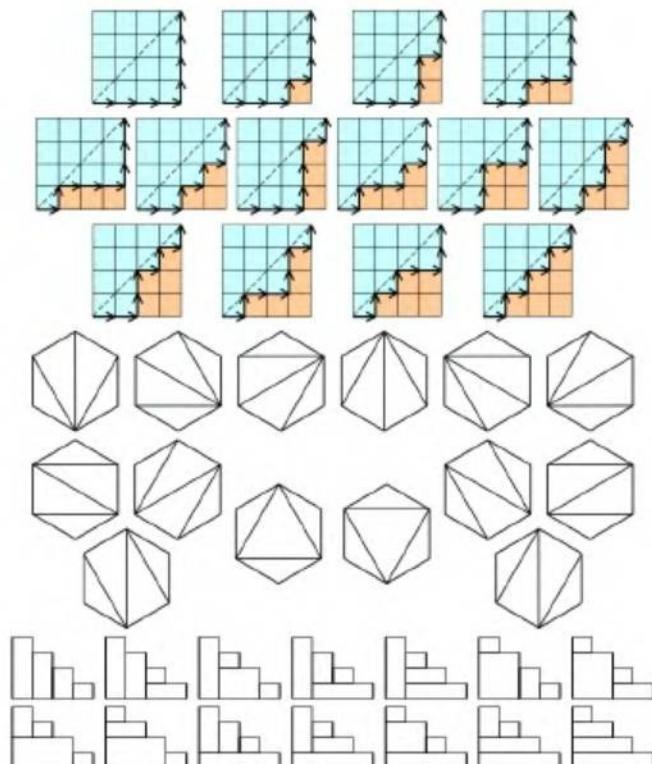
lesz a kedvező esetek száma, és $\frac{n}{n+1} \binom{2n}{n}$ esetben szakad meg a kiszolgálás.

5.7.2. definíció. Az (5.4)-ben definiált számokat **Catalan-számoknak** nevezzük.

A 5.4. táblázatban a Catalan-számok sorozatának első néhány tagja látható. A 5.7. ábra a mozipénztár-probléma $n = m = 4$ esetét mutatja.

n	0	1	2	3	4	5	6	7	8	9	10	11	12
C_n	1	1	2	5	14	42	132	429	1430	4862	16796	58786	208012

5.4. táblázat. Az első néhány Catalan-szám.

5.7. ábra. Felül: A mozipénztár-probléma megoldásai $n = m = 4$ esetére. Középen: az $n + 2 = 6$ oldalú konvex sokszög lehetséges háromszögelései száma. Alul: Téglalapokkal történő lépcsőzetes csempézések száma $n = 4$ esetére.

Az 5.4. képletből rövid számolás után adódik a

$$\begin{aligned} C_0 &= 1, \\ C_{n+1} &= \frac{2(2n+1)}{n+2} C_n \end{aligned}$$

rekurzió, ami hatékony eljárást kínál a Catalan-számok kiszámítására.

5.36. példa. A Catalan-számok számos kombinatorikai problémában előbukkanak:

- C_n megadja azt a számot, ahányféleképpen $n+1$ szorzótényezőt egyértelműen zárójelezhetünk. Ha például $n=2$, akkor két lehetőség van: $(a_0 \cdot a_1) \cdot a_2$ és $a_0 \cdot (a_1 \cdot a_2)$, tehát $C_2 = 2$. Ha $n=3$, akkor a lehetőségek: $((a_0 \cdot a_1) \cdot a_2) \cdot a_3$, $(a_0 \cdot (a_1 \cdot a_2)) \cdot a_3$, $a_0 \cdot ((a_1 \cdot a_2) \cdot a_3)$, $a_0 \cdot (a_1 \cdot (a_2 \cdot a_3))$, és $(a_0 \cdot a_1) \cdot (a_2 \cdot a_3)$, ezek száma $C_3 = 5$, etc.
- C_n a $2n$ hosszúságú **Dyck-szavak** száma. A Dyck-szó olyan karakterlánc, amelyben n db 0 és n db 1 szerepel oly módon, hogy a szó semelyik kezdeti szakaszában nincs több 1 mint 0. Például a 6 karakter hosszúságú Dyck-szavak: 000111, 010011, 010101, 0011010010110.
- C_n az $n+2$ oldalú konvex sokszög háromszögeléseinek (egymást nem metsző átlókkal való háromszögekre bontásainak) száma.
- C_n megadja, hogy n db téglalappal egy n magasságú lépcsőzetes alakzat hányféle csempézése (átfedés- és hézagmentes lefedése) adható meg.
- C_n az $\{1, \dots, n\}$ számok olyan permutációinak száma, amik elkerülik az 123 mintát (vagy bármely egyéb 3 hosszúságú mintát); azaz megadja az olyan permutációk számát, melyekben nincs 3 hosszú növekvő részsorozat.

A 5.36. példában látott helyes zárójelezések számából további rekurzív formula származtatható. Legyen $n \geq 1$ tetszőleges, és tekintsük $a_0, a_1, a_2, \dots, a_n$ valamely helyes zárójelezését. Figyeljük meg, hogy pontosan egy olyan szorzásjel van, amely minden zárójelen kívül esik. Ha ez a szorzásjel az a_k és a_{k+1} közé esik, akkor az előtte lévő a_0, a_1, \dots, a_k változók C_k -féleképpen zárójelezhetők, az utána lévő $n-k$ változó pedig C_{n-k-1} -féleképpen, így a lehetőségek száma rögzített k -ra $C_k C_{n-k-1}$, összesen pedig

$$C_0 = 1 \quad \text{és} \quad C_{n+1} = \sum_{i=0}^n C_i C_{n-i}, \quad \text{ahol } n \geq 0.$$

5.7.5. Stirling és Bell

Jelölje $\{n\}_k$ egy n -elemű halmazt k részhalmazra való osztályfelbontásainak számát. Az $\{1, 2, 3, 4\}$ négyelemű halmazt például hétféleképpen lehet két osztályra bontani, $\{1\} \cup \{2, 3, 4\}$, $\{2\} \cup \{1, 3, 4\}$, $\{3\} \cup \{1, 2, 4\}$, $\{4\} \cup \{1, 2, 3\}$, $\{1, 2\} \cup \{3, 4\}$, $\{1, 3\} \cup \{2, 4\}$, $\{1, 4\} \cup \{2, 3\}$, így $\{4\}_2 = 7$. A cél az, hogy rekurzív formulát adjunk $\{n\}_k$ kiszámítására.

5.7.3. definíció. Legyen $n, k \geq 1$. Egy n -elemű halmaz k részhalmazra való osztályfelbontásainak $\{n\}_k$ számát **másodfajú Stirling-számnak** nevezzük. Az összes lehetséges osztályfelbontás

$$B(n) = \sum_{k=1}^n \left\{ \begin{matrix} n \\ k \end{matrix} \right\}$$

száma a **Bell-szám**.

$B(n)$ tehát nem más, mint egy n elemű halmazon definiálható ekvivalenciarelációk száma. A másodfajú Stirling-számokat szokás még $S_2(n, k)$ -ként is jelölni. A definícióból látszik, hogy ha $k > n$, akkor $\{n\}_k = 0$, továbbá $n \geq 1$ esetén $\{n\}_1 = \{n\}_n = 1$. Megállapodás szerint $\{0\}_0 = 1$, és minden $n \geq 1$ -re $\{n\}_0 = 0$.

n	$\{^n_1\}$	$\{^n_2\}$	$\{^n_3\}$	$\{^n_4\}$	$\{^n_5\}$	$\{^n_6\}$	$\{^n_7\}$	$B(n)$
1	1							1
2	1	1						2
3	1	3	1					5
4	1	7	6	1				15
5	1	15	25	10	1			52
6	1	31	90	65	15	1		203
7	1	63	301	350	140	21	1	877

5.5. táblázat. Másodfajú Stirling-számok és Bell-számok.

5.7.4. téTEL. Ha $1 \leq k \leq n$, akkor

$$\left\{^n_k\right\} = k \left\{^{n-1}_k\right\} + \left\{^{n-1}_{k-1}\right\}. \quad (5.5)$$

Bizonyítás. Elegendő a $2 \leq k \leq n$ esettel foglalkozni. Tekintsük egy n -elemű $\{1, 2, \dots, n\}$ halmaz k osztályra történő bontását. Két esetet különböztetünk meg. Első eset: ha $\{n\}$ egyelemű osztály, akkor $n - 1$ elemet kell még $k - 1$ osztályra osztani, és ez $\left\{^{n-1}_{k-1}\right\}$ -féleképpen lehetséges. Második eset: ha az n elemet tartalmazó osztály nem egyelemű, akkor soroljuk először az $\{1, 2, \dots, n - 1\}$ halmaz elemeit k osztályba, amit $\left\{^{n-1}_k\right\}$ -féleképpen tehetünk, majd minden a k osztályhoz vegyük hozzá az n elemet, ami k -féleképpen lehetséges. ■

A 5.5. táblázat az első néhány másodfajú Stirling-számot és Bell-számot tartalmazza. A 5.5. rekurzív képlet szerint (amely hasonló a binomiális együtthatók addíciós képletéhez) minden $\left\{^n_k\right\}$ szám egyenlő a táblázatban felette álló szám k -szorosának és a tőle egy helyel balra álló számnak az összegével. Ennek alapján a táblázat könnyen kiegészíthető újabb sorokkal.

Az alábbiakban megpróbálunk egyszerű rekurzív formulát találni a Bell-számokra. A definíció alapján $B(0) = B(1) = 1$.

5.7.5. téTEL. $n \geq 1$ esetén

$$B(n+1) = \sum_{k=0}^n \binom{n}{k} B(k).$$

Bizonyítás. Tekintsük az $\{1, 2, \dots, n+1\}$ halmaz összes osztályfelbontását aszerint, hogy az $n+1$ elem osztálya hány elemet tartalmaz. Tegyük fel, hogy az $n+1$ osztályában j számú elem van, ahol $1 \leq j \leq n+1$. Ekkor az osztály többi elemét $\left(\begin{smallmatrix} n \\ j-1 \end{smallmatrix}\right)$ -féleképpen lehet megválasztani. A többi $n+1-j$ számú elemet $B(n+1-j)$ -féleképpen lehet

particionálni. Így

$$\begin{aligned}
 B(n+1) &= \sum_{j=1}^{n+1} \binom{n}{j-1} B(n+1-j) = \sum_{j=1}^{n+1} \binom{n}{n-j+1} B(n+1-j) \\
 &= \binom{n}{n} B(n) + \binom{n}{n-1} B(n-1) + \cdots + \binom{n}{1} B(1) + \binom{n}{0} B(0) \\
 &= \sum_{k=0}^n \binom{n}{k} B(k).
 \end{aligned}$$

■

Gyakorlatok

5.7-1. Keressük meg az

$$a_{n+1} = \frac{(2n-1)a_n - (2n+1)}{(2n+1)a_n - (2n+3)}, \quad a_0 = -1$$

rekurzió megoldását.

5.7-2. Keressük meg az

$$a_{n+1} = 4(1 + \sqrt{a_1 + a_2 + \cdots + a_n}), \quad a_1 = 1$$

sorozat 2013-adik tagját.

5.7-3. n hangya mászik egy szűk járatban, melynek középén egy zsákutca található. A járat olyan szűk, hogy két hangya már nem fér el egymás mellett, azaz nem előzhetik meg egymást. Aki bemegy a zsákutcába, azt akárhányan meg tudják előzni, de a zsákutcában is egyszerre legfeljebb egy hangya tartózkodhat. Hányfélé sorrendben jöhetnek ki a hangyák?

5.7-4. FIBONACCI eredeti problémája (1202) arról szólt, hogy ideális körülmények közzött a nyulak milyen gyorsan, milyen rendszerességgel ellenek. Tegyük fel, hogy egy mezőn él egy újszülött nyúl pár, egy hím és egy nőstény. A nyulak egy hónapos korukra lesznek ivarérettek, így a második hónap végén már megszülethetnek az első kicsinyek. Tegyük fel, hogy a mi nyulaink soha nem halnak meg és hogy a nőstények minden pár ellenek, egy hímet és egy nőstényt, mégpedig a második hónaptól kezdve minden hónapban. Számoljuk ki, hogy hány pár nyulunk lesz egy éven belül.

5.7-5. Tanulmányozzuk az egymást követő Fibonacci-számok hányadosának F_{n+1}/F_n sorozatát ($n = 1, 2, \dots$). Mi a kapcsolat ϕ -vel?

5.7-6. Bizonyítsuk be a Fibonacci-számokra vonatkozó mátrix-alakot:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}. \quad (5.6)$$

5.7-7. (5.6) segítségével mutassuk meg az alábbiakat:

$$\begin{aligned}
 (-1)^n &= F_{n+1}F_{n-1} - F_n^2 \quad (\text{Cassini-azonosság}), \\
 F_m F_n + F_{m-1} F_{n-1} &= F_{m+n-1}, \\
 F_{n+1} F_m + F_n F_{m-1} &= F_{m+n}, \\
 F_{2n-1} &= F_n^2 + F_{n-1}^2, \\
 F_{2n} &= (F_{n-1} + F_{n+1})F_n \\
 &= (2F_{n-1} + F_n)F_n.
 \end{aligned} \quad (5.7)$$

5.7-8. A Binet-formula átrendezésével mutassuk meg, hogy egy n természetes szám pontosan akkor Fibonacci-szám, ha $5n^2 + 4$ vagy $5n^2 - 4$ teljes négyzet.

5.7-9. Bizonyítsuk be az alábbi egyenlőségek teljesülését:

$$\begin{aligned}\sum_{i=1}^n F_i &= F_{n+2} - 1, \\ \sum_{i=0}^{n-1} F_{2i+1} &= F_{2n}, \\ \sum_{i=1}^n F_{2i} &= F_{2n+1} - 1, \\ \sum_{i=1}^n F_i^2 &= F_n F_{n+1}.\end{aligned}$$

5.7-10. Számoljuk ki F_{1000} közelítő értékét.

5.7-11. Legyen $\alpha, \beta, \gamma \in \mathbb{R}$. Oldjuk meg a Fibonacci számok segítségével az alábbi rekurziót:

- a) $R_0 = \alpha, R_1 = \beta, R_n = R_{n-1} + R_{n-2}, (n \geq 2)$,
- b) $R_0 = \alpha, R_1 = \beta, R_n = R_{n-1} + R_{n-2} + \gamma, (n \geq 2)$.

5.7-12. Határozzuk meg azon csupa 1-ből és 0-ból álló n -esek számát, amelyek nem tartalmaznak két szomszédos 1-est.

5.7-13. Hányféleképpen lehet felmenni egy n lépcsőfokból álló lépcsőn, ha egyszerre csak egy vagy két lépcsőt léphetünk?

5.7-14. Hányféleképpen lehet 1×2 -es dominókkal lefedni egy $2 \times n$ -es táblát?

5.7-15. Helyezzünk két üvegtáblát egymásra. Hányféle módon haladhat át vagy verődhet vissza egy fénysugár, ha közben pontosan n -szer változtatott irányt?

5.7-16. 15 házaspár hanyféleképpen táncolhat úgy, hogy egyik férj sem táncol a saját feleségével?

5.7-17. 15 férfi és 13 nő hanyféleképpen mehet be egy táncterembe, ha sosem lehet bent több nő mint férfi? Általánosítsuk a feladatot n nő és $n+m$ férfi esetére.

5.7-18. Bizonyítsuk be, hogy ha $4 < n \in \mathbb{N}$, akkor

$$\binom{2n}{n} < 4^{n-1}.$$

5.7-19. Mennyi 11^{10} értéke? Miért könnyű kiszámítani, ha ismerjük a binomiális együtthatókat?

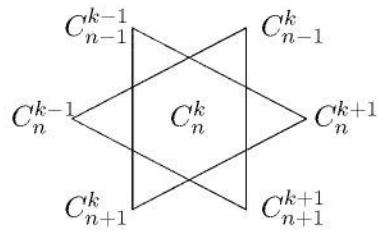
5.7-20. Bizonyítsuk be a binomiális együtthatók *trinomiális alakját*:

$$\binom{n}{k} \binom{k}{m} = \binom{n}{m} \binom{n-m}{k-m}$$

minden $1 \leq m \leq k \leq n$ esetén.

5.7-21. Bizonyítsuk be a *hexagon-tulajdonságot* (a Pascal-háromszög valamely elemt „szimmetrikusan körül fogó” számok a szokásos felírásban (5.8. ábra) egy hexagont képeznek, például 21 esetén a hexagon elemei 15, 6, 7, 28, 56, 35):

$$\binom{n-1}{k-1} \binom{n}{k+1} \binom{n+1}{k} = \binom{n-1}{k} \binom{n+1}{k+1} \binom{n}{k-1}.$$



5.8. ábra. A Pascal-háromszög hexagon tulajdonsága. A két háromszög csúcsainál lévő binomialis együtthatók szorzata egyenlő.

5.7-22. Bizonyítsuk be az

$$\binom{n}{k} \leq \frac{n^n}{k^k(n-k)^{n-k}}$$

5.7-23. A Stirling-formula alkalmazásával becsüljük meg a Catalan-számok növekedésének nagyságrendjét.

5.7-24. Bizonyítsuk be a Catalan-számokra vonatkozó

$$C_n = \frac{1}{n+1} \sum_{i=0}^n \binom{n}{i}^2$$

formulát ($n \geq 0$).

5.7-25. Írunk három újabb sort a másodfajú Stirling-számokat és a Bell-számokat tartalmazó 5.5. táblázathoz.

5.7-26. Jelölje $s(n, k)$ az n -elemű halmaz k -elemű halmazba való szürjekciói számát. Bizonyítsuk be, hogy ekkor $s(n, k) = k! \binom{n}{k}$.



Az (5.7) azonosság felhasználásával tervezünk és implementálunk hatékony algoritmust F_n kiszámítására nagy n esetére.



Számítógéppel keressük meg azt az egyetlen természetes számot, ami a tízes számrendszerben felírva megegyezik jegyei szubfaktoriálisainak összegével.



Pozitív természetes számok egy szigorúan monoton növekvő véges vagy végtelen a_1, a_2, \dots sorozatát *Sidon-sorozatnak* nevezzük, ha elemeiből képezhető valamennyi kéttagú $a_i + a_j$ ($i \leq j$) összeg különböző (a sorozat névadója Sidon Simon magyar matematikus). Keressük meg a leghosszabb Sidon-sorozatot $a_i, a_j \leq 1000$ -ig. Keressünk felső korlátot a Sidon-sorozat hosszára n -ig.

Megjegyzések a fejezethez

A „véletlen matematikájának” megalapozói közt első sorban említendő FERMAT és PASCAL, bár néhány ilyen tárgyú mű már az ő működésük előtt is megjelent. Levelezésükben FERMAT és PASCAL a kockázáshoz és egyéb játékokhoz kapcsolódó problémákat,

feladatokat tárgyaltak és oldottak meg, amellyel a „klasszikus” vagy „kombinatorikus” valószínűségszámítás alapjait fektették le. A valószínűségszámítás mint matematikai elmélet születési évének az 1654-es esztendőt (FERMAT és PASCAL egyik ilyen tárgyú levelének kelte) tekintjük. A „valószínűség” (probabilitas) szó BERNOULLI-nak az *Ars conjectandi* avagy *A találgaatás művészete* (1713) című munkájában fordul elő először. A valószínűségszámítás klasszikus elméletét LAPLACE foglalta össze a XVIII. században (*Théorie analytique des probabilités*, avagy *A valószínűségek analitikai elmélete*), a modern, axiomatikus elméletét pedig a halmaelméetre (mértékelmétre) támaszkodva KOLMOGOROV dolgozta ki 1933-ban. A valószínűségszámítás talán jelenleg legfontosabb alkalmazási területe a hírközlés és információelmélet.

A Fibonacci-sorozatot először 1150-ben írta le két indiai matematikus, GOPALA és HEMACCSANDRA, akik a szanszkrit költészet elméleti kérdéseit vizsgálva ütköztek abba az összegre bontási problémába, hogy hányféleképpen lehet rövid és hosszú szótágakkal kitölteni egy adott időtartamot, ha egy hosszú szótag két rövidnek felel meg. Európában tőlük függetlenül találta meg 1202-ben FIBONACCI, aki *Liber Abaci* (*Könyv az abakuszról*) című művében egy képzeletbeli nyúlcsalád növekedését adta fel gyakorlófeladatként. A Fibonacci-sorozatot KEPLER 1611-es könyvében, a *The Six-Cornered Snowflake*-ben újra felfedezte, és különféle természeti jelenségekkel hozta kapcsolatba.

A Catalan-sorozatot először EULER írta le a 18. században, amikor azt vizsgálta, hányféleképpen lehet háromszögekre bontani egy sokszöget. Nevét EUGÈNE CHARLES CATALAN belga matematikusról kapta, aki felismerte a sorozat zárójelezett kifejezésekkel való kapcsolatát, miközben a hanoi-tornyai problémát vizsgálta. Catalan a C_n számokat Segner-számoknak nevezte. SEGNER JÁNOS (1704–1777) magyar tudós volt, aki 1758-ban oldotta meg az $a_n = a_0a_{n-1} + a_1a_{n-2} + \dots + a_{n-1}a_0$ rekurziót EULER-nek a konvex sokszögekre vonatkozó probléma felvetésére.

A természetes számok sorozatai nagyon sok helyen bukkannak elő. A matematikai jelentéssel és értékkel rendelkező sorozatok rendszerezését az Egész Sorozatok Online Enciklopédiája (*Sloane-sorozatok*) tartalmazza, <https://oeis.org/>.

6. Halmazok számossága

Ezidáig csak intuitív fogalmunk volt arról, hogy mit jelent a végtelen. Vajon lehet-e „ugyanannyi” eleme két végtelen halmaznak? Van-e bővebb halmaz egy végtelen halmaznál? – kérdezhetjük. A pontos válasz csak a „halmaz számossága” fogalom tisztázása útján lehetséges. A halmazok számossága elméletének alapjait CANTOR fektette le.

6.1. Számosság

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

Ilyenkor azt 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 $\{1, 3, 5, 7, 9, 11, \dots\}$ és a $\{0, 6, 12, 18, 24, \dots\}$ 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 a bijektív leképezések tulajdonságainak felhasználásával könnyen be is láthatunk.

6.1. példa. Az azonos számosság eldöntéséhez nincs szükség magukra a számokra. Régen, amikor a birkapásztorok kihajtották állataikat az akóból, a pásztor a birkákat egyesével kiengedvén egy kavicsot tett egy tarisznyába, betereléskor pedig kivett egy követ a tarisznyából. Így meg tudta állapítani, ugyanannyi állat tért-e vissza.

A naiv halmazelméletben a halmazok számosságát úgy vezetjük be, hogy minden halmazhoz hozzárendelünk egy-egy „objektumot” oly módon, hogy két halmazhoz pontosan akkor rendeljük ugyanazt az objektumot, ha ekvivalensek egymással. Egy tetszőleges halmazhoz az így hozzárendelt objektum a halmaz **számossága**. Ahogy korábban a véges halmazoknál tettük, tetszőleges A halmaz esetén A számosságát $|A|$, $\text{card}(A)$, vagy $\sharp A$ jelöli.

Éles szemű olvasónknak feltűnhet, hogy az azonos számosság ekvivalenciarelációja segítségével a halmazok összességén hányadoshalmazt képeztünk. Csakhogy minden halmazok összessége nem halmaz. Precízen csak a kiválasztási axiómát magában foglaló axiomatikus halmazelméletben lehet definiálni a halmazok számosságát. Ekkor a halmazokhoz rendelt objektumok speciális halmazok lesznek.

6.2. Végtelen halmazok

6.2.1. definíció. Egy A halmazt **végtelennek** nevezünk, ha létezik egy valódi $B \subset A$ részhalmaza, amelyre $A \sim B$.

Halmazok számossága

Ellenkező esetben A -t végesnek mondjuk. A definíció szerint \mathbb{N} végtelen halmaz, míg $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, 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 $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, stb. által reprezentált számosságok tették lehetővé a természetes számok halmazának halmazelméleti megalapozását.

A véges és végtelen halmazok viselkedésbeli különbözőségét mutatja az alábbi tréfás példa.

6.2. példa. Képzeljünk el egy végtelen szállodát, amelynek szobái minden szobának van egy egyedi pozitív egész sorszáma, amelyet 1-től kezdve egyesével növekvően a szobaajtókra írtak. Tegyük fel, hogy a szálloda megtelt. Mi történik, ha egy új vendég érkezik? Véges szálloda esetén a portás sajnálkozva széttárná a kezét, de esetünkben mosolyogva megkéri az összes vendéget, hogy költözzenek át az 1-gyel nagyobb sorszámmú szobába, és az így felszabaduló 1-es sorszámmú lakrészbe helyezi el az újonnan érkezettet. Hasonló a helyzet, ha $2, 3, \dots, k$ új vendég érkezik. De mi történik akkor, ha egyszerre ugyanannyi vendéget kell elhelyezni, mint ahányan már a szállodában laknak? (Például minden vendég meghívja a barátját, barátnőjét.) Szerencsére ekkor sincs probléma: a portás megkéri a már bentlakók mindegyikét, hogy költözzen a kétszer akkora sorszámmú szobába, és a felszabaduló helyekre szállásolja el az újonnan érkezetteket.

A halmazok számosságai között 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 hasonlóan ahoz, ahogy ezt a véges számosságok esetében tettük:

$$\begin{aligned} |A| + |B| &:= |A \cup B|, \quad \text{ha } A \cap B = \emptyset, \\ |A| \cdot |B| &:= |A \times B|, \\ |A|^{|B|} &:= |A^B|, \quad \text{ahol } A^B = \{f \mid f : B \rightarrow A\}. \end{aligned}$$

A műveletekre érvényesek a kommutativitás, asszociativitás és a disztributivitás szabályai, valamint a hatványokra vonatkozó szokásos törvények. A bizonyításokat nem részletezzük.

Ha eltekintünk attól a ténytől, hogy minden halmazok halmaza nem halmaz, egy halmazrendszer számosságainak halmazában rendezési relációt lehet definiálni.

6.2.2. definíció. $|A| \preceq |B| := \exists C (C \subseteq B \wedge A \sim C)$.

A rövidsg 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. Észrevehetjük, hogy $A \preceq B$ pontosan akkor áll fenn, ha létezik közöttük egy $A \rightarrow B$ injektív leképezés.

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 választ adnak ezekre a kérdésekre.

6.2.3. téTEL (Cantor–Schröder–Bernstein). *Ha $A \preceq B$ és $B \preceq A$, akkor $A \sim B$.*

6.3 Megszámlálható és nem megszámítható halmazok

Bizonyítás. Feltehetjük, hogy A és B diszjunktak. Legyenek $f : A \rightarrow B$ és $g : B \rightarrow A$ injektív, amelyek a feltétel miatt léteznek. Azt kell belátni, hogy ekkor létezik egy $\varphi : A \rightarrow B$ bijekció.

Jelöljünk egy $a_0 \in A$ -hoz tartozó $\langle a_0, b_0 = f(a_0), a_1 = g(f(a_0)), b_1 = f(g(f(a_0))), \dots \rangle$ sorozatot – pályát – röviden $a_0, b_0, a_1, b_1, \dots$ -al. Hasonlóan értelmezzük a $b_0 \in B$ -ből induló $b_0, a_0, b_1, a_1, \dots$ pályát. Mindkét esetben $a_i \in A$ és $b_i \in B$ minden i -re. Tekintsük az összes olyan A -ból vagy B -ból induló pályát, amelyeket nem tartalmaz más pálya részsorozatként (tehát ezek a legbővebb sorozatok). A keletkezett sorozatok diszjunktak, és alapvetően két eset lehetséges.

A eset. A pálya véges kör, vagyis egy $a_0, b_0, a_1, b_1, \dots, a_n, b_n$ sorozat esetén $g(b_n) = a_0$. Legyen ekkor $\varphi(a_i) = b_i$, ami nyilván kölcsönösen egyértelmű. Hasonló állítás tehető egy $b_0 \in B$ -ből induló $b_0, a_0, b_1, a_1, \dots, b_n, a_n$ véges kör esetén.

B eset. A pálya nem véges. Ha egy sorozat $\dots, a_{-2}, b_{-2}, a_{-1}, b_{-1}, a_0, b_0, a_1, b_1, \dots$ alakú, akkor a $\varphi(a_i) = b_i$ ismét bijekció. Ha egy pálya $a_0, b_0, a_1, b_1, \dots$ alakú, akkor a $\varphi(a_i) = b_i$ leképezés újra bijekció. Ugyanez a gondolat működik egy $b_0 \in B$ -ből induló $b_0, a_0, b_1, a_1, \dots$ pálya esetén is.

Összességében a φ leképezést A minden elemére definiáltuk, és az is világos, hogy B minden eleme pontosan egy A -beli elem képe lesz, így φ bijektív. ■

6.2.4. Következmény. $A \preceq$ reláció a számosságok körében részbenrendezés.

A Cantor–Schröder–Bernstein-tétel ereje abban rejlik, hogy két halmaz számosságának egyenlőségét nem kell egy konkrét bijekció megadásával igazolni: elegendő két injekciót mutatni.

6.2.5. téTEL. $A \preceq$ reláció gyengén trichotom.

Bizonyítás. Azt kell megmutatni, hogy bármely A, B halmaz esetén $A \preceq B$ vagy $B \preceq A$. Vagyis találni kellene egy olyan kölcsönösen egyértelmű $g \in A \rightarrow B$ függvényt, amelyre vagy $\text{dmn}(g) = A$ vagy $\text{rng}(g) = B$.

Jelölje \mathcal{F} az összes $f \in A \rightarrow B$ kölcsönösen egyértelmű függvény halmazát. Legyen $f_1 \leq f_2$, ha f_1 az f_2 megszorítása. Könnyű meggondolni, hogy az így definiált reláció részbenrendezés. Ha $\mathcal{G} \subseteq \mathcal{F}$ lánc, akkor a \mathcal{G} -beli függvények egyesítése szintén kölcsönösen egyértelmű $A \rightarrow B$ -beli függvény, amely felső korlátja \mathcal{G} -nek. A Zorn-lemma szerint \mathcal{F} -nek így létezik maximális eleme, legyen ez f . Ha létezne $a \in A \setminus \text{dmn}(f)$ és $b \in B \setminus \text{rng}(f)$, akkor az $f \cup \{(a, b)\}$ is egy kölcsönösen egyértelmű $A \rightarrow B$ függvény lenne, ami ellentmondana f maximális voltának. ■

Az is megmutatható, hogy $a \preceq$ reláció jólrendezés.

6.3. Megszámlálható és nem megszámítható halmazok

A legkisebb végtelen halmazt a természetes számok alkotják. \mathbb{N} számosságát \aleph_0 -lal jelöljük (ejtsd: alef null vagy alef zéró¹). Eszerint \aleph_0 a legkisebb végtelen számoság.

¹ \aleph a héber ábécé első betűje. Ezt követi a \beth (bet), \daleth (gimel), \daleth (dalet), majd további 18 betű.

Halmazok számossága

6.3.1. definíció. Valamely A halmazt **megszámlálhatónak** nevezünk, ha $A \preceq \aleph_0$, **megszámlálhatóan végtelennek**, ha $A \sim \aleph_0$, és **nem megszámlálhatónak** mondjuk, ha $A \succ \aleph_0$.

Az alábbi számolási szabály a végtelen halmazok sokrétűségét mutatja:

6.3.2. Tétel (biz. nélkül). Ha A végtelen és B megszámlálható halmaz, akkor

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

■

Ennek megfelelően

6.3.3. Következmény. Megszámlálható halmaz bármely részhalmaza is megszámlálható.

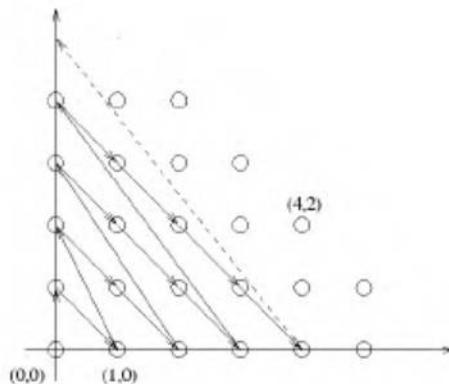
Valamely A halmaz megszámlálhatóan végtelen voltának igazolásához szükséges $\aleph_0 \rightarrow A$ bijekció megadása nem más, mint egy olyan $a_0, a_1, \dots, a_n, \dots$ sorozat megadása, amely A minden elemét pontosan egyszer tartalmazza. Ezeket a sorozatokat gyakran A elemei végtelen sorozatba rendezésének, vagy A elemei felsorolásának hívjuk. Ezek szerint egy végtelen halmaz pontosan akkor megszámlálható számosságú, ha elemei sorozatba rendezhetőek.

6.3.4. tétele. Az $\mathbb{N} \times \mathbb{N}$ halmaz megszámlálhatóan végtelen.

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

(0, 0)	(0, 1)	(0, 2)	(0, 3)	...
(1, 0)	(1, 1)	(1, 2)	(1, 3)	...
(2, 0)	(2, 1)	(2, 2)	(2, 3)	...
(3, 0)	(3, 1)	(3, 2)	(3, 3)	...
:	:	:	:	

A táblázat elemei



$(0, 0), (0, 1), (1, 0), (0, 2), (1, 1), (2, 0), (0, 3), (1, 2), (2, 1), (3, 0), \dots$ sorozatba rendezhetőek, $\mathbb{N} \times \mathbb{N}$ elemeiből álló halmaz tehát megszámlálhatóan végtelen. ■

6.3.5. téTEL. \mathbb{Z} megszámíthatóan végtelen.

Bizonyítás. \mathbb{Z} elemeit például a

$$0, -1, 1, -2, 2, -3, 3, \dots$$

módon rendezhetjük sorozatba. ■

Ellenőrző feladat. Hogy lehetne megmutatni, hogy $\mathbb{Z} \times \mathbb{Z}$ megszámíthatóan végtelen?

6.3.6. téTEL. \mathbb{Q} megszámíthatóan végtelen.

Bizonyítás. Az 6.3.4. tétel bizonyításhoz hasonlóan járunk el. Ha az alábbi táblázat elemeit az iménti eljárással sorba rendezzük, egy szürjektív $f : \mathbb{N} \rightarrow \mathbb{Q}$ leképezést kapunk.

0,	$\frac{1}{1}$	$-\frac{1}{1}$	$\frac{2}{1}$	$-\frac{2}{1}$...
	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{2}{2}$	$-\frac{2}{2}$...
	$\frac{1}{3}$	$-\frac{1}{3}$	$\frac{2}{3}$	$-\frac{2}{3}$...
	\vdots	\vdots	\vdots	\vdots	

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

6.3.7. téTEL. Megszámlálhatóan végtelen halmazok megszámíthatóan végtelen családjának egyesítése megszámíthatóan végtelen.

Bizonyítás. Legyen I megszámíthatóan végtelen, és A_i megszámíthatóan 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 $B_i \cap B_j = \emptyset$ ($i \neq j$) és $\cup A_i = \cup B_i$. Mivel minden $i \in I$ -re $B_i \subseteq A_i$, ezért a B_i halmazok is megszámítható számosságúak (végesek vagy végtelenek), 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 a korábban is alkalmazott eljárással újat készítve bijektív módon képeztük le $\cup A_i$ ($i \in I$) elemeit \mathbb{N} -be. ■

6.3.8. Következmény. \mathbb{N}^n ($n \in \mathbb{N}^+$), $\cup_{n=0}^{\infty} \mathbb{N}^n$ megszámíthatóan végtelen halmazok.

Vajon minden végtelen halmaz megszámítható?

6.3.9. téTEL (Cantor). Bármely A halmazra $A \prec \wp(A)$.

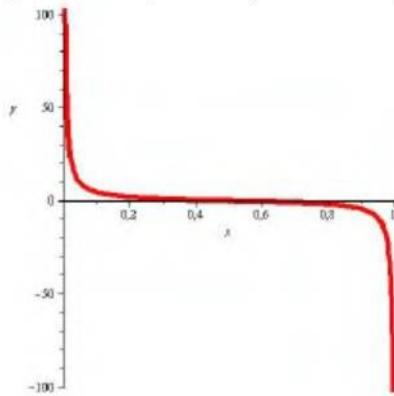
Bizonyítás. Az $a \mapsto \{a\}$ injektív leképezése A -nak $\wp(A)$ -ba, ezért $A \preceq \wp(A)$. A továbbiakban indirekt módon tegyük fel, hogy létezik egy f bijektív leképezés A -ból $\wp(A)$ -ba. Legyen $B = \{a \in A \mid a \notin f(a)\}$. Nyilván $B \in \wp(A)$. Legyen $b \in A$ olyan, hogy $f(b) = B$ (ilyen b a bijektív feltételezés miatt létezik). Ekkor ha $b \in B$, akkor B definíciója szerint $b \notin B$. Ha pedig $b \notin B$, akkor hasonló okok miatt $b \in B$ következne. Mindkettő ellentmondás. ■

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 6.3.9. tétel következménye, hogy \mathbb{N} -ből könnyen lehet nagyobb számosságú végtelen halmazt konstruálni, más szóval a végtelen halmazok számossága nem azonos. Sőt, megadható κ_i számosságok egy szigorúan monoton növő $\kappa_0 \prec \kappa_1 \prec \kappa_2 \prec \dots$ sorozata.

6.3.10. téTEL. \mathbb{R} nem megszámlálható.

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



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

függvény bijektív (nem bizonyítjuk), ezért elegendő J nem megszámlálhatóságát bizonyítani. Indirekt módon tegyük fel, hogy létezik egy $\mathbb{N} \rightarrow J$ bijekció. A (7.5.1.) fejezetben látni fogjuk, 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. ■

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

Kontinuum-számosságú halmazok természetesen végtelenek.

6.3.12. Tétel (biz. nélkül). $\wp(\mathbb{N}), \mathbb{R}^n$ ($n \in \mathbb{N}^+$) (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 kiválasztási axiómával bővített Zermelo–Fraenkel axiómarendszer (ZFC) ellentmondásmentességét feltételezve (ezt reméljük) a kontinuumhipotézist sem benne megcáfogni, sem bebizonyítani nem lehet.

6.4. Bizonyítási módszerek jólrendezett halmazokon

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 tételek választ adnak erre a kérdésre. Az általánosítás alapját a jólrendezett halmazok képezik.

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

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

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

6.4.1. tétel (transzfinit indukció). Legyen $(W; \leq)$ egy jólrendezés. Tegyük fel, hogy $B \subseteq W$ egy olyan halmaz, amelyre minden $t \in W$ esetén

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

Ekkor $B = W$.

² Néha magát CANTOR-t is kétségek gyötörték. Amikor három évi ellenkező irányú próbálkozás után bebizonyította, hogy az n -dimenziós térfelületek pontosan ugyanannyi pontja van, mint az egydimenziósnak, ezt írta: „Látom, de nem hiszem el.” REYMOND egyenesen úgy fogalmazott: „A józan éss 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 üzhet ki minket a CANTOR által teremtett paradicsomból.”

Bizonyítás. Legyen $A = W \setminus B$. Tegyük fel, hogy A nem üres. A jólrendezés miatt A -nak van legkisebb eleme, legyen ez t . Ekkor minden $x < t$ esetén $x \notin A$, vagyis seg $t \subseteq W \setminus A = B$. A feltétel miatt tehát $t \in B$, ami ellentmond annak, hogy $t \in A$. Eszerint $A = \emptyset$, s így $B = W$. ■

A tételet az alábbi módon is kimondhatjuk: Legyen $(W; \leq)$ tetszőleges jólrendezett halmaz és legyen hozzárendelve a W halmaz minden $i \in W$ eleméhez egy W_i állítás. Ha valahányszor minden $j < i$ ($j \in W$) elemre a W_j állítás teljesül, mindenkor a W_i állítás is teljesül, akkor minden W_i ($i \in W$) állítás teljesül.

A módszer a teljes indukció általánosítása. Felhasználhatóságát a jólrendezési tétele biztosítja. A tételel 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 lépésekben 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 4.1.4. 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 öt megelőzőtől néhány (esetleg más és más számú) értéktől függ? Ilyenkor a rekurziótétel nem használható. A rekurziótétel általánosabb változata, a *transzfinit rekurziótétel*, lehetővé teszi, hogy egy sorozat egy tagját az összes előző tag függvényeként adhassuk meg. A tételel általában \mathbb{N} -re alkalmazzuk, de tetszőleges jólrendezett halmazra érvényes.

A jólrendezett halmazokon bevezetjük a *rendszám* fogalmát. minden jólrendezett halmazhoz hozzárendelünk egy rendszámot oly módon, hogy két jólrendezett halmaznak a rendszáma pontosan akkor egyezzen meg, ha létezik közöttük egy rendezéstartó bijekció (izomorfak). A rendszámok között megadunk továbbá egy rendezést úgy, hogy az α rendszám legyen kisebb a β rendszámnál (jelölésben $\alpha \leq \beta$), ha az α rendszámú ($A; \leq$) és a β rendszámú ($B; \leq$) jólrendezett struktúrákra ($A; \leq$) izomorf ($B; \leq$) valamely kezdőszeletével. Belátható, hogy a rendszámok rendezése

- irreflexív
- tranzitív
- trichotom
- egy α rendszámnál kisebb rendszámok jólrendezett halmazt alkotnak, melynek rendszáma α .

A probléma abban áll, hogy a rendszámok nem alkotnak halmazt. Ha ugyanis egy R halmazt alkotnának, akkor az jólrendezett lenne valamilyen r rendszámmal, amire $r \in R$ teljesülne, és egyenlő lenne a nála kisebb elemei halmazának rendszámával, ami r -nél kisebb.

A rendszámokon értelmezünk egy hozzárendelést, egy operációt (ami nem függvény, hiszen nem halmazon van értelmezve). Viszont minden α -ra az α -nál kisebb rendszámokra megszorított operáció már függvény.

6.4.2. téTEL (transzfinit rekurziótétel). *Ha adott egy, az összes függvények osztályán értelmezett G operáció, akkor pontosan egy olyan F operáció létezik, ami a rendszámok*

osztályán van értelmezve és tetszőleges α rendszámra teljesül, hogy

$$F(\alpha) = G(F|_{\{\beta: \beta < \alpha\}}).$$

A transzfinit rekurziótétel 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.

Gyakorlatok

6.4-1. Adjunk bijektív leképezést

- (a) két különböző hosszúságú szakasz pontjai között,
- (b) a $[0, 1]$ intervallum és az egységnyi oldalú négyzet pontjai között,
- (c) \mathbb{R}^+ és \mathbb{R} pontjai között,
- (d) a $[0, 1]$ és a $[1, \infty]$ intervallumok pontjai között.

6.4-2. Tetszőleges A, B, C halmazok esetén adjunk bijekciókat az alábbi halmazok között:

- (a) $(A \times B) \times C$ és $A \times (B \times C)$;
- (b) $(A \times B)^C$ és $A^C \times B^C$;
- (c) $A^{B \times C}$ és $(A^B)^C$.

6.4-3. Tekintsük az $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$,

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

függvényt, ahol $k = m + n$. Bizonyítsuk be, hogy f bijektív. Ezzel az 6.3.4. téTEL egy alternatív bizonyítását adtuk.

6.4-4. 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.

6.4-5. 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.

6.4-6. Mutassuk meg, hogy az alábbi halmazok kontinuum számosságúak:

- (a) a valós együtthatós polinomok halmaza;
- (b) az $\mathbb{N} \rightarrow \mathbb{N}$ injektív leképezések halmaza;
- (c) az \mathbb{N} halmaz összes permutációinak halmaza.

Megjegyzések a fejezethez

Furcsa mód a Cantor–Schröder–Bernstein-tételre először DEDEKIND adott bizonyítást 1887-ben. Mivel akkoriban még lényegében nem létezett halmazelmélet, az eredményre nem figyelt fel az akkori tudományos világ. 1895-ben azonban CANTOR, a halmazelmélet talán legnagyobb alakja ugyanezt sejtésként mondta ki. SCHRÖDER 1896-ban adott egy hibás bizonyítást, majd BERNSTEIN 1898-ban talált egy helyeset.

7. Elemi szármelmelet

A szármelmelet a matematika azon ága, amely a természetes számok oszthatósági tulajdonságait vizsgálja. Megnevezésére a latinos „aritmetika” kifejezés is használatos, amit a latin is a görögöből vett át („arithmosz”, vagyis szám). A természetes számok szármelmeleti tulajdonságai vizsgálhatók egészben elemi eszközökkel (*elemi szármelmelet*), de a felsőbb matematika eszköztár (komplex függvényanalízis) segítségével is (*analitikus szármelmelet*). A természetes számok körében felvetődő bizonyos kérdések tanulmányozása vezetett a szármelmelet problémáinak és fogalmainak gyűrűkre vonatkozó kiterjesztéséhez, amit *algebrai szármelmeletnek* nevezzük. A fejezetben foglalkozunk még $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ elemei különböző ábrázolási lehetőségeinek vizsgálatával is.

7.1. Alapvető fogalmak

7.1.1. Oszthatóság

A fejezetben a definíciókat, tételeket az $(R; +, \cdot)$ egységelemes integritási tartományban értelmezzük.

7.1.1. definíció. Az $a \in R$ elemet $a \in R$ elem **osztójának** nevezzük, ha létezik olyan $q \in R$ elem, amelyre $b = aq$.

Jelölése: $a | b$. Az $a = b = 0$ esetet kivéve egyetlen ilyen q létezik, mert ha $b = aq_1$ is teljesülne, akkor $0 = a(q - q_1)$ miatt a nullsztó lenne. Ugyanezt a kapcsolatot úgy is kifejezhetjük, hogy b **osztatható** a -val, illetve hogy b **többszöröse** vagy **többeje** 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 elemmel osztatható (a 0-val is!), hiszen minden a -ra $0 = a \cdot 0$. Másrészt az 1 egységelem minden elem osztója.

7.1. példa. \mathbb{Z} -ben $2 | 10$, mert $2 \cdot 5 = 10$, de $4 \nmid 6$. A kettővel osztatható egész számokat **párosaknak**, a többöt **páratlanoknak** nevezzük.

Ellenőrző feladat. Mi az oka annak, hogy $0 | 0$, de $0/0$ osztásnak még sincs értelme?

Az alábbiakban az osztathóság fontosabb tulajdonságait vizsgáljuk.

7.1.2. tételek (az osztathóság tulajdonságai).

- (1) $a | a$ minden $a \in R$ -re,
- (2) $a | b$ és $b | c \Rightarrow a | c$,
- (3) $a_1 | b_1$ és $a_2 | b_2 \Rightarrow a_1 a_2 | b_1 b_2$,
- (4) $a | b \Rightarrow ac | bc$ minden $c \in R$ -re,
- (5) $ac | bc$ és $c \neq 0 \Rightarrow a | b$,
- (6) $a | b_i$ és $c_i \in R$ ($i = 1, 2, \dots, k$) $\Rightarrow a | \sum_{i=1}^k b_i c_i$.

Bizonyítás. A bizonyítások a definícióból következnek. Példaképp tekintsük (4)-et. Ha $a \mid b$, akkor létezik olyan $k \in R$ amelyre $ak = b$. Tetszőleges c -vel szorozva $ack = bc$, vagyis $ac \mid bc$. ■

Az (1)–(2) tulajdonságok azt fejezik ki, hogy az oszthatóság reflexív és tranzitív reláció. (6)-ot *lineáris kombinációs tulajdonságnak* nevezzük. Az oszthatóság nyilvánvalóan nem szimmetrikus.

7.2. példa. \mathbb{N} -ben az oszthatóság antiszimmetrikus is, így (\mathbb{N}, \mid) részbenrendezés. \mathbb{Z} -ben az antiszimmetria nem teljesül, hiszen például $2 \mid -2, -2 \mid 2$ de $2 \neq -2$.

Ellenőrző feladat. Igaz-e, hogy ha $c \mid 2a + 5b$ és $c \mid 3a + 7b$, akkor $c \mid a$ és $c \mid b$?

7.3. 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

$$a^{2n} - b^{2n} = (a^n)^2 - (b^n)^2.$$

7.1.3. definíció. *Azt az elemet, amely minden elemnek osztója, egységnak nevezzük.*

Ellenőrző kérdés. Mik az egységek \mathbb{N} -ben és \mathbb{Z} -ben?

Az egységek R azon elemei, amelyeknek a szorzásra nézve létezik inverzük. Megjegyezzük, hogy az egységek halmaza változatos képet mutat. Tekintsük például az $(\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}; +, \cdot)$ egységelemes integritási tartományt. Ebben a struktúrában, amint azt később látni fogjuk, végtelen sok egység van. Jegyezzük meg, hogy R -ben akár végtelen sok egység is lehet, míg egységelem pontosan egy van.

7.1.4. 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 $\delta b = \delta(\varepsilon r)(aq) = (\varepsilon a)(\delta qr)$, 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 pozitív egészekre.

7.1.5. definíció. *Azt mondjuk, hogy $a, b \in R$ 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 $a \in R$ elem asszociáltai az εa alakú elemek, ahol ε egység.

7.4. példa. Tekintsük a $G = \{a + bi \mid a, b \in \mathbb{Z}\}$ halmazt, az ún. *Gauss-egészeket*. A halmaz elemei a komplex sík egész rácpontjai. 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 $\bar{\varepsilon} \mid \bar{1}$ is teljesül, amiből $\varepsilon \cdot \bar{\varepsilon} \mid 1 \cdot \bar{1} = 1$ 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. Például az $\alpha = 3 + 5i$ elem asszociáltai: $-\alpha = -3 - 5i, i\alpha = -5 + 3i$, és $-i\alpha = 5 - 3i$.

7.1.2. Prímek, felbonthatatlanok

A 7.1.4. téTEL szerint bármely $0 \neq a \in R$ nem-egység és bármely ε egység esetén $\varepsilon | a$ és $\varepsilon a | a$ teljesül. Ezeket az *a triviális osztóinak* nevezzük. Lényeges szerepet játszanak azok az elemek, amelyeknek csak triviális osztói vannak:

7.1.6. definíció. Legyen $0 \neq a \in R$ nem-egység. Az *a elem felbonthatatlan* (idegen szóval *irreducibilis*), 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 „kizárt vagy” szerepel. Másrészt a 7.1.6. definíció miatt a felbonthatatlan elemeknek csak triviális osztóik vannak. Ha egy nem-nulla és nem-egység elemnek a triviálistól különböző osztója is van, akkor **összetettnek** nevezzük.

7.1.7. definíció. Legyen $0 \neq p \in R$ nem egység. A *p elemet prímnak* nevezzük, ha $p | bc \Rightarrow p | b$ vagy $p | c$.

A definícióban most „megengedő vagy” szerepel, hiszen előfordulhat, hogy p a bc szorzat mindenkét tényezőjét osztja.

7.5. példa. Az egész számok körében a 7 és a 11 felbonthatatlanok és egyben prímek is. A 4 nem prím, mert például $4 | 12 = 2 \cdot 6$, de $4 \nmid 2$ és $4 \nmid 6$.

7.1.8. téTEL. Minden prímelem felbonthatatlan.

BIZONYÍTÁS. Legyen p prím és $p = xy$. Mivel egységelemes integritási tartományban dolgozunk, ezért $p | xy$. A 7.1.7. definíció szerint ekkor $p | x$ vagy $p | y$. Feltehető, hogy $p | x$. 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.

7.1.3. Legnagyobb közös osztó, legkisebb közös többszörös

7.1.9. definíció. Legyen a_1, a_2, \dots, a_n az R egységelemes integritási tartomány tetszőleges eleme. Egy $a \in R$ az a_1, a_2, \dots, a_n elemek közös osztója, ha $a | a_i$ minden $i = 1, 2, \dots, n$ esetén.

Nyilvánvaló, hogy az egységelem minden közös osztó.

7.1.10. definíció. Legyen R egységelemes integritási tartomány. Az $l \in R$ elem az $a_1, a_2, \dots, a_n \in R$ elemek legnagyobb közös osztója, ha közös osztó, továbbá

$$\forall l_1 | a_i \quad (i = 1, 2, \dots, n) \Rightarrow l_1 | l.$$

Ha l legnagyobb közös osztó, akkor minden asszociáltja is az, és más legnagyobb közös osztó nincs. Ez a legnagyobb közös osztó fogalom látszólag eltér a középfokú oktatásban \mathbb{N} -ben látott legnagyobb közös osztó fogalomtól, de előnye, hogy tetszőleges egységelemes integritási tartományban érvényes. Látni fogjuk, hogy \mathbb{N} -re a két megközelítés ugyanazt szolgáltatja.

A legnagyobb közös osztók L halmaza az a_1, a_2, \dots, a_n elemek közös osztóinak osztályai között maximális az oszthatóságra nézve.

7.6. példa. Keressük meg \mathbb{Z} -ben a 8, a 12, és a 20 elemek legnagyobb közös osztóit. Az osztók: 8 esetén $\pm 1, \pm 2 \pm 4 \pm 8$,

12 esetén $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$,

20 esetén $\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20$.

A közös osztók tehát a $\pm 1, \pm 2, \pm 4$. Azok a közös osztók, amelyek minden közös osztónak többesei így a $\{-4, 4\}$ halmazt alkotják.

7.1.11. definíció. Ha minden legnagyobb közös osztó egység, akkor azt mondjuk, hogy a_1, a_2, \dots, a_n **relatív prímek**.

7.1.12. definíció. Az $a_1, a_2, \dots, a_n \in R$ elemek **páronként relatív prímek**, ha közülük semelyik kettőnek sincs az egységtől különböző közös osztója.

Megjegyezzük, hogy az $a_1, a_2, \dots, a_n \in R$ elemekre „erősebb” feltételt jelent, hogy páronként relatív prímek, mintha „csak” relatív prímek lennének. Amennyiben az adott n elem páronként relatív prím, akkor ebből következik, hogy relatív prímek, míg megfordítva ez nem igaz.

7.7. 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 $2 \mid 16$.

7.1.13. definíció. Legyen a_1, a_2, \dots, a_n az R egységelemes integritási tartomány tetszőleges eleme. Egy $a \in R$ az a_1, a_2, \dots, a_n elemek **közös többszöröse**, ha $a_i \mid a$ minden $i = 1, 2, \dots, n$ esetén.

Észrevehetjük, hogy az $a_1 \cdot a_2 \cdots a_n$ elem minden közös többszörös.

7.1.14. definíció. Legyen R egységelemes integritási tartomány. A $t \in R$ elem az $a_1, a_2, \dots, a_n \in R$ elemek **legkisebb közös többszöröse**, ha közös többszörös, továbbá

$$\forall a_i \mid t_1 \quad (i = 1, 2, \dots, n) \Rightarrow t \mid t_1.$$

A legkisebb közös többszörökök T halmaza az a_1, a_2, \dots, a_n elemek közös többszöröseinék osztályai között minimális az oszthatóságra nézve.

7.8. 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.

7.1-3. A páros számok halmaza a szokásos műveletekkel olyan integritási tartományt alkot, amelyben nincs egységelem. Az oszthatósági kérdések ennek ellenére vizsgálhatók benne. Hány olyan elem van köztük, amelyeknek

a) egyáltalán nincs osztója?

b) pontosan két (pozitív vagy negatív) osztója van?

7.1-4. Mutassuk meg, hogy ha egy egységelemes integritási tartományban az a és b elemeknek létezik l legnagyobb közös osztója és $a = la_1$, $b = lb_1$, akkor a_1 és b_1 relatív prímek.

7.1-5. Bizonyítsuk be, hogy egy integritási tartományban $a \mid b$ pontosan akkor teljesül, ha létezik a -nak és b -nek legnagyobb közös osztója, és ha ez l , akkor l és a asszociáltak.

7.2. Aritmetika \mathbb{Z} -ben

Azt a korábbi észrevételünket, miszerint az egészek körében pontosan két egység van, könnyen be is bizonyíthatjuk.

7.2.1. 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. ■

7.2.2. téTEL. Ha $a \mid b$ és $b \mid a$, akkor $|a| = |b|$.

Bizonyítás. Ha a vagy b valamelyike 0, akkor szükségszerűen a másik is az, így feltehető, hogy $a, b \neq 0$. A feltétel szerint ekkor léteznek olyan a_1 és b_1 egészek, amelyekkel $aa_1 = b$ és $bb_1 = a$. Ekkor a $bb_1a_1 = b$ összefüggést kapjuk, amiből $b \neq 0$ miatt $b_1a_1 = 1$, vagyis $a_1 = \pm 1$ és $b_1 = \pm 1$. ■

7.2.3. 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 $|aq| = |a| \cdot |q| = |b|$. De $|q| < 1$ esetén $b = 0$ lenne, ezért $|q| \geq 1$. Ebből $|b| = |a| \cdot |q| \geq |a|$ következik. ■

7.2.4. Következmény. $0 \neq b \in \mathbb{Z}$ esetén b -nek véges sok osztója van.

7.2.1. Számrendszerek

A számábrázolás kritikus fontosságú az informatikában. Lényegében egy olyan speciális grammatikáról (nyelvtanról) van szó, ami véges sok alapjel és formális képzési szabály segítségével képes egy szám megjelenítésére. A helyiértékes ábrázolás legelemibb építőköve a maradékos osztás.

7.2.5. téTEL (maradékos osztás tétele). Tetszőleges $a \neq 0$ 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. A hányados szokásos jelölése $q = a \text{ quo } b$, a maradéké $r = a \text{ rem } b$ vagy $r = a \text{ mod } b$ ¹

¹A quotient (hányados), és a remainder (maradék) angol szavakból.

7.9. példa. Most délután 1 óra van. Mennyi lesz az idő 101 óra műlva?

Megoldás: Legyen $b = 24$ és $a = 13 + 101 = 114$. Ekkor $114 = 4 \cdot 24 + 18$. Vagyis 101 óra műlva 18 óra (délután 6 óra) lesz.

Bizonyos feladatoknál kényelmesebb, ha negatív maradékot is megengedünk.

7.2.6. tétele. Tetszőleges a és $b \neq 0$ egész számokhoz egyértelműen léteznek olyan q és r egész számok, melyekre $a = bq + r$ és $-|b|/2 < r \leq |b|/2$.

Bizonyítás. A bizonyítás analóg a maradékos osztás tételenek bizonyításával. ■

A maradékos osztás tétele felhasználható a pozitív egészek **számrendszeres** ábrázolásához.

7.2.7. tétele (számrendszer). *Legyen $q > 1$ rögzített egész. Ekkor bármely N pozitív egész szám egyértelműen írható fel*

$$N = \sum_{i=0}^n a_i q^i \quad (7.1)$$

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 -lal. Ekkor az

$$N_0 = \frac{N - a_0}{q} = a_n q^{n-1} + a_{n-1} q^{n-2} + \cdots + a_2 q + a_1$$

felírásból az iménti eljárást folytatva egy $N > N_0 > N_1 > \cdots > N_n$ szigorúan monoton csökkenő véges sorozatot kapunk, ami a megfelelő a_i -k létezését és egyértelműségét is bizonyítja. ■

Az iménti előállításban q -t a **számrendszer alapszámának** nevezik, az a_i számok pedig a q -alapú számrendszer **számjegyei**. Legismertebb ilyen ábrázolás $q = 16$ esetén a hexadecimális, $q = 10$ esetén a decimális (tízes alapú), $q = 8$ esetén az oktális és $q = 2$ esetén a bináris számrendszer. A 7.1. szám szokásos jelölése

$$N = (a_n a_{n-1} \dots a_1 a_0)_q.$$

A $q = 10$ esetén a zárójelet és az alapszám feltüntetését általában elhagyjuk.

7.10. példa. $21 = (21)_{10} = (10101)_2$, hiszen $21 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1$.

7.11. 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. táblázatban látható jelölések használhatók. Például 3 GHz, 8 TByte, stb. A 7.2. táblázat a nagyságrendekre vonatkozó néhány referenciát sorol fel.

7.12. példa. Legyenek $a = 10111$ és $b = 101$ bináris számok. A kettes számrendszerbeli műveleteket alkalmazva számítsuk ki $a + b$ -t és $a \cdot b$ -t.

Az összeadás:

$$\begin{array}{r} & 1 & 0 & 1 & 1 & 1 \\ & + & & 1 & 0 & 1 \\ \text{Átvitel} & 1 & 1 & 1 \\ \hline & 1 & 1 & 1 & 0 & 0 \end{array}$$

Mennyiség	Elnevezés	Rövidítés	Mennyiség	Elnevezés	Rövidítés
10^{24}	yotta	Y	10^{-24}	yocto	y
10^{21}	zetta	Z	10^{-21}	zepto	z
10^{18}	exa	E	10^{-18}	atto	a
10^{15}	peta	P	10^{-15}	femto	f
10^{12}	tera	T	10^{-12}	pico	p
10^9	giga	G	10^{-9}	nano	n
10^6	mega	M	10^{-6}	mikro	μ
10^3	kilo	k	10^{-3}	milli	m

7.1. táblázat. A tízes számrendszerbeli mennyiségek szokásos jelölése.

Referencia	Nagyságrend
Másodpercek száma egy évben	$\approx 3 \times 10^7$
A naprendszer kora (évben)	$\approx 6 \times 10^9$
Eltelt másodperc a naprendszer keletkezésétől	$\approx 2 \times 10^{17}$
Órajel-periódusidő egy évben, 5GHz processzor	$\approx 1.6 \times 10^{17}$
64 jegyű bináris sztringek száma	$2^{64} \approx 1.8 \times 10^{19}$
Egy sakkjátszma lehetséges állapotainak száma	$2^{113} \approx 10^{34}$
128 jegyű bináris sztringek száma	$2^{128} \approx 3.4 \times 10^{38}$
256 jegyű bináris sztringek száma	$2^{256} \approx 1.2 \times 10^{77}$
75 jegyű prímek száma	$\approx 5.2 \times 10^{72}$
Elektronok száma az univerzumban	$\approx 8.37 \times 10^{77}$

7.2. táblázat. Mi mekkora a világunkban?

A szorzás:

$$\begin{array}{r}
 & 1 & 0 & 1 & 1 & 1 & * & 1 & 0 & 1 \\
 & & & & & & 1 & 0 & 1 & 1 \\
 + & & & 1 & 0 & 1 & 1 & 1 \\
 \text{Átvitel} & & & & 1 & 1 & 1 \\
 \hline
 & 1 & 1 & 1 & 0 & 0 & 1 & 1
 \end{array}$$

7.13. példa. Az algoritmusok futásideje mindenkor minden inputtól függ. Amennyiben az input egy $n \in \mathbb{N}$ természetes szám, akkor az input mérete az n számjegyeinek száma (tehát nem n értéke maga). Egy adott $q > 1$ alapú számrendszerben adott n szám jegyeinek száma $\lfloor \log_q n \rfloor + 1$. Például 2^{100} decimális jegyei száma $\lfloor 100 \log_{10} 2 \rfloor + 1 \approx \lfloor 100 \cdot 0.3 \rfloor + 1 = 31$. Hasonlóan, egy 100 jegyű decimális szám binárisan $\lfloor 100 \log_2 10 \rfloor + 1 \approx \lfloor 100 \cdot 3.322 \rfloor + 1 = 333$ jegyű.

7.14. példa. A $q > 1$ alapú számrendszerenél a $\{0, 1, \dots, q - 1\}$ jegyhalmazt **kanonikus jegyhalmaznak** nevezzük. Ha $q > 2$ egész és a $\{-\lfloor (q-1)/2 \rfloor, \dots, \lceil (q-1)/2 \rceil\}$ **szimmetrikus jegyhalmazt** alkalmazzuk, akkor az összes *egész szám előjel nélküli* végesen kifejthető lesz. A bizonyítás hasonló a 7.2.7. téTEL bizonyításához, azzal a különbséggel, hogy most az $|N_i|$ sorozat lesz szigorúan monoton csökkenő. Legyen $q = 10$, a jegyhalmaz pedig $\{-4, -3, \dots, 4, 5\}$. Jelöljük a negatív jegyeket felülvonással, vagyis például $\bar{3} = -3$. Ekkor a -2468 tízes számrendszerbeli szám felírása $\bar{3}532$ lesz (ellenőrizzük!).

7.15. példa. A hexadecimális ábrázolással gyakran találkozunk honlapok html forrásában, és a hálózati eszközök MAC címét (Media Access Control) is így adják meg.

7.16. példa. A Nim egy kétszemélyes stratégiai játék, amelyben több kupacban kavicsok vannak és a két játékos felváltva vehet el kavicsokat, mégpedig egy kupacból annyit, amennyit jónak lát (akkár az összeset). Az nyer, aki az utolsó kavicsot vagy kavicsokat elveszi. A nyerő stratégia kulcsa a kettes számrendszerbeli átvitel nélküli összeadás. A játék miatt ezt **nim-összegnek** is szokás nevezni. A nyerő stratégia az alábbi: úgy kell lépni, hogy a lépés után létrejövő helyzetben a kupacokban lévő kavicsok számának nim-összege 0 legyen. Látható, hogy ha nem 0 ez az összeg, akkor minden el lehet érni, hogy 0 legyen, és ha 0 összegnél kell lépnünk, akkor csak úgy tudunk lépni, hogy a lépés után az összeg nem lesz 0. A végállapot az, hogy minden kupacból elfogytak a kavicsok, vagyis a végső nyerő helyzetben a nim-összeg 0. Követve a leírt stratégiát az tud nyerni, aki először be tud lépni a 0 nim-összegű állapotba.

Gyakorlatok

7.2-1. Indokoljuk az alábbi oszthatósági szabályokat:

- 3: Azok a számok oszthatók 3-mal, ahol a számjegyek összege is osztható 3-mal.
- 4: Azok a számok oszthatók 4-gyel, amelyeknél az utolsó két számjegyből képzett kétjegyű szám is osztható 4-gyel.
- 5: Azok a számok oszthatók 5-tel, amelyeknek utolsó számjegye is osztható 5-tel.
- 7: Az oszthatóságot úgy vizsgáljuk meg, hogy a szám első számjegyétől az utolsó előtti számjegyéig képzett számból vonjuk ki az utolsó számjegy kétszeresét. Ha az így kapott szám osztható 7-tel akkor az eredeti is. Ha még nem tudjuk eldönthető, akkor ugyanezt az eljárást kell folytatni amíg olyan számot nem kapunk amiről biztosan eldönthető a héttel való oszthatóság. Például $8638 \rightarrow 863 - 16 = 847 \rightarrow 84 - 14 = 70$ osztható 7-tel, tehát 8638 is.
- 8: Azok a számok oszthatók 8-cal, amelyeknek az utolsó három számjegyből képzett háromjegyű szám is osztható 8-cal.
- 9: Azok a számok oszthatók 9-cel, amelyeknek számjegyeinek összege is osztható 9-cel.
- 11: Az oszthatóságot úgy vizsgáljuk meg, hogy a szám első számjegyétől az utolsó előtti számjegyéig képzett számból vonjuk ki az utolsó számjegyet. Ha az így kapott szám osztható 11-gyel, akkor az eredeti is. Az eljárás ismételhető. Például $13574 \rightarrow 1357 - 4 = 1353 \rightarrow 135 - 3 = 132 \rightarrow 13 - 2 = 11$, vagyis az eredeti szám is osztható volt 11-gyel. Más megközelítésben egy szám pontosan akkor osztható 11-gyel, ha számjegyeinek váltakozó előjellel vett összege osztható 11-gyel.

- 13:** A szám első számjegyétől utolsó előtti számjegyéig képzett számhoz adjuk hozzá az utolsó számjegy négyszeresét, majd az eldönthetőséig ismételjük a folyamatot. Például $16042 \rightarrow 1604 + 8 = 1612 \rightarrow 161 + 8 = 169 = 13^2$.
- 16:** Azok a számok oszthatók 16-tal, amelyeknek utolsó négy számjegyből képzett négyjegyű szám is osztható 16-tal.
- 17:** A szám első számjegyétől az utolsó előtti számjegyéig képzett számból vonjuk ki az utolsó számjegy ötszörösét. A folyamat itt is ismételhető. Például $20978 \rightarrow 2097 - 40 = 2057 \rightarrow 205 - 35 = 170$.
- 19:** A szám első számjegyétől az utolsó előtti számjegyéig képzett számhoz adjuk hozzá az utolsó számjegy kétszeresét. A folyamat ismételhető. Például $23446 \rightarrow 2344 + 12 = 2356 \rightarrow 235 + 12 = 247 \rightarrow 24 + 14 = 38 = 2 \cdot 19$.
- 23:** A szám első számjegyétől az utolsó előtti számjegyéig képzett számhoz adjuk hozzá az utolsó számjegy 7-szeresét.
- 27:** A számot blokkokba kell rendezni a legkisebb helyiérték felől úgy, hogy egy blokkban 3 számjegy legyen. A blokkokat (tehát a képzett háromjegyű számokat) adjuk össze. Ha ez az összeg osztható 27-tel akkor az eredeti szám is.
- 29:** A szám első jegyétől az utolsó előtti számjegyéig képzett számhoz adjuk hozzá az utolsó számjegy háromszorosát. Ha ez a szám osztható 29-cel, akkor az eredeti is.

Tervezzünk további szabályokat!

7.2-2. Igazoljuk az alábbi oszthatóságokat:

- a) $3^{n+1} \mid 2^{3^n} + 1$,
- b) $4 \mid 7^n + 10n - 5$,
- c) $4 \mid 11^n + 6n - 1$,
- d) $6 \mid n(2n+1)(7n+1)$,
- e) $7 \mid 5^{2n} + 3 \cdot 2^{5n-2}$,
- f) $8 \mid 5^n + 2 \cdot 3^{n-1} + 1$,
- g) $9 \mid 2^{2n} + 24n - 10$,
- h) $9 \mid 7^n + 3n - 1$,
- i) $13 \mid 3^{n+2} + 4^{2n+1}$,
- j) $18 \mid 2^{2n} + 24n - 10$,
- k) $25 \mid 11^n + 15n - 1$.

7.2-3. Hány olyan $n \in \mathbb{N}$ adható, amelyre $29 \mid 2^n + 5^n$?

7.2-4. Mutassuk meg, hogy $(b-1)^2 \mid b^n - 1$ pontosan akkor teljesül, ha $b-1 \mid n$.

7.2-5. Mutassuk meg, hogy három szomszédos egész szám szorzata osztható 6-tal.

7.2-6. Bizonyítsuk be, hogy minden 3-nál nagyobb prím két szomszédjának szorzata osztható 24-gyel.

7.2-7. Mutassuk meg, hogy öt egymást követő természetes szám szorzata osztható 120-szal.

7.2-8. Létezik-e végtelen hosszú, $d > 0$ differenciájú csupa prímszámokból álló számtani sorozat?

7.2-9. Milyen $n \in \mathbb{N}$ esetén lesznek az alábbi számok mind prímek:

- a) $n, n+2, n+7$,
- b) $n, n^2 + 8$.

7.2-10. Bizonyítsuk be, hogy ha egy háromjegyű számot kétszer egymás mellé írunk, a keletkezett szám osztható 13-mal. Igaz-e az állítás, ha háromszor írjuk egymás mellé?

7.2-11. Tegyük fel, hogy az a, b, c jegyekből álló abc háromjegyű szám osztható 37-tel. Bizonyítsuk be, hogy ekkor bca is osztható 37-tel.

7.2-12. Létezik-e kettőnek olyan pozitív egész kitevős hatványa, amelyben minden számjegy ugyanannyiszor fordul elő?

7.2-13. Mutassuk meg, hogy minden páratlan n -hez létezik olyan m egész, hogy $n \mid 2^m - 1$ -nek.

7.2-14. Mutassuk meg, hogy minden n -hez végtelen sok olyan kettőhatvány létezik, amelyek közül bármely kettő különbsége osztató n -nel.

7.2-15. Keressünk választ az alábbi számpiramisokra:

$1 \cdot 8 + 1 = 9$	$1 \cdot 9 + 2 = 11$
$12 \cdot 8 + 2 = 98$	$12 \cdot 9 + 3 = 111$
$123 \cdot 8 + 3 = 987$	$123 \cdot 9 + 4 = 1111$
$1234 \cdot 8 + 4 = 9876$	$1234 \cdot 9 + 5 = 11111$
$12345 \cdot 8 + 5 = 98765$	$12345 \cdot 9 + 6 = 111111$
$123456 \cdot 8 + 6 = 987654$	$123456 \cdot 9 + 7 = 1111111$
$1234567 \cdot 8 + 7 = 9876543$	$1234567 \cdot 9 + 8 = 11111111$
$12345678 \cdot 8 + 8 = 98765432$	$12345678 \cdot 9 + 9 = 111111111$
$123456789 \cdot 8 + 9 = 987654321$	$123456789 \cdot 9 + 10 = 1111111111$
$9 \cdot 9 + 7 = 88$	$1 \cdot 1 = 1$
$98 \cdot 9 + 6 = 888$	$11 \cdot 11 = 121$
$987 \cdot 9 + 5 = 8888$	$111 \cdot 111 = 12321$
$9876 \cdot 9 + 4 = 88888$	$1111 \cdot 1111 = 1234321$
$98765 \cdot 9 + 3 = 888888$	$11111 \cdot 11111 = 123454321$
$987654 \cdot 9 + 2 = 8888888$	$111111 \cdot 111111 = 12345654321$
$9876543 \cdot 9 + 1 = 88888888$	$1111111 \cdot 1111111 = 1234567654321$
$98765432 \cdot 9 + 0 = 888888888$	$11111111 \cdot 11111111 = 123456787654321$
$987654321 \cdot 9 - 1 = 8888888888$	$111111111 \cdot 111111111 = 12345678987654321$

7.2-16. Keressük meg azokat az (x, y, z) egészeket, amelyekre $x + y + z = 3$ és $x^3 + y^3 + z^3 = 3$.

7.2-17. Létezik-e olyan szám, amelyben csak az 1 és a 2 jegyek fordulnak elő, és amely osztató 2^{2003} -mal?

7.2-18. Válasszunk ki az $1, 2, \dots, 2n$ számok közül tetszőleges $n+1$ darabot. Mutassuk meg, hogy a kiválasztott számok között biztosan lesz két olyan, hogy az egyik a másik osztója.

7.2-19. Bizonyítsuk be, hogy az $1 < q \in \mathbb{N}$ egész alapú számrendszerben felírt $n \in \mathbb{N}^+$ szám helyiértékes ábrázolásában q^j együtthatója $[n/q^j] - q[n/q^{j+1}]$ ($j \in \mathbb{N}$).

7.2-20. Alkossunk egy tetszőleges négyjegyű számot az 1, 2, 2, 3 jegyekből. A kapott számot emeljük a 2003-adik hatványra. Vegyük az így kapott szám jegyeinek összegét, majd ezen szám jegyeinek összegét stb., amíg egyjegyű számhoz nem jutunk. A végeredmény 8. Ellenőrizzük!

7.2-21. (Vegyes alapú számrendszer.) Legyenek q_1, q_2, \dots, q_n tetszőleges egynél nagyobb egészek. Bizonyítsuk be, hogy minden $N \in \mathbb{N}$ egyértelműen írható

$$N = a_n q_n q_{n-1} \cdots q_1 + a_{n-1} q_{n-1} \cdots q_1 + \cdots + a_1 q_1 + a_0$$

alakban, ahol $a_n \neq 0$ és $0 \leq a_i \leq q_{i+1}$.

7.2-22. Csupaegy számoknak nevezzük azokat a pozitív egészeket, amelyeknek minden számjegyük egyes. (A csupaegy számok speciális palindrómák, lásd a projektfeladatokat alább.) A tízes számrendszerben mely számoknak létezik csupaegy többszörösök?

7.2-23. Tekintsük az összes olyan természetes számot, amelyek a három valamilyen (különböző) nemnegatív egész hatványának összegeiből képezhetők. Rakjuk növekvően sorba őket. Ekkor a sorozat első néhány tagja az alábbi: 1, 3, 4, 9, 10, 12, 13, ... Határozzuk meg a sorozat ezredik elemét! Általánosítsuk a feladatot!



Tervezzük és implementálunk hatékony algoritmust a bináris, oktális, decimális és hexadecimális számrendszer közötti átváltásra. Vizsgáljuk meg az algoritmusok műveletigényét.



A palindromszám (palindróma, számpalindróm) olyan számot jelent, amelynek számjegyeit fordított sorrendben írva az eredeti számot kapjuk vissza. Ilyen „szimmetrikus” szám például a (tízes számrendszerben vett) 12421.

- Keressük meg egymilliőig az összes palindromszámot és állapítsuk meg, hogy közülük hány páros, páratlan, prím, négyzetszám, köbszám, prímnégyzet.
- Vannak olyan számok, amelyek egyszerre több számrendszerben is palindromszámok. Ilyen például az 1991, ami hexadecimálisan 7C7. Keresünk olyan palindrómákat, amelyek a tízes számrendszer mellett 1) binárisan, 2) oktálisan, 3) hexadecimálisan is palindromszámok.



Tekintsük az alábbi algoritmust: (1) Ha egy szám palindromszám, az algoritmus véget ér. (2) Ha nem, a számot megfordítjuk, és hozzáadjuk az eredetihez. Az eredmény számra GOTO (1). Ez a Lychrel-algoritmus^a. A sejtés az, hogy bármely kezdőértékkel indulva az algoritmus véget ér. Például $57 \rightarrow 57 + 75 = 132 \rightarrow 132 + 231 = 363$. A 10 000 alatti számokat megvizsgálva határozzuk meg, hogy az algoritmus az egyes esetekben hány lépésben ér véget. (Vigyázat, a 196-tal problémák lesznek!) Az eredményt rajzoljuk ki hisztogramon.

^aAz elnevezés a szerző, WADE VAN LANDINGHAM barátnőjének, Cheryl-nek az anagrammájából ered.



Írunk programot a Julián naptár, a Gergely naptár és a mája naptár számítására. Hasonlítsuk össze a hibákat napi, hónapos, éves, tízéves, százéves és ezer éves vonatkozásban.

7.2.2. Euklideszi algoritmus

Ha létezik az $a_1, a_2, \dots, a_n \in \mathbb{Z}$ számok legnagyobb közös osztója, akkor a legnagyobb közös osztók közül az egyik nemnegatív, ezt $\text{lko}(a_1, a_2, \dots, a_n)$ -nel jelöljük. (A $\text{gcd}(a_1, a_2, \dots, a_n)$ és az (a_1, a_2, \dots, a_n) jelölés is elterjedt; ha nem okoz félreérteést, akkor ez utóbbit fogjuk használni). Nyilván $(0, \dots, 0) = 0$, egyébként pedig a 0-kat elhagyva a közös osztók nem változnak. Az, hogy a_1, a_2, \dots, a_n relatív prímek, azt jelenti, hogy $(a_1, a_2, \dots, a_n) = 1$. Hasonlóan, ha létezik az $a_1, a_2, \dots, a_n \in \mathbb{Z}$ számok legkisebb közös többszöröse, akkor a legkisebb közös többszörök közül az egyik nemnegatív, ezt $\text{lkkt}(a_1, a_2, \dots, a_n)$ -nel jelöljük. (Az $\text{lcm}(a_1, a_2, \dots, a_n)$ és az $[a_1, a_2, \dots, a_n]$ jelölés is gyakori, a rövidség kedvéért mi ez utóbbit használjuk). Ha valamelyik a_i nulla, akkor az egyetlen közös többszörös a 0.

Egyáltalan nem magától értetődő azonban, hogy bármely két egész számnak létezik legnagyobb közös osztója.

Előfeltétel: $a, b \in \mathbb{Z}, b \neq 0$

Eredmény: az a és b egészek legnagyobb közös osztója

```

1: function EUKLIDESZ $\mathbb{Z}(a, b)$ 
2:    $r \leftarrow a \bmod b$ 
3:   while  $r \neq 0$  do
4:      $a \leftarrow b$ 
5:      $b \leftarrow r$ 
6:      $r \leftarrow a \bmod b$ 
7:   end while
8:   return  $b$ 
9: end function

```

7.1. ábra. Az egész számokon értelmezett euklideszi algoritmus iteratív pszeudokódja.

7.2.8. téTEL (két egész szám legnagyobb közös osztójának 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 mindenkor, amíg 0 maradékhoz nem jutunk. Megmutatjuk, hogy az eljárás véges, és az utolsó osztó ($b \nmid a$ esetén 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 tételeit alkalmazva alkalmas q_i, r_i egészekkel

$$\begin{aligned}
a &= bq_1 + r_1, & \text{ahol } 0 < r_1 < |b|, \\
b &= r_1 q_2 + r_2, & \text{ahol } 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, & \text{ahol } 0 < r_3 < r_2, \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, & \text{ahol } 0 < r_n < r_{n-1}, \\
r_{n-1} &= r_n q_{n+1}, & (r_{n+1} = 0).
\end{aligned}$$

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 7.1.2. 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 $c \mid a - bq_1 = r_1$, majd a másodikból $c \mid b \wedge c \mid r_1 \Rightarrow c \mid b - r_1 q_2 = r_2$. Ugyanígy folytatva végül az utolsó előtti egyenlőségből azt kapjuk, hogy $c \mid r_n$. ■

Az algoritmus pszeudokódját a 7.1. ábra tartalmazza.

7.2.9. Következmény. Bármely $a_1, a_2, \dots, a_n \in \mathbb{Z}$ számoknak létezik legnagyobb közös osztója, és

$$(a_1, a_2, \dots, a_n) = ((\dots((a_1, a_2), a_3), \dots, a_{n-1}), a_n).$$

Bizonyítás. Két szám közös osztóinak halmaza megegyezik a két szám legnagyobb közös osztója osztóinak halmazával. A többit indukcióval kapjuk. ■

7.2.10. Következmény. Ha $c > 0$, akkor $(ca, cb) = c(a, b)$.

Bizonyítás. Tekintsük az (a, b) előállítására szolgáló euklideszi algoritmust, legyen az utolsó nem-nulla maradék $r_n = (a, b)$. Ha minden egyenlőséget megszorzunk c -vel, akkor éppen a (ca, cb) -t előállító euklideszi algoritmushoz jutunk. Ebben az utolsó nem-nulla maradék $(ca, cb) = cr_n = c(a, b)$. ■

7.2.11. téTEL (Rekurziós téTEL a legnagyobb közös osztó kiszámítására). Legyen $a \neq 0$. Ha $b = 0$, akkor $(a, b) = |a|$. Ha $b \neq 0$, akkor $(a, b) = (|b|, a \text{ rem } |b|)$.

Bizonyítás. A $b = 0$ eset nyilvánvaló. Legyen tehát $b \neq 0$. A maradékos osztás tétele miatt létezik olyan q egész, amelyre $a = |b|q + (a \text{ rem } |b|)$. Az euklideszi algoritmus első két lépését tekintve az a és b számok legnagyobb közös osztója megegyezik a $|b|$ és az $a \text{ rem } |b|$ legnagyobb közös osztójával. ■

7.2.12. téTEL (Bézout). 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

$$r_2 = b - r_1 q_2 = b - (a - bq_1) q_2 = a(-q_2) + b(1 + q_1 q_2),$$

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. ■

7.17. 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 az 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.

$$\begin{aligned} 4 &= 12 - 8 = 12 - (44 - 3 \cdot 12) = -44 + 4 \cdot 12 = -44 + 4(56 - 44) = -5 \cdot 44 + 4 \cdot 56 \\ &= -5(2004 - 35 \cdot 56) + 4 \cdot 56 = -5 \cdot 2004 + 179 \cdot 56. \end{aligned}$$

Az iménti eljárásnak megfelelő **bővített euklideszi algoritmus** meghatározza az a, b egészek d legnagyobb közös osztóját, valamint azon $x, y \in \mathbb{Z}$ számokat, amelyre $d = ax + by$. Az alábbiakban két Python implementációt ismertetünk, az első iteratív, a második rekurzív.

```
def BovitettEuklideszInZ(a, b):
    x,y, u,v = 0,1, 1,0
    while a != 0:
        q,r = b//a, b%a # maradekos osztas
        m,n = x-u*q, y-v*q
        b,a, x,y, u,v = a,r, u,v, m,n
    return b, x, y

def BovitettEuklideszInZrek(a, b):
    if a == 0:
        return (b, 0, 1)
    else:
        g, y, x = BovitettEuklideszInZrek(b % a, a)
        return (g, x - (b // a) * y, y)
```

A bővített euklideszi algoritmus segítségével tehát 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 megfelelők, 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 7.2.12. téTEL fontos következménye a kétismeretlenes **lineáris diofantikus egyenlet** megoldhatóságára vonatkozó alábbi téTEL. Diofantikus egyenletnek olyan egész együtthatós algebrai egyenletet nevezünk, amelynek 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.

7.2.13. téTEL. Rögzített a, b és 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 $(a, b) \mid ax_0 + by_0 = c$. Megfordítva, tegyük fel, hogy $(a, b) \mid c$, vagyis valamelyen t -re $c = (a, b)t$. Ekkor a 7.2.12. 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.

7.18. példa. Egy szigeten 7 fejű és 24 fejű sárkányok élnek. Összesen 500 fejük van. Hány sárkány él a szigeten, ha tudjuk, hogy kizárolag hármasával járnak? A megoldandó feladat tehát a

$$7x + 24y = 500$$

lineáris diofantikus egyenlet pozitív megoldásainak megkeresése, amiből $x + y$ adja a sárkányok összlétszámát. Először megvizsgáljuk, vajon létezik-e megoldás.

$$\begin{aligned} 24 &= 7 \cdot 3 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 3. \end{aligned}$$

Mivel $1 \mid 500$, ezért létezik megoldás, továbbá $1 = 7 - 3 \cdot 2 = 7 - 2(24 - 7 \cdot 3) = -2 \cdot 24 + 7 \cdot 7$, amiből

$$500 = -1000 \cdot 24 + 3500 \cdot 7.$$

Minket csak a pozitív megoldások érdekelnek, ezért $1000 = 142 \cdot 7 + 6$ miatt

$$500 = (-1000 + 143 \cdot 7) \cdot 24 + (3500 - 24 \cdot 143) \cdot 7 = 1 \cdot 24 + 68 \cdot 7.$$

De nem ez az egyetlen megoldás. $68 = 2 \cdot 24 + 20$ miatt még két megoldás létezik,

$$500 = 8 \cdot 24 + 44 \cdot 7 = 15 \cdot 24 + 20 \cdot 7.$$

A szigeten így 69, 52, vagy 35 sárkány élhet. A feladat kritériuma szerint csak a 69 osztható hárommal, így a szigetnek egyetlen 24 fejű és 68 hétfejű sárkány lakója van.

Vajon az euklideszi algoritmus hány lépében fejeződik be? Elegendő vizsgálni az $a > b \geq 1$ esetet.

7.2.14. téTEL. Legyen $a > b \geq 1$ és legyen $\phi = (1 + \sqrt{5})/2$. Ekkor az (a, b) kiszámítására szolgáló euklideszi algoritmus legfeljebb $\lfloor \log_{\phi} b \rfloor + 1$ lépében befejeződik.

BIZONYÍTÁS. Az euklideszi algoritmus lépései legyenek $r_{k-1} = r_k q_{k+1} + r_{k+1}$, $1 \leq k \leq n-1$, $r_0 = a$, $r_1 = b$, $r_n = (a, b)$. A maradéksorozat hosszára, vagyis n -re vonatkozó felső becslést keresünk. Észrevehetjük, hogy $q_k \geq 1$ minden $1 \leq k \leq n-1$ esetén. Továbbá $q_{n+1} \geq 2$ is teljesül, mert ha $q_{n+1} = 1$ lenne, akkor $r_{n-1} = r_n$ miatt a maradéksorozat nem volna szigorúan monoton csökkenő. A 7.2.10. következmény miatt feltehető továbbá az is, hogy $(a, b) = r_n = 1$. Teljes indukcióval bebizonyítjuk, hogy

$$r_k \geq \phi^{n-k}, \quad 0 \leq k \leq n \tag{7.2}$$

teljesül. Ekkor

$$b = r_1 \geq \phi^{n-1}.$$

A logaritmusfüggvény tulajdonságait használva kapjuk, hogy

$$n \leq \log b / \log \phi + 1 = \log_{\phi} b + 1,$$

amiből az állítás következik. A (7.2) egyenlőtlenséget rögzített n esetén $(n-k)$ -ra vonatkozó indukcióval bizonyítjuk. $k = n$ esetén

$$r_n = 1 = \phi^0,$$

és $k = n-1$ esetén

$$r_{n-1} = q_{n+1} r_n = q_{n+1} \geq 2 > \phi.$$

Legyen $0 \leq k \leq n-2$ és tegyük fel, hogy $k+1 = k'$ esetén fennáll az egyenlőtlenség. Ekkor

$$\begin{aligned} r_k &= q_{k+2} r_{k+1} + r_{k+2} \geq r_{k+1} + r_{k+2} \\ &\geq \phi^{n-k-1} + \phi^{n-k-2} = \phi^{n-k-1} \left(1 + \frac{1}{\phi}\right) = \phi^{n-k}. \end{aligned}$$

Ezzel a bizonyítás kész. ■

A Fibonacci-számoknál látott ϕ aranymetszés vajon csak véletlenül szerepel a téTELben? Az 7.2.14. téTEL következménye világosabb magyarázattal szolgál.

7.2.15. Következmény (Lamé tétele). *Tetszőleges $n \geq 1$ esetén ha $a > b \geq 1$ és $b < F_{n+1}$, akkor az (a, b) kiszámítására szolgáló euklideszi algoritmus lépésszáma legfeljebb $n - 1$.*

Megmutatjuk, hogy a Lamé-tétel korlátja a lehető legjobb. A euklideszi algoritmus be-menetéül tekintsünk szomszédos Fibonacci-számokat. $(F_2, F_3) = (1, 2) = 1$, $(F_3, F_4) = (2, 3) = 1$. $n \geq 3$ -ra $F_{n+1} \text{ rem } F_n = F_{n-1}$, így a 7.2.11. tételt alkalmazva

$$(F_n, F_{n+1}) = (F_n, (F_{n+1} \text{ rem } F_n)) = (F_n, F_{n-1}) = (F_{n-1}, F_n).$$

Következésképpen az $(F_{n+1}, F_n) = 1$ kiszámításakor az euklideszi algoritmus pontosan $n - 1$ lépésben hajtódik végre. Azt is mondhatjuk, hogy az euklideszi algoritmus lépésszáma $|a| > |b| \geq 1$ méretű input esetén $O(\log(|b|))$.

Gyakorlatok

7.2-24. Euklideszi algoritmussal számoljuk ki 2004 és 520 legnagyobb közös osztóját és az eredményt fejezzük ki a két szám lineáris kombinációjaként.

7.2-25. Keressük meg a $354x + 138y = 12$ egyenlet megoldásait az egész számok körében.

7.2-26. A síkon hány rácspontot tartalmazhat egy

- a) racionális
- b) iracionális

meredekségű egyenes?

7.2-27. Milyen $n \in \mathbb{N}$ esetén egyszerűsíthetőek az alábbi törtek:

$$\text{a)} \quad \frac{3n+1}{7n+2} \quad \text{b)} \quad \frac{3n^2+1}{4n^2+3}.$$

7.2-28. Hány olyan 100-nál kisebb n természetes szám van, amelyre $(n, 72) = 6$ és $(n, 35) = 5$?

7.2-29. Süsünek csupa 7 és tízfejű unokatestvérei vannak, akiknek összesen 116 fejük van. Hány unokatestvére van a sárkánygyereknek?

7.2-30. Becsüljük meg az euklideszi algoritmus futásidéjét adott $a > b \geq 1$ esetén b jegyszámának függvényében.



Írunk programot az általános $a_1x_1 + \dots + a_nx_n = c$ lineáris diofantikus egyenlet megoldására (a_i, c egészek, $n \geq 3$). Hasonlóan az $n = 2$ esethez, az egyenletnek pontosan akkor létezik megoldása, ha $(a_1, a_2, \dots, a_n) \mid c$. A megoldásokat $n - 1$ egész paraméter segítségével adjuk meg.



Legyenek a_1, a_2, \dots, a_n relatív prím 1-nél nagyobb egészek. Tervezzünk algoritmust, amely meghatározza azon F egészek maximumát, amelyekre az $a_1x_1 + \dots + a_nx_n = F$ egyenletnek nincs megoldása a nemnegatív x_1, \dots, x_n egészeken. Vizsgáljuk az $n = 2, 3$ eseteket. A problémát *Frobenius-problémának* vagy *pénzváltó problémának* is nevezik.

7.2.3. A szármelmélet alaptétele

Az alábbi tétel fontos szerepet játszik a szármelmélet alaptételének bizonyításánál.

7.2.16. téTEL. Ha $c \mid ab$ 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 7.2.10. következmény alapján $c \mid (ab, cb) = (a, c) \cdot b = b$. ■

7.2.17. téTEL. Az egész számok körében p akkor és csak akkor prím, ha felbonthatatlan.

Bizonyítás. Azt kell beláttni, 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 7.2.16. 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 **törzszámoknak** 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 $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$.

7.2.18. téTEL (a számlelmélet 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 $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, ahol a p_i és q_j számok felbonthatatlanok, akkor $r = s$ és a p_i és q_j számok valamelyen sorrendben egymás egységszeresei.

7.19. példa. $20 = 2 \cdot 2 \cdot 5 = (-2) \cdot 2 \cdot (-5) = 5 \cdot (-2) \cdot (-2)$.

Bizonyítás. (1) 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 nem-triviális 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 $a = p_1 p_2 \cdots p_{k+1}$ előállítást nyerjük.

(2) Az egyértelműség bizonyítása. Tegyük fel indirekt, hogy a -nak (legalább) két lényegesen különböző felbontása létezik, vagyis

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \tag{7.3}$$

Ha itt valamelyik p_i egységszerese valamelyik q_j -nek, például $p_1 = \varepsilon q_1$, akkor q_1 -gyel egyszerűsítve

$$a' = \frac{a}{q_1} = \varepsilon p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s,$$

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 (7.3) előállítás ilyen. Ekkor $p_1 \mid q_1 q_2 \cdots q_s$. 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 mindenkető ellentmondás. ■

Figyeljük meg, hogy az egyértelműség bizonyítása lényegében a maradékos osztás elvé-gezhetőségére 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 egész számok pozitív egész osztóival foglalkozunk, és prímszámon is pozitív prímszámot fogunk érteni. Ekkor a számelmélet alaptételében szereplő prímtényezős felbontás az alábbiakat jelenti:

7.2.19. téTEL. *Minden $n > 1$ egész szám*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = \prod_{i=1}^r p_i^{\alpha_i}$$

alakban írható, ahol p_1, p_2, \dots, p_r különböző (pozitív) prímek és $\alpha_i > 0$ egészek. Ez a felirás a prímhátránytényezők sorrendjétől eltekintve egyértelmű. Az előállítást az n szám **kanonikus alakjának** nevezik.

7.20. példa. 123456 kanonikus alakja $2^6 \cdot 3 \cdot 643$, de nem kanonikus alakja például $2^5 \cdot 6 \cdot 643$.

Ellenőrző kérdés. Hogyan olvasható le egy szám kanonikus alakjából, hogy négyzetszám, köbszám, illetve általában k -adik hatvány?

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.

7.21. 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.

7.2.20. téTEL. Az

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

kanonikus alakú szám

a) pozitív osztói pontosan a

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$$

alakú számok, ahol $0 \leq \beta_i \leq \alpha_i, i = 1, 2, \dots, r$,

b) pozitív osztóinak száma

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1).$$

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, hogy legyen. b) Az összes pozitív osztót úgy kapjuk, hogy a β_i kitevők minden i -re egymástól függetlenül végigfutnak a $0, 1, \dots, \alpha_i$ értékeken, a kitevők egymástól független megválasztására így $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$ lehetőség van. A pozitív osztók előállításának egyértelműségét felhasználva a tétel bizonyítása kész. ■

7.22. 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?

7.2.21. 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 $t \cdot (T/a, T/b) = ab/(a, b) \cdot (T/a, T/b) = (Tb/(a, b), Ta/(a, b)) = T(b/(a, b), a/(a, b)) = T$. Ha a és b valamelyike (vagy mindkettő) negatív, akkor hasonló megfontolással $t = [a, b] = |ab|/(a, b)$. ■

7.2.22. Következmény. Legyen $a, b \in \mathbb{Z}$. Ekkor $(a, b)[a, b] = |ab|$.

7.2.23. Következmény. Legyen $a, b \in \mathbb{Z}$, $(a, b) = 1$. Ekkor $|ab| = [a, b]$.

7.2.24. 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 többszöröképben $[a, b]$ többszörösei. ■

7.2.25. téTEL. Ha az a és b pozitív egészek módosított kanonikus alakja

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad \text{és} \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}, \quad \text{ahol } \alpha_i \geq 0, \beta_j \geq 0,$$

akkor

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_r^{\min(\alpha_r, \beta_r)},$$

$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_r^{\max(\alpha_r, \beta_r)}.$$

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 $\alpha_i \neq \beta_i$, és 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. ■

7.2.26. Következmény. Két szám pontosan akkor relatív prím, ha nincs közös prímosztójuk, vagyis

$$(ab, c) = 1 \Leftrightarrow (a, c) = 1 \text{ és } (b, c) = 1.$$

7.23. 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 ismereteket hatékony algoritmusok. Egy nagy egész szám prímsége tehát algoritmikusan eldönthető, míg faktorizálására nem ismerünk gyors módszert. Ez a tény titkosírások konstrukciójára használható, amit az XX fejezetben vizsgálunk meg részletesen.

Gyakorlatok

7.2-31. Keressünk olyan pozitív egész számot, amelyet 2-vel szorozva négyzetszámot, 3-mal szorozva köbszámat, 5-tel szorozva teljes ötödik hatványt kapunk.

7.2-32. Határozzuk meg a felírt számok hiányzó számjegyeit úgy, hogy teljesüljön az oszthatóság. Keressük meg az összes megoldást.

a) $36 | 52x2y$,

b) $72 | x378y$,

c) $45 | 24x68y$.

7.2-33. Osztható-e 1599-cel $\binom{3400}{1700}$?

7.2-34. Bizonyítsuk be, hogy minden $n \geq 2$, $1 \leq k \leq n - 1$ esetén $n | \binom{n}{k}$.

7.2-35. Bizonyítsuk be, hogy tetszőleges p prímról és a, b egészekre $(a + b)^p \equiv a^p + b^p \pmod{p}$.

7.2-36. Hányféleképpen írható fel egy egész szám felbonthatatlanok szorzatait, ha a sorrendben és egységszeresekben való eltérést is különböző felbontásnak vesszük?

7.2-37. 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) $[a, (b, c)] = ([a, b], [a, c])$.

7.2-38. Melyek azok a háromjegyű számok, amelyeknek pontosan 5 pozitív osztójuk van?

7.2-39. Határozzuk meg azt a legkisebb természetes számot, amelynek pontosan 42 osztója van és osztható 42-vel.

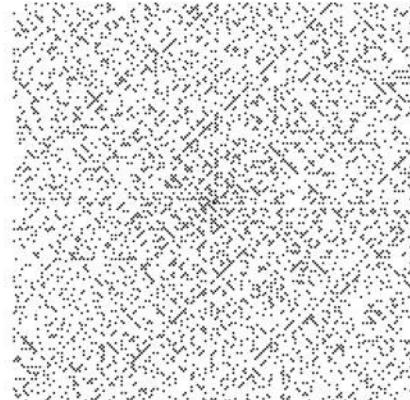
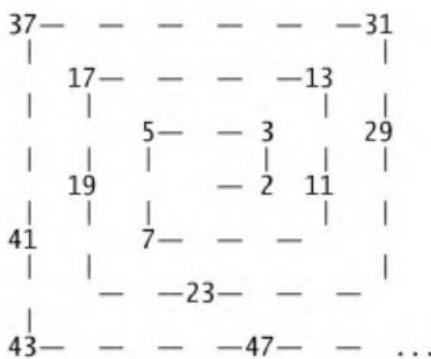
7.2-40. Mely számoknak van pontosan 2003 darab osztója?

7.2-41. A szultán születésnapján néhány rabot kegyelemben akar részesíteni. 100 cel-lás kazamatáborrönének minden cellájában rabskodik valaki. A szultán egymás után leküldi 100 emberét. Az elsőnek leküldött ember minden ajtót kinyit. A másodiknak leküldött minden második ajtót bezár. A harmadik ember minden harmadik ajtót kinyit, ha zárva volt, és bezár, ha nyitva volt. Hasonlóan nyit-zár a többi leküldött ember is. Mely cellák ajtaja marad a végén nyitva?

7.2-42. Bizonyítsuk be, hogy

$$\tau(n) \leq n/2 + 1,$$

$$\tau(n) \leq n/3 + 2,$$



7.2. ábra. Az Ulam-spirál négyzetrácsban kicsiben és egy 200×200 -as tartományon.

$$\tau(n) \leq 2\sqrt{n}.$$

7.2-43. Mivel egyenlő egy $n \in \mathbb{N}$ szám pozitív osztóinak szorzata?

7.2-44. Bizonyítsuk be a Legendre-formulát: az $n!$ kanonikus alakja

$$n! = \prod_{p \leq n} p^{\alpha_p}, \text{ ahol } \alpha_p = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

7.2-45. Mutassuk meg, hogy az n -nel osztható számok körében nem érvényes a számelmélet alaptétele.

7.2.4. 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:

7.2.27. téTEL. *A prímszámok száma végtelen.*

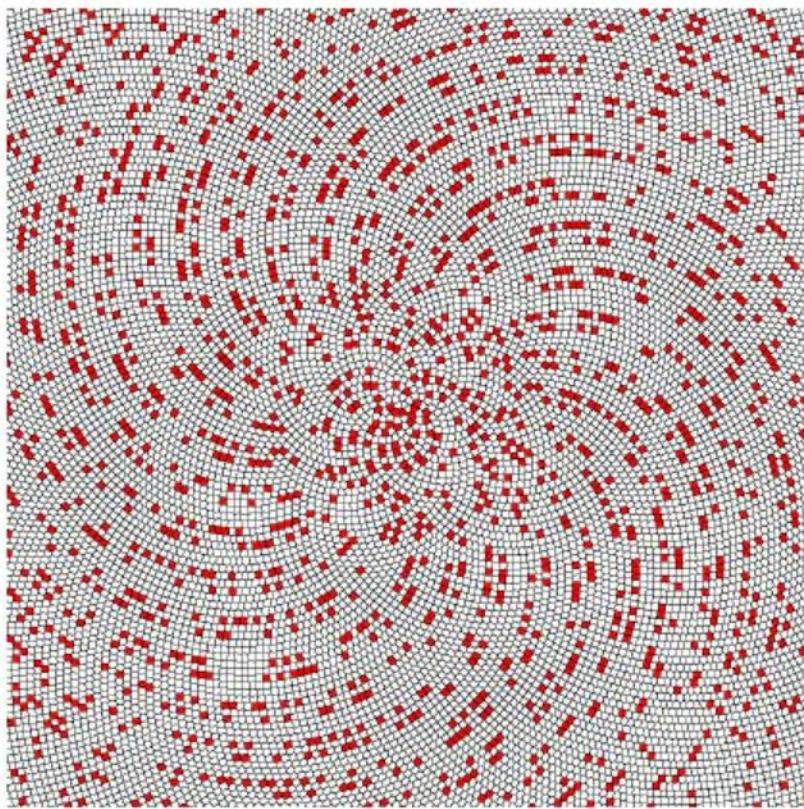
Bizonyítás. Tegyük fel indirekt, hogy csak véges sok prímszám van, p_1, p_2, \dots, p_k , és legyen $n = \prod_{j=1}^k p_j$. Ekkor $n+1$ nyilván $p_1 = 2, p_2, \dots, p_k$ egyikével sem osztható, ugyanakkor a számelmélet alaptétele miatt bizonyosan létezik prímosztója. Ez ellentmond az indirekt feltevésnek. ■

Az **Ulam-spirál** a prímszámok egy olyan spirális elrendezése, amikor egy négyzetrács mentén, spirálvonalon haladva rajzoljuk fel az egészket, és kihúzzuk a nem-prímeket.² A prímek többnyire átlók mentén helyezkedtek el, sőt, a jelenség nagyobb léptékben is megfigyelhető (7.2. ábra).

Ha a számokat négyzetrács helyett egy hatszögrácsra tekerjük fel, a prímek elhelyezkedésének nem véletlen volta még szembetűnőbb (7.3. ábra).

Már EULER is foglalkozott a prímek elhelyezkedésével. Az $n^2 + n + 17$ képlete minden 0 és 15 közötti értékre prímszámot ad. Ezek a prímek ($17, 19, 23, 29, 37, 47, 59, 73, 89, 107, 127, 149, 173, 199, 227$ és 257) az Ulam-spirál átlójában meg is jelennek. EULER később egy másik képletet is talált: $n^2 + n + 41$, ami 0 és

²Nevét felfedezőjéről, STANISŁAW ULAM lengyel matematikusról kapta, aki 1963-ban egy unalmas értekezleten rajzolta fel először a spirált.



7.3. ábra. Az Ulam-spirál a hatszögrácson.

40 közötti helyettesítési értékekre minden prím. Ez egy másik átló, ami mentén különösen sok a prím: 10 millióig a helyettesítési értékek 47,5%-a ilyen.

A következő tételből az derül ki, hogy a prímek között azért tetszőlegesen nagy hézagok is találhatók.

7.2.28. téTEL. *Tetszőleges pozitív egész N szához 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 $n_k + 2, n_k + 3, n_k + 4, \dots, n_k + p_k$ minden 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 minden páros. Ugyanakkor időnként előfordulhatnak egymáshoz igen közelí prímek, úgynévezett **ikerprímek**, amikor p és $p+2$ is prím. 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”. Az a probléma, hogy létezik-e végtelen sok ikerprímpár, máig megoldatlan. 2013 áprilisában Csang Bebizonította, hogy végtelen sok olyan prímszámpár létezik, amelyek különbsége kevesebb mint 70 millió. Azóta ezt a számot sikerült 246-ra leszorítani. Az ikerprímpárok általánosabban is megfogalmazható: a szomszédos prímek különbsége vajon végtelen sokszor lesz-e „nagyon kicsi”. Az ikerprímek mindenkorban „nagyon ritkán” helyezkednek el a prímek között, az ikerprímek reciprok-összege ugyanis konvergens (Brun-konstans), míg a prímeké divergens. Ez utóbbi tény azt is mutatja, hogy a prímszámok „elég sűrűen” helyezkednek el. Ha

$\pi(x)$ jelöli az x -nél nem nagyobb prímek számát, akkor a prímszámtétel szerint

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln(x)} = 1.$$

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.

7.2.29. tétele (Eratoszthenészi-szita). *Írjuk fel a számokat 2-től n -ig. Az első szám, a 2 prím, amelynek összes többszöröse összetett, ezeket húzzuk ki. A megmaradt számok közül az első, a 3 prím, ennek többszörösei összetettek, ezeket húzzuk ki, stb. Ismétljük 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 $p \leq k$. De ekkor $p^2 \leq pk = n$, amiből $p \leq \sqrt{n}$.

Érdekes kérdés, hogy bizonyos tulajdonságú sorozatokban van-e végtelen sok prím. Az alábbi tételt bizonyítás nélkül közöljük.

7.2.30. tétele (Dirichlet-tétel). *Ha $a, d \in \mathbb{Z}$, $d > 0$ és $(a, d) = 1$, akkor az $a + kd$, $k = 0, 1, 2, \dots$ számtani sorozat végtelen sok prímet tartalmaz.*

A prímszámok elméletében számos nevezetes sejtés létezik, az alábbiakban kettőt sorunk fel:

- Két egymást követő négyzetszám között mindenig 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 emlíjük meg, az előbbieket **Fermat-prímeknek**, az utóbbiakat **Mersenne-prímeknek** nevezzük. Megmutatható, hogy ha $2^k + 1$ prím, akkor k szükségképpen kettő-hatvány, 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 $0 \leq n \leq 4$ esetén prím, míg $5 \leq n \leq 23$ 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 $n = 2^\alpha p_1 \cdots p_r$, ahol $\alpha \geq 0$, $r \geq 0$ és a p_i számok különböző Fermat-prímek. Az első néhány érték: 3, 4, 5, 6, 8, 10, 12, 15, stb.

A Mersenne-féle prímekhez a **tökéletes számok** keresése során jutunk. A tökéletes számok olyan n természetes számok, amelyek n -től különböző osztóik összegével egyenlők. Például $6 = 1 + 2 + 3$. Páratlan tökéletes számok 10^{20} alatt bizonyosan nincsenek, feltehetően egyáltalán nincsenek. A páros számok pontosan akkor tökéletesek, ha $n = M_p 2^{p-1}$ alakúak (p prím). 2013. január 25-én találták meg a 48-adik Mersenne-prímet, ez a $2^{57885161} - 1$ szám, amely 17 425 170 számjegyből áll. Könyvünk írásakor ez a legnagyobb ismert prímszám. Máig megoldatlan az a kérdés, hogy a tökéletes számok (Mersenne-prímek) sorozata véges vagy végtelen.

Ellenőrző kérdés. Ha p egy olyan prím, amelyre M_p Mersenne-prím, akkor M_p bináris felírárában hány egyes van?

Gyakorlatok

7.2-46. Mutassuk meg, hogy 2 kivételtől eltekintve minden prím $6k \pm 1$ alakú ($k \in \mathbb{N}$).

7.2-47. Mutassuk meg, hogy végtelen sok

- a) $4k - 1$ alakú
- b) $6k - 1$ alakú

prímszám van ($k \in \mathbb{N}^+$).

7.2-48. Hány prím található 1000 -ig az $a_1 = 5$, $a_{i+1} = a_i + 3 + (-1)^i$ sorozatban ($i \geq 1$)?

7.2.5. Pithagoraszi számhármasok

Pithagoraszi számhármasoknak az

$$x^2 + y^2 = z^2 \quad (7.4)$$

egyenlet pozitív egész megoldásait nevezzük. Geometriai értelemben azon derékszögű háromszögek oldalhosszait jelentik, amelyeknél az oldalak hosszai egészek. Ilyen számhármasok nyilván léteznek, mert például a $3, 4, 5$ megfelelők, sőt, ha x, y, z megoldás, akkor tetszőleges pozitív d egésszel dx, dy, dz is. Ezért elegendő a **primitív** megoldásokat (**alapmegoldásokat**) megkeresni, amikor $(x, y, z) = 1$. Ekkor azonban x, y, z nem csak relatív prímek, hanem páronként relatív prímek is, mert ha közülük bármely kettőnek lenne egynél nagyobb közös osztója, akkor (7.4) miatt a harmadik is osztható lenne ezen közös osztóval.

Az x, y „befogók” nem lehetnek tehát egyszerre párosak, de páratlanok sem. Ugyanis tegyük fel, hogy x és y neggyel osztva 1 vagy -1 maradékot ad. Ekkor $z^2 = x^2 + y^2$ neggyel osztva $1+1=2$ maradékot ad, vagyis z^2 páros, de neggyel nem osztható. Viszont ez nem lehetséges, mert ha z^2 páros, z is az, így négyzete neggyel osztható. Kapjuk tehát, hogy x és y közül az egyik páros, a másik páratlan. Az általánosság megszorítása nélkül feltehető, hogy x páros és y páratlan. Ekkor természetesen z is páratlan.

A (7.4) egyenletet írjuk át:

$$\left(\frac{x}{2}\right)^2 = \frac{z^2 - y^2}{4} = \frac{z+y}{2} \cdot \frac{z-y}{2}.$$

A felbontás tényezői y és z azonos paritása miatt egészek. Sőt, relatív prímek, mert ha $d | (z+y)/2$ és $d | (z-y)/2$, akkor d osztója összegüknek és különbségüknek is, vagyis z -nek illetve y -nak. De mivel $(z, y) = 1$, így d is csak 1 lehet. Viszont relatív prím párok szorzata csak úgy lehet négyzetszám, ha maguk is négyzetszámok. Ezek szerint

$$\frac{z+y}{2} = m^2 \quad \text{és} \quad \frac{z-y}{2} = n^2$$

alkalmas m, n egészekre, ahol $(m, n) = 1$. Innen összeadással és kivonással nyerjük, hogy

$$z = m^2 + n^2 \quad \text{és} \quad y = m^2 - n^2, \quad (7.5)$$

m	n	x	y	z
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	4	40	9	41

7.3. táblázat. A Pithagoraszi számhármasok néhány alapmegoldása.

továbbá $x^2 = 4m^2n^2$ miatt

$$x = 2mn. \quad (7.6)$$

Azért, hogy ne legyen x és y egyszerre páros, fel kell tennünk, hogy m és n nem mindenketten páratlanok. Emellett természetesen $m > n$ áll.

Azt kaptuk, hogy ha m és n olyan relatív prímek, amelyek nem mindenketten páratlanok, akkor (7.5) és (7.6) alapmegoldások. Mindezt könnyen ellenőrizhetjük:

$$(2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2,$$

továbbá $(2mn, m^2 - n^2, m^2 + n^2) = 1$. Ez utóbbi teljesüléséhez elég igazolni, hogy a három szám közül valamelyik kettő relatív prím. Például $2mn$ és $m^2 - n^2$ relatív prímek, mert sem 2 nem lehet közös osztó (az első szám páros, a második páratlan), sem pedig $m^2 - n^2$ nem lehet osztható $(m, n) = 1$ miatt m és n egyetlen prímosztójával sem. Az alábbi tételek bizonyítottak:

7.2.31. téTEL. Az $x^2 + y^2 = z^2$ másodfokú diofantoszi egyenlet alapmegoldásai az alábbi alakúak:

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2,$$

ahol $(m, n) = 1$, $m > n$ és m, n különböző paritásúak. Az összes megoldást az alapmegoldások tetszőleges $d \in \mathbb{N}$ számmal való szorzásával kapjuk.

A 7.3. táblázat néhány alapmegoldást tartalmaz.

A Pithagoraszi számhármasok problémájának általánosítása, hogy az $a^n + b^n = c^n$ diofantoszi egyenletnek nincs megoldása 2-nél nagyobb egész n esetén a nem-nulla egész számok körében. A sokáig nagy Fermat-sejtésként ismert állítást 1995-ben sikerült bizonyítani ANDREW WILES-nek. A Wiles–Fermat-tétel volt az egyik leghosszabban bizonyítatlanul maradó szármelmeleti sejtés.

7.3. 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.

7.3.1. 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 $a \equiv b \pmod{m}$ -mel 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 $a \equiv b \pmod{m}$ illetve $a \not\equiv b \pmod{m}$ jelölés is.

7.24. példa. $16 \equiv 4 \pmod{3}$, mert $3 \mid 12 = 16 - 4$.

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. A fejezet hátralévő részében legyen $m \geq 2$.

7.3.2. téTEL (a kongruencia tulajdonságai).

- (1) $a \equiv a \pmod{m}$ minden $a \in \mathbb{Z}$ -re,
- (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. Az (1)–(4) állítások nyilvánvalóak. Például a (4) tulajdonság azért teljesül, mert 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 $a + c \equiv b + d \pmod{m}$. Az (5) tulajdonságnál $m \mid a - b$ és $m \mid c - d$, amiből $a = mx + b$ és $c = my + d$ alkalmas $x, y \in \mathbb{Z}$ -re. Az egyenletek alapján $ac = m(mxy + dx + by) + bd$, amiből $ac \equiv bd \pmod{m}$. A (6) tulajdonság bizonyításához alkalmazzuk a (4) és (5) tulajdonságokat $c = d$ esetére: $a \equiv b \pmod{m} \Rightarrow a + c \equiv b + c \pmod{m}$ és $a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$. Az (5) tulajdonság $c = a$, $d = b$ esetének többszöri alkalmazásából $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$ adódik, ami bizonyítja (6)-ot. ■

Ellenőrző kérdés. Igaz-e, hogy ha $a \equiv b \pmod{m}$, akkor minden $m_1 \mid m$ -re $a \equiv b \pmod{m_1}$?

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.

7.3.3. 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 létezik 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

7.3.4. Következmény. $(c, m) = 1$ és $ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{m}$.

A 7.3.2. téTEL szerint az egészeket ekvivalenciaosztályokba sorolhatjuk. De vajon mely számok kerülnek egy osztályba?

7.3.5. 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 $0 \leq r_a, r_b < m$. 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.

7.3.6. definíció. Rögzített m modulus mellett az a -val kongruens elemek halmazát az a által reprezentált **maradékosztálynak** nevezzük és $[a]_m$ -mel jelöljük.

A definíció szerint $[a]_m = \{a + km : k \in \mathbb{Z}\}$, valamint $a \equiv b \pmod{m} \Leftrightarrow [a]_m = [b]_m$.

7.25. példa. $[3]_7 = \{\dots, -11, -4, 3, 10, 17, \dots\} = [80]_7$.

Az összes maradékosztályt tartalmazó halmaz jelölése:

$$\mathbb{Z}_m = \{[a]_m \mid 0 \leq a \leq m - 1\}.$$

7.3.7. 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.

7.26. 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.

7.3.8. 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 a $(b, m) \mid (a, m)$ oszthatóság is, ezért $(a, m) = (b, m)$. ■

7.3.9. definíció. Az $[a]_m$ maradékosztályt **redukált maradékosztálynak** nevezzük, ha $(a, m) = 1$.

A 7.3.8. téTEL miatt ha egy maradékosztály egy eleme relatív prím a modulushoz, akkor a maradékosztály összes eleme ilyen.

7.3.10. definíció. Ha minden m szerinti redukált maradékosztályból pontosan egy reprezentáns elemet választunk, akkor **redukált maradékrendszer** kapunk.

7.27. példa. A $\{-7, 7, 11, -11\}$ halmaz redukált maradékrendszer modulo 12.

Adott modulus szerinti összes redukált maradékosztályt tartalmazó halmaz jelölése:

$$\mathbb{Z}_m^* = \{[a] \in \mathbb{Z}_m : 1 \leq a \leq n, (a, m) = 1\}.$$

7.3.11. definíció (Euler-féle φ függvény). Tetszőleges m pozitív egész esetén jelentse $\varphi(m)$ az m -nél kisebb, m -hez relatív prím természetes számok számát.

7.28. 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 téTELt bizonyítottuk:

7.3.12. téTEL. Egész számok egy tetszőleges halmaza pontosan akkor alkot

- (1) teljes maradékrendszeret modulo m , ha a halmaz elemszáma m és elemei páronként inkongruensek modulo m ,
- (2) redukált maradékrendszeret modulo m , ha a halmaz elemszáma $\varphi(m)$, elemei páronként inkongruensek modulo m és valamennyien relatív prímek m -hez.

A most következő téTEL szerint teljes maradékrendszer, illetve redukált maradékrendszer bizonyos tulajdonságú lineáris transzformációk után is teljes, illetve redukált maradékrendszer marad.

7.3.13. 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) $\{ca_i + d : 1 \leq i \leq m\}$ teljes maradékrendszer modulo m ,
- (2) $\{cb_i : 1 \leq i \leq \varphi(m)\}$ redukált maradékrendszer modulo m .

Bizonyítás. (1) igazolása: mivel az új halmaz elemszáma is m , ezért a 7.3.12. 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 7.3.4. következmény miatt c -vel egyszerűsíthetünk, így $a_i \equiv a_j \pmod{m}$, vagyis $i = j$, hiszen az a_i -k teljes maradékrendszer 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 7.2.25. téTEL (2) állítása miatt ekkor $(cb_i, m) = 1$ is teljesül.

■

A téTEL egy nagyon fontos alkalmazása a következő.

7.3.14. 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 maradékrendszer 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 $1 \leq i, j \leq \varphi(m)$ 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 elégges, 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, de nem minden a legkisebbet. Abban a speciális esetben, ha a modulus egy p prímszám, $\varphi(p) = p - 1$, így az alábbi összefüggést kapjuk.

7.3.15. Következmény (Fermat-téTEL egyik alakja). *Ha p prímszám, $a \in \mathbb{Z}$ és $p \nmid a$, akkor $a^{p-1} \equiv 1 \pmod{p}$.*

7.3.16. 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 minden oldal osztható p -vel. Ha $p \nmid a$, akkor az előző következmény miatt lesz igaz. ■

Figyeljük meg, hogy a Fermat-téTEL első alakja csak $p \nmid a$ esetén, míg második alakja az a egészre vonatkozó megkötés nélkül is teljesül.

Gyakorlatok

7.3-1. Milyen maradékot adnak a természetes számok négyzetei hárommal és öttel osztva?

7.3-2. Bizonyítsuk be, hogy 12 egymást követő egész szám négyzetének összege sosem lehet négyzetszám.

7.3-3. Létezik-e csupa azonos jegyből álló legalább kétjegyű négyzetszám?

7.3-4. Mutassuk meg, hogy egy tetszőleges egész három tetszőleges páratlan kitevőjű hatványának összege osztható hárommal.

7.3-5. Teljes maradékrendszer-e $\{7, 22, 37, 52, 67, \dots, 11632, 11647\}$ (mod 777)?

7.3-6. Redukált maradékrendszer-e $\{5, 15, 25, 35, 45, 55, \dots, 155\}$ (mod 32)?

7.3.1. 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 másnéven $[a_1 + b_1]_m = [a_2 + b_2]_m$ következik. Hasonlóan járhatunk el a szorzás esetében is.

7.3.17. 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.

$$\begin{aligned}[a]_m \oplus [b]_m &= [a + b]_m \\ &= [b + a]_m \\ &= [b]_m \oplus [a]_m, \\ ([a]_m \oplus [b]_m) \oplus [c]_m &= [a + b]_m \oplus [c]_m \\ &= [(a + b) + c]_m \\ &= [a + (b + c)]_m \\ &= [a]_m \oplus [b + c]_m \\ &= [a]_m \oplus ([b]_m \oplus [c]_m).\end{aligned}$$

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.

7.3.18. téTEL. A modulo m maradékosztályok között pontosan a redukált maradékosztályoknak létezik multiplikatív inverzük.

BIZONYÍTÁS. Megvizsgáljuk, hogy milyen $[a]_m$ esetén létezik olyan $[c]_m$, amelyre

$$[a]_m \otimes [c]_m = [1]_m. \tag{7.7}$$

A (7.7) egyenlet megoldhatósága azt jelenti, hogy $[ac]_m = [1]_m$, vagyis az $ac \equiv 1 \pmod{m}$ kongruencia c -re megoldható. A kongruencia definíciója miatt ekkor létezik olyan x egész, amelyre $mx = 1 - ac$, vagyis $ac + mx = 1$. Így az $ac \equiv 1 \pmod{m}$ kongruencia akkor és csak akkor oldható meg, ha az $ac + mx = 1$ diofantikus egyenlet megoldható, aminek a szükséges és elégsges feltétele az, hogy $(a, m) \mid 1$ teljesüljön (7.2.13. téTEL), vagyis $(a, m) = 1$ legyen. Ez azt jelenti, hogy az $[a]_m$ redukált maradékosztály. ■

7.3.19. Következmény. A modulo m maradékosztályok akkor és csak akkor alkotnak testet, ha m prím.

A továbbiakban a modulo m vett maradékosztályok additív csoportját röviden \mathbb{Z}_m -mel, multiplikatív csoportját pedig \mathbb{Z}_p^* -gal jelöljük (p prím). Jegyezzük meg, hogy \mathbb{Z}_m elemszáma m , míg \mathbb{Z}_p^* elemszáma $p - 1$.

7.3.2. 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.

7.3.20. definíció. Lineáris kongruencia megoldásszámán a páronként inkongruens megoldásokat értjük.

7.3.21. 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 ekkor 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 elégsges feltétele az $(a, m) \mid b$ oszthatóság teljesülése (7.2.13. 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 $\{c_1, c_2, \dots, c_m\}$ teljes maradékrendszer, akkor a 7.3.13. téTEL miatt $\{c_1a, c_2a, \dots, c_ma\}$ is teljes maradékrendszer modulo m , így pontosan egy elem van közöttük, 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 $a_1x \equiv b_1 \pmod{m_1}$ kongruenciákat ugyanazok az egész számok elégítik ki, elég azt megvizsgálni, hogy a modulo m_1 egyetlen maradékosztályt alkotó megoldások hány inkongruens maradékosztályt jelentenek modulo m . Ha x_0 megoldása az $a_1x \equiv b_1 \pmod{m_1}$ kongruenciának, akkor pontosan az

$$x_0, x_0 + m_1, x_0 + 2m_1, \dots, x_0 + (d-1)m_1$$

elemek esnek különböző maradékosztályokba modulo m . Ez pedig d darab inkongruens megoldást jelent modulo m . Vagyis a teljes megoldást az

$$[x_0], [x_0 + m_1], [x_0 + 2m_1], \dots, [x_0 + (d-1)m_1]$$

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.

7.29. példa. Oldjuk meg a 7.18. sárkányos példát kongruenciákkal. A megoldandó lineáris diofantikus egyenlet a $7x + 24y = 500$. Térjünk át kongruenciáakra és válasszuk modulusnak a 7-et. Ekkor a megoldandó egyenlet $24y \equiv 500 \pmod{7}$, vagyis $3y \equiv 3 \pmod{7}$. Mivel $(3, 7) = 1$, ezért a kongruenciának egyetlen maradékosztály megoldása lesz. A kongruenciát 3-mal osztva $y \equiv 1 \pmod{7}$ adódik. A szöveges feladat nemnegatív megoldásai így $y = 1, 8, 15, 22, \dots$ stb, a hozzájuk tartozó x értékek pedig rendre $68, 44, 20, -4, \dots$ Mivel csak az első három eset jöhet szóba megoldásként, a szigetlakó sárkányok száma 69, 52 vagy 35 lehet, ebből a 69 osztható hárommal.

7.3.22. téTEL. Legyen $(a, m) = 1$. Ekkor az $ax \equiv b \pmod{m}$ kongruencia egyetlen megoldása az $x_0 \equiv a^{\varphi(m)-1}b \pmod{m}$ 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 $a^{\varphi(m)}x_0 \equiv a^{\varphi(m)-1}b \pmod{m}$ kongruenciát 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 modulust is osztjuk) megoldjuk a kapott kongruenciát, majd ennek az x_0 megoldásából

$$x_k = x_0 + k \frac{m}{(a, m)}$$

segítségével előállítjuk a többöt, ahol $0 \leq k < (a, m)$.

7.30. 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 $x \equiv 1134 \pmod{1234}$.

Gyakorlatok

7.3-7. Oldjuk meg az alábbi kongruenciák közül a megoldhatókat:

- a) $3x \equiv 5 \pmod{7}$,
- b) $111x \equiv 1111 \pmod{11}$,
- c) $12x \equiv 8 \pmod{18}$,
- d) $12x \equiv 8 \pmod{20}$,
- e) $25x \equiv 17 \pmod{37}$.
- f) $27x \equiv 15 \pmod{39}$,
- g) $123x \equiv 456 \pmod{78}$,
- f) $27x \equiv 18 \pmod{99}$,
- i) $555x \equiv 5555 \pmod{55\,555}$.

7.3-8. A pincénkben pókok és százlábúak élnek. minden póknak 8 és minden százlábúnak 100 lába van. Hány pók és hány százlábú lehet a kastélyban abban a pillanatban, amikor összesen 2012 lábuk van?

7.3-9. LVIII. Lajos igencsak elbizakodott uralkodó volt: csak 5 és 8 talléros érméket veretett. Ha valaki történetesen 7 tallért akart fizetni, az kénytelen volt például úgy intézni, hogy 3-szor 5 tallért fizetett, majd 8 tallért visszakapott.

- a) Milyen módokon lehetett 99 tallért kifizetni ebben a birodalomban?
 b) Milyen összegeket lehetett egyáltalán kifizetni?
 c) Milyen összegeket lehet kifizetni egy hasonlóan egoista kései utód, LXIX. Lajos uralkodása alatt?

7.3-10. Melyek azok a háromjegyű pozitív egészek, amelyeknek a négyzete is ugyanarra a háromjegyű számra végződik?

7.3.3. Szimultán kongruenciák

Lineáris kongruenciák után most lineáris kongruencia-rendszerek közös megoldásait keresük. Legyen $k \in \mathbb{N}$, $m_1, m_2, \dots, m_k \in \mathbb{N}$, $a_i, b_i \in \mathbb{Z}$ ($1 \leq i \leq k$). Az

$$\begin{aligned} a_1x &\equiv b_1 \pmod{m_1} \\ a_2x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_kx &\equiv b_k \pmod{m_k} \end{aligned}$$

kongruencia-rendszer **szimultán megoldása** x_0 , ha egyszerre elégíti ki az összes kongruenciát. Nyilvánvaló, hogy ha valamelyik kongruenciára nem teljesül a megoldhatóság feltétele, akkor a kongruencia-rendszerek sincs megoldása. Másrészt, ha külön-külön létezik is az iménti kongruenciáknak megoldása, ez nem feltétlenül jár azzal, hogy létezik szimultán megoldás.

A megoldhatóság keresését kezdjük a $k = 2$ esettel.

7.3.23. téTEL. Az $x \equiv c_1 \pmod{m_1}, x \equiv c_2 \pmod{m_2}$ szimultán kongruencia pontosan akkor oldható meg, ha $(m_1, m_2) \mid c_1 - c_2$. Megoldhatóság esetén az összes megoldás egyetlen maradékosztállyba esik modulo $[m_1, m_2]$.

BIZONYÍTÁS. A kongruencia definíciója alapján az egyenletek azt jelentik, hogy alkalmas z_1, z_2 egészekre $x = c_1 + z_1 m_1 = c_2 + z_2 m_2$, vagyis $m_2 z_2 - m_1 z_1 = c_1 - c_2$. A lineáris diofantikus egyenlet pedig pontosan akkor oldható meg, ha $(m_1, m_2) \mid c_1 - c_2$. Megoldhatóság esetén legyen s, t két szimultán megoldás. Ekkor $s \equiv t \pmod{m_1}$ és $s \equiv t \pmod{m_2}$, amiből $m_1 \mid t - s$ és $m_2 \mid t - s$. Ez pedig azt jelenti, hogy $[m_1, m_2] \mid t - s$, vagyis $t \equiv s \pmod{[m_1, m_2]}$. ■

7.31. példa. Az $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{4}$ kongruencia-rendszer nem megoldható, mert $(2, 4) = 2 \nmid 1 = 2 - 1$.

Indukcióval általánosítva kapjuk az alábbi téltet:

7.3.24. téTEL. Az $x \equiv c_i \pmod{m_i}$ ($1 \leq i \leq k$) szimultán kongruencia-rendszer akkor és csak akkor oldható meg, ha $c_i \equiv c_j \pmod{(m_i, m_j)}$ minden különböző $1 \leq i, j \leq k$ párra. A megoldás ekkor modulo $[m_1, m_2, \dots, m_k]$ egyértelmű.

A továbbiakban azt a speciális esetét tárgyaljuk, amelyben a modulusok páronként relatív prímek. Ekkor ugyanis az 7.3.24. tétel miatt a kongruencia-rendszer biztosan megoldható, és a megoldások egyetlen maradékosztályt alkotnak modulo $m_1 \cdots m_k$. A megoldási módszer **kínai maradékététel** néven ismert.

7.32. példa. Időszámításunk szerint 100 körül Szun-ce kínai matematikus oldotta meg azt a problémát, hogy hogyan lehet olyan x egészket 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).

7.3.25. tételel (kínai maradéktétel). *Ha m_1, \dots, m_k páronként relatív prím modulusok, akkor az*

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_k \pmod{m_k}, \end{aligned} \tag{7.8}$$

kongruencia-rendszernek bármely c_1, \dots, c_k egészek esetén van megoldása, s ez a megoldás modulo $M = m_1 \cdots m_k$ egyértelmű.

Bizonyítás. Legyen

$$M_i = M/m_i \quad (1 \leq i \leq k),$$

vagyis $M_i = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k$. 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 minden $1 \leq i \leq k$ esetén megoldhatók, mert M_i és m_i relatív prímek minden $1 \leq i \leq k$ esetén. Jelöljük megoldásait sorban y_1, y_2, \dots, y_k -val és legyen

$$g_i = M_i y_i \quad (1 \leq i \leq k). \tag{7.9}$$

Legyen

$$x_0 \equiv (c_1 g_1 + c_2 g_2 + \cdots + c_k g_k) \pmod{M}. \tag{7.10}$$

Megmutatjuk, hogy ebből az egyenletből $x_0 \equiv c_i \pmod{m_i}$ ($1 \leq i \leq k$) következik. Ha $i \neq j$, akkor $M_j \equiv 0 \pmod{m_i}$, amiből (7.9) miatt $g_j = M_j y_j \equiv 0 \pmod{m_i}$. Azt is észrevehetjük, hogy $g_i \equiv 1 \pmod{m_i}$ minden $1 \leq i \leq k$ esetén, így

$$\begin{aligned} x_0 &\equiv c_i g_i \pmod{m_i} \\ &\equiv c_i \pmod{m_i} \end{aligned}$$

minden i -re teljesül. A (7.10) szerint kiszámolt x_0 tehát valóban megoldás.

Tegyük fel, hogy a (7.8) kongruencia-rendszernek több inkongruens megoldása is van modulo M , vagyis tegyük fel, hogy $x_0 \not\equiv x_1 \pmod{M}$ a kongruencia-rendszer megoldásai. Mivel $x_0 \equiv x_1 \pmod{m_i}$ minden $1 \leq i \leq k$ esetén, ezért $m_i \mid x_0 - x_1$. 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 (7.8) kongruencia-rendszer 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 $1 \leq i \leq k$ esetén. Ez azt jelenti, hogy $x_0 \equiv x_1 \pmod{m_i}$, vagyis x_1 is kielégíti (7.8) minden egyenletét. ■

A bizonyítás módszert is ad a szóban forgó kongruencia-rendszer megoldására.

7.3.26. Következmény. Ha m_1, \dots, m_k páronként relatív prím pozitív egészek, továbbá $M = m_1 \cdots m_k$, akkor az x és c egészekre az

$$x \equiv c \pmod{m_i} \quad (i = 1, 2, \dots, k)$$

egyenletek akkor és csak akkor teljesülnek egyidejűleg, ha

$$x \equiv c \pmod{M}.$$

Ellenőrző kérdés. Milyen előnye lehet az általunk adott kínai maradéktétel bizonyítást megvalósító algoritmusnak az alábbi verzióval szemben: Vegyük a (7.8) kongruencia-rendszer első két egyenletét és keressük meg a megoldását. Az így kapott megoldás egy új kongruenciát jelent, így összesítve egygyel csökkent a kongruencia-egyenletek száma. Iteratívan haladunk tovább, amíg el nem érünk a végső megoldáshoz.

7.33. példa. Oldjuk meg az

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 2 \pmod{4} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

kongruencia-rendszert. A kínai maradéktétel feltételei teljesülnek, mert a modulusok páronként relatív prímek. A korábbi jelölésünk szerint $c_1 = 1$, $c_2 = 2$, $c_3 = 3$, $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $M = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 4 \cdot 5 = 60$, $M_1 = 4 \cdot 5 = 20$, $M_2 = 3 \cdot 5 = 15$, és $M_3 = 3 \cdot 4 = 12$. Az $M_i y_i \equiv 1 \pmod{m_i}$ kongruenciákat rendre megoldva kapjuk, hogy $y_1 \equiv 2 \pmod{m_1}$, $y_2 \equiv 3 \pmod{m_2}$, és $y_3 \equiv 3 \pmod{m_3}$, így $g_1 = M_1 y_1 = 40$, $g_2 = M_2 y_2 = 45$, és $g_3 = M_3 y_3 = 36$. Az eredmény pedig

$$x_0 \equiv c_1 g_1 + c_2 g_2 + c_3 g_3 \equiv 40 + 2 \cdot 45 + 3 \cdot 36 \equiv 40 + 90 + 108 \equiv 238 \equiv -2 \pmod{60}.$$

7.34. példa. Megmutatjuk, hogy bármely pozitív természetes számokból álló (növekvő) számtani sorozatnak van 2003 egymást követő olyan tagja, amelyik minden összetettséget.

Feltehető, hogy $d > 1$, egyébként a 7.2.28. tétel bizonyítja az állítást. Tekintsük a pozitív tagokból álló $a, a+d, a+2d, \dots$ számtani sorozatot. A sorozat összes tagja kielégíti az $x \equiv a \pmod{d}$ kongruenciát. Válasszunk olyan $p_1, p_2, \dots, p_{2003}$ (különböző) prímeket, amelyek nem szerepelnek d törléstényezőkbe bontásában. Ekkor az

$$\begin{aligned} x &\equiv a \pmod{d} \\ x &\equiv -d \pmod{p_1} \\ x &\equiv -2d \pmod{p_2} \\ &\vdots \\ x &\equiv -2003d \pmod{p_{2003}} \end{aligned}$$

egyenletekben a modulusok páronként relatív prímek, így a kongruencia-rendszer megoldható. A megoldást követő számtani sorozatbeli elem megadja a csupa összetett számokból álló 2003 elemű részsorozat első tagját.

Emlékeztetünk, hogy korábbi megállapodásunk szerint $\mathbb{Z}_m = \{a \in \mathbb{Z} \mid 0 \leq a < m\}$, $m \in \mathbb{Z}^+$.

7.3.27. tétele (Moduláris számábrázolás tétele). *Legyenek m_1, \dots, m_k páronként relatív prím pozitív egészek, $M = m_1 \cdots m_k$, legyen továbbá $a \in \mathbb{Z}_M$, és $a_i \in \mathbb{Z}_{m_i}$ olyanok, hogy*

$$a_i \equiv a \pmod{m_i} \quad (1 \leq i \leq k).$$

Tekintsük a

$$\begin{aligned} \phi : \mathbb{Z}_M &\rightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k} \\ \phi(a) &= (a_1, a_2, \dots, a_k) \end{aligned}$$

megfeleltetést. Ekkor ϕ az összeadáson, kivonáson és szorzáson bijektív homomorfizmus (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

$$\begin{aligned} (a+b) &\leftrightarrow ((a_1+b_1) \pmod{m_1}, \dots, (a_k+b_k) \pmod{m_k}), \\ (a-b) &\leftrightarrow ((a_1-b_1) \pmod{m_1}, \dots, (a_k-b_k) \pmod{m_k}), \\ (ab) &\leftrightarrow (a_1b_1 \pmod{m_1}, \dots, a_kb_k \pmod{m_k}). \end{aligned}$$

Bizonyítás. A ϕ függvény bijektivitása és a művelettartás a kínai maradéktételből következik. ■

A tétele gyakran alkalmazzuk gyors algoritmusok készítésekor, mivel az egyes \mathbb{Z}_{m_i} hal-mazokban hatékonyabban lehet műveleteket végezni (bitműveletekben számolva), mint \mathbb{Z}_M -ben.

7.3.1. megjegyzés. *A tételben nem látunk osztást. Bizonyos feltételek mellett az osztás is elvégezhető: ha $a \cdot b^{-1} \pmod{M}$ -et kell kiszámítani és $(b, M) = 1$, akkor az*

$$(ab^{-1}) \leftrightarrow (a_1b_1^{-1} \pmod{m_1}, \dots, a_kb_k^{-1} \pmod{m_k})$$

megfeleltetés már működik. Ha $(b, M) > 1$, akkor át kell térni egy másik, immáron megfelelő prímekből álló ábrázolásra. Ez viszont viszonylag költséges.

7.35. 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 egészével képes gyors egész aritmetikát végezni. Erre az aritmetikára építve valósítunk meg az architektúránkon olyan egész aritmetikát (összeadás, kivonás, szorzás), amellyel az $I_2 = [0, 2000]$ intervallumban is tudunk számolni.

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 egész tehát egy I_1 intervallumból vett számhármas-sal 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 moduláris számábrázolás 7.3.27. tétele miatt

$$a + b \leftrightarrow (2 + 10 \bmod 14, 9 + 7 \bmod 13, 1 + 7 \bmod 11) = (12, 3, 8).$$

Az ellenőrzéshez meg kell oldani az

$$\begin{aligned} x &\equiv 12 \pmod{14} \\ x &\equiv 3 \pmod{13} \\ x &\equiv 8 \pmod{11} \end{aligned}$$

kongruencia-rendszert. A kínai maradéktétel jelöléseivel

$$M_1 = 13 \cdot 11 = 143, M_2 = 14 \cdot 11 = 154, M_3 = 14 \cdot 13 = 182.$$

A következőkben megoldjuk az alábbi kongruenciákat:

- (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, $a+b = 100+150 = 250 \pmod{2002}$. A kivonásra és a szorzásra hasonló gondolatmenet alkalmazható.

A kínai maradéktétel további fontos következménye, hogy tetszőleges összetett modulusú kongruencia visszavezethető prímhátrány modulusú kongruencia-rendszerre. Ha ugyanis a modulus kanonikus alakja $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, akkor az $f(x) \equiv 0 \pmod{m}$ kongruencia ekvivalens az $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ szimultán kongruencia-rendszerrel. Itt aztán minden kongruenciát külön-külön megoldunk (ha valamelyik nem oldható meg, akkor az eredetinek sincs megoldása), majd a kínai maradéktételt alkalmazva sorban megkaphatjuk az eredeti kongruencia megoldásait.

7.36. példa. Gondoltam egy egész számra 1000 és 2000 között. Ha a szám 1001-edik és 2001-edik hatványát összeadom, majd hozzáadom a gondolt számot, az eredmény 202-re végződik. Melyik számra gondoltam?

Meg kell oldanunk az $x^{2001} + x^{1001} + x \equiv 202 \pmod{1000}$ kongruenciát. Mivel $1000 = 2^3 \cdot 5^3$, ezért két egyenletet vizsgálunk. Először megoldjuk az $x^{2001} + x^{1001} + x \equiv 202 \pmod{2^3}$ kongruenciát. Ha $8 \mid x$, akkor az iménti egyenletnek nincs megoldása, mert $8 \nmid 202$. Ha x páros, akkor $x^{2001} \equiv 0 \pmod{8}$ és $x^{1001} \equiv 0 \pmod{8}$, így az $x \equiv 2 \pmod{8}$ kongruenciát kapjuk. Ha $(x, 8) = 1$, akkor az Euler-tétel miatt $x^{2001} \equiv x \pmod{8}$ és $x^{1001} \equiv x \pmod{8}$, de a $3x \equiv 2 \pmod{8}$ kongruencia megoldása $x \equiv 6 \pmod{8}$ lenne, ami x páratlansága miatt lehetetlen. Vagyis modulo 8 egyetlen megoldás van csupán, amikor $x \equiv 2 \pmod{8}$.

A továbbiakban megoldjuk az $x^{2001} + x^{1001} + x \equiv 202 \pmod{5^3}$ kongruenciát. Észrevehetjük, hogy $(x, 125) > 1$ nem lehetséges. Ha pedig $(x, 125) = 1$, akkor ismét az Euler-tétel miatt $3x \equiv 77 \pmod{125}$, vagyis $x \equiv -16 \pmod{125}$. Azt kapjuk, hogy modulo 125 esetén a megoldás $x \equiv 109 \pmod{125}$.

Az $x \equiv 2 \pmod{8}$ és $x \equiv 109 \pmod{125}$ közös megoldása a kínai maradéktétel szerint $x \equiv 2 \cdot 125 \cdot 5 + 109 \cdot 8 \cdot 47 \equiv 234 \pmod{1000}$, így a keresett intervallumban a megoldás $x = 1234$.

Gyakorlatok

7.3-11. Oldjuk meg az alábbi kongruencia-rendszereket:

- a) $5x \equiv 3 \pmod{11}$ és $6x \equiv 4 \pmod{14}$,
- b) $21x \equiv 6 \pmod{30}$ és $15x \equiv 3 \pmod{36}$,

- c) $x \equiv 7 \pmod{13}$ és $x \equiv 11 \pmod{17}$,
- d) $x \equiv 13 \pmod{28}$ és $x \equiv 20 \pmod{21}$,
- e) $x \equiv 3 \pmod{7}$, $x \equiv 7 \pmod{13}$ és $x \equiv 13 \pmod{17}$,
- f) $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{4}$, $x \equiv 1 \pmod{5}$.

7.3-12. Egy részeg szárlábú próbálja megszámolni a lábait. 12-esével számolva 4 marad, 15-ösével számolva pedig 8. Nem érti az eredményt. Segítsünk neki!

7.3-13. Bizonyítsuk be, hogy van olyan számtani sorozat, amelynek 7 darab egymás utáni tagja teljes hatvány.

7.3-14. Bizonyítsuk be, hogy van a természetes számok között 100 darab egymás utáni szám, amelyek mindegyike osztható valamely egynél nagyobb négyzetszámmal.

7.3-15. Van-e olyan a és b pozitív egész szám, amelyre az alábbi legnagyobb közös osztók mindegyike nagyobb egynél: (a, b) , $(a, b + 1)$, $(a + 1, b)$, $(a + 1, b + 1)$.

7.3-16. Nevezünk a koordináta-rendszerben egy rácspontot *láthatónak*, ha az origóval öt összekötő szakasz másik rácspontot nem tartalmaz. Látható például a $(2, 5)$ pont, de nem látható az $(5, 5)$ pont, mert eltakarja többek között az $(1, 1)$ pont. Bizonyítsuk be, hogy van olyan (a, b) rácspont, hogy az $(a + r, b + s)$ rácspontok egyike sem látható, ahol $1 \leq r, s \leq 3$. (A megoldás menete kínálja az általánosítás lehetőségét. Tetszőlegesen nagy „láthatatlan” rácsnégyzet vagy akár rácstéglalap is van a koordináta-rendszerben. Sőt, a gondolatmenet általánosítható magasabb dimenzióra is.)

7.4. Szármelmeleti függvények

7.4.1. definíció. A szármelmeletben az $\mathbb{N}^+ \rightarrow \mathbb{C}$ leképezéseket *szármelmeleti függvényeknek* vagy *aritmetikai függvényeknek* nevezzük.

Ilyen például a korábban definiált Euler-féle φ függvény, vagy a pozitív osztók számát jelölő τ függvény.

7.4.2. definíció. Egy f szármelmeleti 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.

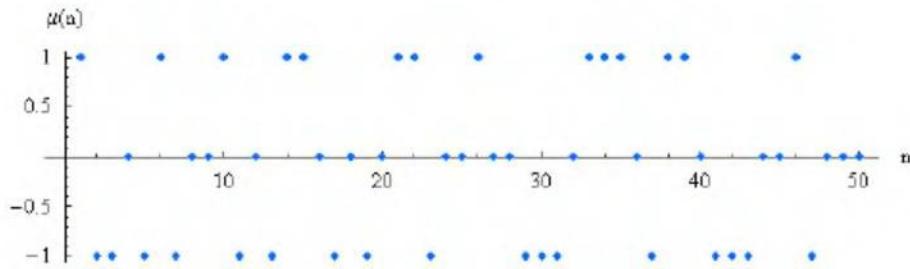
Jelölje $v(n)$ az $1 < n \in \mathbb{N}$ különböző prímosztói számát, és legyen $v(1) = 0$. Ha $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ az n kanonikus alakja, akkor $v(n) = r$. Könnyen látható, hogy a v függvény additív, de nem teljesen additív szármelmeleti függvény. Például $v(4) = 1 \neq 2 = 2v(2)$.

Legyen $1 < a \in \mathbb{R}$, 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 a $\log_a n$ függvény teljesen additív.

7.4.3. definíció. Egy f szármelmeleti 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.

A definíciókban az $m = 1$ helyettesítéssel azt kapjuk, hogy egy additív szármelmeleti függvény 1 helyen felvett értéke minden nullá, valamint egy nem azonosan nulla



7.4. ábra. A Möbius-függvény értékei az első 50 helyen.

multiplikatív szárméleti függvény 1 helyen felvett értéke minden 1.

7.4.4. definíció (Möbius-függvény). *A $\mu : \mathbb{N}^+ \rightarrow \{-1, 0, 1\}$,*

$$\mu(n) = \begin{cases} 1 & \text{ha } n = 1, \\ (-1)^r & \text{ha } n = p_1 p_2 \cdots p_r \text{ (} p_i \text{-k páronként különböző prímek),} \\ 0 & \text{különben.} \end{cases}$$

függvényt **Möbius-függvénynek** nevezzük.

A Möbius-függvény első néhány értékét láthatjuk a 7.4. ábrán.

7.4.5. téTEL. *A Möbius-függvény multiplikatív.*

Bizonyítás. Legyen $m, n \in \mathbb{N}^+$, $(m, n) = 1$. Feltehető, hogy $m, n > 1$, egyébként a multiplikativitás nyilvánvaló. Ha m és n közül legalább az egyik nem négyzetmentes, mondjuk $p^2 \mid m$, akkor $p^2 \mid mn$ miatt $\mu(m) = \mu(mn) = 0$, így $0 = \mu(mn) = \mu(m)\mu(n) = 0$. Ha mindkettő négyzetmentes, mondjuk $m = p_1 p_2 \cdots p_r$ és $n = q_1 q_2 \cdots q_s$, akkor a relatív prím tulajdonság miatt nincs közös prímosztójuk, így $\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n)$. ■

A Möbius-függvény nem teljesen multiplikatív, hiszen például $\mu(4) = 0 \neq 1 = \mu(2)^2$.

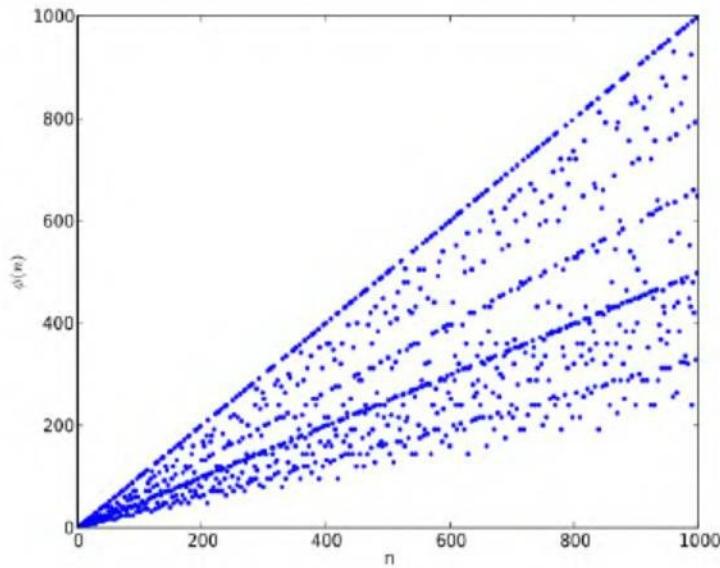
7.4.6. téTEL. *Az Euler-féle φ függvény multiplikatív, és ha $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ az $n > 1$ természetes szám kanonikus alakja, akkor*

$$\varphi(n) = n \prod_{j=1}^k \left(1 - \frac{1}{p_j}\right) = \prod_{j=1}^k (p_j^{\alpha_j} - p_j^{\alpha_j-1}) = \prod_{j=1}^k p_j^{\alpha_j-1} (p_j - 1).$$

Bizonyítás. Először φ multiplikativitását látjuk be. Legyen $m, n \in \mathbb{N}^+$, és $(m, n) = 1$. Készítsük el az alábbi táblázatot:

1	2	3	...	m
$m + 1$	$m + 2$	$m + 3$...	$2m$
$2m + 1$	$2m + 2$	$2m + 3$...	$3m$
\vdots	\vdots	\vdots		\vdots
$(n - 1)m + 1$	$(n - 1)m + 2$	$(n - 1)m + 3$...	nm

A táblázatban $\varphi(mn)$ olyan szám van, amelyik mn -hez relatív prím, továbbá a 7.2.25. téTEL (2) része miatt ezek mindegyike relatív prím m -hez és n -hez is. Keressük meg



7.5. ábra. Az Euler-féle φ függvény értékei az első 1000 helyen.

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 7.3.13. téTEL miatt minden ilyen oszlop teljes maradékrendszer 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 $\varphi(m)\varphi(n)$.

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 $0 \leq x \leq p^\alpha$ pontosan akkor nem relatív prím p^α -hoz, ha többszöröse p -nek. ■

A Euler-féle φ függvény első néhány értékét láthatjuk a 7.5. ábrán.

7.37. 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

$$x \equiv 2003^{2003} \equiv (2000 + 3)^{2003} \equiv 3^{2003} \equiv 3^{40 \cdot 50 + 3} \equiv (3^{40})^{50} \cdot 3^3 \equiv 3^3 \equiv 27 \pmod{100}.$$

A számelméleti függvények definíciójából következik, hogy ha $n \in \mathbb{N}^+$ kanonikus alakja $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, akkor bármely

(1) f additív számelméleti függvény esetén

$$f(n) = f(p_1^{\alpha_1}) + f(p_2^{\alpha_2}) + \cdots + f(p_k^{\alpha_k}),$$

(2) f teljesen additív számelméleti függvény esetén

$$f(n) = \alpha_1 f(p_1) + \alpha_2 f(p_2) + \cdots + \alpha_k f(p_k),$$

(3) f multiplikatív számelmeleti függvény esetén

$$f(n) = f(p_1^{\alpha_1})f(p_2^{\alpha_2}) \cdots f(p_k^{\alpha_k}),$$

(4) f teljesen multiplikatív számelmeleti függvény esetén

$$f(n) = f(p_1)^{\alpha_1}f(p_2)^{\alpha_2} \cdots f(p_k)^{\alpha_k}.$$

Gyakorlatok

7.4-1. Bizonyítsuk be a 7.4.6. téttel a logikai szita formula segítségével.

7.4-2. Mi a $39^{39^{39}}$ szám utolsó két számjegye?

7.5. Racionális és valós számok ábrázolása

A fejezetben már megvizsgáltuk a természetes számok helyiértékes és moduláris ábrázolási lehetőségeit (7.2.7. és 7.3.27. tételek). Helyiértékesen az egész számok is leírhatók, szükség szerint előjellel egészítve ki a természetes számokat. A moduláris esetben az egészek leírására használhatunk például szimmetrikus jegyrendszert.

Az alábbiakban a racionális és valós számok előállításának egyéb lehetőségeit vizsgáljuk.

7.5.1. q -adikus törtek

Ebben a fejezetben megmutatjuk, hogy a racionális számok helyiértékesen ábrázolva véges vagy végtelen szakaszos q -adikus törtként is megadhatók, míg az irracionális számokat végtelen, nem szakaszos tizedes törtekkel írhatjuk le.

Legyen $q > 1$ tetszőleges egész. A q -adikus tört a valós számok leggyakrabban alkalmazott **kanonikus** felírása. A minden nap életben a $q = 10$ **tizedestört** alakot használjuk.

A valós számok axiomatikus megalapozásánál láttuk, hogy minden $q > 1$ egész alaphoz létezik egy hozzá tartozó $[a_n, b_n]$ intervallum-skatulyázás, ahol $b_n - a_n = q^{-n}$. Ezért minden $0 \neq x \in \mathbb{R}$ valós szám felírható

$$x = s \cdot \left(\sum_{i=0}^m q^i \cdot d_i + \sum_{i=1}^{\infty} q^{-i} \cdot d_i^* \right) \quad (7.11)$$

alakban, ahol $s = \pm 1$ (ez az x szám előjele), továbbá $m \in \mathbb{N}$, $d_i, d_i^* \in \{0, 1, \dots, q-1\}$, $d_m \neq 0$ ha $m > 0$.

A (7.11) formulában az összeg első része a már ismert *egészrész*, a második része a *törtrész*. A fenti forma bármilyen különböző s előjel, és d_i, d_i^* jegysorozat esetén kijelöl egy egyértelműen meghatározott valós számot, ám ez fordítva nem igaz: egy számhoz több ilyen felírás is tartozhat. Azokat a nem-nulla racionális számokat, amelyeknek egyszerűsített törtfelírásában a nevező q prímosztóin kívül más prímszámmal nem osztható, kétfeleképpen is felírhatjuk.

7.38. példa. $q = 10$ esetén a tizedestört egyik lehetséges formájában egy bizonyos helyiérték után csupa 0, a másik formájában csupa 9-es áll:

$$\frac{5}{4} = 1,25 = 1,250000\dots = 1,249999\dots$$

Ha megköveteljük, hogy ne lehessen valamely helyiérték után csupa 9-es a felírásban, akkor minden szám egyértelműen előállítható lesz.

Az ilyen típusú racionális számok egyik felírásában tehát valamely helyiérték után csupa 0 szerepel (amit már nem szokás kiírni). A kapott alakot **véges q -adikus törtnak** nevezzük (ha mégis kiírunk valahány 0-t a q -adikus tört végére, akkor általában csak az érték pontosságát szeretnénk hangsúlyozni). Ha egy bizonyos helyiérték után a q -adikus jegyek szakaszosan ismétlődnek, akkor **végtelen szakaszos (periodikus) q -adikus törtről**, egyébként pedig **végtelen nem szakaszos (aperiodikus) q -adikus törtről** beszélünk. Összességében a véges és végtelen q -adikus törtek halmazát \mathbb{R} -rel lehet azonosítani.

Az alábbiakban vizsgálódásunkat a $q = 10$ tizedestörtek rendszerére korlátozzuk, de az eredmények tetszőleges $1 < q \in \mathbb{N}$ -re általánosíthatók.

Tizedestörtek

7.5.1. téTEL. *Minden pozitív $x = m/n$ racionális szám megadható véges vagy végtelen szakaszos tizedestört alakban.*

Bizonyítás. Legyen az m és n számok osztásánál kapott hányados sorozat a_1, a_2, \dots , maradék sorozat pedig r_0, r_1, \dots , ($0 \leq r_i \leq n - 1$). Ha a maradék valamikor 0, az osztási algoritmus véget ér, és m/n tizedestört kifejtése véges. Ha az algoritmus nem ér véget $n - 1$ lépésben sem, akkor a skatulya-elv miatt léteznek olyan $i < j$ egészek, hogy $a_{i+1} = a_{j+1}$, $r_{i+1} = r_{j+1}$, $a_{i+2} = a_{j+2}$, ..., vagyis a tizedestört alak végtelen szakaszos.

■

Az ismétlődő végtelen szakaszt felülvonással fogjuk jelölni.

7.39. példa.

$$\frac{23}{198} = 0,116161616\dots = 0,1\overline{16}\dots$$

Általában, $(m, n) = 1$ esetén

$$\frac{m}{n} = M, a_1 a_2 \dots a_k \overline{b_1 \dots b_l}, \quad (7.12)$$

ahol $M \in \mathbb{N}$, $0 \leq a_i, b_j < 10$. Vajon hogyan lehetne gyorsan kiszámolni k és l értékét?

Legyen $n = n_1 n_2$, ahol $n_2 = 2^\alpha 5^\beta$, $(n_1, n_2) = 1$ ($\alpha, \beta \in \mathbb{N}$). Vagyis n_1 jelöli n kanonikus felbontásában a 10-zel közös osztót nem tartalmazó részt.

7.5.2. lemma. *Az iménti jelölésekkel (7.12)-ben a tizedesvessző utáni jegyek k száma az a legkisebb y egész, amelyre n/n_1 osztója 10^y -nek. A periódus l hossza az a legkisebb z $\in \mathbb{N}$, amelyre n_1 osztója $10^z - 1$ -nek.*

7.40. példa. Az iménti példában $n = 198 = 2 \cdot 3^2 \cdot 11$, $n_1 = 3^2 \cdot 11 = 99$, így $n/n_1 = 2$. Mivel $2 | 10^1$ de $2 \nmid 10^0$, ezért $k = 1$, és $99 | 10^2 - 1$ de $99 \nmid 10^1 - 1$, ezért $l = 2$.

7.41. példa. A tizedesvessző után mikor kezdődik, és milyen hosszú a periódusa a $\frac{131}{242}$ racionális számnak? A vizsgálandó szám számlálója és nevezője relatív prímek (131 prím). $n = 242 = 2 \cdot 11^2$, így $n_1 = 11^2 = 121$ és $n/n_1 = 2$. Az iménti példához hasonlóan ekkor $k = 1$, és $121 \nmid 10^s - 1$, $s = 3, 4, \dots, 21$ esetén, de $121 \mid 10^{22} - 1$, ezért $l = 22$. Valóban, $131/242 = 0.54132231404958677685950\dots$

Bizonyítás. Ha (7.12)-ben az egyenlet minden oldalát megszorozzuk 10^k -val, azt kapjuk, hogy $10^k m \equiv 10^{k+l} m \pmod{n}$, amiből $(m, n) = 1$ miatt $n \mid 10^k(10^l - 1)$. Ekkor a feltételek miatt $n_2 \mid 10^k$ és $n_1 \mid 10^l - 1$. ■

7.5.3. téTEL. *Minden periodikus tizedestört egyértelműen előállít egy racionális számot, aminek közönséges tört alakját az alábbi formulából számolhatjuk:*

$$M, a_1 a_2 \dots a_k \overline{b_1 \dots b_l} \dots = M + \frac{(10^l \sum_{i=1}^k a_i 10^{k-i} + \sum_{i=1}^l b_i 10^{l-i}) - \sum_{i=1}^k a_i 10^{k-i}}{(10^l - 1) 10^k},$$

ahol M a szám egészrészze.

Bizonyítás. Nyilván elegendő a törtrésszel foglalkozni. Legyen a tízes számrendszerbeli helyiértékes ábrázolásban $A = (a_1 a_2 \dots a_k)_{10} \in \mathbb{N}$, $B = (b_1 b_2 \dots b_l)_{10} \in \mathbb{N}$ és $x = (0, A\overline{B})$. Ez utóbbit azt jelenti, hogy a tizedesvessző után A jegyei, majd B jegyei következnek ismétlődve. Ha $y = (0, \overline{B})$, akkor $10^l y = B + y$, vagyis $y = B/(10^l - 1)$. Továbbá $10^k x = A + (0, \overline{B}) = A + y = A + B/(10^l - 1)$ miatt

$$x = \frac{A}{10^k} + \frac{B}{(10^l - 1) 10^k} = \frac{(10^l A + B) - A}{(10^l - 1) 10^k}.$$

■

7.42. példa. $0,2\overline{54}$ esetén $k = 2, l = 1$, így

$$0,2\overline{54} \dots = \frac{254 - 25}{9 \cdot 10^2} = \frac{229}{900}.$$

Gyakorlatok

7.5-1. Adjunk magyarázatot az alábbi jelenségre:

$$\begin{aligned} 1/7 &= 0,\overline{142857} \\ 2/7 &= 0,\overline{285714} \\ 3/7 &= 0,\overline{428571} \\ 4/7 &= 0,\overline{571428} \\ 5/7 &= 0,\overline{714285} \\ 6/7 &= 0,\overline{857142} \end{aligned}$$

7.5-2. Tetszőleges $n \in \mathbb{N}^+$ esetén jelölje $\lambda(n)$ az $1/n$ tizedestört alakjában a periódus hosszát. Mutassuk meg, hogy ekkor $\lambda(n) \mid \varphi(n)$, ahol $\varphi(n)$ az Euler-függvény. Egyenlőség pedig pontosan akkor áll fenn, ha minden $a \in \mathbb{N}$ -re $(a, n) = 1$ esetén létezik olyan $k \in \mathbb{N}$, hogy $10^k \equiv a \pmod{n}$ (azt is mondjuk, hogy 10 primitív gyök modulo n).

7.5.2. Intervallum-aritmetika

Tekintsünk két olyan α, β mennyiséget, amelyek pontos értékét nem ismerjük (például két valós számokat tartalmazó kifejezést). Tegyük fel, hogy a rendelkezésünkre álló információ alapján minden összeadásban annyit tudunk, hogy α ismeretlen értéke valahol az $[\underline{a}, \bar{a}]$ intervallumban, míg β értéke valahol a $[\underline{b}, \bar{b}]$ intervallumban van. Mit mondhatunk például $\alpha + \beta$ értékéről? Fogalmazzunk másiképpen: mi a legkisebb és legnagyobb értéke $\alpha + \beta$ -nak a rendelkezésre álló információ alapján? Könnyű meggondolni, hogy $\alpha + \beta$ értéke valahol az $[\underline{a} + \underline{b}, \bar{a} + \bar{b}]$ intervallumba esik.

7.5.4. definíció. Legyenek $I_a = [\underline{a}, \bar{a}]$ és $I_b = [\underline{b}, \bar{b}]$ valós intervallumok és o a valós számokon értelmezett négy alapművelet (összeadás, kivonás, szorzás, osztás) valamelyike. Ekkor az alapműveleteket kiterjeszhetjük az intervallumok között végzett megfelelő aritmetikai műveletté az alábbi módon:

$$I_a \circ I_b := \{x \circ y \mid x \in I_a, y \in I_b\},$$

ahol az osztás esetén feltesszük, hogy $0 \notin I_b$.

Nyilvánvaló, hogy a műveletek eredménye szintén valós intervallum. Ennek kiszámításához elegendő az I_a és I_b végpontjait használnunk. Vagyis ahelyett, hogy α és β közelítő értékével számolnánk, számolhatunk a pontos értéket tartalmazó alsó és felső végpontú intervallumokkal is. Ekkor eredményül egy, a pontos eredményt tartalmazó intervallumot kapunk.

7.43. példa. Az IEEE 754 lebegőpontos aritmetikai szabványnak eleget tevő modern mikroprocesszorok támogatják az ilyen **intervallum-aritmetikai** számításokat azzal, hogy különböző kerekítési irányok állíthatók be.

7.5.5. téTEL. Az alábbi számítási szabályok érvényesek:

$$\begin{aligned} I_a + I_b &= [\underline{a} + \underline{b}, \bar{a} + \bar{b}], \\ I_a - I_b &= [\underline{a} - \bar{b}, \bar{a} - \underline{b}], \\ I_a \cdot I_b &= [\min\{\underline{a}\underline{b}, \underline{a}\bar{b}, \bar{a}\underline{b}, \bar{a}\bar{b}\}, \max\{\underline{a}\underline{b}, \underline{a}\bar{b}, \bar{a}\underline{b}, \bar{a}\bar{b}\}], \\ I_a / I_b &= [\underline{a}, \bar{a}] \cdot [1/\bar{b}, 1/\underline{b}]. \end{aligned}$$

A bizonyítások elemiek, az Olvasóra bízzuk őket.

7.44. példa. Legyen $I_1 = [-1, 1]$ és $I_2 = [2, 3]$. Ekkor $I_1 + I_2 = [1, 4]$, $I_1 - I_2 = [-4, -1]$, $I_1 \cdot I_2 = [-3, 3]$, $I_1 / I_2 = [-1/2, 1/2]$.

7.5.6. definíció. Ha $\underline{x} = \bar{x} = x$, akkor azt mondjuk, hogy az I_x intervallum **degenerált**. Ekkor I_x az x valós számra redukálódik.

Így a fent definiált intervallum-aritmetika valóban kiterjesztése a klasszikus aritmetikai műveleteknek. Az algebrai struktúrát tekintve azonban lényeges eltérések is vannak. Habár a nem-degenerált I intervallumok ($I; +$) struktúrája asszociatív, kommutatív, a semleges elem a degenerált $[0, 0]$ (így a struktúra kommutatív egységelemes félcsoport), ennél többet nem mondhatunk:

- Az összeadás nem invertálható, például $I_a = [-1, 1]$ ellentettje $-[-1, 1]$, de $[-1, 1] - [-1, 1] = [-2, 2] \neq [0, 0]$. Mindössze annyit mondhatunk, hogy $0 \in I_a - I_a$.

Hasonló kijelentés tehető a nem-degenerált I intervallumok ($I; \cdot$) struktúrájáról: kommutatív egységelemes félcsoport az $[1, 1]$ egységelemmel. Az inverzzel az iméntihez hasonló problémák adódnak:

- A szorzás nem invertálható, például $I_a = [1, 2]$ inverze $[1, 1]/[1, 2] = [1, 1] \cdot [1/2, 1] = [1/2, 1]$ lenne, de $[1/2, 1] \cdot [1, 2] = [1/2, 2] \neq [1, 1]$.

Nem-degenerált intervallumok esetében a disztributivitás sem teljesül.

- Legyen $I_a = [1, 2]$, $I_b = [2, 3]$ és $I_c = [-2, 4]$. Ekkor $I_a(I_b + I_c) = I_a \cdot [0, 7] = [1, 2] \cdot [0, 7] = [0, 7]$, de $I_aI_b + I_aI_c = [1, 2][2, 3] + [1, 2][-2, 4] = [2, 6] + [-4, 8] = [-2, 14]$.

Az azonban általában is igaz, hogy $I_a(I_b + I_c) \subseteq I_aI_b + I_aI_c$. Ezt a tulajdonságot **szub-disztributivitásnak** nevezzük.

Bár az intervallumokkal történő számolás egyszerű, sorozatos alkalmazása után az eredményül kapott intervallum túl szélessé válhat. Emiatt a gyakorlatban az eredmények akár használhatatlanok is lehetnek. Az intervallum-aritmetika alkalmazása előtt ezért a szóban forgó kifejezéseket egyszerűsíteni kell, hogy a paraméterek ismételt előfordulását elkerüljük. Amikor nincsenek ismétlődő paraméterek, az intervallum-aritmetika a lehetséges legszűkebb eredményt adja (a bemenő paraméterek adott bizonytalansága esetén). Bármilyen széles is az eredményül kapott intervallum, biztosan tartalmazza a valódi (de ismeretlen) értéket.

Gyakorlatok

7.5-2. A televíziós dalverseny abszolút döntőjébe 3 versenyző jutott: Falsi, Hamiskás és Sükike. minden zsűritag pontosan egy versenyzőre szavazhatott. A műsorvezető a szavazás végén megállapította, hogy az 59 zsűritag közül Falsira és Hamiskásra 15, Hamiskásra és Sükikrére 18, Falsira és Sükikrére összesen 20 szavazat érkezett. mindenki tudja, hogy a műsorvezető rosszul számol, de mind a négy említett érték legfeljebb 13-mal tér el a helyes értéktől. Ki nyerte a dalversenyt?

7.5.3. Lánctörtek

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

$$q_2 = \left\lfloor \frac{1}{\alpha_1} \right\rfloor, \quad \alpha_2 = \left\{ \frac{1}{\alpha_1} \right\}.$$

Így

$$\alpha = q_1 + \alpha_1 = q_1 + \frac{1}{q_2 + \alpha_2}.$$

Ha $\alpha_2 \neq 0$, akkor $1/\alpha_2$ egész és törtrészét képezzük, stb. Általában, ha a q_1, q_2, \dots, q_n és $\alpha_1, \alpha_2, \dots, \alpha_n$ 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

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots \cfrac{1}{q_n + \cfrac{1}{q_{n+1} + \alpha_{n+1}}}}}}$$

Eljárásunk akkor ér véget, ha valamelyen m -re $\alpha_m = 0$.

Az iménti kifejezést **egyszerű lánctörtnek** nevezzük, és a könnyebb írásmód kedvéért bevezetjük rá a $//q_1; q_2, \dots, q_n, q_{n+1} + \alpha_{n+1}//$ jelölést. (Lánctörtek felírására szokásos még a $\langle q_1; q_2, q_3, \dots \rangle$, illetve a $[q_1; q_2, q_3, \dots]$ jelölés is.) Az ily módon kapott q_1, q_2, q_3, \dots egész számokat a lánctört-előállítás **jegyeinek** nevezzük. A konstrukció alapján világos, hogy a lánctörtjegyek egyértelműen meghatározott egész számok, és $q_i > 0$, ha $i > 1$.

7.45. 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 $\alpha = //3; 7, 16//$.

7.46. 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 $\sqrt{2} = //1; 2, 2, \dots //$.

7.5.7. téTEL. Az α valós szám lánctörtjegyeinek sorozata pontosan akkor véges, ha α racionális.

BIZONYÍTÁS. Ha a lánctörtjegyek sorozata véges, mondjuk $//q_1; q_2, q_3, \dots, q_n//$, akkor az emeletes törteket lebontva α végül két egész szám hánnyadosaként 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 lépéseinak felelnek meg, így a lánctörtjegyeket előállító algoritmus véges sok lépésben befejeződik.

Hajtsuk végre az a, b számokon az euklideszi algoritmust.

$$\begin{aligned} a &= bq_1 + r_1, & 0 < r_1 < b, \\ b &= r_1q_2 + r_2, & 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2, \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_nq_{n+1}. \end{aligned}$$

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 $//q_1; q_2, q_3, \dots, q_{n+1}//$ lánctört-előállítását kapjuk. ■

A továbbiakban feltesszük, hogy α valós, és megmutatjuk, hogy a lánctörtek segítségével α -t jól közelítő racionális számokat tudunk előállítani. Ezek α lánctörtalakjának „szeletei” lesznek.

7.5.8. definíció. Az α valós szám $//q_1; q_2, q_3, \dots, q_n, \dots//$ lánctört-alakjának n -edik szeletén a $\delta_n = //q_1; q_2, q_3, \dots, q_n//$ lánctörtet értjük.

A 7.5.7. téTEL szerint ha α megegyezik lánctört alakjának valamely szeletével, akkor racionális.

7.5.9. téTEL. Legyen az α valós szám lánctört alakja $//q_1; q_2, q_3, \dots, q_n, \dots//$.

(1) Ekkor a

$$\begin{aligned} P_0 &= 1 & Q_0 &= 0 \\ P_1 &= q_1 & Q_1 &= 1 \\ P_k &= q_k P_{k-1} + P_{k-2} & Q_k &= q_k Q_{k-1} + Q_{k-2} \end{aligned}$$

rekurzió a lánctört szeleteit állítja elő, vagyis ha $1 \leq k \leq n$, akkor $\delta_k = P_k/Q_k$, ahol a P_k és Q_k egészek relatív prímek.

(2) minden $1 < k \leq n$ esetén

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_k Q_{k-1}}.$$

(3) *Minden $1 < k \leq n$ esetén*

$$|\alpha - \delta_{k-1}| \leq \frac{1}{Q_k Q_{k-1}},$$

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 $\delta_{k-1} = //q_1, q_2, \dots, q_{k-1}//$ -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

$$\begin{aligned} \delta_k &= \frac{(q_{k-1} + 1/q_k)P_{k-2} + P_{k-3}}{(q_{k-1} + 1/q_k)Q_{k-2} + Q_{k-3}} = \frac{q_k(q_{k-1}P_{k-2} + P_{k-3}) + P_{k-2}}{q_k(q_{k-1}Q_{k-2} + Q_{k-3}) + Q_{k-2}} \\ &= \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}} = \frac{P_k}{Q_k}. \end{aligned}$$

Most indukcióval meggemutatjuk, hogy minden $1 \leq k \leq n$ 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 $P_2 Q_1 - Q_2 P_1 = (q_1 q_2 + 1) - q_1 q_2 = 1 = (-1)^2$. Tegyük fel, hogy az állítás teljesül $2 < k - 1$ -re. Ekkor

$$\begin{aligned} P_k Q_{k-1} - Q_k P_{k-1} &= (q_k P_{k-1} + P_{k-2})Q_{k-1} - (q_k Q_{k-1} + Q_{k-2})P_{k-1} \\ &= Q_{k-1} P_{k-2} - P_{k-1} Q_{k-2} = (-1) \cdot (-1)^{k-1} = (-1)^k. \end{aligned}$$

Ebből egyszerűen 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 ($2 \leq k \leq n$) becsléséhez a (2) állítást és az $\alpha = //q_1; q_2, \dots, q_k, \alpha_{k+1}//$ összefüggést használjuk fel. Ekkor ugyanis

$$\alpha - \delta_{k-1} = \frac{(-1)^k}{Q_{k-1}((q_k + \alpha_{k+1})Q_k + Q_{k-1})},$$

ahol a nevező $q_k > 0$ miatt minden pozitív. Ez azt is jelenti, hogy ha k páros, akkor $\alpha - \delta_{k-1}$ minden pozitív, ha k páratlan, akkor $\alpha - \delta_{k-1}$ minden negatív, továbbá a (2) állítás miatt a páratlan indexű közelítő törtek növekvő, a páros indexűek csökkenő sorozatot alkotnak. Azt kaptuk tehát, hogy

$$\frac{P_1}{Q_1} < \frac{P_3}{Q_3} < \dots \leq \alpha \leq \dots < \frac{P_4}{Q_4} < \frac{P_2}{Q_2},$$

amiből a (3) állítás következik. Egyenlőség nyilván csak az $\alpha = \delta_n$ esetben állhat fenn.

■

7.47. példa. Tekintsük a $\pi = //3; 7, 15, 1, 292, 1, 1, 2, 1, 3, 1, 14, 2, 1, \dots //$ lánctörtközelítést. A rekurziós-formulával előállított lánctört-szeletek ekkor

$$\delta_2 = \frac{22}{7}, \delta_3 = \frac{333}{106}, \delta_4 = \frac{355}{113}, \delta_5 = \frac{103993}{33102}, \delta_6 = \frac{104348}{33215},$$

$$\delta_7 = \frac{208341}{66317}, \delta_8 = \frac{312689}{99532}, \delta_9 = \frac{833719}{265381}, \delta_{10} = \frac{1146408}{364913}, \dots$$

ARKHIMÉDESZ δ_2 -t használta π közelítésére, ami 3 értékes jegyre pontos. Megjegyezzük, hogy δ_4 hétközött 3 értékes jegyre pontos.

A 7.5.9. 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-közeliítés közül az egyik eleget tesz az

$$|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$$

egyenlőtlenségnek, sőt, három egymás utáni lánctört-közeliítés 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.

Lényeges észrevétel, hogy az adott korlántról nem nagyobb nevezőjű törtek közül a lánctört-kifejtések adják a legjobb közelítéseket.

7.5.10. 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 $q \geq Q_{k+1}$.

Történeti érdekesség, hogy a görögök lánctörteket használtak az irracionális számok leírására.

7.5.11. Tétel (biz. nélküli). Egy β irracionális szám lánctört-kifejtése pontosan akkor periodikus valahonnan kezdve, ha β gyöke valamelyen racionális együtthatós másodfokú egyenletnek. ■

7.48. példa. Határozzuk meg a $\sqrt{14}$ lánctört-kifejtését. Mivel $3^2 < 14 < 4^2$, ezért $\sqrt{14} = 3 + 1/x_1$, ahol $x_1 = 1/(\sqrt{14} - 3)$. Gyöktelenítés után azt kapjuk, hogy $x_1 = (\sqrt{14} + 3)/(14 - 9) = (\sqrt{14} + 3)/5$. Második lépében $x_1 = 1 + 1/x_2$, ahol $x_2 = 5/(\sqrt{14} - 2)$. Ismét gyöktelenítve $x_2 = (\sqrt{14} + 2)/2$ lesz. Harmadik lépében $x_2 = 2 + 1/x_3$, ahol $x_3 = 2/(\sqrt{14} - 2) = (\sqrt{14} + 2)/5$. Negyedik lépében $x_3 = 1 + 1/x_4$, ahol $x_4 = 5/(\sqrt{14} - 3) = \sqrt{14} + 3$. Mivel ez utóbbi szám nem tört, megállhatunk, és felírhatjuk az eredményt: $\sqrt{14} = //3; 1, 2, 1, \sqrt{14} + 3// = //3; 1, 2, 1, 6, 1, 2, 1, 6, \dots// = //3; 1, 2, 1, 6, \dots// = //3; 1, 2, 1, 6, \dots//$.

7.49. példa. Adjuk meg az $\alpha = //2; \bar{1}, \dots //$ végtelen lánctört értékét. Mivel $\alpha = //2; \bar{\alpha - 1} //$ ezért $\alpha = 2 + (\alpha - 1)/\alpha$. Átrendezve kapjuk, hogy $\alpha^2 - 3\alpha + 1 = 0$, amit megoldva $\alpha = (\sqrt{5} + 3)/2$.

Gyakorlatok

7.5-3. Határozzuk meg az alábbi valós számok lánctörtjegyeit:

- a) $123/21$,
- b) $131/242$,
- c) $\sqrt{3}$,
- d) $(1 + \sqrt{5})/2$.

7.5-4. Alakítsuk át a $//1; 2, 3, 4//, // - 3; 2, 1//$ lánctörteket racionális törtekké.

7.5-5. Mi lesz az értéke a $//2; 1, 4, 3, n//$ racionális számnak, ha $n = 3, 4, 5, 6, 7, 8$?

7.5-6. Mi lesz a lánctalakja az alábbi racionális számoknak: $(2n+1)^2/(2n)^2$, ahol $n > 1$?

7.5-7. Mi lesz a lánctalakt a alakja az $F(i)/F(i+1)$ számoknak ($i \geq 2$), ahol $F(i)$ az i -edik Fibonacci-számot jelöli?

7.5-8. Igaz-e, hogy $//q_1; q_2, \dots, q_n// = //q_1; q_2, \dots, q_n - 1, 1//$?

7.5-9. Igaz-e, hogy a $//1; 1, 1, \dots, 1, \sqrt{2} //$ számok minden irracionálisak?

7.5-10. Határozzuk meg az alábbi végtelen lánctaltek értékét:

- a) $//2; 3, \overline{1}, \dots //$,
- b) $//1; \overline{2, \overline{1}}, \dots //$,
- c) $//2; \overline{1, 2}, \dots //$,
- d) $//2; 3, \overline{1, 2}, \dots //$.

7.5-11. Keressünk olyan, 100-nál kisebb nevezőjű törtet, amelynek az eltérése $\sqrt{2}$ -től kisebb, mint 0,001.

7.5-12. Bizonyítsuk be, hogy $Q_n > F_n$ minden ($n \in \mathbb{N}$) esetén, ahol F_n az n -edik Fibonacci-szám.

7.5-13. Mutassuk meg, hogy a $//a_1; a_2, \dots, a_n//$ és a $//a_n; a_{n-1}, \dots, a_1//$ „fordított” lánctalteknek ugyanaz a számlálója. (Az eredményt már Euler is ismerte.)

7.5-14. Mutassuk meg, hogy ha

$$A/B = //a_1; a_2, \dots, a_{n-1}, a_n//,$$

$$C/D = //a_1; a_2, \dots, a_{n-1}//,$$

akkor

$$A/C = //a_n; a_{n-1}, \dots, a_2, a_1//.$$

Például $8/5 = //1; 1, 2//$, $3/2 = //1; 1, 1//$, így $8/3 = //2; 1, 1, 1//$.

7.5-15. Keressünk olyan p/q racionális számokat, amelyekre az $|n - p/q| < 1/(\sqrt{5}q^2)$ egyenlőtlenség teljesül, ahol $n = \sqrt{2}, \sqrt{3}, \pi, e$.



Melyek leszenek a prímek az $1, 101, 10101, 1010101, 101010101, \dots$ (decimális számokból álló) végtelen sorozatban?



Egy p prímet ciklikusnak nevezünk, ha az $1/p$ tizedestört alakjában az ismétlődő rész hossza éppen $p - 1$. Keressük meg az első egymillió ciklikus prímet.



Tervezzünk és implementálunk hatékony algoritmust olyan valós számok lánctal-kifejtésének meghatározására, amelyek valamely racionális együtthatós másodfokú egyenlet gyökei.



Tervezzünk és implementálunk hatékony algoritmust egy tetszőleges végtelen lánctalrt értékének meghatározására.

Megjegyzések a fejezethez

A számábrázolási rendszereknek történetileg három fajtája különböztethető meg: az alfabetikus, a hieroglifikus, és a helyiértékes ábrázolás.

Alfabetikus ábrázolás. Ezt a rendszert az jellemzi, hogy a számok jelölésére nem használtak külön jeleket, hanem az írásra szolgáló ábécé betűit alkalmazták. Nagyon

1	I	α'	40	ΔΔΔΔ	μ'
2	II	β'	50	Ρ	ν'
3	III	γ'	60	ΡΔ	ξ'
4	IV	δ'	70	ΡΔΔ	ο'
5	Γ	ε'	80	ΡΔΔΔ	π'
6	Π	ρ'	90	ΡΔΔΔΔ	ϙ'
7	ΠΙ	ϟ'	100	Η	ϙ'
8	ΠΙΙ	Ϟ'	200	ΗΗ	ο'
9	ΠΙΙΙ	Ϛ'	300	ΗΗΗ	τ'
10	Δ	Ϛ'	400	ΗΗΗΗ	υ'
11	ΔΙ	ϙα'	500	Ϛ	ϙ'
12	ΔΙΙ	ϙβ'	600	ϚΗ	ϗ'
13	ΔΙΙΙ	ϙγ'	700	ϚΗΗ	ϙ'
14	ΔΙΙΙΙ	ϙδ'	800	ϚΗΗΗ	ϙ'
15	ΔΓ	ϙε'	900	ϚΗΗΗΗ	ϙ̄'
16	ΔΓΙ	ϙϚ'	1000	Ϛ	ϙ̄'
17	ΔΓΙΙ	ϙϟ'	2000	ϚϚ	ϙ̄β̄'
18	ΔΓΙΙΙ	ϙϞ'	3000	ϚϚϚ	ϙ̄γ̄'
19	ΔΓΙΙΙΙ	ϙϚ'	10,000	Ϛ	ϙ̄ῑ'
20	ΔΔ	ϙ'	20,000	ϚϚ	ϙ̄κ̄'
21	ΔΔΙ	ϙϙ'	50,000	Ϛ	ϙ̄ϙ̄'
30	ΔΔΔ	ϙϙϙ'	100,000	ϚϚϚ	ϙ̄ϙ̄ϙ̄'

7.6. ábra. Görög alfabetikus számjegyek. A harmadik és a hatodik oszlop alfabetikus ábrázolása az i.e. ötödik századtól kb. az i.e. első századig volt használatos, amit a római uralom hatásaként felváltott az akrofon írásmód (második és negyedik oszlop).

sok népnél megtaláljuk a nyomait. Az alfabetikus ábrázolás előnye, hogy a számok leírására kevés jel kell, és egy jel csak egyszer szerepel a sorozatban. Komoly hiányosság azonban, hogy nagy számok nem írhatók le újabb számjegyek bevezetése nélkül. A többi rendszerrel összehasonlítva megállapítható, hogy az alfabetikus ábrázolás csak a számok leírására alkalmas, és bár igen tömör, műveletvégzés szempontjából a lehető legrosszabb. A ma ismert klasszikus görög ábécé 24 betűjével szemben az ókorban még 26 betűs ábécét használtak, amelyben az epsilon és a zéta között a digamma (6), a pi és rhó között a kappa (90) nevű (v.ö.: latin q) betűk kaptak helyet, és a számíráshoz a betűsor végére tettek még egy 27-ik, csak erre a célra szolgáló jelet, amelynek a neve szampi (900).

Hieroglifákkal történő ábrázolás. A hieroglifikus számírásban nem (csak) betűk, hanem speciális írásjelek szolgálnak alapjelként. Ezeknek a jeleknek alaki értékük van. Például a római számírásban ezek az alábbiak:

- egy = I (lat. „unus”)
- öt = V (lat. „quinqüe”);
- tíz = X (lat. „decem”);
- ötven = L (lat. „quinquaginta”);
- száz = C (lat. „centum”);
- ötszáz = D (lat. „quingenti”);
- ezer = M (lat. „mille”);

Az ábrázolás szabályai:

- Egymás mellé maximum 3 egyforma szimbólum írható;
- Ha kisebb értékű szimbólum a nagyobbat követi, az összeadást jelent;
- Ha pedig a kisebb a nagyobbat megelözi, az kivonást.

Ily módon minden szám I-től MMMDCCCLLXXXVIII-ig (4998) ábrázolható. A római számábrázolás már az egyiptomi feliratokban és papiruszokon is megtalálható. Kialakulásuk döntően a számolótáblák használatának köszönhető. A számolótáblán levő pálcikák lerajzolása, az állapot rögzítése természetes foly-

matként vezethetett az absztrakt írásbeliség kifejlődéséhez. A számtáblák nyomai tetten érhetők az ó-kínai, a sumér-babiloni-asszír, a föníciai és az azték kultúrákban egyaránt.

Helyiértékes ábrázolás. A ma használatos helyiértékes ábrázolást arab számírásnak nevezik, ami arra utal, hogy közvetlen az arab matematikai munkák nyomán vált Európában ismertté. II. Szilveszter pápa volt az első olyan befolyással rendelkező személy, aki az arab számokat bizonyíthatóan használta és tudatosan terjesztette Európában (nem mellesleg ő küldte István királyunknak a koronát). Az arabok mindezt a hinduktól tanulták el, akik a 10-es számrendszer használták. Ők pedig a Mezopotámiában használt hieroglifikus rendszerből vehették át. Az igazi találmány a helypótló zérus szisztematikus használata volt (kb. az V. századtól). Azonban a helypótló zérust nemcsak Indiában, hanem Amerikában is ismerték. A mayák, noha a számokat a hieroglifikus írásrendszer szerint jelölték, következetesen használták a helyiértékes írásmódot és a nulla számot jelölő zérust. A helyiérték használatának legrégebbi nyoma a számok írásának babiloni rendszerében található meg.

Egy kis csendes-óceáni Francia Polinéziához tartozó sziget (Mangareva) lakói a gyarmatosítás előtt a kettes és a tízes számrendszer keverve fejezték ki a számokat, és minden nyelvészeti feljegyzésekben bizonyíthatóan már 1450 előtt is használták. Egytől tízig megvannak a számnevek, de tíz fölött megjelenik a kettő alap. Például $80 = 40 + 20 + 10$. Ez azért érdekes, mert európai utazók csak 1797-ben jelentek meg a szigeten, száz évvel azután, hogy LEIBNIZ német matematikus megfogalmazta a bináris rendszert („Teoria algoritmica della complessita”). Egyesek úgy vélik, hogy Leibnizhez is Európán kívülről juthatott el a bináris rendszer gondolata, amit arab közvetítéssel vehettek át. Talán nem is az a fontos, hogy ki volt az első, hanem az, hogy az emberi kultúra még elszigetelve is képes a matematikai innovációra.

A tökéletes számok problémáját az ókori görögök vetették fel. Különös jelentőséget tulajdonítottak azoknak a számoknak, amelyek „részekből visszanyerhetők”, azaz részeinek összege éppen az eredeti számmal egyenlő. Ezen harmóniát testesítik meg a tökéletes számok, amelyek közül négyet a régi görögök is ismertek: 6, 28, 496, 8128. EUKLIDÉSZ így ír az ELEMEK IX. könyvének 36. tételeben³: „Ha az egységtől kezdve kétszeres arányban képezünk egy mértani sorozatot, amíg a sorösszeg prím nem lesz, és az összeggel megsorozzuk az utolsó tagot, akkor a szorozat tökéletes szám lesz.”

Ebben az áll, hogy ha $1 + 2 + 2^2 + \dots + 2^n$ 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:

7.5.12. 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.*

7.5.13. 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.*

³Mayer Gyula fordítása

Megjegyzések a fejezethez

Ezek a tesztek egyszerűségük miatt könnyen alkalmazhatók prímszámkeresésre, így a legnagyobb ismert prímek továbbra is várhatóan Mersenne-prímek lesznek.

A kínai csillagász Tsu Csung-Chih (430–501) már ismerte a π 6 tizedes jegyre pontos $\frac{355}{113}$ 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.

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., *Algebra I*. Nemzeti Tankönyvkiadó, Budapest, 2000.
- [10] Fried, E., *Algebra II*. Nemzeti Tankönyvkiadó, Budapest, 2002.
- [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] Gonda, J., *Bevezető fejezetek a matematikába III*. Egyetemi jegyzet, ELTE TTK, Budapest, 2000.
- [16] Graham, R.L., Knuth, D.E., Patashnik, O., *Konkrét matematika*. Műszaki Könyvkiadó, Budapest, 1998.
- [17] Hajnal, A., Hamburger, P., *Halmazelmélet*. Tankönyvkiadó, Budapest, 1983.
- [18] Hajnal, P., *Elemi kombinatorikai feladatok*. Polygon Kiadó, Szeged, 1997.
- [19] Halmos, P.R., *Elemi halmazelmélet*. Siegler, L., E., *Halmazelméleti feladatok*. Műszaki Könyvkiadó, Budapest, 1981.
- [20] Iványi, A., (ed.) *Informatikai Algoritmusok I.-II*. Eötvös Kiadó (ELTE), Budapest, 2004, 2005.
- [21] Járai, A., (ed.) *Bevezetés a matematikába*. Eötvös Kiadó (ELTE), Budapest, 2006.

Irodalomjegyzék

- [22] Kalmár, L., *A matematika alapjai, I./I., I./II., II./I., II./II.* Kézirat. Tankönyvkiadó, Budapest, 1978, 1969, 1969, 1971.
- [23] Környei, I., *Algebra (Turán Pál előadásai alapján)*. Tankönyvkiadó, Budapest, 1974.
- [24] Knuth, D.E., *A számítógépprogramozás művészete, I.-II.-III. kötet*. Műszaki Könyvkiadó, Budapest, 1987.
- [25] Láng, Cs., *Bevezető fejezetek a matematikába. I.-II.* Egyetemi jegyzet (ELTE), Budapest, 2000.
- [26] Láng, Cs., *Komplex számok – Példák és feladatok*. Egyetemi jegyzet (ELTE), Eötvös Kiadó, 2003.
- [27] Láng, Cs., *Számelmélet – Példák és feladatok*. Egyetemi jegyzet (ELTE), Eötvös Kiadó, 2005.
- [28] Lavrov, I.A., Makszimova, L.L., *Halmazelméleti, matematikai logikai és algoritmuselméleti feladatok*. Műszaki Könyvkiadó, 1987.
- [29] Megyesi, L., *Bevezetés a számelméletbe*. Polygon Kiadó, Szeged, 1997.
- [30] Mendelson, E., *Introduction to mathematical logic*. D. van Nostrand Company Inc., Princeton, New Jersey, 1964.
- [31] Niven, I., Zuckerman, H.S., *Bevezetés a számelméletbe*. Műszaki Könyvkiadó, 1978.
- [32] Pásztorné, V.K., *A matematikai logika és alkalmazásai*. Egyetemi jegyzet (ELTE), Tankönyvkiadó, Budapest, 1991.
- [33] Penrose, R., *A császár új elméje. Számítógépek, gondolkodás és a fizika törvényei*. Akadémiai Kiadó, Budapest, 1993.
- [34] Quine, W.V.O., *A logika módszerei*, Akadémiai Kiadó, Budapest, 1968.
- [35] Rudin, W., *A matematikai analízis alapjai*. Műszaki Könyvkiadó, Budapest, 1978.
- [36] Sain, M., *Nincs királyi út! – Matematikatörténet*. Gondolat kiadó, Budapest, 1986.
- [37] Sárközy, A., *Számelmélet és alkalmazásai*. Műszaki Könyvkiadó, Budapest, 1978.
- [38] Sárközy, A., Surányi, J., *Számelmélet – feladatgyűjtemény*. Kézirat. Tankönyvkiadó, Budapest, 1964.
- [39] Sierpiński, W., *200 feladat az elemi számelmélet köréből*. Tankönyvkiadó, Budapest, 1964.
- [40] Szalay, M., *Számelmélet*. Tankönyvkiadó, 1998.
- [41] Szendrei, Á., *Diszkrét matematika; logika, algebra, kombinatorika*. Polygon Kiadó, Szeged, 2000.
- [42] Totik, V., *Halmazelméleti feladatok és tételek*. Polygon Kiadó, Szeged, 1997.
- [43] Tremblay, J., Mahonar, R., *Discrete Mathematical Structures with Applications to Computer Science*. McGraw-Hill Inc., New York, 1975.
- [44] Varga, Á., *Absztrakt algebra feladatgyűjtemény*. Tankönyvkiadó, Budapest, 1983.
- [45] Vilenkin, N.J., *Kombinatorika*. Műszaki Könyvkiadó, Budapest, 1971.
- [46] Vinogradov, I.M., *A számelmélet alapjai*. Tankönyvkiadó, Budapest, 1968.

Névmutató

A

Abel, Niels Henrik (1802–1829)	vi
Al-Hvarizmi, Abu Abdalláh Muhammad ibn Músza (kb. 780–845)	vi
Arisztotelész (Kr.e. 384–322)	39

B

Bell, Eric Temple (1883–1960)	138
Bernays, Edward Louis (1891–1995)	40
Bernoulli, Jacob (1655–1705)	30
Bolyai János (1802–1860)	13

C

Cantor, Georg Ferdinand Ludwig Philipp (1845–1918)	vi, 107, 145, 151
Cardano, Gerolamo (1501–1576)	vi
Catalan, Eugène Charles (1814–1894)	136
Cauchy, Augustin Louis (1789–1857)	107
Cayley, Arthur (1821–1895)	47, 106
Church, Alonzo (1903–1995)	12
Cohen, Paul Joseph (1934–2007)	151
Csebisev, Pafnutyij Lvovics, (1821–1894)	176

D

De la vallée-Poussin, Charles-Jean (1866–1962)	177
Dedekind, Julius Wilhelm Richard (1831–1916)	107
Descartes, René (1596–1650)	vi
Diophantosz (i.sz. 3. század)	v

E

Epimendész, (Kr.e. VII. sz.)	37
Eratoszthenész (Kr.e. 276–194)	177
Euklidész, (Kr.e. 300)	v, 13, 15, 166, 175, 206
Euler, Leonhard (1707–1783)	vi, 53, 132, 206

F

Fermat, Pierre de (1601–1665)	vi
-------------------------------------	----

NÉVMUTATÓ

Ferrari, Lodovico (1522–1565)	vi
Ferro, Scipione del (1465–1526)	vi
Fibonacci, Leonardo Pisano Bigollo (kb. 1170–1250)	70, 130
Fraenkel, Abraham Halevi (Adolf) (1891–1965)	37
Frobenius, Ferdinand Georg (1849–1917)	100

G

Gödel, Kurt (1906–1978)	15
Galois, Évariste (1811–1832)	vi
Gauss, Carl Friedrich (1777–1855)	vi, 177
Gibbs, Josiah Willard (1838–1903)	108
Grassmann, Hermann Günter (1809–1877)	108

H

Hadamard, Jacques Salomon (1865–1963)	177
Hamilton, William Rowan (1805–1865)	98
Hermite, Charles (1822–1901)	97
Hilbert, David (1862–1943)	13, 107
Hurwitz, Adolf (1859–1919)	106

K

Karinthy Frigyes (1887–1938)	37
Klein, Felix Christian (1849–1925)	47
Kuratowski, Kazimierz (1896–1980)	40

L

Lambert, Johann Heinrich (1728–1777)	108, 207
Legendre, Adrien-Marie (1752–1833)	177
Leibniz, Gottfried Wilhelm (1646–1716)	vi, 39, 206
Lindemann, Carl Louis Ferdinand von (1852–1939)	97, 108, 207
Liouville, Joseph (1809–1882)	107
Lobacsevszkij, Nyikolaj Ivanovics (1792–1856)	13
Lucas, Francois Édouard Anatole (1842–1891)	206
Łukasiewicz Jan (1878–1956)	48

N

Neumann János (1903–1957)	vi
Newton, Sir Isaac (1642–1727)	vi, 39

P

Pascal, Blaise (1623–1662)	vi, 134
Peano, Giuseppe (1858–1932)	13, 61, 106

NÉVMUTATÓ

Pheidias (kb. Kr.e. 500–430)	132
Pithagorasz (Kr.e. 582–496)	v, 76
Platón, (Kr.e. 427–347)	39
Prótagorasz (kb. Kr.e. 480–410)	37
Puskás Ferenc (1927–2006)	132

R

Russel, Bertrand (1872–1970)	37
------------------------------------	----

S

Sidon Simon (1892–1941)	142
Sierpinski, Waclaw (1882–1969)	62
SLOANE, NEIL JAMES ALEXANDER (1939–)	143
Stirling, James (1692–1770)	138
Szun-ce (kb. Kr.e. 544–496)	188

T

Tartaglia, Niccolo Fontana (1499–1557)	vi
--	----

W

Wiles, Andrew (1953–)	179
-----------------------------	-----

Z

Zénón (kb. Kr.e. 488–430)	39
Zemelo, Ernst Friedrich Ferdinand (1871–1953)	37

Tárgymutató

Symbols

összeg	68
összetett szám	157
ítéletkalkulus	3
ítéletlogika	3, 9

A

Abel-csoport	49, 158
abszolút érték	73, 78, 87
addíciós képlet	134
additív írásmód	68
algebra	47, 100
normált	106
algebrai	
struktúra	47
struktúra típusa	47
szám	97
zártsgág	93
algoritmus	
futásideje	82
rekurzív	64
alsó	
határ	42
korlát	42
antinómia	36, 39
aranymetszés	132, 169
argumentum	29, 31
aritmetika	155
aritmetikai függvény	192
arkhimédészi tulajdonság	75
asszociáltság	156
asszociativitás	
függvények szorzatára	34
halmazműveleteknél	20
rélaciók szorzatára	25
struktúráknál	49
atom	
normálformáé	33
axióma	7, 13
axiómarendszer	
Fraenkel	37

Zermelo–Fraenkel (ZF)	38
Zermelo–Fraenkel–Choice (ZFC)	38
axiomatikus halmazelmélet	17

B

bázis	94
Backus–Naur forma	63
beágyazás	71
algebrai struktúráknál	55
Bell-szám	138
belső	
függvény	34
művelet	47
szorzat	100
Bernoulli-egyenlőtlenség	84
Beth-tétel	14
bijektív függvény	31
binér reláció	23
kiterjesztése	24
leszűkítése	24
Binet-formula	131
binomiális	
együttható	125, 134
téTEL	125
binomiális együtthatók	
becslése	135
bizonyítás	13
Boole-algebra	120
Boole-függvény	32
Braille-írás	116
Brun-konstans	176
busz	5

C

Cantor-féle átlós módszer	150
Cassini-azonosság	141
Catalan-szám	136
Cayley-táblázat	48
Celsius-skála	84
Church-tézis	12
csoporth	49
Klein	47

TÁRGY MUTATÓ

D

De Moivre-azonosság	89
De Morgan-azonosság	6, 20, 62, 118
decibel-skála	81
Descartes-szorzat	23
differencia	70
dimenzió	94
diofantikus egyenletek	168
direkt szorzat	23
Dirichlet-tétel	177
diszjunkció	4
diszjunkt halmazok	19
diszjunktív normálforma	33
disztributivitás	
algebrai struktúráknál	50
halmazműveleteknél	20
dualitás elve	118
Dyke-szó	138

E

egész szám	
páratlan	155
páros	155
egészrész	195
alsó	78
felső	78
együtttható	
binomiális	125
polinomiális	126
egyiptomi tört	76
egység	156
egységelemes	
félcsoport	49
egységgöök	91
primitív	91
egységmátrix	58
ekvivalencia	4
ekvivalenciaosztály	27
ekvivalenciareláció	27, 138
elégsges feltétel	14
előjelfüggvény	78
elemi konjunkciók	33
ellentett	49
előjelű szám	73
elnyelési tulajdonság	134
elsőrendű logika	9–13
Eratoszthenészi-szita	177
esemény	116
biztos	117
ellentettje	117

komplementere	117
lehetetlen	117
eseményalgebra	116, 119
események	
összege	117
láncolata	117
euklideszi	
algoritmus	166
Euler-féle φ függvény	182, 192, 197
Euler-tétel	183

F

függvény	
algebrai	97
belső	34
bijektív	31
definíciója	29
exponenciális	80
injektív	31
inverze	35
külső	34
leszűkítése	32
lineáris	56
logikai	32
monoton csökkenő	44
monoton növő	44
periodikus	82
racionális	56
szürjektív	31
számelméleti	192
szigorúan monoton csökkenő	44
szigorúan monoton növő	44
transzcendens	97
trigonometrikus	81
függvényérték	29
függvények kompozíciója	34
félcsoport	49
fő argumentum	92
Fahrenheit-skála	84
faktorhalmaz	27
faktoriális	110
faktorstruktúra	53
felbonthatatlan elem	157
felső	
összegzés	134
határ	42, 76
tulajdonságú test, 76	
korlát	42
ferdetest	51
Fermat-prím	177
Fermat-tétel	183
Fibonacci-sorozat	130, 204
fordított lengyel jelölés	48
Frobenius-probléma	170

TÁRGY MUTATÓ

G

gépi szó	5
Gauss-egész	156
Gauss-féle számsík	87
generátorfüggvények	130
Goldbach-sejtés	3, 177
grupoid	48
gyökvonás	
valós	79
gyűrű	50
egységeleme	50
egységelemes	50
kommutatív	50
nulleleme	50
nulosztómentes	51

H

hányados	74, 159
hányadosstruktúra	53
Héron-képlet	85
halmaz	
<i>n</i> -elemű	110
ösképe	31
képe	30
véges	146
végételen	146
halmazcsalád	19
halmazok ekvivalenciája	145
halmazrendszer	19
Hanoi tornyai	63
Hasse-diagram	43, 72
hányadoshalmaz	27
Heaviside-függvény	85
helyettesítési érték	29
hexagon-tulajdonság	141
hidrosztatikai nyomás	85
hiperbolikus rendszer	95
homogén reláció	23
homomorfizmus	54, 190

I

identikus leképezés	31
identitás	31
igazságérték	3
igazságtáblázat	4
igazság tartomány	17
ikerprímek	176
implikáció	4

TÁRGY MUTATÓ

indexek	32
indexelt	
halmazcsalád	33
rendszer	32
indexhalmaz	32
indirekt bizonyítás	14
indukált részben rendezés	42
indukció	
teljes	14, 61
transzfinit	14, 151
infimum	42
injektív függvény	31
integritási tartomány	51
interpretáció	6, 9
intervallum	
nyílt	44
zárt	44
intervallum-aritmetika	198
inverz	
kép	31
irrationális számok	77
irreducibilis elem	157
izomorfizmus	55, 190

J

jólrendezett halmaz	45
jegyhalmaz	
kanonikus	162
szimmetrikus	162
Julia-halmaz	97

K

kötött változó	10
következetetői szabályok	7
közvetlen bizonyítás	14
különbséghalmaz	19
külső	
függvény	34
művelet	52
kínai maradéktétel	187, 188
kétértekűség elve	3
kanonikus	
alak	172
függvény	31
karakterisztikus függvény	32
Karnaugh-tábla	5, 34
kijelentés	3
kijelentések összekapcsolása	4
kijelentéskalkulus	<i>lásd</i> ítéletlogika
kijelentéslogikai formula	4
általános érvényű	6

TÁRGY MUTATÓ

kielégíthető	6
kiválasztási axióma	38
Klein-csoport	47, 49
kombináció	
ismétlés nélküli	112
ismétléses	113
kommutatív	
halmazműveletek	20
művelet	49
komplementer halmaz	19
komplex szám	86
algebrai alakja	88
Euler-féle alakja	88
trigonometrikus alakja	88
kongruencia	179
konjugált	88
konjunkció	4
konjunktív normálforma	34
konstans	
logikai	9
konstansfüggvény	31
kontinuum-számosság	151
kontinuumsejtés	151
általánosított	151
Kronecker-féle delta	32
kvantor	10
kvaterniós	98
abszolút értéke	99
konjugáltja	99
skalár része	99
vektor része	99

L

lánc	44, 45
lánctört	199
egyszerű	200
latin négyzet	53
Legendre-formula	175
legkisebb	
elem	42
felső korlát	42
közös többszörös	158
legnagyobb	
alsó korlát	42
elem	42
közös osztó	157
Lehmer, Derrick Henry (1905–1991)	206
lengyel jelölés	48
levezetés	7
lexikografikus rendezés	54
lineáris	
függvény	56
kombinációs tulajdonság	156
kongruencia	185

kongruencia-rendszer	187
leképezések	56
rendezés	44
térfelület	52
literál	33
logaritmusképzés	80
logarléc	81
logika	
elsőrendű	9
nulladrendű	3
logikai	
összekötőjel	4
ekvivalencia	6
kapuk	5
konstans	9
modell	6
szita formula	129
Lychrel-algoritmus	165

M

Möbius-függvény	193
mátrix	56
kvadratikus	58
négyzetes	58
mátrixok	
összege	57
kompatibilitása	57
szorzata	57
módosított kanonikus alak	172
művelet	
összeférhetősége	54
műveletek	
operandusai	47
precedenciája	47
műveleti táblázat	47
művelettartó leképezés	54
Mandelbrot-halmaz	62, 96
maradék	159
maradékosztály	181
matematikai logika	3
maximális	
elem	42
megelőzési reláció	43
Mersenne-prím	177, 206
metrika	107
metrikus tér	107
metszet	19
minimális	
elem	42
monoton függvény	44
multiplikatív	
írásmód	68
inverz	184, 186
multiplikativitás	

TÁRGYGYUTATÓ

szignum függvényé 78

N

- nagy ordó 82
- naiv halmazelmélet 17
- naptár
 - Gergely 165
 - Julián 165
 - maja 165
- negáció 4
- neutrális elem 48
- nim-összeg 162
- normálforma
 - diszjunktív 33
- normált
 - algebra 106
 - vektortér 106
- nulladrendű logika 3
- nullgyűrű 51
- nullosztó 51
- nyílt
 - kezdőszelet 76
 - kezdet 76
- nyitott formula 10

O

- oktav
- abszolút értéke 105
- képzetes része 105
- konjugáltja 105
- valós része 105
- operátortartomány 52
- operandus 47
- őskép 31
- osztályfelbontás 21
- osztályozás 21
- osztó 155

P

- páronként relatív prímek 158
- pénzváltó probléma 170
- palindromszám 165
- paradoxon 39
- paralelogramma-azonosság 96
- parciális
 - függvény 29
 - leképezés 29
- Pascal-háromszög 134
- periodikus függvény 82

permutáció

- fixpont nélküli 132
- ismétlés nélküli 110
- ismétléses 114
- permutáció-függvény 31
- Pithagorasz-tétel 81
- Pithagoraszi számhármasok 178
- polinom
 - együtthatói 55
 - főegyütthatója 56
 - foka 56
 - gyöke 56
 - helyettesítési értéke 56
 - zérushelye 56
- polinomfüggvény 56
- polinomiális
 - együttható 126
 - tétel 125
- pozitív osztók száma 173
- prímelem 157
- prímtáblázat 177
- precedencia 6, 47
- predikátum 9
- predikátumkalkulus 9
- projekció 31
- Ptolemaiosz-tétel 82

Q

Quine–McCluskey-algoritmus 5

R

- részbenrendezés 41
- részbenrendezett
 - halmaz 42
 - struktúra 42
- részhalmaz 18
- részstruktúra 53
- racionális
 - függvény 56
 - szám 74
- racionális számok
 - ábrázolása 195
- redukált
 - maradékosztály 182
 - maradékrendszer 182
- reflexív-tranzitív lezárt 46
- rekurzív
 - sorozat 129
- rekurzió 62
- megoldása 130
- rekurziótétel 62

TÁRGY MUTATÓ

reláció	23
értékkészlete	24
értelmezési tartománya	24
inverze	24
mátrixa	58
tulajdonságai	26
relációk kompozíciója	24
relációszorozat	24
relatív	
gyakoriság	120
prímek	158
rendezés	
topologikus	45
rendezési	
diagram	43
struktúra	41
rendezett	
n-es	23
integritási tartomány	53, 73
pár	22
test	53, 75
rendszer	152
reprezentáns	27
Rhind-papirusz	v
Richter-skála	81
megszámlálható	148
nem megszámítható	148
számpiramis	164
számrendszer	160
alapszáma	160
jegyei	160
számítani sorozat	70
szabad változó	10
σ -algebra	119
szigorú részbenrendezés	41
szimmetria-tulajdonság	134
szimmetrikus	
differencia	22
különbség	22
szimultán kongruencia	187
szita	
eratoszthenészi	129
formula	129
szorzat	
skaláris	100
vektoriális	101
szorzatstruktúra	53
szubadditív	78
szubdisztributivitás	199
szubfaktoriális	132
szupréum	42

S

sejtés	3
Sidon-sorozat	142
Sierpinski-szönyeg	62
skaláris szorzat	100
skatulya-elv	127
általános	127
sorozat	67
Stirling-formula	111, 116, 135
Stirling-szám	
másodfajú	138
Study-féle rendszer	95
szükséges feltétel	14
szürjektív függvény	31
számábrázolás	
bináris	160
decimális	160
hexadecimális	160
oktális	160
számegyenes	45
számelméleti függvény	192
additív	192
multiplikatív	192
teljesen additív	192
teljesen multiplikatív	192
számolótábla	205
számosság	110, 145
kontinuum	151

T

többes	155
többszörös	155
tökéletes szám	177
törtrész	79, 195
törzsszám	171
tartóhalmaz	47
tartalmazás-kizáras elve	129
tautológia	6
Taylor-sor	82
teljes	
indukció	61
maradékrendszer	181
rendezés	44
reprezentáns-rendszer	27
topologikus tér	107
test	
arkhimédeszi tulajdonságú	75
felső határ tulajdonságú	76
tizedestört	195
topologikus	
rendezés	45
tér	119
transzcendens számok	97
transzfinit	
indukció	151
rekurzió	152

TÁRGY MUTATÓ

tranzitív lezárt	28
trigonometrikus függvény	81
trinomiális alak	141
triviális osztó	157

U

Ulam-spirál	175
unió	19
üres halmaz	18

V

véges sorozat	67
valódi részhalmaz	18
valós szám	77
valós számok ábrázolása	195

valószínűség	120
valószínűségi mező	120
klasszikus	122
Vandermonde-azonosság	134
variáció	
ismétlés nélküli	111
ismétléses	112
vektortér	52
verem	64

Z

zárt formula	10
Zénón paradoxonja	39
zérógyűrű	51
zérusmátrix	57
Zermelo–Fraenkel axiómarendszer	38, 151
Zermelo–Fraenkel–Choice axiómarendszer	
38, 151	
Zorn-lemma	45

