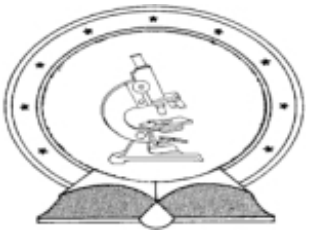
DE TTK



1949

Axiomatikai vizsgálatok

Doktori (PhD) értekezés

Csabay Károly

Témavezető: dr. Daragó József

Debreceni Egyetem
Természettudományi Doktori Tanács
Matematika- és Számítástudományok Doktori Iskola
Debrecen, 2012.

Édesanyám emlékének

Ezen értekezést a Debreceni Egyetem Természettudományi Doktori Tanács Matematika- és Számítástudományok Doktori Iskola Matematikadidaktika programja keretében készítettem a Debreceni Egyetem természettudományi doktori (PhD) fokozatának elnyerése céljából.
Debrecen, 2012. .....

.....
Csabay Károly

Tanúsítom, hogy Csabay Károly doktorjelölt 2007.- 2011. között a fent megnevezett Doktori Iskola Matematikadidaktika programjának keretében irányításommal végezte munkáját. Az értekezésben foglalt eredményekhez a jelölt önálló alkotó tevékenységével meghatározóan hozzájárult. Az értekezés elfogadását javasolom.
Debrecen, 2012. .....

.....
Dr. Daragó József

Axiomatikai vizsgálatok

Értekezés a doktori (Ph.D.) fokozat megszerzése érdekében
a matematika- és számítástudományok tudományágban

Írta: Csabay Károly okleveles programozó és programtervező
matematikus, szakinformatikus, könyvtáros

Készült a Debreceni Egyetem Matematika- és
Számítástudományok doktori iskolája
(Matematikadidaktika programja) keretében

Témavezető: Dr. Daragó József

A doktori szigorlati bizottság:

elnök:	Dr. Gaál István	.....
tagok:	Dr. Kántor Sándorné	.....
	Dr. Király Bertalan	.....

A doktori szigorlat időpontja: 2011. február 11.

Az értekezés bírálói:

Dr. ....
Dr. ....
Dr. ....

A bírálóbizottság:

elnök:	Dr.	. .....
tagok:	Dr.	. .....
	Dr.	. .....
	Dr.	. .....
	Dr.	. .....

Az értekezés védésének időpontja: 2012. …… … .

Tartalomjegyzék

Köszönetnyilvánítás

Mindenekelőtt köszönet illeti témavezetőmet — barátomat és korábbi tanszékvezetőmet — *dr. Daragó Józsefet* állhatatos buzdításáért, amellyel nem szűnt meg bíztatni, úgy is, mint munkahelyi vezető, úgy is mint idősebb és tapasztaltabb kolléga és úgy is, mint jó barát. Tisztelettel mondok köszönetet a *Debreceni Egyetem Matematika- és Számítástudományok Doktori Iskolájának*, a tanároknak és az adminisztrációban dolgozó munkatársaknak, akik minden esetben méltányosan és segítőkészen jártak el velem, a sokszor „problémás” hallgatóval szemben. Köszönetemet fejezem ki munkahelyemnek, a mezőberényi *Orlai Petrics Soma Kulturális Központnak*, azon belül is személy szerint *Smiriné Kokauszki Erika* igazgatónőnek a lehetséges mértékig mindenben megadott támogatásért és alkalmazkodásért. S végül hálatelt szívvel gondolok *családtagjaimra*, akik hittek e munka befejezésében, és szeretetükkel mindvégig támogattak.

Bevezetés

Csaknem két évtizedes *matematikaoktatási múlttal* arról számolhatunk be, hogy a matematikatanárok minden remélt igyekezete ellenére a matematikát tanuló átlagos iskolás axiómákkal kapcsolatos fogalomalkotása jelentősen elmarad — legalábbis az oktató által megfogalmazott elvárástól. Tipikusan az történik, hogy *a tanuló olyan tulajdonságokat, feltételezéseket is adottnak vél, amelyek a kiindulásul vett axiómarendszerben nem voltak benne*.

Hogy e téren példával is szolgáljunk: nem egyszerűen arról van szó, hogy diák mondjuk kommutatívként kezel egy műveletet, mert természetesnek veszi, hogy a műveletek kommutatívak, s ezzel számolási hibát ejt. Ilyen esetekben, amikor az oktató felhívja erre a figyelmet, „ja persze” válasz érkezik, és a diák a hibát készséggel kijavítja.

> Például megteszi azt a lépést, hogy $(x + y)^2 = x^2 + 2xy + y^2$. Aztán, amikor felhívjuk rá a figyelmét, hogy a tárgyalt környezetben a szorzás nem kommutatív, rögtön kijavítja: $(x + y)^2 = x^2 + xy + yx + y^2$.

Ezzel szemben, ha például arról van szó, hogy kik a testvérek: tudniillik egyazon édesapától és édesanyától származó személyek; nos, ennek a relációnak a tanulmányozásakor általános megdöbbenést és elutasítást vált ki az a közlés, hogy mindenki testvére saját magának. A hallgató tehát implicite él azzal a kiegészítő feltételezéssel, hogy testvér csak *másvalaki* lehet.

> A *testvér* ugyebár ekvivalenciareláció, s mint ilyen — reflexív. Az oktató kénytelen rávezetni a hallgatóságot erre a relációtulajdonságra, de a megütközést nem lehet elkerülni.

Ugyanilyen elutasítással találkozunk akkor is, amikor az *őse* (*leszármazottja*) relációt vizsgáljuk. Senki sem hajlandó természetesnek venni, hogy mindenki őse saját magának. Amikor aztán a legfiatalabb közös őst keressük egy rokonság kimutatása céljá-

ból, érdekes eredményre jutunk: azért vagyok rokona apámnak, mert van a nagypapa, aki a rokonságot garantálja. Ez megmosolyogtató, s emiatt a hallgató végülis beadja a derekát: elfogadja, hogy apámnak és nekem legfiatalabb közös ősünk maga az apám. Láthatóan nem szigorú parciális rendezésről van szó, amelynek az esetében a hallgatói elutasítás ismét a reláció reflexivitása körül forog. A példákban személyek szerepeltek (testvérek, ősök, leszármazottak), emiatt a reflexivitás okozta meghökkenés igen erős. Nem feltétlenül okoz elutasítást például az a közlés, hogy minden természetes szám osztója saját magának. A szám elég absztrakt fogalom ahhoz, hogy a közlést a hallgatóság úgy fogadja mint *szabályt*. Ám a testvér olyan fogalom, amelyről a hallgató tudja, hogy mi, nem kell ahhoz szabály, hogy értse.

Hasonlóképpen a reflexivitás okoz nehézséget az *őse* reláció tanulmányozásakor is. A *határeset* benne van avagy nincsen benne a tárgyalt intervallumban, érvényességi körben — erre a kérdésre igen eltérőek a válaszok, és minden válaszadó evidenciának érzi a saját válaszát. Ami azt illeti, a természetes nyelvi fordulatok nem segítik az analógiák rögzülését. A szőnyeg *faltól-falig* ér: ez azt jelenti, hogy a szőnyeg nem megy be a *fal alá*. De az, hogy az üzlet *hétfőtől péntekig* van nyitva, az *igenis* azt jelenti, hogy az üzlet *hétfőn is és pénteken is* nyitva van. *Elválasztási rendszerek* című fejezetünkben részben éppen ennek a kérdésnek az axiomatizálási lehetőségeit igyekszünk körüljárni.

Szeretnénk nyomatékosítani azon álláspontunkat, mely szerint a matematikadidaktikai célok és megfontolások hatóköre *nem ér véget* az általános- és középiskolai matematikaoktatással. Meggyőződésünk, hogy jelen dolgozatunkban ajánlott eszközökkel jelentős eredmények érhetők el akár a felsőoktatás bevezető stúdiumaiban is.

Jelen dolgozat **három területen** végez axiomatikai vizsgálatokat. Mindhárom esetben didaktikai ajánlattételre vállalkozik: tanárok, előadók számára kínál megközelítési lehetőségeket.

A három terület közül az elsővel a már említett *Elválasztási rendszerek* c. fejezet foglalkozik, amelyben *Eukleidész* posztulátumaiból kiindulva rögzítünk egy *saját axiómarendszert*, s megvizsgál-

juk, milyen geometria tanulmányozására ad lehetőséget ez a kiindulás.

> Az *axióma* és a *posztulátum* szó között — bár ismerjük annak történelmi eltéréseit — jelen összefüggésben már nem teszünk különbséget.

Figyelemreméltó, hogy egy ilyen egyszerű axiómarendszer milyen messzemenő következtetések megtételére ad lehetőséget. Ha adva van például egy sík egészkoordinátájú rácspontszerkezete, és szomszédosnak mondjuk azokat a rácspontokat, amelyeket összekötő szakaszon nincs rácspont, azt kapjuk, hogy egy-egy rácspontnak *végtelen* sok szomszédja lesz.

> Egy adott (a, b) rácspontnak (x, y) a szomszédja, ha $a - x$ és $b - y$ egészek relatív prímek. Ilyen (x, y) bármely (a, b)-hez nyilvánvalóan végtelenül sok van.

Ugyancsak mély meggondolást fog jelenteni az a távolságfogalom, amely két pont távolságát a közrefogott pontok számával hozza összefüggésbe.

> Ebben a megvilágításban azt kapjuk, hogyha a teljes sík a rácsszerkezettel együtt egyenletesen tágul, akkor a bármely rácsponton helyet foglaló megfigyelő ebből a tágulásból nem vesz észre semmit. (Hiszen a távolodó rácspont és a megfigyelő rácspontja közötti közrefogott pontok száma nem növekszik.) Azt is mondhatnánk, hogy ha egy táguló szobában ülünk, de mi magunk is tágulunk, továbbá a kezünkben levő méterrúd is tágul (ami jelen esetben fontos: nyúlik), akkor a szobát mindig ugyanakkorának mérjük. *Edwin Hubble* mégis észrevette a világegyetem tágulását, amiből az következik, hogy kell legyen egy abszolút, a tér tágulásától független méterrudunk. És csakugyan van: ez a fény hullámhossza.

Fontos eredménynek érezzük, hogy az axiómarendszer segítségével olyan didaktikai *modellek* bemutatására nyílik lehetőség, amelyek jó lehetőséget kínálnak a *Dedekind-* illetve a *Cantor-féle tulajdonság* vizsgálatára; ezeknek a fogalmaknak az elmélyítésére — és végül demonstrálják egymástól való függetlenségüket.

Ugyancsak jó terepet kínálnak a modellek a *nyílt halmaz* fogalma tisztázására; kiemelt jelentőséget kap ekkor az axiómarendszer nyílt illetve zárt alternatívája. Úgy véljük, didaktikai szempontból értékesek a topológiai párhuzamok, és a véges modellek leszámlálásakor adódó számelméleti problémafelvetések, megfontolások.

Már a kicsi gyerek is szereti szétszedni karácsonyra kapott autóját, minden apuka nagy bosszúságára. Az *analízis* iránti igény, a *deduktív* megközelítés alapvető a megismerési folyamatban. Ennek a törekvésnek a vizsgálatára irányítja a figyelmet a második fejezet (*Prímek*), amely algebrai struktúrák tovább nem bontható építőköveinek — *prímjeinek* — felkutatásában szolgál didaktikai javaslattal. A prímfogalom axiomatizálásával annak nagyléptékű kiterjesztését éri el, s matematikai eszközt is ajánl a prímek kutatásának céljára.

A *Prímek* c. fejezet legjelentősebb *didaktikai eredménye* a *felbontható prímeket* tartalmazó egységelemes félcsoport bemutatása. A matematikadidaktikai irodalom a prímtulajdonságot és a felbonthatatlanságot kvázi szinonimaként említi; ennek a példának a fényében a két tulajdonság eltérései — és ugyanakkor a köztük meglevő mély fogalmi és formai analógia is — elmélyültebben tanulmányozható.

Akárcsak az első fejezetben, a másodikban is bemutatunk egy *tőlünk származó algebrai struktúrát*. Ez — az ún. *HT-rendszer* — bizonyos, jól ismert programozástechnikai fogalomnak, a karakterláncokon értelmezett *head* és *tail* függvénynek nyújt kitágított értelmezési lehetőséget, miáltal hozzásegít azok megalapozottabb megértéséhez; jelentőségét azonban a prímek előállítása, leszámlálása terén nyeri el: bemutatunk általa egy eszközt, amellyel prímek a „szorzás” művelet ismeretében, mint e szorzásnak az atomjai (tovább nem „szeletelhető” elemei) állnak elő.

Végül hatékony átfogalmazásnak érezzük azt a definíciót, amelyet a *Prímek* fejezet végén az *ikerprím* fogalmára adunk, mellyel az ikerprímek vizsgálata jelentősen kiterjeszthető a természetes (avagy egész-) számokénál általánosabb struktúrákra.

A *Bevezetés* elején leírt ellenérzés, amelyet a testvérfogalom axiomatikus megközelítése vált ki, kimondott paradoxonhatást eredményezhet legalapvetőbb fogalmaink tárgyalásakor. Ezért a harmadik (*Ciklikus halmazok*) fejezetben szemügyre vesszük legalapvetőbb — a halmazelmélet felépítését célzó — axiómáink némelyikét, hogy e vizsgálattal didaktikai útvonalat ajánljunk, és néhány kapcsolódó területre rátekintve kutatási témát is kínáljunk.

Ebben — a harmadik — fejezetben az *általános iskolai* illetve *szakköri foglalkozások* didaktikai kelléktárának is nyújtunk kínálatot, amint azt [0.1] cikkünkben részletesen is bemutattuk. A fiatalabbak számára is közkeletű és vonzó olyan fogalmakkal, mint például a közösségi portálok csoportjai, könnyebben tudjuk matematikailag is szigorú megvilágításba helyezni halmazelméleti alapfogalmainkat. (A cikk mindenre kiterjedően bemutatja az elvégzett kísérleteket, azok kiértékelésével együtt, ezért ezeknek bemutatását jelen dolgozatban mellőztük.)

A különböző axiómáknak eleget tevő véges „univerzumok” *leszámlálásának* feladatköre, amelyet a „*bekorongozásnak*” elnevezett eljárással interpretálunk komoly kihívást nyújthat akár a felsőoktatásban is a matematikusképzés első évfolyama számára. Ugyanezek a problémák egyszersmind kiváló *programozási feladatokat* is kínálnak a programozó / programtervező matematikusok képzése keretében; esetükben akár a magasabb évfolyamokon is.

Jelölések

A dolgozatban alkalmazott saját jelöléseket (pl. bontás) az első előforduláskor bevezetjük.

$\&$	logikai ÉS
$\mid$	logikai VAGY, avagy a halmazjelölés elhatároló jele
$\neg$	logikai NEM
$\Rightarrow$	logikai implikáció
$\Leftrightarrow$	logikai ekvivalencia
$\lvert a \rvert$	a szám abszolút értéke
$\lvert A \rvert$	A halmaz elemszáma
$\overline{A}$	A halmaz komplementere
$\varnothing$	az üreshalmaz
$\mathbb{N}$	természetes számok
$\mathbb{N}^+$	pozitív természetes számok (ugyanígy pl. $\mathbb{Q}^+$)
$\mathbb{Z}$	egészszámok
$\mathbb{Q}$	racionális számok
$\mathbb{R}$	valós számok
$\mathbb{C}$	komplex számok

A kvantorok, az unió, a metszet, a Descartes-szorzat műveletek, az eleme, nem eleme, halmaztartalmazási és a hagyományos egyenlő, nem egyenlő, közelítőleg egyenlő, kisebb, nagyobb (vagy egyenlő) relációk jelölése valamint a „végtelen” szimbólum a szokásos.

Elválasztási rendszerek

Bevezetés az 1. fejezethez

Mottó: *Ő azonban áthaladt közöttük….* [1.1]

Amikor az ETO (Egyetemes Tizedes Osztályozás) kategóriái definiálásra kerülnek (ez a folyamat beérkezett javaslatok alapján egy nemzetközi központban történik), akkor senki nem foglalkozik egyikkel sem azon gyűjtemények közül, amelyeket majd az ETO segítségével fel fognak tárni. Vegyük például az Országos Széchényi Könyvtár többmillió címes gyűjteményét! Ebben lehetnek olyan dokumentumok „közel" egymáshoz, amelyeket az ETO „tudorai" távolra helyeztek, és persze fordítva ugyanígy. (Az ETO egy fa, amelyben a távolságot kézenfekvően a két csomópont közötti út hossza adja — ismeretes, hogy ez a mérték egy fában metrikát ad.) Ugyanezeket a megállapításokat tehetjük a természetesnyelvi tárgyszórendszerekkel kapcsolatban is; bár e tezauruszok sohasem egyetemesek, és ezért ez a torzító hatás némileg mérséklődik.

E fejezet célja többrétű. Egyrészt arra teszünk kísérletet, hogy a fenti munkamódszerrel ellentétben nem kívánjuk előre megmondani, hogy egy gyűjtemény (halmaz) bibliográfiai leírásai (elemei) között melyek vannak távol illetve közel; azaz nem egy *a priori* kész metrikát akarunk alkalmazni a halmazra, hanem abban bízunk, hogy a halmaz majd előállítja saját metrikáját. A munkahipotézis szerint a halmaz elemeinek távolsága (közelsége) magából a halmaz szerkezetéből fakad: azok az elemek vannak egymástól távol, amelyek *között* sok egyéb elem található, és azok vannak közel, amelyek *között* kevés. Hogy e definíciónak értelme legyen, definiálni kell a „*között*" fogalmát, azaz meg kell tudni mondani, hogy két elem mikor fog közre egy harmadikat.

Másrészt az is célunk, hogy az így absztrahált kérdés axiomatikai vizsgálatának tanulságait levonjuk. Az elválasztás (közrefogás) négy axiómája tőlünk származik abban az értelemben, hogy mi válogattuk össze éppen ezt a négyet. Az általunk „folytatásaxiómának" illetve „keveredésaxiómának" nevezett posztulátumokat már *Eukleidész* is közli (majdnem pontosan ebben a for-

mában[*]), majd különböző variánsokkal dolgozott *Pasch* [1.2], *Dedekind* [1.3] és *Cantor* [1.4]. A szimmetria a közrefogás fogalmához olyan evidens módon tartozik hozzá, hogy az axióma idevételét — úgy gondoljuk — nem kell indokolni. A legtöbb „fejfájást" a nyílt illetve a zárt rendszerek megkülönböztetése, azaz a „határaxiómának" nevezett követelmény bevezetése okozza. Az axiomatikai vizsgálat talán éppen e téren lesz a legérdekesebb.

Alapvető fogalomalkotás

Definíció (1)

Legyen A tetszőleges, nem üres halmaz! Egy $E \subseteq A^3$ relációról azt mondjuk, hogy **nyílt elválasztási reláció**, ha

E1NY $(a,b,a) \notin E$ (határaxióma)

E2 $(a,b,c) \in E \Rightarrow (c,b,a) \in E$ (a szimmetria axiómája)

E3NY $\forall\, a,\ b \neq a \in A\ \exists\, c \in A : (a,b,c) \in E$ (folytatásaxióma)

E4NY $(a,b,c) \in E \Rightarrow (b,a,c) \notin E$ (keveredésaxióma)

Szóhasználat:

A későbbiekben, ha a „nyílt" jelzőt elhagyjuk, mindig nyílt elválasztási relációt értünk alatta. Amikor majd zárt elválasztási relációról fogunk beszélni, a jelzőt mindig használni fogjuk. **E1NY**, **E3NY** és **E4NY** tulajdonságot (axiómát) ezután **E1**-gyel, **E3**-mal illetve **E4**-gyel jelöljük.

Jelölés:

A kényelem kedvéért a továbbiakban az $(a,b,c) \in E$ tényt egyszerűen abc-vel jelöljük.

[*] L. [1.9]!

Szóhasználat:

Ha abc fennáll, a következőket mondjuk: b **elválasztja** a-t és c-t; b a és c **között** van; a és c **közrefogja** b-t. Ha A halmaz felett E elválasztási reláció adott, akkor rólunk, mint (A, E) **elválasztási rendszerről** fogunk beszélni. Egy konkrét A és E esetén **modellt** mondunk. Szóhasználatunkban a modell **elemszáma** (illetve számossága) A elemszáma (számossága). Amikor az E elemszámáról (számosságáról) beszélünk, **reláció-elemszámot** mondunk. Az $(\{a\},\varnothing)$ modellt **triviális modellnek** nevezzük.

Korollárium (1)

Az axiómarendszer egyszerű következménye, hogy $\neg\exists\, a, b \in A$, hogy aab vagy abb fennállna. Tudniillik aab eleve ellentmond **E4**-nek, másfelől, ha abb, akkor **E2** miatt bba, ami ismét ellentmond **E4**-nek.

Korollárium (2)

Ugyancsak következik az axiómarendszerből, hogy $abc \Rightarrow \neg acb$; hiszen abc maga után vonja cba-t (**E2**), ami **E4** miatt kizárja mind bca, mind acb fennállását.

Lemma (1)

Legyen (A, E) elválasztási rendszerben $|A| = n$.
Ekkor $n(n-1) \leq |E| \leq n(n-1)(n-2)/3$.

Bizonyítás:

E3 miatt minden $a, b \neq a \in A$ párhoz kell lennie hármasnak E-ben, ezért E elemszáma nem lehet kevesebb, mint $n(n-1)$. **E1** és **Korollárium (1)** kizárja, hogy egy E-beli hármasban két egyforma elem legyen, emiatt E elemszáma legföljebb $n(n-1)(n-2)$ lehetne. Ám **E4** minden E-beli hármassal kizár a további lehetőségek közül kettőt, így E elemszáma nem lehet $n(n-1)(n-2)$, hanem annak csak a harmada. □

Példák:

Egy algebrai struktúra tanulmányozására legalkalmasabbak a már ismert illetve a véges modellek. Példák generálása érdekében kimondunk két lemmát:

Lemma (2)

Legyen A olyan teljesen rendezett halmaz, amelynek nincs se szuprémuma, se infimuma, illetve, ha van, akkor ezek nincsenek A-ban. Ekkor az

$$abc \Leftrightarrow a < b < c \mid a > b > c$$

definícióval adott reláció elválasztási reláció.

Bizonyítás:

E1 a szigorú egyenlőtlenségek miatt fennáll. **E2** a definícióból nyilvánvaló. **E3** biztosításához volt szükséges kimondani, hogy A vagy ne legyen korlátos, vagy, ha igen, akkor ne tartalmazza torlódási pontjait; így, ha pl. $a < b$, akkor mindig lehessen egy $b < c$ tulajdonságú c elemet találni. **E4** az A teljesen rendezett volta miatt ismét nyilvánvaló.

Szóhasználat:

A **Lemma (2)**-ben bemutatott elválasztási relációt **hagyományos** elválasztási relációnak fogjuk hívni, és H-val fogjuk jelölni.

Elválasztási rendszerek generálása algebrai struktúrák segítségével

Lemma (3)

Legyen G csoport a következő tulajdonságokkal:

1. $|G| > 1$
2. $\forall a, b \in G : a^2 = b^2 \Rightarrow a = b$
3. $\forall a, b \in G : a^3 = b^3 \Rightarrow a = b$

4. G *Abel*-csoport

Az ilyen csoportot *elválasztási csoportnak* fogjuk nevezni, és állítjuk, hogy az
$abc \Leftrightarrow a \neq c,\ ac = b^2$
definícióval nyert relációval G elválasztási rendszer.

Bizonyítás:

E1 teljesül, mert aba-t a definíció kizárja, **E2** teljesül, mert G *Abel*-csoport. **E3** teljesülése azt jelenti, hogy az abx, azaz $ax = b^2$ egyenlet minden a és $b \neq a$ esetén megoldható. Valóban, mert G csoport $x = a^{-1}b^2$. Állítjuk, hogy ez az x mindig megfelel, tudniillik se nem a, se nem b. Ha ugyanis $a^{-1}b^2 = a$, akkor $a^2 = b^2$, ahonnan G 2. tulajdonsága miatt $a = b$ következik, ha pedig $a^{-1}b^2 = b$, ebből azonnal $a = b$ következne. Végül belátjuk, hogy **E4** is fennáll: Tegyük fel tehát, hogy abc és bac egyszerre teljesül valamely $a \neq b,\ b \neq c,\ c \neq a$ hármasra! Ekkor $ac = b^2$ és $bc = a^2$ teljesülnek, ahonnan c-re támaszkodva $a^{-1}b^2 = b^{-1}a^2$, amiből $a^3 = b^3$ adódik. Ez viszont G 3. tulajdonsága miatt azt jelenti, hogy $a = b$. □

Következmények:

1. Elválasztási csoport nem lehet párosrendű. Valóban, a véges Abel-csoportok alaptétele szerint párosrendű Abel-csoportban direkt osztó a kételemű ciklikus csoport, amelyben az e egységelem melletti a elemre $a^2 = e$, miáltal sérül az elválasztási csoportok 2. tulajdonsága.

2. Elválasztási csoport rendje nem lehet osztható 3-mal. Valóban: ha egy véges Abel-csoport rendje osztható 3-mal, akkor található benne 3-elemű ciklikus csoport, mint direkt osztó, melynek elemeire $x^3 = e$ áll fenn, miáltal sérül az elválasztási csoportok 3. tulajdonsága.

3. Elválasztási csoport rendje legalább 5. Ha $|G| = 1$ lenne, akkor nem lenne benne $a \neq c$ tulajdonságú

két elem, azaz nem adna elválasztási rendszert (pontosabban csak triviálist adna). Az előző megfontolások alapján pedig látható, hogy $|G|$ nem lehet 2, 3 és 4.

Példák:

1. $(\mathbb{Z},+)$ — az egészszámok halmaza az összeadással — elválasztási csoport.

2. $(\mathbb{Q}^+,\cdot)$ — a pozitív racionális számok halmaza a szorzással — elválasztási csoport.

3. Az m-modulusú kongruenciák az összeadással elválasztási csoportot alkotnak, ha m páratlan, m nem osztható hárommal és $m \geq 5$.

4. Az m-modulusú kongruenciák szorzása sohasem alkot elválasztási csoportot. (Tudvalevő egyébként, hogy a kongruenciák szorzása csak akkor csoport — az $m = 0$ kivételével —, ha a modulus prím. Ha $m = 2$, akkor a 3. Következmény miatt nem lehet elválasztási csoport, ha $m > 2$, akkor pedig egy $k \neq 0$ esetében $-k$ (k-nak a kongruencia szerinti additív inverze) mindig eltér k-tól, ennek ellenére $k^2 = (-k)^2$.)

Látható, hogy az elválasztási csoport fogalma a számtani illetve a mértani közép általánosítása csoportokra. A gondolatmenetet folytatva az abc definíciójában pl. az $a^2b = b^3$ követelményt elhelyezve egy *súlyozott középhez* jutunk. Erre a kiterjesztési lehetőségre világít rá a következő lemma:

Lemma (4)

Legyen R egységelemes gyűrű. A gyűrű additív egységelemét jelölje 0, a multiplikatívat jelölje 1. Ideiglenesen bevezetjük azt az írásmódot, hogy a gyűrű elemeit félkövér karakterekkel írjuk: Legyen $n \in \mathbb{N}$, és jelölje $n\boldsymbol{a}$ az $\boldsymbol{a} + \boldsymbol{a} + \ldots + \boldsymbol{a}$ n-tagú összeget R-ben. E jelölés mellett jelölje $\boldsymbol{0}, \boldsymbol{1}, \boldsymbol{2}, \ldots, \boldsymbol{k}, \ldots$ a $0\boldsymbol{1}, 1\boldsymbol{1}, 2\boldsymbol{1}, \ldots, k\boldsymbol{1}, \ldots$ gyűrűelemeket. Ezeknek az elemek-

nek a halmazát jelöljük L-lel. Megállapodunk abban, hogy ha $i, j \in \mathbb{N}, i \neq j \ \& \ i\mathbf{1} = j\mathbf{1}$, akkor a szóbanforgó gyűrűelem jeléül a kisebbik természetes számot választjuk. Megemlítjük, hogy L részgyűrű R-ben; L lehet véges vagy végtelen halmaz — ha R véges, akkor nyilvánvalóan L is véges, de, ha R végtelen, akkor L lehet véges is és végtelen is. Rögzítsünk ezután egy $\boldsymbol{k} \in L$ elemet az alábbi tulajdonságokkal:

— ***k* nem bal oldali nullosztó**
— ***k* – 1 sem bal oldali nullosztó**
— $\boldsymbol{k^2 - ij}$ ***nem bal oldali nullosztó semmilyen*** $\boldsymbol{i, j \in \{1, 2, \ldots k - 1\}}$ ***esetén***

(Innentől a gyűrűelemeket nem emeljük ki félkövér szedéssel.) E rögzített k mellett vezessük be a következő relációt:

$abc \Leftrightarrow a \neq c$, és $\exists i \in \{1, 2, \ldots k - 1\}$, úgy, hogy i nem bal oldali nullosztó, $k - i$ sem bal oldali nullosztó, és $(k - i)a + ic = kb$. Amennyiben az így nyert reláció nem üres, úgy R elválasztási rendszer ezzel a relációval.

Bizonyítás:

A bizonyításhoz előrebocsátunk két megjegyzést:

M1: $1 \in L$ biztosan nem (bal oldali) nullosztó (ez ugyanis $1x = 0 \Leftrightarrow x = 0$ miatt lehetetlen).
M2: Ha R nem kommutatív gyűrű, L elemei egymás közt akkor is felcserélhetőek, tudniillik: $\boldsymbol{ij} = i\mathbf{1}j\mathbf{1} = ij\mathbf{1} = ji\mathbf{1} = j\mathbf{1}i\mathbf{1} = \boldsymbol{ji}$.

Most rátérünk a bizonyításra:

E1 axióma közvetlenül teljesül a definícióból.

E2 teljesül, mert ha abc fönnáll, akkor $\exists i \in \{1, 2, \ldots k - 1\}$, úgy, hogy i nem bal oldali nullosztó, $k - i$ sem bal oldali nullosztó, és $(k - i)a + ic = kb$. Ez

után $j = k - i$ választással: $ja + (k - j)c = (k - j)c + ja = kb$; azaz cba.

E3 axióma sérül, ha abx „egyenletet” $a \neq b$ esetén nem lehet megoldani x-re. Állítjuk, hogy az $x = kb - (k - 1)a$ választás minden esetben kielégíti az abx „egyenletet”; tudniillik i-t 1-nek választva (l. M1 megjegyzés):

$$(k - 1)a + 1(kb - (k - 1)a) = kb$$

Belátjuk, hogy az így nyert x mindig megfelel, vagyis, hogy x nem lehet sem a, sem b, hiszen, ha:

$kb - (k - 1)a = a$ — és ekkor:
$kb = ka$ (k nem bal oldali nullosztó)
$b = a$ — amit kizártunk;

másrészt, ha:

$kb - (k - 1)a = b$
$(k - 1)b - (k - 1)a = 0$
$(k - 1)(a - b) = 0$ ($k - 1$ nem bal oldali nullosztó)
$a - b = 0$
$a = b$ — amit kizártunk;

E4 axióma sérül, ha abc mellett acb fennáll (l. **Korollárium (2)**). Megmutatjuk, hogy abc és acb kizárják egymást. Tegyük fel ugyanis, hogy abc és acb, azaz:

$(k - i)a + ic = kb$ $\quad / \cdot j$ (balról)
$(k - j)a + jb = kc$ $\quad / \cdot k$ (balról)

$j(k - i)a + jic = jkb$
$k(k - j)a + kjb = k^2c$

$k(k - j)a + j(k - i)a + jic = k^2c$ (l. M2 megjegyzés)
$k^2a - kja + jka - jia + jic = k^2c$
$ji(c - a) = k^2(c - a)$
$(k^2 - ij)(c - a) = 0$

Ám feltettük, hogy $k^2 - ij$ nem bal oldali nullosztó, s minthogy $c \neq a$, ezért $(k^2 - ij)(c - a) = 0$ nem lehetséges. □

Néhány megjegyzés a gyűrűből generált elválasztási rendszerre

— Nem mindig lehet alkalmas k-t találni. Ha pl. a gyűrűben $a + a = 0$, (Boole-gyűrű), akkor a $0, 1, 2, ..., k, ...$ elemek így alakulnak: $0, 1, 0, 1, ...$; azaz $L = \{0, 1\}$. Ennélfogva, ha $k = 1$ (s így nem nullosztó), akkor $k - 1 = 0$ (azaz nullosztó); alkalmas k tehát nincs.

— Ha viszont van alkalmas k, akkor alkalmas i mindig van, tudniillik az $i = 1$ választás mindig megfelel a célnak.

— Elképzelhető ugyanakkor, hogy csak egyetlen alkalmas i van, hiszen pl. $k = 2$ rögzítése esetén csakis az $i = 1$ választható.

— Alkalmas k és i léte már garantálja, hogy a reláció nem lesz üres, tudniillik 1 és $k + 1$ mindig közrefogja $i + 1$-et (lévén, hogy $(k - i)1 + i(k + 1) = k - i + ik + i = ki + k = k(i + 1)$).

— Adott a és c esetén (még, ha $c - a$ nem is 0), nem biztos, hogy létezik alkalmas b. Ez azt jelenti, hogy nem bármely két elem fog közre harmadikat, hanem csak bizonyosak. Ez a helyzet azonban csak végtelen gyűrűben fordulhat elő, hiszen véges gyűrűben minden elem vagy nullosztó vagy egység, ezért k (lévén, hogy nullosztó nem lehet) egység. Így — minthogy alkalmas i, mint láttuk mindig létezik — adott a-hoz és c-hez mindig lehet b-t találni, tudniillik: $b = k^{-1}((k - i)a + ic)$.

A legkisebb modell — és további modellek

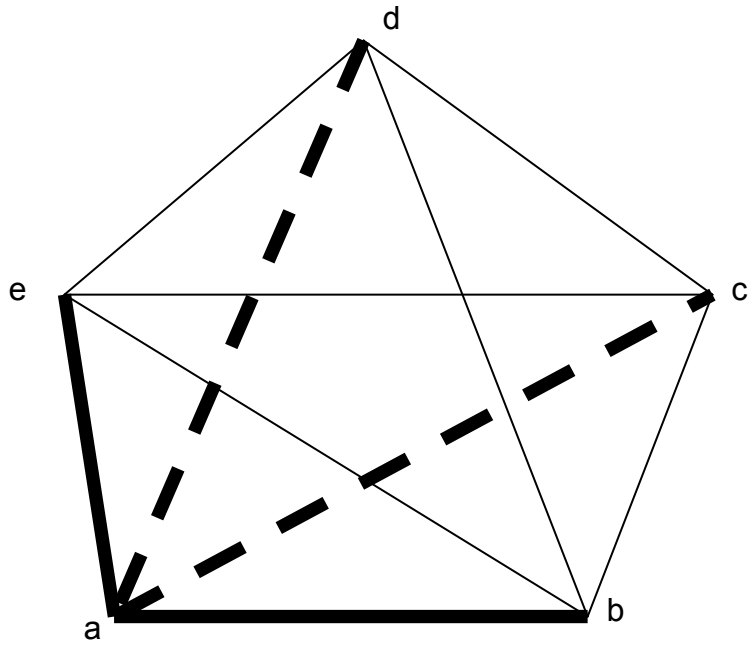
Mekkora a legkisebb nem triviális modell?

A válaszhoz vezető megfontolásokat félig-meddig már megtettük **Lemma (3)** következményeinek tárgyalásakor. Most a gyűrű-modell felől nézve haladunk:

Ha valamilyen *mod n* maradékgyűrűből szeretnénk generálni elválasztási rendszert, hamar beláthatjuk, hogy n nem lehet páros, ugyanis ezekben a maradékgyűrűkben minden második elem nullosztó, azaz alkalmas k-t nem lehet találni, hiszen, ha k nem nullosztó, akkor $k - 1$ az lesz. Vizsgáljuk a *mod 3* maradékgyűrűt! Itt $L = \{0, 1, 2\}$, ahol *0* és *1* nyilván nem felel meg k-nak, de *2* sem, mert $2^2 = 1$, és az ij szorzat is csak *1* lehet (hiszen mind i, mind j eleve csak *1* lehet). A *mod 5* maradékgyűrűből $k = 2$ rögzítése mellett adódik az alábbi modell, amely egyben a legkisebb nemtriviális modell[*]:

M1 *({a, b, c, d, e}, {(a, b, c), (a, c, e), (a, d, b), (a, e, d),* ***(b, a, e),*** *(b, c, d), (b, d, a), (b, e, c),* ***(c, a, d)****, (c, b, a), (c, d, e), (c, e, b),* ***(d, a, c)****, (d, b, e), (d, c, b), (d, e, a),* ***(e, a, b)****, (e, b, d), (e, c, a), (e, d, c)})*

[*] Ezt az állítást bizonyítás nélkül közöljük; de az Olvasó próbálgatással viszonylag könnyen meggyőződhet arról, hogy kisebb modellt, illetve **M1**-gyel nem izomorf ötelemű modellt nem lehet találni.



1.1. ábra

A rajz értelmezése: Az ötszög kerületén minden elemet közrefog a két szomszédja (így tehát a-t b és e) valamint a két második szomszédja (azaz megint a-t c és d). (A vastagított vonalaknak megfelelő elemhármasok az ábrát megelőző felsorolásban félkövérek.)

A fenti modellt $R(5, 2)$-vel fogjuk jelölni. ($R(n, k)$ jelöljük a $mod\ n$ maradékgyűrűből k rögzítésével nyert elválasztási rendszert.)

M1-hez hasonló további modellek készíthetők: $R(n, 2)$ mind megfelelő modell, ha n nem osztható se 2-vel, se 3-mal. (Ezt az állítást már bizonyítottuk akkor, amikor beláttuk, hogy elválasztási csoport rendje nem lehet osztható se 2-vel, se 3-mal. Az $R(n, 2)$ additív csoportja ugyanis elválasztási csoport. L. 17. o.!)

Az illusztráció kedvéért megmutatjuk, hogy 1-től 100-ig mely $n \in \mathbb{N}$-ekre, mely k-kal lehet $R(n, k)$ elválasztási rendszert készíteni:

n	A szóba jöhető k értékek																
5	2																
7	2																

n	A szóba jöhető *k* értékek																
11	2	3	4														
13	2	3															
17	2	3	4														
19	2	3	4		6												
23	2	3	4		6												
25	2																
29	2	3	4	5	6			9									
31	2	3	4	5				9									
35	2																
37	2	3	4	5	6		8										
41	2	3	4	5	6		8										
43	2	3	4	5	6			9									
47	2	3	4	5	6		8	9									
49	2																
53	2	3	4	5	6	7	8		10		12						
55	2																
59	2	3	4	5	6	7		9	10		12						
61	2	3	4	5	6	7			10								
65	2																
67	2	3	4	5	6	7	8		10				14				
71	2	3	4	5	6	7	8		10						16		
73	2	3	4	5	6	7	8				12						
77	2																
79	2	3	4	5	6	7	8				12			15			
83	2	3	4	5	6	7	8	9	10	11	12			15			
85	2																
89	2	3	4	5	6	7	8	9	10					15			18
91	2																
95	2																
97	2	3	4	5	6	7	8	9			12			15	16		

Érdekes kérdés, hogy nem algoritmikus úton (tehát valamilyen zárt algebrai alakban) hogyan lehet egy adott n-hez a megfelelő k-kat megkapni.

Annak vizsgálata sem érdektelen, hogy milyen és mennyire éles csak n-től függő felső becslés adható a szóba jöhető legnagyobb k értékre. Erre vonatkozólag a következőt mondhatjuk: $R(n, k)$ reláció-elemszáma $n(n - 1)(k - 1)$, hiszen minden intervallumban $k - 1$ osztópont van. Eszerint $n(n - 1)(k - 1) \leq n(n - 1)(n - 2) / 3$, ahonnan $k \leq (n + 1) / 3$. Ez a becslés biztosan jó, és $n = 5$-nél és $n = 11$-nél be is áll, valamint $n = 7$-nél és $n = 19$-nél gyakorlatilag beáll, egyelőre nem tudjuk, magasabb n-ekre van-e élesebb.

Természetesen nem állítjuk, hogy csak ezek a véges modellek léteznek; a későbbiekben be fogunk mutatni pl. 6-elemű modellt is. (Meg fogjuk mutatni — l. **Korollárium (7)** —, hogy minden $n > 4$-re létezik n-elemű elválasztási rendszer.) Mindössze annyit állítunk, hogy gyűrűkből a **Lemma (4)** szerinti módon lehet elválasztási rendszereket generálni; véges gyűrűkből pedig természetesen véges modellek keletkeznek — amelyek megkönnyítik az elválasztási rendszerek tanulmányozását.

Megjegyzés:

E generálási eljárás kapcsán felvetődhet az a kérdés, hogy a véges testek — melyek úgyszintén gyűrűk — nem nyújtanak-e többletet a maradékgyűrűkhöz képest; azaz nincsenek-e további lehetőségek elválasztási rendszerek generálására esetleg más, alkalmas k-k választásával. (A hangsúly ebben a kérdésben a további alkalmas k-k felbukkanásának lehetőségén van.) A válasz nemleges. Tudvalevő ugyanis, hogy minden véges test úgy áll elő, mint egy prímszámrendű maradékgyűrű (azaz test) feletti valahány dimenziós algebra. Egy $q = p^m$-rendű testben a p-rendű prímtest résztestként van jelen, és ezért tartalmazza a multiplikatív egységelemet, az 1-et. Ennélfogva világos, hogy a q-rendű testben a fent bevezetett L halmaz $\{0, 1, 2, \ldots, p-1\}$, azaz a szóba jöhető k-k ugyanazok, mint az $R(p, k)$-kban. (Ennek megvilágítására bizonyítás nélkül közöljük, mert nyilvánvalónak érezzük, hogy ha K_n-nel jelöljük azon k-k halmazát, amelyekkel $R(n, k)$ elválasztási rendszer generálható, akkor $K_{nm} = K_n \cap K_m$. Innen rögtön adódik, hogy $K_q = K_p$, hiszen $q = p^m$.) Eszerint pl. a 25-rendű testben ($GF(25)$-ben) is csak a $k = 2$ választás jöhet szóba, ugyanúgy, mint a $mod\ 25$ maradékgyűrűben. (Más kérdés, hogy a $GF(25)$-ből $k = 2$ választásával származtatott elválasztási rendszer ***szerkezete*** más lesz, mint $R(25, 2)$-é. Az ilyen

szerkezetű elválasztási rendszereket később, a származtatott elválasztási rendszereknél tárgyaljuk.)

Méretkorlátok

Az E elemszámára vonatkozó korlátok ($n(n - 1) \leq |E| \leq n(n - 1)(n - 2) / 3$ — l. **Lemma (1)**) egyúttal támpontot nyújtanak a kis elemszámú elválasztási rendszerek létezésére vonatkozóan — anélkül, hogy próbálgatással vizsgálnánk őket:

n	n(n - 1)	n(n - 1)(n - 2) / 3
0	0	0
1	0	0
2	1	0
3	6	2
4	12	8
5	20	20
6	30	40
7	42	70
…	…	…

A táblázatból látható, hogy elvileg létezik az $(\varnothing, \varnothing)$ modell, ezt a definícióval zártuk csak ki, az $(\{a\}, \varnothing)$ modellt neveztük triviális modellnek, 2-, 3- és 4-elemű modell azonban elvileg sem létezhet, mert a hozzá szükséges reláció elemszámának alsó korlátja nagyobb, mint a felső. A táblázat bizonyítani nem bizonyítja, de erősen alátámasztja azt a próbálgatással is ellenőrizhető megállapítást, hogy ötelemű modell csak egy van.

További példák

M2 A talán legkézenfekvőbb modell az egészszámok halmaza ($\mathbb{Z}$) a hagyományos közrefogással: $(\mathbb{Z}, H)$.

M3 Ha $R = (\mathbb{Z}, +, \cdot)$, és $k = 2$, akkor a következő, gyűrűből generált modellt nyerjük: x és z fogja közre y-t,

abban az esetben, ha $x \neq z$, paritásuk azonos, és y egyenlő számtani közepükkel.

M4 Bemutatunk egy elválasztási rendszert $\mathbb{Z}^2$ fölött is: (a, b) és (e, f) fogja közre (c, d)-t, ha $(e - a)(d - b) = (f - b)(c - a)$, azaz (c, d) rajta van (a, b) és (e, f) egyenesén, és $a < c < e$ és $b < d < f$ vagy $a > c > e$ és $b > d > f$, azaz (c, d) az (a, b) és (e, f) pontok által meghatározott szakaszon van.

A Dedekind- és a Cantor-féle tulajdonság értelmezése

Definíció (2)

Azt mondjuk, hogy egy (A, E) elválasztási rendszer **megjeleníti a Dedekind-féle tulajdonságot** (avagy: **kielégíti a Dedekind-féle feltételt**), ha

D1 $(B \cap C = \varnothing \,\&\, B \cup C = A \,\&\, B \neq \varnothing \,\&\, C \neq \varnothing \,\&\, (a, b \in B \Rightarrow \neg\exists\, c \in C : acb) \,\&\, (a, b \in C \Rightarrow \neg\exists\, c \in B : acb)) \Rightarrow$
$(\exists\, d \in A : (a \in B \,\&\, b \in C \,\&\, a \neq d \,\&\, b \neq d) \Rightarrow adb)$

Szavakkal: Ha van A-nak olyan két részhalmazból álló diszjunkt osztályozása, melyben a halmazok egyike sem üres, és nincs egyikben sem olyan elem, amely a másikból kettőt elválasztana, akkor van olyan d elem A-ban, amely bármely két, különböző osztályba eső elemet elválaszt.

Szóhasználat:

Ha (A, E) elválasztási rendszer, és B és C A-nak olyan osztályozása, amely kielégíti **D1** premisszáját (azaz nincs egyikben sem olyan elem, amely a másikból kettőt elválasztana), akkor azt mondjuk, hogy ez az osztályozás A-nak **Dedekind-féle felosztása** (osztályozása vagy **vágása**). Ha egy (A, E) elválasztási rendszer olyan, hogy nem lehet benne Dedekind-féle felosztást találni, akkor azt mondjuk, hogy (A, E) **triviálisan teljesíti** a Dede-

kind-féle feltételt. Azt (azokat) az elemet (elemeket), amelynek (amelyeknek) létezését a Dedekind-féle feltétel állítja, **Dedekind-féle „d”-elemnek** (elemeknek) fogjuk nevezni.

Példák:

M1 olyan modell, amelyben nem lehet Dedekind-féle felosztást találni, mely modell ezáltal triviálisan teljesíti a Dedekind-féle feltételt.

M2 olyan modell, amely nem triviálisan elégíti ki a Dedekind-féle feltételt.

M3 és **M4** olyan modellek, amelyek nem elégítik ki a Dedekind-féle feltételt.

Tétel (1)

Ha (A, E) elválasztási rendszer nem triviálisan elégíti ki a Dedekind-féle feltételt, akkor A-ban egy rögzített felosztás mellett legföljebb két Dedekind-féle „d” elem van.

Bizonyítás:

D1 jelöléseit használva állítjuk, hogy mind B-ben, mind C-ben legföljebb egy Dedekind-féle „d”-elem lehet. Tételezzük föl ugyanis, hogy pl. B-ben két Dedekind-féle „d”-elem van: e és f. Legyen ekkor g tetszőleges elem C-ből! Ezekután fennáll, hogy

— efg, mert f Dedekind-féle „d”-elem, és e és g egyike sem f, és különböző osztályokban vannak;
— feg, mert e Dedekind-féle „d”-elem, és f és g egyike sem e, és különböző osztályokban vannak;

ám ez ellentmond **E4**-nek. □

Definíció (3)

Ha (A, E) elválasztási rendszerben a és $b \neq a \in A$ elemekre teljesül, hogy

$$\neg\exists\, c \in A : acb$$

akkor azt mondjuk, hogy a és b **szomszédos** elemek. A viszonyt így jelöljük: $a \leftrightarrow b$.

Példák:

— Semmilyen $R(n, k)$ elválasztási rendszerben nincsenek szomszédos elemek (l. erről a **Lemma (3)** bizonyításához fűzött 5. megjegyzést a(z) 21. oldalon!)

— A $(\mathbb{Z}, H)$ elválasztási rendszerben (**M2**-es modell) pl. 0 és 1 egészszámok szomszédosak. $(\mathbb{Z}, H)$-ban minden elemnek két szomszédja van.

— Az **M3**-as (számtani közepes) modellben a páros számok szomszédai a páratlan számok (és természetesen viszont): **M3**-ban minden elemnek végtelen sok szomszédja van.

— **M4** is olyan modell, amelyben minden elemnek végtelen sok szomszédja van.

Tétel (2)

Ha egy (A, E) elválasztási rendszer nem triviálisan teljesíti a Dedekind-féle feltételt, és egy adott osztályozás mellett két Dedekind-féle „d”-elem van, akkor azok szomszédosak.

Bizonyítás:

A **Definíció (2)** jelöléseit használva legyen a B-beli Dedekind-féle „d”-elem d, a C-beli pedig e. Tegyük föl az állítással ellentétben, hogy nem szomszédosak, azaz $\exists\, b \in A : dbe$. E b elemnek valamelyik osztályba kell esnie, legyen pl. $b \in B$. Nyilván nem lehet $b = d$, mert az ellentmondana **Korollárium (1)**-nek. De, mivel d „d”-elem, és $b \in B$ és $e \in C$, ezért bde, ami ellentmond **E4**-nek. Hasonlóképpen látható be, hogy b nem lehet C eleme sem. □

Tétel (3)

Ha (A, E) elválasztási rendszer, és A-nak van Dedekind-féle felosztása, akkor mindkét osztály legalább háromelemű.

Bizonyítás:

Először tegyük föl az állítással ellentétben, hogy az eddigi jelöléseket használva pl. B egyelemű, és így $B = \{b\}$. Ekkor nyilván $C = A \setminus \{b\}$. Legyen c C-nek tetszőleges eleme. Ám ekkor a Dedekind-féle felosztás követelménye miatt nincs a C-nek olyan további, mondjuk d eleme, amellyel cbd lehetne — ami ellentmond **E3**-nak.

Most tegyük fel, hogy $B = \{b_1, b_2\}$. Ekkor az előbb mondottak miatt cb_1b_2 és cb_2b_1 egyszerre fönnáll, ami ellentmond **E4**-nek. □

Definíció (4)

Valamely (A, E) elválasztási rendszerben ***a-b* nyílt intervallumnak** nevezzük és (a, b)-vel jelöljük az

$$(a, b) := \{\, c \in A \mid acb \,\}$$

halmazt.

A definíció néhány egyszerű következménye:

Korollárium (3) $(a, a) = \varnothing$
Korollárium (4) $(a, b) = (b, a)$
Korollárium (5) $a \leftrightarrow b \Leftrightarrow (a, b) = \varnothing$

Szóhasználat:

Ha a „nyílt” jelzőt elhagyjuk, nyílt intervallumot értünk alatta.

Definíció (5)

Valamely (A, E) elválasztási rendszerben ***a és b b*-n túli folytatásának (félegyenesének)** nevezzük és $\overrightarrow{ab}$-vel, vagy, ha az olvashatóság megkívánja, $\overrightarrow{a,b}$-vel jelöljük az

$$\overrightarrow{ab} := \{ c \in A \mid abc \}$$

halmazt.

Definíció (6)

Ha (a, b) és (c, d) intervallumokra fönnáll, hogy $a \in (c, d) \,\&\, b \in (c, d)$, akkor azt mondjuk, hogy (c, d) **tartalmazza** (a, b)-t, és ezt a viszonyt így jelöljük: $(a, b) < (c, d)$.

Figyelem! Az intervallumtartalmazásra szándékosan nem a $\subset$ jelet alkalmaztuk, nehogy azt a félrevezető látszatot keltsük, hogy az egymást a **Definíció (6)** szerint „tartalmazó” intervallumok egymást, mint halmazok is tartalmazzák! A definícióból ez nem következik. Az illusztráció kedvéért képzeljük el, hogy az egészszámok halmazán elválasztási rendszer a következő: x és z egészszámok fogják közre az általuk meghatározott szakasz felezőpontját, ha az egészszám, illetve harmadoló pontjaikat, ha azok egészszámok. Ez — mint könnyen belátható — elválasztási rendszer. Ebben

az elválasztási rendszerben $(0, 12) = \{4, 6, 8\}$ és $(4, 6) = \{5\}$. Amint látható, $(4, 6) < (0, 12)$, de nem igaz, hogy $(4, 6) \subset (0, 12)$ lenne.

Igazság szerint még a $<$ jel használata is félrevezető. Az intervallumtartalmazás ugyanis nem tranzitív reláció. Legyen ugyanis $(A, E) = (\mathbb{Z}, T)$, ahol T-t úgy értelmezzük, hogy x és z egészek közrefogják harmadoló pontjaikat, amennyiben azok egészek: $xyz \Leftrightarrow x, y, z \in \mathbb{Z} \ \& \ y = min(x, z) + k|x - z| / 3; k = 1, 2$. Amint az könnyen látható, $(\mathbb{Z}, T)$ elválasztási rendszer. Ugyanakkor ebben a rendszerben pl. $(12, 15) < (9, 18) < (0, 27)$, de $\neg((12, 15) < (0, 27))$.

Ebben a felfogásban, ahol AB egyenes csupán $\{A, B\} \cup (A, B) \cup \overrightarrow{AB} \cup \overrightarrow{BA}$ (a felül nyílról l. **Definíció (5)**), nem teljesül *Pasch* és *Veblen* 12.25-ös axiómája (l. [1.5] 186. o.!). Vegyük újra azt a példát, hogy x és z egészszámok fogják közre az általuk meghatározott szakasz felező-pontját, ha az egészszám, illetve harmadoló pontjaikat, ha azok egészszámok! Ekkor $(0, 12) = \{4, 6, 8\}$; $\overrightarrow{0,12} = \{18, 24, 36\}$ és $\overrightarrow{12,0} = \{-24, -12, -6\}$. Az egész $0—12$ egyenes ezekszerint csak $\{-24, -12, -6, 0, 4, 6, 8, 12, 18, 24, 36\}$. Másfelől viszont $(4, 6) = \{5\}$; $\overrightarrow{4,6} = \{7, 8, 10\}$ és $\overrightarrow{6,4} = \{0, 2, 3\}$. Eszerint a $4—6$ egyenes a $\{0, 2, 3, 4, 5, 6, 7, 8, 10\}$ halmaz. Vagyis 4 s 6 rajta van $0—12$ egyenesen, de 12 nincs rajta a $4—6$ egyenesen[*].

[*] Példa arra, hogy két ponton több egyenes megy át.

Definíció (7)

Azt mondjuk, hogy egy (A, E) elválasztási rendszer teljesíti a **Cantor-féle feltételt**, ha

C1 $(I_0, I_1, I_2, \ldots I_n, \ldots : \forall n \in \mathbb{N}: I_{n+1} < I_n) \Rightarrow (\exists c \in A : \forall n \in \mathbb{N}: c \in I_n)$

Szavakkal: Ha létezik (A, E)-ben olyan végtelen intervallumsorozat, amelyben minden előző tartalmazza a következőt, akkor van ehhez az intervallumsorozathoz egy olyan elem, amely az intervallumsorozat minden tagjában benne van.

Szóhasználat:

Cantor-féle intervallumsorozatnak nevezzük egy elválasztási rendszerben intervallumok olyan sorozatát, amelyben minden előző tartalmazza a következőt. Ha egy elválasztási rendszer olyan, hogy nem lehet benne **C1** premisszájában leírt intervallumsorozatot találni, akkor azt mondjuk, hogy az elválasztási rendszer **triviálisan teljesíti** a Cantor-féle feltételt. Bármely $R(n, 2)$ vagy $(\mathbb{Z}, H)$ például triviálisan teljesítik a Cantor-féle feltételt. $(\mathbb{Q}, H)$ nem teljesíti, míg $(\mathbb{R}, H)$ nem triviálisan teljesíti azt.

Megjegyzések:

Korollárium (3) miatt ha valamely (a, b) a **C1**-beli intervallumsorozat eleme, akkor $a \neq b$; sőt

Korollárium (5) miatt, ha valamely (a, b) a **C1**-beli intervallumsorozat eleme, akkor a és b nem lehetnek szomszédosak; sőt

ha valamely (a, b) a **C1**-beli intervallumsorozat eleme, akkor $|(a, b)| > 1$.

Felmerülhet a kérdés, hogy van-e olyan véges modell, amely nem teljesíti a Cantor-féle feltételt. A válasz pozitív: pl. az $R(43, 9)$ modell ilyen; ebben pl. $(2, 7) < (0, 9) < (2, 7)$, ám mivel $(2, 7) = \{0, 9, 16, 18, 25, 27, 34, 36\}$ ugyanakkor $(0, 9) = \{1, 2, 3, 4, 5, 6, 7, 8\}$, tehát a két intervallumnak, mint halmaznak a

metszete üres, ezért a Cantor-féle feltétel nem teljesül.

(Megemlítjük, hogy $R(43, 9)$ 903 egymást kölcsönösen tartalmazó intervallumpárt tartalmaz, s a halmazelméleti metszet mindegyik pár estében üres — leszögezve természetesen, hogy a Cantor-féle feltétel nemteljesüléséhez egyetlen metszet üres volta is elegendő lenne.)

Hasonló érdeklődésre tarthat számot az a kérdés is, hogy van-e olyan véges modell, amely nem triviálisan teljesíti a Cantor-féle feltételt. A válasz kicsit bonyolultabb, mint az előző kérdésre: ebben az esetben minden lehetséges Cantor-féle intervallumsorozatot meg kell vizsgálni abból a szempontból, hogy a benne szereplő intervallumok metszete nem üres-e. Ha az $R(n, k)$ típusú elválasztási rendszereket vizsgáljuk, azonnal megállapíthatjuk, hogy csak a $k > 3$ esetek jöhetnek szóba, hiszen $k = 2$ esetén minden intervallum egyelemű, azaz nem is léteznek egymást tartalmazó intervallumok, míg $k = 3$ esetén minden intervallum kételemű, azaz, ha $(a, b) < (c, d)$ fönnáll, akkor biztosan: $(a, b) \cap (c, d) = \varnothing$ — ami egyszerű következménye **E1**-nek.

Egy véges elválasztási rendszerben nyilván csak ciklikus Cantor-féle intervallumsorozatot lehet találni. A ciklus hosszára vonatkozóan a következő megfontolást tehetjük:

Képzeljük el, hogy amikor egy (a, c) intervallumban elemeket keresünk, az alábbi hozzárendeléssel választjuk ki az (a, c)-ben levő tartalmazott intervallumot:

$$(a, c) \rightarrow (k^{-1}((k-1)a + c), k^{-1}(a + (k-1)c))$$

Itt k^{-1} k (bal oldali) multiplikatív inverzét jelöli, mely akkor is létezik, ha R nem nullosztómentes gyűrű, tudniillik k nem nullosztó. Ezt a leképezést R gyűrűben a $\begin{pmatrix} 1-k^{-1} & k^{-1} \\ k^{-1} & 1-k^{-1} \end{pmatrix}$ mátrix valósítja meg, mely $I + k^{-1}T$ alakba írható, ahol I az egységmátrix — $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ —

és T a $\begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}$ mátrix. $I + k^{-1}T$ hatványait vizsgálva a következőkre jutunk:

$$\left(I + k^{-1}T\right)^h = \sum_{i=0}^{h} \binom{h}{i} I^{h-i} k^{-i} T^i = \sum_{i=0}^{h} \binom{h}{i} k^{-i} T^i =$$

$$I + \sum_{i=1}^{h} \binom{h}{i} k^{-i} T^i = I + \sum_{i=1}^{h} \binom{h}{i} k^{-i} (-1)^{i-1} 2^{i-1} T = I - \frac{1}{2} T \sum_{i=1}^{h} \binom{h}{i} (-1)^i k^{-i} 2^i =$$

$$I - \frac{1}{2} T \left(\left(\sum_{i=0}^{h} \binom{h}{i} (-1)^i k^{-i} 2^i \right) - 1 \right) = I - \frac{1}{2} T \left(\left(1 - 2k^{-1}\right)^h - 1 \right)$$

A fenti átalakításban kihasználtuk, hogy I mátrix minden mátrixszal felcserélhető a szorzás műveletben, illetve $\frac{1}{2}$ alakban írtuk a 2 multiplikatív inverzét (ezt azért tehettük meg, mert $R(n, k)$ modellben n nem lehet páros). A most adott módszerrel egymás után generált intervallumok ciklust képeznek, ha $I + k^{-1}T$ valahányadik hatványa I-vel egyenlő. Ez bekövetkezik akkor, ha a fenti formulában a $\frac{1}{2} T \left(\left(1 - 2k^{-1}\right)^h - 1 \right)$ tag eltűnik, vagyis, ha $(1 - 2k^{-1})^h$ valamely h-ra 1 lesz. $1 - 2k^{-1}$ nem lehet nullosztó[*], azaz $(1 - 2k^{-1})$-nek is lesz olyan hatványa, amely R-ben egyenlő 1-gyel[**].

Megjegyezzük, hogy az $I + k^{-1}T$ mátrix $k = 2$ esetén szinguláris, ami egybecseng azzal, hogy egy $R(n, 2)$ típusú elválasztási rendszerben elvileg nem lehetnek egymást tartalmazó intervallumok. Látnunk kell azonban azt is, hogy ezt a kizárást a mátrix $k = 3$ esetén már nem tükrözi. Tükrözi azonban azt a tényt, hogy például az egészek gyűrűjében (azaz 0 karakterisztikájú gyűrűben) $(1 - 2k^{-1})^h$ semmilyen h-ra nem lehet 1, hiszen ehhez $2k^{-1}$-nek 0-nak kellene lennie, ami lehetetlen.

A fenti gondolatmenet csak azt igazolja, hogy egy $R(n, k)$ modellben, ahol $k > 3$ lennie kell Cantor-féle intervallumsorozatnak, azt

[*] $1 - 2k^{-1}$ és $k - 2$ egyszerre nullosztók, és $k - 2$ nem lehet nullosztó. Ezt az állítást ezen a helyen csak azzal támasztjuk alá, hogy az $R(n, k)$ modellben k nem mehet nullosztó fölé — l. ezzel kapcsolatban a Megjegyzést a 25. oldalon!

[**] „Kis” Fermat-tétel.

nem állítja, hogy annak hossza a most megtalált h-val egyenlő. Elképzelhető, hogy egy így generált Cantor-féle intervallumsorozat már ismétli önmagát, és az ismétlés nélküli intervallumsorozat hossza h valamely osztójával egyenlő.

> Mindezekből arra a feltételezésre jutunk, hogy véges gyűrűből generált elválasztási rendszerben a Cantor-féle feltétel nem triviálisan nem teljesülhet. Ha a gyűrű nullosztómentes (azaz test), akkor a sejtés bizonyos alátámasztást kap. Ilyenkor ugyanis a fenti eljárással képzett intervallumok vélhetően bejárják az egész gyűrűt, azaz nem lehet olyan b eleme a gyűrűnek, amelyik mindegyikben benne van; azokban az intervallumokban nem lehet benne, amelyeknek b az egyik határeleme — ezt a határaxióma kizárja. Ez a felvetés további kutatási irányt inspirálhat.

Nem nullosztómentes gyűrűkben rövidebb ciklusok is felléphetnek — $(1 - 2k^{-1})^h$ nem csak $h = (n - 1) / 2$ esetén lesz 1, hanem már kisebb h-kra is —, így elképzelhető, hogy az intervallumok egyéb, határpontként sorra nem vett elemeket tartalmazhatnak.

Elválasztási rendszerekből származtatott elválasztási rendszerek

Definíció (8)

> Legyenek (A, E) és (B, F) elválasztási rendszerek. Ha $B \subseteq A$ és $F \subseteq E$ fönnáll, akkor azt mondjuk, hogy (B, F) **elválasztási részrendszer** (A, E)-ben.

Jelölés:

Ha nem okoz félreértést — és általában nem okoz — nem különböztetjük meg a jelölésben a reláció megszorítottját a részrendszerben. Ha tehát (B, F) elválasztási részrendszer (A, E)-ben, akkor (B, F) helyett (B, E)-t írunk; s ez utóbbi írásmódban automatikusan E-nek B-re megszorítottját értjük.

Példák:

— $(\mathbb{Z}, H)$ elválasztási részrendszer $(\mathbb{Q}, H)$-ban
— az **M3** modell elválasztási részrendszer $(\mathbb{Z}, H)$-ban
— $(\mathbb{Z}, H)$ elválasztási részrendszer az **M4** modellben

Tétel (4)

Ha (R, E) az R gyűrűből a **Lemma (4)** szerint generált elválasztási rendszer, és I (bal)ideál R-ben, akkor (I, E) elválasztási részrendszer (R, E)-ben.

Bizonyítás:

Amikor E-ről annak megszorítottjára (E') térünk át, elhagyjuk E azon elemeit, ahol a Descartes-szorzat nem mind a három komponense származik I-ből. Nyilvánvaló, hogy ezzel az eljárással **E1** és **E4** axióma nem sérülhet. Egyszerűen látható, hogy **E2** is megőrződik, hiszen $(a, b, c) \in E' \Leftrightarrow a, b, c \in I$, s, mivel $(c, b, a) \in E$ ezért $(c, b, a) \in E'$. Az elhagyásra egyedül az **E3** axióma „érzékeny". Be kell látnunk, hogy ha $a, b \in I$, akkor $\exists\, c \in I$, amellyel abc fönnáll. **Lemma (4)** bizonyítása során megmutattuk, hogy adott a és b elemekhez a $kb - (k-1)a$ elem megfelel közrefogó c-nek. De mert $a, b \in I$, ezért $kb - (k-1)a \in I$. □

Illusztrációk Tétel (4)-hez:

— A páros számok (P) ideált alkotnak $\mathbb{Z}$-ben. Ha az **M3** modellt megszorítjuk P-re, ismét elválasztási rendszert ((P, H)) nyerünk.
— Az öttel osztható számok ideált alkotnak a $mod\ 25$ maradékgyűrűben. Ha $R(25, 2)$-t megszorítjuk rájuk, az $R(5, 2)$-vel izomorf* elválasztási rendszert nyerünk.

* Az „*izomorf*" fogalmát l. **Definíció (12)**, 47. o.!

— Az öttel osztható számok ideált alkotnak a $mod\ 35$ maradékgyűrűben. Ha $R(35, 2)$-t megszorítjuk rájuk, az $R(7, 2)$-vel izomorf elválasztási rendszert nyerünk.
— A 11-gyel osztható számok ideált alkotnak a $mod\ 143$ maradékgyűrűben. Ha $R(143, 3)$-at megszorítjuk rájuk, az $R(13, 3)$-mal izomorf elválasztási rendszert nyerünk.

Definíció (9)

Legyen A tetszőleges, nem üres halmaz! Egy $E \subseteq A^3$ relációról azt mondjuk, hogy **zárt elválasztási** reláció, ha

E2 $(a,b,c) \in E \Rightarrow (c,b,a) \in E$ (a szimmetria axiómája)

E3Z $\forall a, b \in A\ \exists c \neq b \in A : (a,b,c) \in E$ (folytatásaxióma)

E4Z $(a,b,c) \in E \ \&\ a \neq b \Rightarrow (b,a,c) \notin E$ (keveredésaxióma)

Hogyha ezt a definíciót **Definíció (1)**-gyel összevetjük, **E1Z**-t hiányolhatjuk.

Épp ezért kimondjuk a következőt:

Korollárium (6)

Ha (A, E) zárt elválasztási rendszer, akkor
— $\forall a \in A\ \exists b \in A : aab$
— $\forall b \in A\ \exists a \in A : abb$
— $aba \Rightarrow b = a$

Bizonyítás:

— a korollárium első állítása következik **E3Z**-ből
— *a második* következik bba-ból és **E2**-ből

— aab-ből **E4Z** miatt következik, hogy aba nem állhat fönn, ha $a \neq b$. □

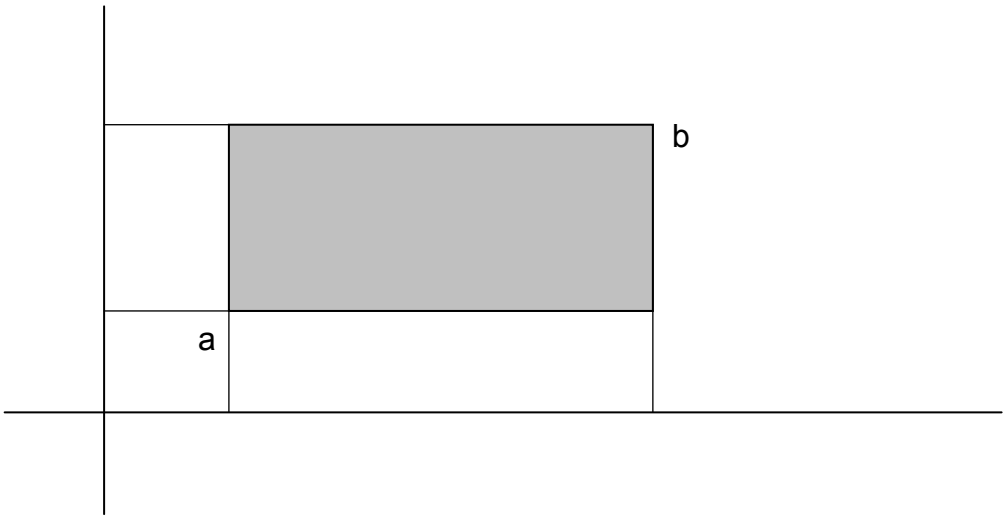
Tétel (5)

Ha (A, E) és (B, F) zárt elválasztási rendszerek, akkor $(A \times B, G)$ zárt elválasztási rendszer a következő definícióval:

$$((a, b), (c, d), (e, f)) \in G \Leftrightarrow (a, c, e) \in E \;\&\; (b, d, f) \in F$$

Bizonyítás nem szükséges, mert az állítás a definícióból nyilvánvaló.

Illusztráció Tétel (5)-höz:



1.2. ábra Az (a, b) intervallum $(A \times B, G)$ zárt elválasztási rendszerben.

Jelölés:

A **Tétel (5)**-ben említett $(A \times B, G)$ zárt elválasztási rendszert $[(A, E) \times (B, F)]$-fel jelöljük.

Tétel (6)

Ha (A, E) és (B, F) nyílt elválasztási rendszerek, akkor $(A \times B, G)$ nyílt elválasztási rendszer a következő definícióval:

$$((a, b), (c, d), (e, f)) \in G \Leftrightarrow a = c = e \;\&\; (b, d, f) \in F \mid b = d = f \;\&\; (a, c, e) \in E \mid (a, c, e) \in E \;\&\; (b, d, f) \in F$$

Bizonyítás:

E1 axióma akkor sérülne, ha $(a, b), (c, d)$ és (e, f) közül bármely kettő azonos lehetne. Ám, ha pl. $(a, b) = (c, d)$, akkor $a = c$, amiből már $a = c = e$ is következik, hiszen G-ben vagyunk. Ám ekkor $(b, d, f) \in F$ miatt b, d és f közül semelyik kettő nem lehet egyenlő. Hasonló a helyzet a második koordinátákkal is.

E2 teljesülése nyilvánvaló a definícióból.

E3 azt követeli meg, hogy $(a, b) \neq (c, d)$-hez lehessen megfelelő (e, f)-et találni. Ha $a = c$, akkor $e := a$, és f-nek válasszunk egy elemet b és d alapján F-ből. Ha $a \neq c$, akkor e-nek válasszunk egy megfelelő elemet E-ből. A másik koordináta kiválasztása analóg.

Végül, ha $((a, b), (c, d), (e, f))$ azért található G-ben, mert $a = c = e$, akkor b, d és f keveredését F kizárja. A második koordináták egyenlősége esetén hasonló a helyzet E-vel. Viszont, ha egyik koordinátán sem egyenlők az elemek, akkor a keveredést E és F külön-külön is és együttvéve is kizárja. □

Jelölés:

A **Tétel (6)**-ban említett $(A \times B, G)$ nyílt elválasztási rendszert $((A, E) \times (B, F))$-fel jelöljük.

Definíció (10)

Ha egy zárt elválasztási rendszer relációjából az aab és az abb alakú elemeket elhagyjuk, annak **nyílt párját** nyerjük; ellenkező irányú hozzávétellel a nyílt reláció **zárt párját** (megfelelőjét) kapjuk.

Példa:

$GF(25)$ a 25-elemű test. Mint korábban tárgyaltuk, $GF(25)$, mint gyűrű $k = 2$ választással elválasztási rendszer a **Lemma (4)** szerinti generálás révén. Ez az elválasztási rendszer nem más, mint $(R(5, 2) \times R(5, 2))$.

Definíció (11)

Legyen (A, E) és (B, F) két elválasztási rendszer, és legyenek $a_0 \in A$ és $b_0 \in B$ kitüntetett elemek. Feltételezhetjük, hogy $A \cap B = \varnothing$, mert, ha nem, szétbetűzzük őket. Az

$$(A \cup B, E \cup F \cup \{(x, y, z), (z, y, x) \mid x \in A, z \in B, y \in A \cup B : xya_0 \mid b_0yz\} \cup \{(x, a_0, z), (x, b_0, z), (z, a_0, x), (z, b_0, x) \mid x \in A \setminus \{a_0\}, z \in B \setminus \{b_0\}\} \cup \{(a_0, b_0, z), (z, b_0, a_0) \mid z \in B \setminus \{b_0\}\} \cup \{(x, a_0, b_0), (b_0, a_0, x) \mid x \in A \setminus \{a_0\}\})$$

rendszert az (A, E) és a (B, F) **zárt áthidalásának** nevezzük. Szavakkal: A zárt áthidalásban **hídfőelemek** szerepelnek. Minden közrefogás, amely a két korábbi rendszerben megvolt, megmarad; a különböző rendszerekből származó elemek közrefogják a saját oldalukon található elemeket a hídfőelemig, a hídfőelemeket, ha ők maguk nem hídfőelemek; egy hídfőelem pedig a másik rendszer elemeivel közrefogja a másik hídfőelemet.

Jelölés:

Az (A, E) és (B, F) alkotta zárt áthidalást $[(A, E)\text{-}(B, F)]$-fel fogjuk jelölni.

Tétel (7)

A zárt áthidalás elválasztási rendszert eredményez.

Bizonyítás:

E1 fennáll, mert az eredeti rendszerekben fennállt, és nem hoztunk létre aba alakú hármasokat a hozzávételnél.

E2 fennáll, mert az eredeti rendszerekben fennállt, és minden hármast szimmetrikusával együtt vettünk föl.

E3-hoz az kell, hogy megoldhatók legyenek az abx alakú "egyenletek". Nyilván csak az $a \in A \ \& \ b \in B$ esetekkel (és a fordítottakkal) merülhet föl ez a kérdés, mert (A, E) és (B, F) eredetileg elválasztási rendszerek voltak. Nos,

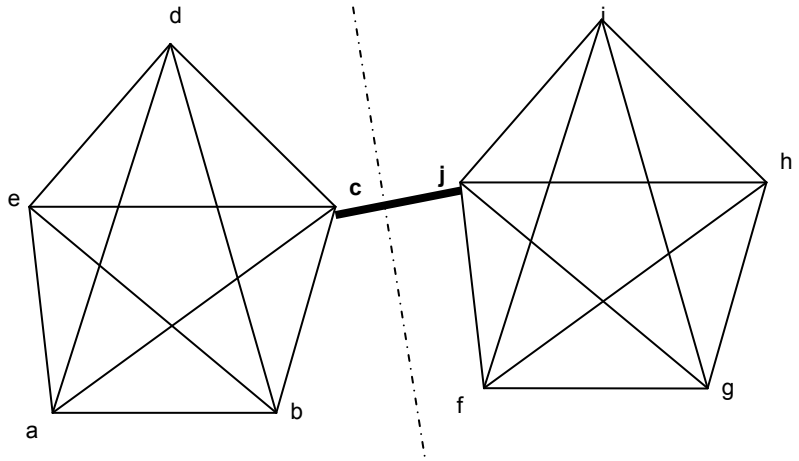
— ha abx-ben $b = b_0$, akkor $\exists\, b_1 \neq b_0 \in B$, és ezzel az elemmel a $b_0 b_1 x$ egyenlet megoldható: legyen egy megoldás b_2. De ab_0b_2 a definíció miatt benne van az áthidalásban;

— ha $b \neq b_0$, akkor a b_0bx megoldható B-ben, legyen egy megoldás c, ekkor a definíció miatt abc.

Az $a \in B \ \& \ b \in A$ eset hasonlóan látható be.

E4 fönnáll, mert az eredeti rendszerekben fönnállt, és nem vettünk hozzájuk olyan hármasokat, amelyek **E4**-et megsérthették volna (kizárólag aa_0b illetve ab_0b alakú hármasok kerültek felvételre, ahol $a \in A$ és $b \in B$. □

Illusztrációképpen bemutatunk egy gráfrészletet $[R(5, 2)\text{-}R(5, 2)]$-ből (**1.3.** ábra):



1.3. ábra

Az ábrán *c* és *j* a hídfőelemek, rajtuk keresztül fut az összes közrefogás *{a, b, c, d, e}* és *{f, g, h, i, j}* részhalmazok között. *[R(5, 2)-R(5, 2)]* reláció-elemszáma 184, ami azt jelenti, hogy az áthidalás jelentősen megnöveli a reláció-elemszámot (az eredeti relációk összesített elemszáma 40).

A példát azért mutattuk be, hogy lássunk véges modellt a Dedekind-féle vágásra. A vágás helyét az ábrán a szaggatott vonal jelzi; a Dedekind-féle "d"-elemek *c* és *j*.

Megjegyzés a Dedekind-féle és a Cantor-féle feltétel viszonyáról

A Dedekind-féle és a Cantor-féle feltételnek semmi közük sincs egymáshoz: bármelyik teljesülhet vagy nem teljesülhet függetlenül a másik teljesülésétől. Ennek szemléltetésére tekintsük az alábbi példákat:

1. *(ℚ, H)* nem teljesíti egyiket sem.
2. *(ℝ, H)* teljesíti mindkettőt.
3. *[R(5, 2)-R(5, 2)]* teljesíti a Dedekind-féle feltételt, de a Cantor-féle feltételt nem.

4. $(\{(1, 2) \cup (3, 4)\}, H)$, ahol $(1, 2)$ és $(3, 4)$ hagyományos értelemben vett nyílt valós intervallumok — teljesíti a Cantor-féle feltételt, de a Dedekind-féle feltételt nem.

További eszközök elválasztási rendszerek generálására

Tétel (8)

Bármely elválasztási rendszer bővíthető egy elemmel.

Bizonyítás:

Legyen (A, E) elválasztási rendszer, és legyen $m \notin A$ egy új elem. Legyen ezenkívül $a \rightarrow a'$ egy A-n értelmezett olyan függvény, amelynek magának, köbének és negyedik hatványának egyaránt nincs fixpontja. (Ilyen függvény mindig létezik, mert a legkisebb elválasztási rendszer ötelemű[*].) Ekkor E-hez a következő hármasokat vesszük hozzá: Álljon fenn $ama', a'ma, maa''$ és $a''am$ minden $a \in A$ esetén. Ekkor

E1 változatlanul fönnáll, mert a függvénynek nincs fixpontja.

E2 és **E3** közvetlenül következik a konstrukcióból.

E4-hez be kell látni, hogy $abc \Rightarrow \neg\, acb$. Nyilván csak azokat az eseteket kell vizsgálni, amikor a, b és c közül valamelyik m. Eszerint:

$mbc \Rightarrow c = b''$; $mcb \Rightarrow b = c''$, e kettőből $c = c''''$, amit kizártunk azzal, hogy a függvény negyedik hatványának nincs fixpontja.

[*] Az állításhoz további bizonyítást nem fűzünk, mert magasabb számosságok esetében is nyilvánvalónak érezzük.

$amc \Rightarrow c = a'$; $acm \Rightarrow mca \Rightarrow a = c''$, e kettőből $c = c'''$, amit kizártunk azzal, hogy a függvény köbének nincs fixpontja.

$abm \Rightarrow mba \Rightarrow a = b''$; $amb \Rightarrow b = a'$, e kettőből $b = b'''$, amit kizártunk azzal, hogy a függvény köbének nincs fixpontja. □

Példák Tétel (8) tételhez:

— $R(5, 2)$ bővítése egy elemmel: Az új elem az 5, a választott függvény A-n a $0 \to 1 \to 2 \to 3 \to 4 \to 0$ hozzárendelés (ennek csak az ötödik hatványa az identitás, az alacsonyabb hatványoknak nincs fixpontjuk), az **M1** modellben bemutatott relációt a következő hármasokkal bővítjük: $051, 152, 253, 354, 450, 502, 513, 524, 530, 542$ és szimmetrikusaik.

— $(\mathbb{Z}, H)$ bővítése egy elemmel: Az új elem az m ($\notin \mathbb{Z}$), a választott függvény az $a \to a + 1$ (semelyik hatványának nincs fixpontja), az új hármasok $am(a + 1)$, $(a + 1)ma$, $ma(a + 2)$ illetve $(a + 2)am$ alakúak.

— $(\mathbb{Q}, H)$ és $(\mathbb{R}, H)$ bővítése egy elemmel ugyanúgy történik, mint $(\mathbb{Z}, H)$-é.

— $(\mathbb{C}, H)$ elválasztási rendszert eddig nem említettük, bár kézenfekvő: $x, y, z \in \mathbb{C}$ komplex számok esetén xyz, ha $\exists\, w \in \mathbb{R} : 0 < |w| < 1 : y = wx + (1 - w)z$. (Érdemes talán közbevetni, hogy w csak valós lehet, nem lehet imaginárius tagot is tartalmazó komplex szám. Ha ugyanis ezt megengednénk, akkor pl. $0, 1$ és $0{,}6 + 0{,}8i$ komplex számokkal $w = 0{,}4 - 0{,}8i$ illetve $w = 0{,}4 + 0{,}8i$ választással a keveredésaxiómába ütköznénk.) Nos, $(\mathbb{C}, H)$ is ugyanazzal a formulával bővíthető, mint $(\mathbb{Z}, H)$.

Korollárium (7)

Tétel (8) következménye: Minden $n > 4$ természetes számhoz létezik n-elemű modell.

Jelölés:

Az (A, E) elválasztási rendszerhez egy elem hozzávételével nyert elválasztási rendszert $(A, E) + 1$-gyel, az ismételt eljárással n elem hozzávételével nyert rendszert $(A, E) + 1^n$-nel fogjuk jelölni. (Az 1^n tehát nem egyenlő 1-gyel, ez csak egy formalizmus.)

Néhány megjegyzés **Tétel (8)**-hoz és következményeihez:

Ha egy függvény negyedik hatványának nincs fixpontja, akkor négyzetének sem lehet.

Ha $(B, F) = (A, E) + 1$ és $|A| < \infty$, akkor $|F| = |E| + 4|A|$. Emiatt az $R(5, 2) + 1$ modell reláció-elemszáma 40, az $R(5, 2) + 1^2$-é pedig 64. Ez nyilván nem lehet izomorf $R(7, 2)$-vel, mert e rendszer reláció-elemszáma 42.

Ha (A, E) véges modell, és $|A| = n$, akkor $|E| \leq n(n-1)(n-2)/3$ (l. **Lemma (1)**). $R(5, 2)$ eszerint „maximális" modell, hiszen relációja 20-elemű, ami a maximum. Ugyanígy $R(5, 2) + 1$ is maximális (40). Ez a helyzet azonban „romlik", tudniillik az n-elemű $R(5, 2) + 1^{n-5}$ modell relációjának elemszáma — amint az pl. teljes indukcióval könnyen belátható — már csak $2n(n-1) - 20$, így a modell „telítettségi aránya" $\frac{6n(n-1)-60}{n(n-1)(n-2)}$, ami nullához tart.

Indokolt **minimálisnak** nevezni (A, E)-t, ha E-ből elem nem hagyható el úgy, hogy (A, E) elválasztási rendszer maradjon. Nyilvánvaló, hogy az $n(n-1)$ reláció-elemszámú modellek minimálisak. $R(5, 2) + 1$, melynek reláció-elemszáma 40, azonban nem az, mert négy hármas elhagyható belőle (párosával elhagyva őket előbb egy 38-elemű relációhoz, majd egy 36-elemű relációhoz jutunk) úgy,

hogy a kapott struktúra elválasztási rendszer marad.

A minimális rendszer fogalma természetesen nem csak véges halmazok felett értelmezhető. $\mathbb{Z}$ felett pl. minimális az **M3** modell (felezőpontok). De $\mathbb{Z}$ felett nem minimális a negyedelőpontokkal alkotott modell, hiszen belőle elhagyással nyerhető **M3**. Érdemes rögzíteni a tényt, hogy k rögzítése mellett a $\mathbb{Z}$ gyűrűből nyerhető modell minimális, ha k prím, és nem minimális, ha nem az.

Értelemszerűen a minimális modell nem minden esetben azonos a **minimális reláció-elemszámú modellel**. ($n = 6$ esetén pl. az elvileg elérhető legkisebb elemszámú reláció 30-elemű, ám 30-elemű relációval rendelkező modell nincs. A legkisebb reláció-elemszámú 6-elemű modell relációjának elemszáma 36.) Tanulmányozandó, hogy a **maximális reláció-elemszámú modell** (MREM) mindig megkonstruálható-e. (Például van-e olyan 7-elemű modell, amelyben a reláció elemszáma 70.) Értelemszerű **maximálisnak** nevezni azt a relációt, amelyhez bármilyen hármast hozzávéve már nem adódik elválasztási rendszer. Ha az MREM nem mindig konstruálható meg, akkor a maximális modell és az MREM nem feltétlenül esik egybe.

Definíció (12)

(A, E) és (B, F) elválasztási rendszerek **izomorfak**, ha $\exists f: A \to B$ bijekció azzal a tulajdonsággal, hogy

$$(a, b, c) \in E \Leftrightarrow (f(a), f(b), f(c)) \in F.$$

Állítás:

Véges izomorf elválasztási rendszerek elemszáma és reláció-elemszáma megegyezik. (Az állítás nyilvánvaló.)

Az „Állítás” megfordítottja nem igaz: vannak olyan véges, egyező elemszámú és reláció-elemszámú modellek, amelyek nem izomorfak. (L. erről a *(GF(25), 2)*-ről és az *R(25, 2)*-ről szóló megjegyzést a(z) 25. oldalon!)

Definíció (13)

Ha *(A, E)* és *(B, F)* elválasztási rendszerek, és $f: A \to B$ függvény olyan, hogy $(a, b, c) \in E \Rightarrow (f(a), f(b), f(c)) \in F$, akkor azt mondjuk, hogy *f* **monoton**.

Jelölés:

Amikor ételemszerű, és nem okoz félreértést, akkor $(a, b, c) \in E \Rightarrow (f(a), f(b), f(c)) \in F$ helyett használhatjuk az egyszerűbb $abc \Rightarrow f(a)f(b)f(c)$ jelölésmódot is.

Megjegyzés és Szóhasználat:

Nyílt elválasztási rendszerek esetében a monoton függvények egyszersmind **szigorúan monoton** függvények, ezért, ha nyílt elválasztási rendszerekről van szó, a jelzőt elhagyjuk. Zárt elválasztási rendszerek monoton leképezései lényegesen eltérhetnek a nyíltakétól. Bármely zárt elválasztási rendszer monoton módon leképezhető pl. az *({a}, {(a, a, a)})* triviális zárt elválasztási rendszerre az $f(x) = a$ függvénnyel. Nyílt elválasztási rendszerekben azonban érvényes a következő

Állítás:

Ha *(A, E)* és *(B, F)* nyílt elválasztási rendszerek, és $f: A \to B$ monoton leképezés, akkor *f* injektív. (Bizo-

nyítás: Tételezzük fel, hogy $\exists\, a,\ b \neq a \in A : f(a) = f(b)$. Ekkor **E3** miatt $\exists\, c \in A : abc$, és, mert f monoton, $f(a)f(b)f(c)$, ami viszont ellentmond **E1**-nek.) Továbbá ha f monoton, akkor $(f(A),\ F)$ elválasztási részrendszer $(B,\ F)$-ben. (Hiszen bármely $x,\ y \neq x \in B$-hez megkereshető az az $a,\ b \neq a \in A,$ amelyekre $f(a) = x$ és $f(b) = y$, ezekhez $\exists\, c \in A : abc$, ezért $(B,\ F)$-ben $xyf(c)$ fennáll.)

Fenti megfontolásainkkal bebizonyítottuk a következőt

Tétel (9)

$(A,\ E)$ és $(B,\ F)$ (nyílt) elválasztási rendszerek akkor és csak akkor izomorfak, ha kölcsönösen monoton módon leképezhetők egymásba (más szóval egymás monoton képei). (A szükségesség nyilvánvaló, az elégségességet most bizonyítottuk.)

Példák:

— $(P,\ H)$ monoton képe $(\mathbb{Z},\ H)$-nak, a leképezés pl. az $f(n) = 2n$, $(\mathbb{Z},\ H)$ monoton képe $(P,\ H)$-nak, a leképezés pl. a $g(n) = n / 2$. $(P,\ H)$ és $(\mathbb{Z},\ H)$ izomorfak.

— $(\mathbb{Z},\ H)$ monoton képe önmagának $(\mathbb{Q},\ H)$-ban, a leképezés pl. az $f(n) = n$, és $(\mathbb{Z},\ H)$ csakugyan részrendszer $(\mathbb{Q},\ H)$-ban. (Megjegyzendő, hogy $(\mathbb{Z},\ H)$ és $(\mathbb{Q},\ H)$ között izomorfizmus nem létesíthető; pl. azért nem, mert $(\mathbb{Z},\ H)$-ban vannak szomszédos elemek, $(\mathbb{Q},\ H)$-ban viszont nincsenek. $(\mathbb{Z},\ H)$ tehát valódi monoton kép $(\mathbb{Q},\ H)$-ban, amellyel nem izomorf.)

— Nem feltétlenül áll fenn, hogy a kölcsönösen monoton képek választott függvényei egymás inverzei. Az első példában pl. $f(n) = 2n + 2$ is állhatott volna, s ekkor $f^{-1} \neq g$, az izomorfizmus ennek ellenére fönnáll.

— **M4** modell és $(\mathbb{Q},\ H)$ nem izomorfak.

— Legyen $A_0 = \mathbb{Z} \times \mathbb{N}^+$. Értelmezzük A_0-on a következő ekvivalenciarelációt: $(a,\ b) \cong (c,\ d) \Leftrightarrow (a,\ b)$

$= n(c, d)$ $(n \in \mathbb{N}^+)$, ahol $n(c, d)$ a vektor szorzása skalárral. Az O ekvivalenciaosztályt reprezentálja (a, b), ha $|(a, b)| \leq |(x, y)| \ \forall (x, y) \in O$; ahol $|(a, b)|$ jelöli a vektor hosszát. A reprezentánsok halmazát jelöljük A-val. Ezután A-ban (a, b) és (c, d) fogja közre (e, f)-et, ha a $\mathbb{Z}^2$ síkon a $(0, 0)(a, b)$ és a $(0, 0)(c, d)$ félegyenes közrefogja $(0, 0)(e, f)$ félegyenest. Jelölje ezt a relációt K. Az így definiált (A, K) elválasztási rendszer, és izomorf $(\mathbb{Q}, H)$-val. Az izomorfizmust a következő monoton leképezés valósítja meg: $(a, b) \rightarrow a / b$.

— Legyen R a **Lemma (4)** szerinti gyűrű, és legyen $q \in R$ nem bal oldali nullosztó, konstans gyűrűelem. Ekkor az $a \rightarrow qa$ $(\forall a \in R)$ leképezés monoton, hiszen valahányszor abc, azaz $(k - i)a + ic = kb$, mindannyiszor $(k - i)qa + iqc = kqb$, azaz $(qa)(qb)(qc)$. Véges gyűrűkben a monoton leképezés (tekintve, hogy q invertálható) egyszersmind izomorfizmus is, vagyis ekkor az $a \rightarrow qa$ leképezés a gyűrűt és ezzel együtt az elválasztási rendszert önmagába viszi. Végtelen gyűrűknek lehet önmagukkal izomorf valódi részhalmazuk, ilyenek a végtelen gyűrűk ideáljai, amilyen P is $\mathbb{Z}$-ben. (Érdekes lehet az az észrevétel, hogy P nem egységelemes gyűrű, P-ben tehát a **Lemma (4)** szerinti eljárást nem lehetne — betű szerint — lefolytatni. De (P, H), mint $(\mathbb{Z}, H)$ monoton képe kézenfekvő módon mégis előáll.)

Definíció (14)

(A, E) és (B, F) elválasztási rendszerek **egyszerű uniója** az $(A \cup B, E \cup F)$ rendszer.

Megjegyzés és Példák:

Elképzelhető, hogy (A, E) és (B, F) elválasztási rendszerek egyszerű uniója maga is elválasztási rendszer. Triviális példa az az eset, amikor egyikük elválasztási részrendszer a másikban, ilyenkor az

unió a másik. Vannak azonban nemtriviális példák is. Így, ha $Z(k)$-val jelöljük a $\mathbb{Z}$ gyűrűből a **Lemma (4)** szerint k rögzítése mellett nyert elválasztási rendszert, akkor minden $Z(k_1) \cup Z(k_2)$ elválasztási rendszer, sőt:

$$\bigcup_{k=2}^{\infty} Z(k) = (\mathbb{Z}, H)$$

Ellenőrzéssel belátható, hogy pl. $R(11, 2) \cup R(11, 3)$ úgyszintén elválasztási rendszer, és gyűrűből generált elválasztási rendszerek esetén igaz a következő

Tétel (10)

Ha (R, E) és (R, F) az R gyűrűből a **Lemma (4)** szerint k_1 illetve k_2 rögzítésével generált elválasztási rendszerek, akkor egyszerű uniójuk akkor és csak akkor elválasztási rendszer, ha $k_1k_2 - ij$ nem bal oldali nullosztó semmilyen $i \in \{1, 2, ..., k_1 - 1\}$ és $j \in \{1, 2, ..., k_2 - 1\}$ esetén. (Speciálisan, ha $R(n, k_1)$, $R(n, k_2)$ elválasztási rendszerek, akkor uniójuk akkor és csak akkor az, ha $k_1k_2 - ij$ relatív prím n-hez minden $i \in \{1, 2, ..., k_1 - 1\}$ és $j \in \{1, 2, ..., k_2 - 1\}$ esetén.)

Bizonyítás:

Az unió műveletére csak a keveredésaxióma érzékeny. Tegyük föl, hogy az unió a keveredésaxiómát megsérti. Ez nyilván csak „keresztbe” képzelhető el, azaz, ha található olyan a, b és c, amelyekre abc $R(n, k_1)$-ben és acb $R(n, k_2)$-ben. (Ugyanabban a rendszerben nem sérülhet a keveredésaxióma, hiszen $R(n, k_i)$, $i = 1, 2$ maguk elválasztási rendszerek.) Vagyis feltételezésünk szerint alkalmas i és j mellett:

$$(k_1 - i)a + ic = k_1b$$
$$(k_2 - j)a + jb = k_2c$$

A **Lemma (4)** bizonyításában használt eljáráshoz hasonló átszorzás, összevonás és rendezés után $(k_1k_2 - ij)(a - c) = 0$ adódik, amiből — mivel $a \neq c$ — annak kellene következnie, hogy $(k_1k_2 - ij)$ bal oldali nullosztó; ám ezt kizártuk. Azaz a keveredésaxióma nem sérülhet. □

Következmények:

— A **Tétel (10)** bizonyítja a $\bigcup_{k=2}^{\infty} Z(k) = (\mathbb{Z}, H)$ formulát is, amelyet az előbb bizonyítás nélkül közöltünk. ($\mathbb{Z}$-ben nincs más nullosztó, csak a 0, és $k_1k_2 - ij$ nem lehet 0, hiszen $i < k_1$ és $j < k_2$.)

— A **Tétel (10)** egy érdekes következménye, hogy ha $R(n, k_1)$ és $R(n, k_2)$ elválasztási rendszerek, és $k_1 + k_2 - Lnko(k_1, k_2) > \frac{n+1}{3}$, akkor $\exists\, i, j : 1 \leq i < k_1,\ 1 \leq j < k_2,\ : Lnko(k_1k_2 - ij, n) > 1$. (Az $Lnko$ függvény a két szám legnagyobb közös osztóját jelenti.) Ez az állítás abból következik, hogy $R(n, k_1) \cup R(n, k_2)$ reláció-elemszáma $n(n - 1)(k_1 + k_2 - Lnko(k_1,k_2) - 1)$, és a reláció-elemszámra vonatkozó fölső becslés miatt $k_1 + k_2 - Lnko(k_1, k_2) \leq \frac{n+1}{3}$ adódik. Ha tehát ez nem teljesül, akkor az unió nem lehet elválasztási rendszer, ám ekkor kell, hogy legyen olyan alkalmas i és j, amellyel $k_1k_2 - ij$ nem relatív prím n-hez[*].

A fenti következmény szerint az alábbi táblázatban megadjuk, hogy az első 100 n-re mely k-kal lehet uniót képezni, azaz, me-

[*] Megjegyezzük, hogy ezt az állítást első ránézésre „nehéz elhinni”. Az embernek az a becslése, hogy $k_1 \approx k_2 \approx n / 6$. Feltételezve, hogy n prímszám, i és j bármilyen kicsi is, $k_1k_2 - ij \approx n^2 / 36$. 36-nál kisebb prímszámok esetén ez várhatóan kisebb, mint n, azaz — várakozásunk szerint — relatív prím n-hez. Az állítás azon feltétele azonban, hogy $R(n, k_1)$ és $R(n, k_2)$ maguk is elválasztási rendszerek, elegendően erős ahhoz, hogy az állítás igaz legyen.

lyek azok a k_1 és k_2 számok, amelyekkel $R(n, k_1) \cup R(n, k_2)$ elválasztási rendszer lesz:

n	A szóba jöhető k_1-k_2 párok
11	2 és 3, 2 és 4
13	2 és 3
17	2 és 3, 2 és 4, 3 és 4
19	2 és 3, 2 és 4, 2 és 6, 3 és 4, 3 és 6
23	2 és 3, 2 és 4, 2 és 6, 3 és 4, 3 és 6
29	2 és 3, 2 és 4, 2 és 5, 2 és 6, 2 és 9, 3 és 4, 3 és 5, 3 és 6, 3 és 9, 4 és 5, 4 és 6
31	2 és 3, 2 és 4, 2 és 5, 2 és 9, 3 és 4, 3 és 5, 3 és 9, 4 és 5
37	2 és 3, 2 és 4, 2 és 5, 2 és 6, 2 és 8, 3 és 4, 3 és 5, 3 és 6, 3 és 8, 4 és 5, 4 és 6, 4 és 8, 5 és 6, 6 és 8
41	2 és 3, 2 és 4, 2 és 5, 2 és 6, 2 és 8, 3 és 4, 3 és 5, 3 és 6, 3 és 8, 4 és 5, 4 és 6, 4 és 8, 5 és 6, 5 és 8
43	2 és 3, 2 és 4, 2 és 5, 2 és 6, 2 és 9, 3 és 4, 3 és 5, 3 és 6, 3 és 9, 4 és 5, 4 és 6, 4 és 9, 5 és 6, 6 és 9
47	2 és 3, 2 és 4, 2 és 5, 2 és 6, 2 és 8, 2 és 9, 3 és 4, 3 és 5, 3 és 6, 3 és 8, 3 és 9, 4 és 5, 4 és 6, 4 és 8, 4 és 9, 5 és 6, 5 és 8, 5 és 9
53	2 és 3, 2 és 4, 2 és 5, 2 és 6, 2 és 7, 2 és 8, 2 és 10, 2 és 12, 3 és 4, 3 és 5, 3 és 6, 3 és 7, 3 és 8, 3 és 10, 3 és 12, 4 és 5, 4 és 6, 4 és 7, 4 és 8, 4 és 10, 4 és 12, 5 és 6, 5 és 7, 5 és 8, 5 és 10, 6 és 7, 6 és 8, 6 és 12, 7 és 10, 7 és 12, 8 és 12
59	2 és 3, 2 és 4, 2 és 5, 2 és 6, 2 és 7, 2 és 9, 2 és 10, 2 és 12, 3 és 4, 3 és 5, 3 és 6, 3 és 7, 3 és 9, 3 és 10, 3 és 12, 4 és 5, 4 és 6, 4 és 7, 4 és 9, 4 és 10, 4 és 12, 5 és 6, 5 és 7, 5 és 9, 5 és 10, 6 és 7, 6 és 9, 6 és 12, 7 és 10, 9 és 10
61	2 és 3, 2 és 4, 2 és 5, 2 és 6, 2 és 7, 2 és 10, 3 és 4, 3 és 5, 3 és 6, 3 és 7, 3 és 10, 4 és 5, 4 és 6, 4 és 7, 4 és 10, 5 és 6, 5 és 7, 5 és 10, 6 és 7, 6 és 10
67	2 és 3, 2 és 4, 2 és 5, 2 és 6, 2 és 7, 2 és 8, 2 és 10, 2 és 14, 3 és 4, 3 és 5, 3 és 6, 3 és 7, 3 és 8, 3 és 10, 3 és 14, 4 és 5, 4 és 6, 4 és 7, 4 és 8, 4 és 10, 4 és 14, 5 és 6, 5 és 7, 5 és 8, 5 és 10, 6 és 7, 6 és 8, 6 és 10, 6 és 14, 7 és 8, 7 és 14, 8 és 10

n	A szóba jöhető k_1-k_2 párok
71	2 és 3, 2 és 4, 2 és 5, 2 és 6, 2 és 7, 2 és 8, 2 és 10, 2 és 16, 3 és 4, 3 és 5, 3 és 6, 3 és 7, 3 és 8, 3 és 10, 3 és 16, 4 és 5, 4 és 6, 4 és 7, 4 és 8, 4 és 10, 4 és 16, 5 és 6, 5 és 7, 5 és 8, 5 és 10, 6 és 7, 6 és 8, 6 és 10, 7 és 8, 7 és 10, 7 és 16, 8 és 16
73	2 és 3, 2 és 4, 2 és 5, 2 és 6, 2 és 7, 2 és 8, 2 és 12, 3 és 4, 3 és 5, 3 és 6, 3 és 7, 3 és 8, 3 és 12, 4 és 5, 4 és 6, 4 és 7, 4 és 8, 4 és 12, 5 és 6, 5 és 7, 5 és 8, 5 és 12, 6 és 7, 6 és 8, 6 és 12, 7 és 8, 8 és 12
79	2 és 3, 2 és 4, 2 és 5, 2 és 6, 2 és 7, 2 és 8, 2 és 12, 2 és 15, 3 és 4, 3 és 5, 3 és 6, 3 és 7, 3 és 8, 3 és 12, 3 és 15, 4 és 5, 4 és 6, 4 és 7, 4 és 8, 4 és 12, 4 és 15, 5 és 6, 5 és 7, 5 és 8, 5 és 12, 5 és 15, 6 és 7, 6 és 8, 6 és 12, 7 és 8, 8 és 12, 8 és 15
83	2 és 3, 2 és 4, 2 és 5, 2 és 6, 2 és 7, 2 és 8, 2 és 9, 2 és 10, 2 és 11, 2 és 12, 2 és 15, 3 és 4, 3 és 5, 3 és 6, 3 és 7, 3 és 8, 3 és 9, 3 és 10, 3 és 11, 3 és 12, 3 és 15, 4 és 5, 4 és 6, 4 és 7, 4 és 8, 4 és 9, 4 és 10, 4 és 11, 4 és 12, 4 és 15, 5 és 6, 5 és 7, 5 és 8, 5 és 9, 5 és 10, 5 és 11, 5 és 12, 5 és 15, 6 és 7, 6 és 8, 6 és 9, 6 és 10, 6 és 11, 6 és 12, 7 és 8, 7 és 9, 7 és 10, 7 és 11, 8 és 9, 8 és 10, 8 és 12, 8 és 15, 10 és 12, 10 és 15, 11 és 15
89	2 és 3, 2 és 4, 2 és 5, 2 és 6, 2 és 7, 2 és 8, 2 és 9, 2 és 10, 2 és 15, 2 és 18, 3 és 4, 3 és 5, 3 és 6, 3 és 7, 3 és 8, 3 és 9, 3 és 10, 3 és 15, 3 és 18, 4 és 5, 4 és 6, 4 és 7, 4 és 8, 4 és 9, 4 és 10, 4 és 15, 4 és 18, 5 és 6, 5 és 7, 5 és 8, 5 és 9, 5 és 10, 5 és 15, 6 és 7, 6 és 8, 6 és 9, 6 és 10, 6 és 18, 7 és 8, 7 és 9, 7 és 10, 7 és 18, 8 és 9, 8 és 10, 8 és 15, 9 és 15, 9 és 18, 10 és 15
97	2 és 3, 2 és 4, 2 és 5, 2 és 6, 2 és 7, 2 és 8, 2 és 9, 2 és 12, 2 és 15, 2 és 16, 3 és 4, 3 és 5, 3 és 6, 3 és 7, 3 és 8, 3 és 9, 3 és 12, 3 és 15, 3 és 16, 4 és 5, 4 és 6, 4 és 7, 4 és 8, 4 és 9, 4 és 12, 4 és 15, 4 és 16, 5 és 6, 5 és 7, 5 és 8, 5 és 9, 5 és 12, 5 és 15, 5 és 16, 6 és 7, 6 és 8, 6 és 9, 6 és 12, 6 és 15, 6 és 16, 7 és 8, 7 és 9, 7 és 12, 8 és 9, 8 és 12, 8 és 15, 8 és 16, 9 és 15, 9 és 16, 12 és 15, 12 és 16

Érdekes lehet az a tény, hogy míg *(ℚ, H) (ℤ, H)*-hoz hasonlóan előállítható megszámlálható számosságú „*k*-as” osztópontos elválasztási rendszer egyesítéseként, *(ℝ, H)* már nem. (Ha ugyanis *p/q, r/s* és *t/u* racionális számok, amelyek a hagyományos érte-

lemben közrefogják egymást, akkor pl. $k = pus - tqs$ és $i = pus - rqu$ választással r/s, mint a p/q és t/u közötti „k-as” osztópont jelenik meg. Ha viszont pl. $1, \sqrt{2}, 2$ valós számokat tekintjük, akkor nem léteznek olyan k és i egészek, amelyekkel $(k - i)1 + i2 = k\sqrt{2}$ lenne.)

Nyílt halmazok

Az alábbi gondolatmenet az elválasztási rendszerek és a topológiák kapcsolatának vizsgálatát célozza:

Definíció (15)

Legyen (A, E) elválasztási rendszer, és legyen $L \subseteq A$. Azt mondjuk, hogy L **gyengén nyílt halmaz** (A, E)-ben, ha $\forall b \in L \; \exists a, c \in L : abc$.

Definíció (16)

Legyen (A, E) elválasztási rendszer, és legyen $W \subseteq A$. Azt mondjuk, hogy W **erősen nyílt halmaz** (A, E)-ben, ha $\forall a, b \neq a \in W \; \exists c \in W : abc$.

Példák:

- Az üres halmaz ($\varnothing$) gyengén nyílt halmaz.
- A gyengén nyílt halmaz (A, E)-ben.
- Ha (B, F) elválasztási részrendszer (A, E)-ben, akkor B gyengén nyílt halmaz (A, E)-ben.
- A fenti megállapítás fordítva nem érvényes: a gyengén nyílt halmazok nem feltétlenül alkotnak elválasztási részrendszert egy elválasztási rendszerben. $\{a, b, c, d\}$ például gyengén nyílt halmaz **M1**-ben, de nem elválasztási részrendszer.
- Az üres halmaz ($\varnothing$) erősen nyílt halmaz.
- Ha $a \in A$, akkor $\{a\}$ erősen nyílt halmaz (A, E)-ben.
- A erősen nyílt halmaz (A, E)-ben.

— Ha (B, F) elválasztási részrendszer (A, E)-ben, akkor B erősen nyílt halmaz (A, E)-ben.
— A fenti megállapítás fordítottja is érvényes: Ha W erősen nyílt halmaz (A, E)-ben, akkor (W, E) elválasztási részrendszer (A, E)-ben. (A bizonyítást az Olvasóra bízzuk.)

Szóhasználat:

Az üres halmazt **triviális gyengén nyílt halmaznak** hívjuk. Az üres halmazt és az egyelemű halmazokat **triviális erősen nyílt halmazoknak** fogjuk nevezni. Látható, hogy a nemtriviális erősen nyílt halmazok egyúttal gyengén nyílt halmazok is.

Jelölés:

Tetszőleges X elválasztási rendszer gyengén nyílt halmazait $\mathcal{L}(X)$-szel, erősen nyílt halmazait $\mathcal{W}(X)$-szel jelöljük. Ha maga az elválasztási rendszer (A, E) alakú a jelölésben, akkor a dupla zárójel helyett csak egyet alkalmazunk, pl.: $\mathcal{L}(A, E)$. A gyengén nyílt halmazok osztálya a definícióból könnyen látható módon zárt az unióra — ezt mondja ki a

Tétel (11)

Legyenek $L_\alpha \in \mathcal{L}(X)$ gyengén nyílt halmazok, úgy, hogy $\alpha \in \mathfrak{I}$ tetszőleges indexhalmaz eleme. Ekkor $\bigcup_{\alpha\in\mathfrak{I}} L_\alpha \in \mathcal{L}(X)$.

Bizonyítás nem szükséges, mert az állítás nyilvánvaló.

Lemmák nyílt halmazokra:

— **L1:** Ha $L \in \mathcal{L}(X)$ nem triviális gyengén nyílt halmaz, akkor $|L| > 3$. (Kevesebb elemmel a keveredésaxiómába ütköznénk.)
— **L2:** Ha $W \in \mathcal{W}(X)$ nem triviális erősen nyílt halmaz, akkor $|W| > 4$. (Lévén, hogy az erősen nyílt halmazok maguk is elválasztási rendszerek.)

— **L3:** Legyen a következőkben (R, E) az R gyűrűből generált (egyik) elválasztási rendszer. Ha $L \in \mathcal{L}(R, E)$, és $L + d := \{x + d \mid x \in L\}$, $d \in R$, akkor $L + d \in \mathcal{L}(R, E)$. (Bizonyítás: (1) Egyértelmű, hogy $|L + d| = |L|$. (2) $b \in L + d \Leftrightarrow b = b' + d : b' \in L \Leftrightarrow \exists\, a', c' \in L : a'b'c' \Leftrightarrow (k - i)a' + ic' = kb'$. Ezért: $a = a' + d$ és $c = c' + d$ mellett $(k - i)(a' + d) + i(c' + d) = (k - i)a' + kd - id + ic' + id = kb' + kd = k(b' + d) = kb$, ami azt jelenti, hogy abc.)
— **L4:** Ha $L \in \mathcal{L}(R, E)$, és $Lp := \{xp \mid x \in L\}$, $p \in R$, úgy, hogy p nem nullosztó R-ben, akkor $Lp \in \mathcal{L}(R, E)$. (Bizonyítás: (1) azért, mert p nem nullosztó; (2) az L-beli egyenlőséget kell p-vel szorozni.)
— **L5-6:** $\mathcal{W}(R, E)$ is invariáns az eltolásra és a nem nullosztóval nyújtásra. (A bizonyítások teljesen hasonlóak, mint **L3-4**-nél.)
— **L7:** Ha I ideál R-ben, akkor I és az I szerinti mellékosztályok elválasztási részrendszerek (R, E)-ben. (**L5-6** és a **Tétel (4)** következménye.) Illusztráció **L7**-hez: A páratlan számok is elválasztási részrendszert alkotnak $(\mathbb{Z}, H)$-ban.

Szemben a gyengén nyíltak esetével, az erősen nyílt halmazok uniója nem feltétlenül erősen nyílt halmaz: Ha $a, b \neq a \in A$, akkor $\{a\}$ és $\{b\}$ erősen nyílt halmazok (A, E)-ben, de $\{a, b\}$ nem az.
Abból, hogy B_1 és B_2 gyengén ileltve erősen nyílt halmazok (A, E)-ben, nem következik, hogy $B_1 \cap B_2$ is gyengén illetve erősen nyílt halmaz (A, E)-ben. Az ellenpéldák a következők: Legyen (A, E) a sík a hagyományos közrefogással, és tekintsünk két egymást metsző, de nem egybeeső egyenest a síkon. Világos, hogy az egyenesek gyengén nyílt halmazok, de metszetük egyelemű, és egyelemű halmaz nem lehet gyengén nyílt halmaz. A másik példa: A legyen ismét a sík, és a és c pontok fogják közre b-t, hogyha az abc háromszögben b-nél tompa szög van.

(Könnyen ellenőrizhető, hogy az így definiált rendszer elválasztási rendszer.) Ebben a rendszerben a (hagyományos értelemben) nyílt félkörök, tehát az olyan félkörívek, amelyekhez az átmérő végpontjai nem tartoznak hozzá erősen nyílt halmazok. Amennyiben két ilyen félkör két pontban metszi egymást, a keletkezett metszet kételemű, ezért nem lehet erősen nyílt halmaz.

Gyengén nyílt halmazok az R(n, k) rendszerekben

Az egyszerűség kedvéért csak a 4-elemű gyengén nyílt halmazok kérdését, és ezen belül azt az esetet vizsgáljuk, amikor a *mod n* maradékgyűrű test (azaz n prímszám).

Legyen a munkahipotézisünk az, hogy rögzítünk egy *(a, b)* párt, és keressük *{a, b, c, d}* gyengén nyílt halmazokat. **Definíció (15)** szerint. Legyen az e szempontok figyelembevételével nyert megoldások száma adott n és k mellett $f_4(n, k)$. Ekkor az *R(n, k)* elválasztási rendszerben található 4-elemű gyengén nyílt halmazok száma:

$$\frac{n(n-1)f_4(n,k)}{4}.$$

Az alábbi táblázatban megadjuk n és k értékeire ($n < 100$), hogy az illető *R(n, k)* elválasztási rendszerben hány 4-elemű gyengén nyílt halmaz van:

n	A szóba jöhető k értékek																
	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
5	5																
11		55	55														
13		39															
17			340														
19			171		855												
23					1265												
29				609	0!			1421									
31				465				1860									
37				666	1665		1998										
41				410	820		820										
43								1806									
47							1081										
53						2067	4134		13780		4823						
59						1711		3422	3422		8555						
61					4575	3660											

n	A szóba jöhető k értékek																
	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
67						2211	11055		0!				15477				
71							2485		2485						22365		
73						2628	6570				18396						
79						3081	3081				9243			18486			
83								17015	0!	3403	3403			44239			
89							9790	23496	0!					23496			52866
97								6984			23280			51216	18624		

A táblázatban szereplő „0!”-ek arra hívják fel a figyelmet, hogy ott az $R(29, 6), R(67, 10), R(83, 10)$ illetve az $R(89, 10)$ elválasztási rendszerek léteznek ugyan, de nincs bennük 4-elemű gyengén nyílt halmaz — ami elég meglepő, mert kisebb és nagyobb k értékek is vannak, amelyekhez találhatók ilyen halmazok. (Egyelőre nem ismerünk zárt formulát az $f_h(n, k)$ kifejezésre; ez adná meg az $R(n, k)$-ban h-elemű gyengén nyílt halmazokra vonatkozó egyenletrendszer megoldásainak számát.)

Annak az esetnek megvilágítására, amikor a $mod\ n$ maradékgyűrű nem test, tekintsük az $R(141, 3)$ elválasztási rendszert. Itt a gyűrűben, 11-gyel osztható számok ideált alkotnak, amely a **Tétel (4)** értelmében elválasztási részrendszer. A faktorgyűrű 11-elemű, amely már test. Az ideál izomorf $R(13, 3)$-mal, melyben 39 négyelemű gyengén nyílt halmaz van. Mivel a gyengén nyílt halmazok osztálya zárt az eltolásra (l. **L3-as lemma** az előző oldalon!), az ideálban és a 10 mellékosztályban összesen $11 \cdot 39$ négyelemű gyengén nyílt halmaz van. Az $R(11, 3)$-mal izomorf ideál felől megközelítve $13 \cdot 55$ adódik. Így $R(141, 3)$-ban összesen $11 \cdot 39 + 13 \cdot 55 = 1144$ négyelemű gyengén nyílt halmaz van. (A példa rávilágít arra, hogy hasonló esetekben hogyan lehet a négyelemű gyengén nyílt halmazok számát meghatározni.)

Egyenesek

Definíció (17)

Legyen (A, E) elválasztási rendszerben $a, b \neq a \in A$ két elem! A már korábban bevezetett intervallum- és félegyenes-jelölést fölhasználva (l. **Definíció (4)** és **Definíció (5)**) definiáljuk

$$k_1(a,b) = \{a,b\} \cup \overrightarrow{ab} \cup (a,b)$$

halmazt valamint

$$k_{n+1}(a,b) = \bigcup_{x,y \in k_n} \overrightarrow{xy} \cup \bigcup_{x,y \in k_n} (x,y)$$

halmazokat. Az

$$e(a,b) = \bigcup_{n=1}^{\infty} k_n(a,b)$$

halmaz neve: az a és b elemek **egyenese**.

Példák

1. Az $R(5, 2)$ elválasztási rendszerben $\overrightarrow{0,1} = \{ 2 \}$, …

2. A $(\mathbb{Z}, H)$ elválasztási rendszerben $\overrightarrow{0,1} = \{ n > 1 \mid n \in \mathbb{Z} \}$, …

3. A $(\mathbb{Z}, H)$ elválasztási rendszerben $\overrightarrow{0,2} = \{ n > 2 \mid n \in \mathbb{Z} \}$, …

4. Az **M4**-es modellben $e((0, 0), (1, 0)) = \{ (n, 0) \mid n \in \mathbb{Z} \}$, …

5. További példa egynél több egyenest tartalmazó elválasztási rendszerre a $GF(25)$-ből, mint gyűrűből a $k = 2$ elemmel a **Lemma (4)** szerint generált elválasztási rendszer. Ebben harminc egyenes van (mert minden ponton 6 egyenes megy át és minden egyenesen 5 pont van, tehát 25 · 6 / 5 = 30 egyenes van). (L. erről kicsit részletesebben [1.8]!)

Az 1. fejezet tézisei

- Az *Eukleidésztől* származó geometriai posztulátumrendszer alapvetően meghatározza a

világról alkotott fogalmainkat. Ezek a posztulátumok a 2300-éves didaktikatörténetben elmélyültek és rögződtek, ezáltal döntően befolyásolják a térről és a **térbeli dolgok elrendeződéséről** kialakított szemléletünket.

- Éppen a megszokás tesz felületessé, az oktatás, a matematikatanítás természetes egyik igénye tehát az kell legyen, hogy megszokott ismereteinket újragondoljuk, illetve a matematikát tanulókkal újragondoltassuk. Ennek a didaktikai célnak a leginkább megfelelő megközelítési mód az **axiomatika**.
- Bolyai korszakalkotó gondolati lépése, a **maradék axiómarendszer** bevezetése teret nyit annak megvilágítására, hogy bizonyos követelmények elhagyásával milyen „új, más világ” tárulhat fel a geometriát tanuló előtt.
- Ebben a fejezetben a Bolyai szabta irányt követve egy tőlünk származó új szempontú (mértékmentes) **axiómarendszert** mutatunk be. Az ebben foglalt axiómák következményeinek néhány rövidebb irányban történt következetes végigvitelével az axiomatikus gondolkodás számára kívánunk stúdiumot teremteni.
- Ennek során bemutatunk eljárásokat az általunk felfektetett axiómarendszernek eleget tevő — **elválasztási rendszernek** nevezett — algebrai struktúra **generálására**, meglevőkből történő **származtatására**.
- Didaktikai szempontból jelentősnek érezzük azokat a modelleket, amelyek megvilágítják a **Pasch–Veblen-axiómarendszer** több axiómájának indokoltságát.
- Az így bevezetett apparátussal vizsgáljuk a **Dedekind**- illetve a **Cantor-féle tulajdonságot**; a Dedekind-féle vágás feltételeinek eleget tevő pontrendszerek esetében kimondunk néhány darabszámra vonatkozó **tételt**.
- Illusztráljuk, hogy a fenti két tulajdonság **független** egymástól.

- A **nyílt** és a **zárt elválasztási rendszer** megkülönböztetésével rámutatunk az axiomatikus tárgyalás didaktikai erejére, az axiómák körében végbevitt csekély változtatás messze ható következményeire.
- Fogalmi elmélyítést szolgál a ponthalmazok nyíltságának vonatkozásában a **gyengén illetve erősen nyílt halmazok** megkülönböztetése. Ezen halmazosztályokat érintően kimondunk néhány **lemmát**.
- A közrefogás fogalmának axiomatizálásával az **intervallum**, a **félegyenes** illetve az **egyenes** fogalmának megragadására nyílik lehetőség. Ezeknek a didaktikai lépéseknek a megtételére nyújtunk példákat. Az irodalomjegyzékben feltüntetett előadásokban és prezentációkban magunk is alkalmaztuk már ezeket a lehetőségeket.

Prímek

Bevezetés a 2. fejezethez

Mottó: *Hán betű van a bibliába?*
Amennyi az ábécébe. [2.1]

Az emberi megismerés, tanulás egyik útja, iránya, megközelítési módszere a dedukció. Deduktív módon gondolkodik az, aki az összetett struktúrák viselkedéséből, megnyilvánulásaiból azok belső összetevőire, építőelemeire kíván következtetni. Nyelvészek állítják, hogy a deduktív gondolkodásmód a kisgyermekkori nyelvtanulás sajátja, és minden bizonnyal jelen van minden tanulási folyamatban. Ebben a fejezetben a matematikai prímfogalom megközelítésén keresztül mutatunk be olyan irányokat, amelyekkel gondolkodásunk eme útvonala demonstrálható, megvilágítható, sőt, reményeink szerint be is gyakoroltatható.

Mindenekelőtt arra irányítjuk a figyelmet, hogy az érintett terület terminológiája korántsem rögzült, az elnevezések, a definíciók váltakoznak, mégpedig oly módon, hogy még az is elképzelhető, hogy fogalmai zavart is okozhatnak. Lássunk néhány példát!

- Nem feltétlenül világos akár még egyetemi hallgatónak sem, hogy a „*prímszám*” és a „*törzsszám*” között mi a különbség, ha van különbség egyáltalán.
- A leggyakrabban elhangzó (sokszor bevallottan felületes) definíció úgy hangzik, hogy prímszám / törzsszám (a továbbiakban maradunk az előbbi elnevezésnél) az, amelynek „*1-en és önmagán kívül nincs más osztója*”. Azt, hogy a szóbanforgó számkör a *természetes számok halmaza*, az előadó általában beleérti a mondanivalóba, de gyakran elmulasztja említeni. Vegyük észre, hogy e szerint a definíció szerint az 1

prímszám[*]. Bizonytalanságot jelenthet ennek a definíciónak az alkalmazása akkor, amikor nincs 1-es (l. páros számok), vagy a hallgató még nincs annak az ismeretnek a birtokában, hogy az 1-es voltaképpen micsoda (ti., hogy *egység-elem*).

- Hogy az 1-et kiküszöbölje, a didaktikai „trükk" a fenti helyett a „*pontosan két osztója van*" fordulat alkalmazását javasolja. Ennek a megoldásnak a következetes továbbvitele az egészszámokra térve a „*pontosan négy osztója van*" definíciót eredményezi. Az osztók számával való „ügyeskedés" reménytelenségét mutatja viszont, hogy például valamely halmaz részhalmazainak esetében, ahol a művelet legyen mondjuk a metszet egy elemnek akár végtelen sok osztója is lehet.
- Tovább bonyolítja a vizsgálatot az a helyzet, amikor valamely elemnek egyáltalán nincs osztója. Valahogyan a műveletekkel kapcsolatos szemléletünk készpénznek veszi, hogy a szorzótábla komplett abban az értelemben, hogy az algebrai struktúra alaphalmazának minden eleme megtalálható benne. Még visszatérünk arra, hogy a páros számok halmazát modellként alkalmazzuk, most csak megemlítjük, hogy ezt a kitűnő és egyszerű terepet az algebra tanítása milyen méltatlanul mellőzi. Jelen esetben ez a halmaz jó példa arra, hogy szorzat csak 4-gyel osztható páros szám lehet, vagyis a 2, 6, 10… stb. páros számok soha nem állnak elő szorzatként.
- Végül didaktikailag indokolatlannak érezzük, hogy a prím / felbonthatatlan fogalmát csak gyűrűkörnyezetben említjük először. A fogalom *jó-*

[*] Megemlítendő, hogy nyomós érvet még nem hallottunk azzal szemben, hogy az 1 prímszám legyen. Az 1 jelenléte nem veszélyezteti az egyértelmű faktorizációt, mint ahogyan a szorzatok tényezőinek esetleges sorrendi különbsége sem: csak egyértelművé kell tenni, hogy két szorzatot mikor tekintünk egyformának. Hagyomány azonban hadakozni az 1-es prím mivolta ellen. Mi igyekszünk egzakt megkülönböztetéssel szolgálni; definiáljuk a *triviális* prímet, és ahhoz a terminológiához tartjuk magunkat, hogy prím az 1-es, csak triviális.

val előbb megjelenik: már a legegyszerűbb algebrai struktúrában (l. lejjebb) tárgyalható.

Tanmese

Ha természetes számok példáján kívánjuk illusztrálni mondanivalónkat, kezdjük azzal, hogy miért összetett szám a 10? A válasz az, hogy a 10 azért összetett szám, mert $10 = 2 \cdot 5$, vagyis a 10 felírható szorzatalakban. Ebben a megvilágításban az összetett szám valamilyen komplex struktúra szerepét játssza, amelynek a belső szerkezetét igyekszünk megismerni, feltárni. Azt feltételezzük, hogy a számok közötti szerkezetépítő „motor" a szorzás, vagyis a kevésbé komplexből a komplexebb felé szorzással haladunk. (Itt megjegyezzük, hogy a legtöbb nyelvben a számnevek képzésében hasonló elv érvényesül, ámbár v.ö.: „négyszáz" ill. „száznégy". E kérdésről kicsit részletesebben tettünk említést [2.2]-ben.)

Azzal tehát, hogy a 10 esetében feltártuk, hogy $2 \cdot 5$, a 10-et, mint komplex struktúrát egyszerűbb építőkövekre bontottuk. Ha úgy tetszik, adtunk egy **magyarázatot** arra a kérdésre, hogy mi a 10.

Ha ez után a 10-ből kinyert építőköveket igyekszünk ugyanilyen analízis alá venni, azt kapjuk például, hogy $5 = 1 \cdot 5$. Az alapvető különbség a 10 analízise és e között az eredmény között az, hogy az 5 „magyarázatában" szerepel maga az 5. A „*miből van a levegő?*" kérdésre értelmes válasz az, hogy „*nitrogénből és oxigénből*", de az nem, hogy „*levegőből és semmi másból*". Magyarán, a probléma az, hogy amikor az 5 komponenseit igyekszünk az 5-ből kikövetkeztetni, minduntalan belebotlunk magába az 5-be. És egy olyan válasz, amely önmagával magyaráz, *érdektelen*. Ezzel szemben a 10 felbontása *érdekes* volt.

> Az *érdektelen felbontás* kifejezést (párhuzamosan használva az *érdekes*, *nem érdekes* kifejezésekkel) *Kiss Emil* alkalmazza [2.3 80. és 82. o.], de nem terminológiai igénnyel. Magyar szakirodalomban nem volna baj, ha az *érdektelen* például

ebben az összefüggésben teret nyerne
az agyonhasznált *triviálissal* szemben.

Tételezzük most fel azt a pedagógiai szituációt, hogy valamelyik hallgató (tanuló) felfedezi, hogy ha a természetes számok körében nem is, de az egészszámok körében az 5-nek igenis adható olyan felbontás, amelyben ő maga nem szerepel, hiszen 5 = (-1) · (-5). Rövid okfejtés útján belátható lesz, hogy a -5 sem újdonság az 5 analízisében. Rávilágíthatunk tehát arra, hogy létezik az egyenlőségnél lazább ekvivalenciareláció, amely úgyszintén érdektelenné teszi a felbontást. Ezzel a módszerrel sort kerít-hetünk az *asszociáltság* fogalmának bevezetésére.

Tanmesénk végén ott tartunk tehát, hogy górcső alá vettük algebrai struktúrák elemeinek a struktúra művelete segítségével más elemekből való előállíthatóságát, és megállapítottuk, hogy lehetnek olyan elemek, amelyek esetében vagy nincs ilyen felbontás, vagy, ha van, akkor csak érdektelen van. Az ilyen elemeket fogjuk — értelemszerűen — *felbonthatatlanoknak* nevezni. Mik lesznek akkor a *prímek*? A kérdés megválaszolása érdekében kezdjük akkor most az alapoknál!

Bonthatóság, asszociáltság

Tekintsünk egy M grupoidot* az egymásmelléírással jelölt művelettel, és definiáljuk M elemei között a következő relációt:

Definíció (18)

$a \angle b \overset{def}{\longleftrightarrow}$ az $ax = b$ egyenlet megoldható (x-re) M-ben

Másképp írva: $a \angle b \overset{def}{\longleftrightarrow} \exists x \in M : ax = b$

* A *grupoid* szót abban az értelemben használjuk, hogy adva van egy (nem üres) *M* halmaz, és rajta egy $M \times M \to M$ művelet. Újabban más szerzők erre a fogalomra a *magma* szót is alkalmazzák. Mi nem követjük ezt a terminológiát, ám a *G* betűt továbbra is fönntartjuk a *csoportnak*, s helyette választottuk (utalva a *magma* megnevezésre) az *M*-et.

Az $a \angle b$-t így olvassuk: „á (balról) **bontja** bét — vagy á (bal oldali) **bontója** bének — vagy bé (balról) **bontható** ával”.

A jobb oldali bontást értelemszerűen az $xa = b$ egyenlet megoldhatósága fogja jelenteni. Ha a szükség megkívánja, a bontás $\angle$ jelét B illetve J betűvel indexeljük így: $\angle_B$, $\angle_J$.

A *bontás* szóval (az *osztás* helyett) azt akarjuk hangsúlyozni, hogy az *oszthatóság* majd a *bonthatóság* egy speciális esete lesz, amikor a hagyományos értelemben használjuk. A *bontás* abszolút tág fogalom: ezért az új név.

Vizsgáljunk most egy grupoidot, amelynek alaphalmaza az $\{a, b, c\}$ halmaz, szorzását pedig az alábbi Cayley-tábla definiálja!

	a	**b**	**c**
a	a	b	b
b	b	b	c
c	c	c	a

Az M01 grupoid Cayley-táblája

Tekintve, hogy a grupoid nem kommutatív, meg fogjuk különböztetni a bal- és jobb oldali bontást. A két bontási reláció képe az alábbi:

	a	**b**	**c**
a			
b			
c			

Az M01 grupoid balról bontási relációjának képe

	a	**b**	**c**
a			
b			
c			

Az M01 grupoid jobbról bontási relációjának képe

A relációk ábrájából leolvasható pl., hogy a balról bontás az alábbi képhalmazokat hozza létre:

$$B_B(a) = \{a, b\},\ B_B(b) = \{b, c\} \text{ és } B_B(c) = \{a, c\}.$$

Definíció (19)

Ha B bontási reláció M-en, akkor egy $m \in M$ elemhez tartozó $B(m) = \{x \mid m \angle x\}$ halmazt m **bontási tartományának** nevezzük.

Ha analógiát keresünk a könnyebb megjegyzés érdekében, azt mondhatjuk, hogy $B(m)$ az m *többszöröseit* tartalmazza, vagy azt, hogy $B(m)$ az m által generált *főideál*. (Ezek a szavak természetesen ***csak analógiák***!)

Ha a fenti bontási relációkat vizsgáljuk, azt látjuk, hogy (véletlenül) reflexívek, a balról bontás (szintén véletlenül) még antiszimmetrikus is, de más közismert relációtulajdonsággal nem rendelkeznek. Így például nem tranzitívek, hiszen például $a \angle_B b$ és $b \angle_B c$, de $a \angle_B c$ nem áll fenn. Könnyen belátható azonban, hogy

Tétel (12)

Asszociatív grupoidban (félcsoportban) a bontás reláció tranzitív.

Bizonyítás: (balról bontást írva) $a \angle b \;\&\; b \angle c \Rightarrow \exists x: ax = b \;\&\; \exists y: by = c \Rightarrow (ax)y = c \Leftrightarrow a(xy) = c \Rightarrow a \angle c$. □

Vegyünk egy félcsoportot, és vizsgáljuk meg bontási relációit!

	a	**b**	**c**
a	a	b	c
b	a	b	c
c	c	c	c

Az M02 félcsoport Cayley-táblája

A két bontási reláció képe a következő:

	a	**b**	**c**
a			
b			
c			

Az M02 félcsoport balról bontási (B_B) relációjának képe

	a	**b**	**c**
a			
b			
c			

Az M02 félcsoport jobbról bontási (B_J) relációjának képe

Ezek tranzitív relációk. Van egy intuitív elvárásunk, hogy a bontásnak (az oszthatósághoz hasonlóan) parciális rendezésnek kellene lennie. Mi a helyzet akkor a reflexivitással illetve a szimmetriaellenességgel*?

Ehhez először tekintsük bármely R reláció tükörképét, az $R^T := \{(x, y) \mid (y, x) \in R\}$ relációt. Esetünkben ezek az alábbi ábra szerint alakulnak:

	a	b	c
a			
b			
c			

Az M02 félcsoport balról bontási (B_B) relációjának B_B^T tükörképe

	a	b	c
a			
b			
c			

Az M02 félcsoport jobbról bontási (B_J) relációjának B_J^T tükörképe

Amennyiben elkészítjük egy R relációhoz a belőle származtatott $R \cap R^T$ relációt, előszöris nyilvánvalóan *szimmetrikus* relációt fogunk kapni. Mielőtt továbblépnénk, vegyük szemügyre ezeket:

	a	b	c
a			
b			
c			

Az M02 félcsoport balról bontási (B_B) relációjának $B_B \cap B_B^T$ származtatottja

	a	b	c
a			
b			
c			

Az M02 félcsoport jobbról bontási (B_J) relációjának $B_J \cap B_J^T$ származtatottja

Ezek a relációábrák tehát azokat az elempárokat mutatják, amelyeknek elemei kölcsönösen bontják egymást. E relációk szimmetrikusak és tranzitívak. Áttekintjük, mi a helyzet a *reflexivitással*.

Amennyiben R tranzitív volt, úgy $S := R \cap R^T$ is tranzitív lesz; szimmetria az előállítás következménye. (Ennek bizonyítását számos tankönyv bemutatja.) Annyit kell most hozzátennünk, hogy tranzitív és szimmetrikus relációk csak izolált elemeikre nézve *nem reflexívek*. Nevezetesen, ha $\exists\, b: aSb,$ akkor $bSa,$ és innen $aSa.$ Tehát ha egy a elemnek van nem üres képe (ősképe) S-ben, akkor S az a-ra nézve reflexív lesz. A **Definíció (19)**-ben definiált bontási tartomány viszont egyetlen elemre nézve sem lehet üres. Szem-

* Ezt a szót azért használjuk, hogy az antiszimmetriát és az aszimmetriát egyszerre lefedjük vele.

léletesen ezt úgy ragadhatjuk meg, hogy egy Cayley-tábla minden sorában van elem. Így csak az fordulhat elő, hogy lehetnek a grupoidban olyan elemek, amelyek egyetlen bontási tartományban sincsenek benne. Például:

	a	**b**	**c**
a	a	b	a
b	b	a	b
c	a	b	a

Az M03 félcsoport Cayley-táblája

	a	**b**	**c**
a			
b			
c			

Az M03 félcsoport bontási (B) relációjának képe

	a	b	c
a			
b			
c			

Az M03 félcsoport bontási relációjának és annak tükörképének B ∩ B^T metszete

Mielőtt rátérnénk az **M03** félcsoport relációinak vizsgálatára, a fenti gondolatmenet nyomán bevezetünk egy fogalmat:

Definíció (20)

A tranzitív és szimmetrikus relációkat **majdnem-ekvivalenciarelációknak** fogjuk nevezni.

M03 félcsoport kommutatív, ennélfogva a bal és jobb oldali bontás nem különbözik. Elvégezve a fent bemutatott származtatást B relációból olyan relációt kapunk, amely tranzitív és szimmetrikus, de nem reflexív. A reflexivitásnak ez a hiánya viszont abból ered, hogy c izolált elem a relációban. c izoláltsága abból következik, hogy c nem szerepel a Cayley-táblában, azaz c nem áll elő szorzatként. (Ez, ahogy említettük, nemcsak véges, hanem végtelen félcsoportnál is előfordulhat, l. a páros számok példáját a szorzással.) Vagyis az **M03** félcsoport B bontási relációjából származtatott $B \cap B^T$ reláció majdnem-ekvivalenciareláció.

Ezt a most bevezetett majdnem-ekvivalenciát fogjuk *asszoci-áltságnak* nevezni.

Definíció (21)

Legyen $\angle$ egy grupoid bontási relációja. Ekkor az

$$a \cong b \xleftrightarrow{def} a \angle b \,\&\, b \angle a$$

relációt **asszociáltságnak** nevezzük.

Az $a \cong b$ jelsorozatot így olvassuk: „á és b **asszociáltak**” vagy „á **asszociáltja** bének”.

Szükség esetén az asszociáltság reláció-jelét is indexeljük B vagy J betűvel, így: $\cong_B$, $\cong_J$.

Összefoglalva; eddigi fejtegetésünkből az alábbi megállapításokhoz jutottunk:

Korollárium (8)

A **Definíció (18)** szerint minden grupoidon értelmezhető *bontási reláció* (B). E relációnak van bal és jobb oldali definíciója, amelyek, ha a grupoid nem kommutatív, eltérnek.

Korollárium (9)

Ahogyan azt **Tétel (12)**-ben kimondtuk (68. o.), ha a grupoid félcsoport, akkor B *tranzitív*.

Korollárium (10)

Minden grupoid felett származtatható annak bontási relációjából, B-ből az $A := B \cap B^T$ — úgynevezett *asszociáltsági reláció*. Ennek is lehet bal és jobb oldali értelmezése.

Definíció (22)

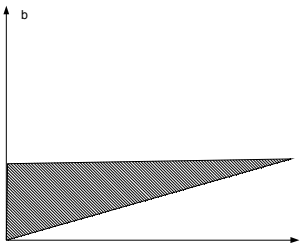
Amennyiben B tranzitív, úgy A *majdnem-ekvivalenciareláció* lesz, ami alatt azt kell érteni, hogy az ekvivalenciaosztályokból csak az izolált elemek maradnak ki. (Az így keletkezett osztályokat később **asszociált osztályoknak** nevezzük. Amikor egy elemhez kapcsolódását kívánjuk hangsúlyozni, akkor **asszociáltsági tartományt** fogunk mondani, és egy $m \in M$ elem esetében az $A(m)$ jelölést fogjuk használni.)

Megjegyezzük, hogy az asszociativitás csak elégséges, de nem feltétlenül szükséges feltétele a bontás tranzitivitásának. Az alábbi példák ezt illusztrálják:

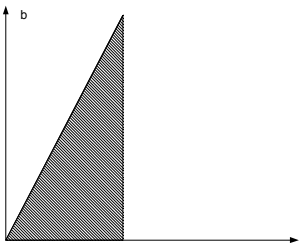
Példák:

1. Legyen ***M04*** = $\mathbb{N}$ (a természetes számok halmaza) és a művelet legyen a hatványozás. Amint az közismert, a struktúra nem asszociatív, a (balról) bontás mégis tranzitív. Tudniillik az $a \angle_B b$ bontás feltétele az, hogy a (hatvány)*alapja* legyen b-nek. Ez tranzitív, hiszen, ha a alapja b-nek és b alapja c-nek, akkor léteznek olyan i és j természetes számok, amelyekkel $a^i = b \;\&\; b^j = c \Rightarrow (a^i)^j = c \Rightarrow a^{ij} = c$ — vagyis a alapja c-nek is.
   Itt megjegyezzük, hogy az ebben a példában a jobbról bontás *nem* tranzitív.

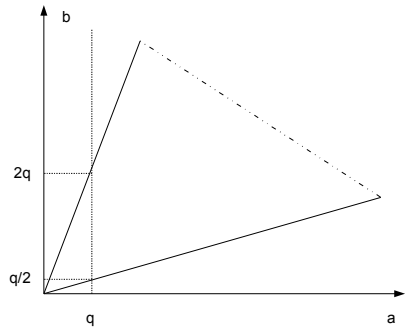
2. Legyen ***M05*** = $\mathbb{Q}^{+0}$ (a nemnegatív racionális számok halmaza) és a művelet legyen a számtani közép. Szintén könnyen ellenőrizhető, hogy bár a művelet nem asszociatív, a bontás az. Ehhez belátjuk, hogy $a \angle b$ szükséges és elégséges feltétele az $a \leq 2b$ feltétel. A reláció képe tehát az alábbi:



2.1. ábra M05 grupoid bontási relációja (B)



2.2. ábra M05 grupoid bontási relációjának tükörképe (B^T)



2.3. ábra M05 grupoid asszociáltsági relációja ($A = B \cap B^T$)

Az asszociáltsági reláció képéről leolvasható, hogy minden $q \in \mathbb{Q}^{+0}$ esetében $A(q) = [0{,}5q;\ 2q]$ zárt intervallum.

További példák:

- ***M06*** **=** $(\mathbb{N},+)$ — a természetes számok halmaza az összeadással. A struktúra kommutatív egységelemes félcsoport. A bontás a *kisebb vagy egyenlő* reláció; az asszociáltság az *egyenlőség*, minden természetes szám a saját egyelemű asszociált osztályában van egyedül.
- ***M07*** **=** $(\mathbb{N},\cdot)$ — a természetes számok halmaza a szorzással. A struktúra kommutatív egységelemes félcsoport. A bontás az *oszthatóság*; az asszociáltság az *egyenlőség*.
- ***M08*** **=** $(\mathbb{Z},+)$ — az egészszámok halmaza az összeadással. A struktúra csoport. A bontás és vele együtt az asszociáltság a *teljes* $\mathbb{Z} \times \mathbb{Z}$ reláció; egyetlen asszociált osztály az egész $\mathbb{Z}$.
  Ennél a példánál rámutatunk arra, hogy csoportban minden elem bont minden elemet, így áll elő a mondott helyzet; *csoportban a bontási vizsgálatok érdektelenek*.
- ***M09*** **=** $(\mathbb{Z},\cdot)$ — az egészszámok halmaza a szorzással. A struktúra kommutatív egységelemes félcsoport. A bontás az *oszthatóság*; az asszociáltság az *abszolút értékre vett egyenlőség*. Az asszociált osztályok a $\{0\}, \{1, -1\}, \{2, -2\}, \{3, -3\}, \ldots$
- ***M10*** **=** $(2^H,\cup)$ — egy H alaphalmaz részhalmazai az unióval. A struktúra kommutatív egységelemes fél-

csoport. A bontás a *halmaztartalmazás* ($\subseteq$) abban az értelemben, hogy $A \angle B \Leftrightarrow A \subseteq B$; az asszociáltság az *egyenlőség*.

- ***M11*** **=** $(2^H, \cap)$ — egy H alaphalmaz részhalmazai a metszettel. A struktúra kommutatív egységelemes félcsoport. A bontás a *halmaztartalmazás* ($\supseteq$) abban az értelemben, hogy $A \angle B \Leftrightarrow A \supseteq B$; az asszociáltság az *egyenlőség*.
- ***M12*** **=** $(V^*,)$ — egy V ábécé (véges) sorozatai a konkatenációval. A struktúra (nem kommutatív) egységelemes félcsoport. A bontás a „*kezdőszeletének lenni*” reláció (p jelsorozat bontja q jelsorozatot, pontosan akkor, ha p kezdőszelete q-nak); az asszociáltság az *egyenlőség*.
- ***M13*** **=** $\mathbb{Z}$ (az egészszámok halmaza) és a műveletet definiáljuk úgy, hogy $ab = min(a, b)+1$. A struktúra nem asszociatív, a bontás feltétele pedig: $a \geq b - 1$. ($min(a, x)+1 = b$ pontosan akkor oldható meg x-re, ha $a \geq b - 1$.) Ez a reláció viszont *nem tranzitív*. Itt megjegyezzük, hogy a nagyon hasonló ***M14*** **=** $(\mathbb{Z}, max(.,.)+1)$ grupoid bontási relációja a „nagyobb” (>) reláció, amely tranzitív, jóllehet az alapstruktúra itt sem volt asszociatív. A bontás szigorú irreflexivitása miatt asszociáltak nincsenek. (Az asszociáltsági reláció üres. Felhívjuk rá a figyelmet, hogy az üres reláció is majdnem-ekvivalencia.)

Prímek, felbonthatatlanok

Azonnal a definícióval kezdjük, majd rátérünk annak különböző szempontú tárgyalására. A definíció nem fog meglepetést okozni:

Definíció (23)

M grupoidban a $p \in M$ elemet **prímnek** nevezzük, ha $\forall a, b \in M$:
$p \angle ab \Rightarrow (p \angle a \vee p \angle b)$.

Megjegyezzük, hogy amennyiben szükséges a bontás bal vagy jobb oldali megkülönböztetése, úgy ennek megfelelően

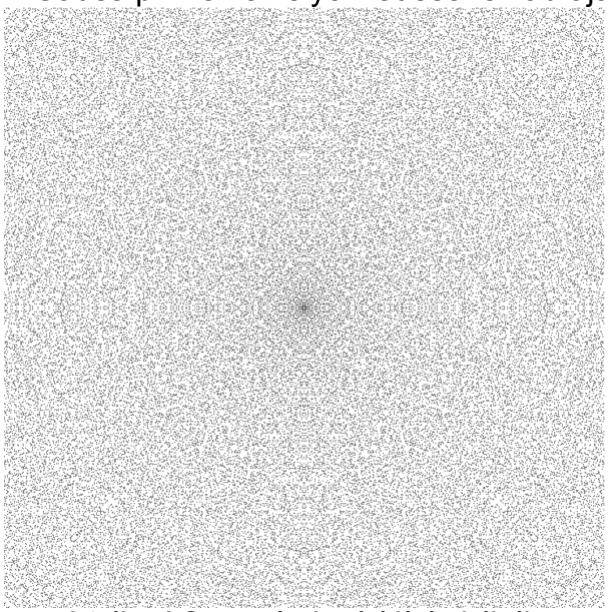
meg fogunk különböztetni *bal* és *jobb oldali prímeket*.

Ez a definíció teljes összhangban van az oszthatósággal kapcsolatosan bevezetett prímfogalommal. Mielőtt rátérnénk a definíció további tárgyalására, vegyük szemügyre, hogy eddigi példáinkban ez a definíció milyen eredményre vezet!

Eszerint:

- **M01**-ben (67. o.) bal oldali prímek csak a b és a c, jobb oldali prím viszont a grupoid mindhárom eleme. Kérdés, miért *nem* bal oldali prím az a elem? A válasz az, hogy jóllehet $a \angle a$ és $a = c \cdot c$, mégsem áll fenn, hogy $a \angle c$. Vagyis a úgy bont egy szorzatot, hogy annak egyik tényezőjét sem bontja.
- Az **M02** (68. o.) félcsoport mindhárom eleme prím.
- Az **M03** (70. o.) félcsoportban nincs prím.
- Az **M04** példában (természetes számok a hatványozással) a bal oldali prímek a 0 és a nemhatvány természetes számok, azaz 2, 3, 5, 6, 7, 10, 11, 12 stb. (Ennek végiggondolására érdemes külön gyakorlatot szentelni, mert a 0 és az 1 helyzetének kiértékelése jól elmélyíti a fogalmat.)
- **M05**-ben (nemnegatív racionális számok a számtani középpel) minden elem prím.
- **M06**: (Természetes számok az összeadással.) Prímek a 0 és az 1.
- **M07**: (Természetes számok a szorzással.) Prímek a 0, az 1 és a hagyományos értelemben vett prímek.
- **M08**: (Egészszámok az összeadással.) A struktúra csoport, tehát minden elem prím.
- **M09**: (Egészszámok a szorzással.) Prímek a 0, a ± 1 valamint a hagyományos értelemben vett pozitív prímek és ellentettjeik.
- **M10**: (Részhalmazok az unióval.) Prímek: az üreshalmaz és az egyelemű halmazok. Célszerű lesz éppezért ezeket a halmazokat *prímhalmazoknak* nevezni.

- **M11**: (Részhalmazok a metszettel.) Prímek: a H és az egyelemű halmazok komplementerei.
- **M12**: (Jelsorozatok a konkatenációval.) Prímek a λ és az egy „betűből” álló jelsorozatok.
- **M13**: (Egészszámok a $min(a,b)+1$-gyel.) Minden elem prím.
- **M14**: (Egészszámok a $max(a,b)+1$-gyel.) Minden elem prím.
- A prímek további tanulmányozása érdekében érdemes megvizsgálni a Gauss-egészeket, a kvaternió-egészeket* és az $a + bsi$ alakú „egészeket” (ahol s olyan irracionális, amelyre s^2 egész, i pedig a $\sqrt{-1}$ komplex egység). Figyelemreméltó lesz didaktikai szempontból a prímek és a felbonthatatlanok viszonyának alakulása (l.81. o.!). (Ezekről a modellekről már tettünk említést [2.4]-ben.) A Gauss-prímek ábrázolása esztétikai szempontból is érdekes. A Gauss-prímek elhelyezkedésének ábrája:



2.4. ábra A Gauss-prímek szóródásának ábrája
(Forrás: http://en.wikipedia.org/wiki/File:Gauss-primes-768x768.png)

Most vegyük még egyszer szemügyre a **Definíció (23)**-ban felállított formulát:

* Más néven Lipschitz-egészeket

$$p \angle ab \Rightarrow (p \angle a \vee p \angle b)$$

Eszerint p és a *szorzat viszonyáról* következtetünk vissza p-nek és a szorzat *komponenseinek viszonyára*. Ha a szorzat *valamilyen*, akkor valamelyik komponens is *ugyanolyan*. Ez a minőség, amelyről ebben a mondatban szó van azzal a tulajdonsággal rendelkezik, hogy ***másmilyenből szorzás útján nem lesz olyan***. Konkrétabban: az a tulajdonság, hogy „valakit" p bontani képes a grupoid szorzása útján nem születik a semmiből, valamelyik komponenstől „örökölnie" kellett a szorzatnak ezt a tulajdonságot.

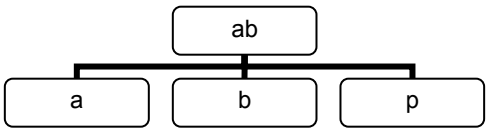
Újabb átfogalmazással (és ezt akár tekinthetjük a prímfogalom alternatív definíciójának):

Definíció (24) **Prím az, akinek a bontási tartományának a komplementere zárt.**

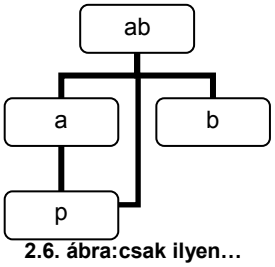
A fenti könnyen memorizálható mondat formálisan:

> M grupoidban a Definíció **(18)** szerint bevezetett bontási relációra nézve a Definíció **(19)**-ben definiált B jelölést alkalmazva $p \in M$ elemet prímnek nevezzük, ha az M-beli komplexusszorzásra fennáll a $\overline{B(p)}\,\overline{B(p)} \subseteq \overline{B(p)}$ tartalmazás.

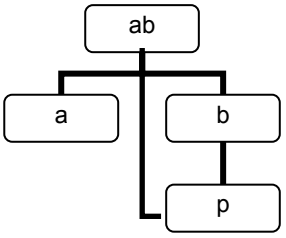
Most képzeljük el, hogy a bontási relációt egy gráfban *fölfelé haladó* élekkel reprezentáljuk. Ekkor a prímtulajdonság azt jelenti, hogy



2.5. ábra: ilyen helyzet nincs,…



2.6. ábra: csak ilyen…



2.7. ábra: vagy ilyen.

A fölfelé haladással való ábrázolás — didaktikai szempontból indokolhatóan — ugyanazt a képzetet erősíti meg, mint amelyet a bontás jelének kiválasztásával igyekeztünk elérni, azzal tudniillik, hogy e relációjel a „kisebb”-re (<) emlékeztessen*. Ebben az összefüggésben tehát azt mondhatjuk, hogy ha a prím *alatta van* egy szorzatnak, akkor alatta van valamely tényezőjének is, így nem közvetlenül, hanem a szorzat valamelyik tényezőjén keresztül, tranzitíve éri el alulról a szorzatot. A prím a bontási gráfban ezért valamilyen értelemben fundamentális szerepet játszik.

Most vegyük elő még egyszer a prímdefiníciót —

$$p \angle ab \Rightarrow (p \angle a \vee p \angle b)$$

—, és vegyük szemügyre *formai* szempontból! Eszerint ez a formula egy

$$p \mathcal{R} ab \Rightarrow (p \mathcal{R} a \vee p \mathcal{R} b)$$

alakzat, ahol $\mathcal{R}$ egy teljesen általános reláció. Most megfogalmazandó didaktikai javaslatunk az, hogy ezt a sémát alkalmazzuk a felbonthatatlanság esetében is. Vagyis

Definíció (25)

> M grupoidban az $f \in M$ elemet **felbonthatatlannak** nevezzük, ha $\forall a, b \in M : f \cong ab \Rightarrow (f \cong a \vee f \cong b)$.

* Ide tartozik, hogy ugyancsak didaktikailag éppen ezért nem szerencsés az oszthatóság hagyományos függőleges vonal (|) alakú jele: azért, mert ez a jel szimmetrikus, miáltal nem sugallja a bontásban rejlő antiszimmetriát.

Megjegyezzük, hogy amennyiben szükséges a felbonthatatlanság bal vagy jobb oldali megkülönböztetése, úgy ennek megfelelően meg fogunk különböztetni *bal* és *jobb oldali felbonthatatlanokat*.

Amint látható, a két definíció gyakorlatilag betű szerint megegyezik, a relációjel kivételével. Hasonló a helyzet az átfogalmazással is:

Definíció (26) **Felbonthatatlan az, akinek az asszociáltsági tartományának a komplementere zárt.**

A formalizálás ezután:

M grupoidban a **Definíció (19)** szerint bevezetett bontási relációra nézve a **Definíció (22)**-ben definiált A jelölést alkalmazva $f \in M$ elemet felbonthatatlannak nevezzük, ha az M-beli komplexusszorzásra fennáll az $\overline{A(p)}\,\overline{A(p)} \subseteq \overline{A(p)}$ tartalmazás.

Figyelembe véve, hogy

$$A(m) \subseteq B(m) \text{ és ennélfogva } \overline{B(m)} \subseteq \overline{A(m)}$$

a prímek és a felbonthatatlanok közötti kapcsolat tanulmányozásakor további intuitív megközelítésre nyerünk lehetőséget. (L. 81. o. és k.!)

A trivialitás megragadása

Most tekintsük újból a prímtulajdonság illetve a felbonthatatlanság definiálására választott

$$m\ \mathcal{R}ab \Rightarrow (m\ \mathcal{R}a \vee m\ \mathcal{R}b)$$

sémát! Amint látható, ez egy P premisszából és egy Q konklúzióból álló $P \Rightarrow Q$ alakú implikáció. Mint ismeretes, egy ilyen implikáció triviálisan igaz, amikor

— a P hamis vagy amikor
— a Q igaz.

Mindkét esetben azt fogjuk mondani, hogy m-nek vagy a prím- vagy a felbonthatatlan tulajdonsága *triviálisan* teljesül, ha akár a premissza (a-tól és b-től függetlenül) tautologikusan hamis, akár a konklúzió tautologikusan igaz.

Hogyan következhet be ez a trivialitás a prímtulajdonságra illetve a felbonthatatlanságra vonatkozó definíció esetében?

1. Lehet-e a premissza tautologikusan hamis a prímdefinícióban? Előfordulhat-e az, hogy az M grupoidnak egy $m \in M$ eleme nem bont semmilyen szorzatot? A válasz az, hogy ez nem lehetséges. Irányítsuk a figyelmet M képzeletbeli Cayley-táblájára! (Ez képzeletben akkor is megtehető, amikor M végtelen halmaz.) Lehet ebben az m sora üres? Nem. Lehet, hogy ami benne van, az nem szorzat? Nem: ha mással nem, az m-mel előáll szorzatként, épp azért van ott[*]. Azt látjuk tehát, hogy egy prím nem lehet triviális prím azért, mert a prímdefiníció premisszája hamis.
2. Lehet-e ugyanakkor a prímdefinícióban a konklúzió tautologikusan igaz? Hogyne! Könnyen elképzelhető, és sok példa is van rá, hogy egy grupoidban egy elem „mindenkit” bont. Az *univerzális bontók automatikusan prímek*. Bal oldali egységelemek például univerzális bontók a balról bontás szempontjából, tehát, mint ilyenek triviális prímek. De lehetnek M-ben más univerzális bontók is. Mint emlékszünk, csoportban minden elem minden elemet bont; épp ezért a csoport minden eleme triviális prím.
3. Más a helyzet a felbonthatatlanokkal. Ha a felbonthatatlanságot definiáló implikációt szemügyre vesszük, látjuk, hogy a premissza is lehet tautologikusan hamis. Mint láttuk, az asszociáltság csak majdnem-ekvivalenciareláció, azaz lehetnek a grupoidnak az asszociált osztályokon kívül eső — izo-

[*] Az elmondottak a balról bontásra vonatkoznak. Jobbról bontás vizsgálatakor oszlopra kell hivatkozni.

lált — elemei. Ezek az elemek nem asszociáltjai senkinek. (Ez a helyzet többféleképpen előadódhat, de a legegyszerűbb úgy elképzelni, hogy az illető elem nem áll elő szorzatként. Gondoljunk a páros számok halmazára a szorzással. Szorzat csak 4-gyel osztható szám lehet, így a 2, 6 stb. páros számok, jóllehet elemei a félcsoportnak, nem lehetnek asszociáltjai senkinek.) Az asszociáltságra nézve *izolált elemek* tehát *triviálisan felbonthatatlanok*.

4. S végül lehetséges-e, hogy egy elem mindenkinek az asszociáltja legyen a grupoidban? Igen lehetséges. Egy ilyen esetben egyetlen asszociált osztály az egész grupoid, mindenki mindenkit bont, s emiatt mindenki mindenkinek asszociáltja is. Éppen a ***kvázicsoportok*** azok az algebrai struktúrák, amelyek ezt a feltételt teljesítik. Eszerint egy kvázicsoport minden eleme triviálisan felbonthatatlan (és persze, triviális prím).

Bennünket érdemben a fenti felsorolás 2. és 3. pontja fog érinteni; célszerű tehát azt megjegyezni, hogy

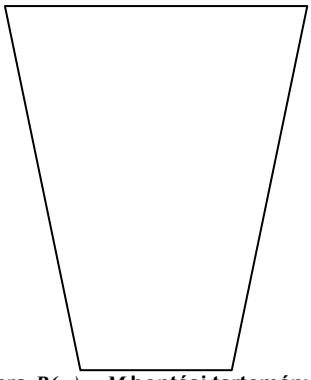
Definíció (27)

az univerzális bontók **triviális prímek**, az asszociáltság izoláltjai pedig **triviális felbonthatatlanok**.

Prímek és felbonthatatlanok viszonya

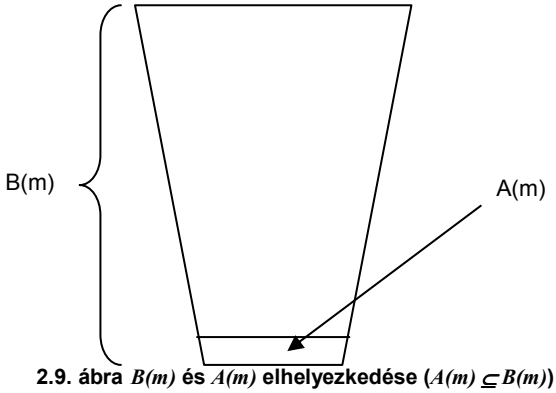
A prímek felbonthatatlanságáról

Mondanivalónk illusztrálása kedvéért tételezzük fel, hogy egy M grupoidban egy m elem $B(m)$ bontási tartománya olyan, mint egy vödör:



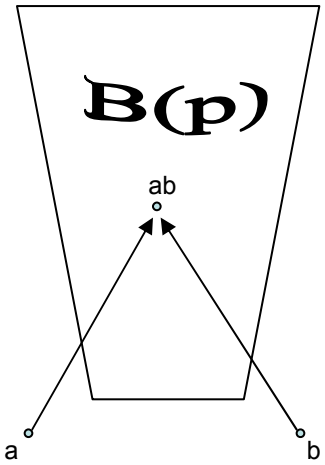
2.8. ábra $B(m) \subset M$ bontási tartomány képe

Ennek a vödörnek van egy kis víz az alján: az az asszociáltsági tartomány:



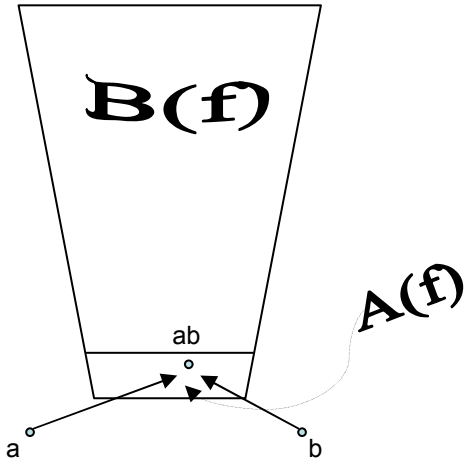
2.9. ábra $B(m)$ és $A(m)$ elhelyezkedése ($A(m) \subseteq B(m)$)

Most ábrázoljuk az M-beli szorzást úgy, hogy nyilak vezessenek a szorzandóktól a szorzat felé. Ha p prím, akkor bontási tartományának ($B(p)$-nek) komplementere zárt, tehát nincs olyan helyzet, mint amilyet az alábbi rajz ábrázol:



2.10. ábra A prím tilalmi helyzete.
Ilyen eset nincs:
Ha a vödör = B(p), akkor két nyíl a vödrön kívülről nem vezethet a vödörbe

A felbonthatatlanság viszont az alábbi helyzetet tiltja:



2.11. ábra A felbonthatatlan tilalmi helyzete.
Ilyen eset nincs:
Ha a vödör alján levő víz = A(f), akkor két nyíl a vízen kívülről nem vezethet a vízbe

Az eddigiek alapján azt gondolhatnánk, egyszerű dolgunk van: ha a két feltételt és a két ábrát szemrevételezzük, azt a következtetést vonhatjuk le, hogy ha két nyíl nem vezethet kívülről a vödörbe, akkor annál kevésbé a vödörben levő vízbe, ***tehát a prímek felbonthatatlanok***.

Ez a sugallat, bár később látni fogjuk nem teljesen helyes, mégiscsak *nagyon jó intuíció*. Ha hozzávesszük azt a képzetet is, hogy a szorzás nyilai valamiképpen mindig *fölfelé* haladnak, akkor a meglátás egyenesen helyes is. Éppen azért választottuk ezt a vödrös-vizes interpretációt, mert nagyon jó képzetet teremt a fogalmak megragadására. Hogy alátámasszuk a most mondottakat, kimondunk egy egyszerű tételt a prímek felbonthatatlanságáról. Látni fogjuk, hogy nem túl szigorú feltétel mellett a prímek felbonthatatlansága már igenis garantálva van.

Tételünkhöz szükségünk lesz egy lemmára; a benne kimondott tény alapvető, és más megfontolások során is igen jó hasznát vesszük, ezért külön lemmaként közöljük.

Lemma (5)

Ha $p \in M$ a tetszőleges M grupoid (bármilyen oldali) prímje, akkor
$p \angle p$.

Bizonyítás: A bontás definíciójából következik, hogy $p \angle pp$. De mivel p prím, ezért $p \angle p$. □

Tétel (13)

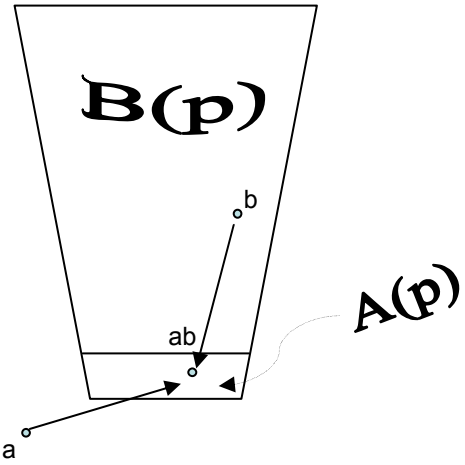
Kommutatív grupoidban a prímek felbonthatatlanok.

Bizonyítás: Legyen $p \in M$ az egyébként tetszőleges kommutatív M grupoid prímje, s álljon fenn, hogy $p = ab$. Ekkor egyszersmind $p = ba$. Maga a $p = ab$ illetve $p = ba$ egyenlőség azt jelenti, hogy $a \angle p$ illetve $b \angle p$. Tudjuk ugyanakkor, hogy $p \angle p$, azaz $p \angle ab$. Lévén, hogy p prím, így vagy $p \angle a$ vagy $p \angle b$ fennáll. Álljon fenn pl. $p \angle a$. Ez $a \angle p$-vel egybevetve $a \cong p$-t eredményezi, ami azt jelenti, hogy p felbonthatatlan. Ha viszont $p \angle b$ áll fenn, akkor $b \cong p$-t kapjuk. □

Felhívjuk a figyelmet arra, hogy ez a levezetés bizonyítja például azt, hogy a Gauss-egészek vagy bármilyen más értelmezésű kommutatív számkonstrukci-

ók[♣] prímjei felbonthatatlanok — teszi ezt minden további apparátus nélkül, kizárólag arra támaszkodva, hogy ezek szorzása kommutatív.

Természetesen felvetődhet a kérdés, hogy az asszociativitás (azaz ***félcsoport***) garantálja-e hasonlóképpen, hogy a prímek felbonthatatlanok legyenek. A válasz *nemleges*. De mielőtt cáfolati példát adnánk, tegyünk egy meggondolást: Hogyan is festene egy félcsoportban egy felbontható prím „vizesvödre”?



2.12. ábra **Felbontható prím ábrája**

Vegyük észre, hogy ha p felbontható prím, akkor olyan ab szorzatot kell találni, amelyre

- ab a vízben van (azaz ab legyen asszociáltja p-nek[*])
- nem lehet a is b is a vödrön kívül (hiszen akkor ab is a vödrön kívül lenne, azaz nem lehetne a vízben)

Itt bemutatott ábránkon a b tényező van a vödörben.

Figyelem! a félcsoport **Tétel (13)** szerint biztosan nem kommutatív, vagyis nem mindegy, hogy az a vagy a b tényezőt rajzoljuk-e a vödörbe. Emlékeztetünk arra,

[♣] Pl. szürreális számok.

[*] Mint emlékszünk **Definíció (26)** szerint (l. 79. o.!) nem feltétlenül szükséges, hogy *magának* p-nek adjunk felbontást, elegendő, ha p valamely asszociáltjának adunk (l. ezt bővebben: 96. o.!).

hogy *bal oldali* bontásról beszélünk. Érdemes megfontolni, hogy ha az a tényező lenne a vödörben (vagy esetleg ő *is* a vödörben lenne) tehát, ha a bal oldali operandus benne lenne a bontási tartományban, akkor az hová esne a rajzon. A megfontolás eredménye az, hogy a bal oldali operandus nemcsak a vödörbe, hanem azon belül rögtön a vízbe is belekényszerülne (szükségképpen asszociáltja lenne p-nek), s mint ilyen, már nem alkalmas a felbonthatatlanság cáfolatára. Tehát a most megadott rajz az egyetlen lehetséges olyan szituációt mutatja, amelyen felbontható prím látható.

A vödörben található tényező (példánkban a b) a vödörben van ugyan, de nincs a vízben! Eszerint ***b a víz fölött van***, miközben ***ab*** a vízben (***a víz „alatt”***). Ez pedig azt jelenti, hogy a szorzás (legalábbis a $b \to ab$ vonatkozásában) ebben az esetben ***„lefelé” hat***. A szorzásnak az ilyen irányú hatása: hogy tudniillik a bontási tartományból visszafelé, az asszociáltak közé visz — csakugyan ritka, és matematikai intuíciónknak is ellentmond. És valóban, „rendes” körülmények között, az általánosan használt algebrai struktúrákban a prímeket felbonthatatlannak találjuk. *Didaktikai szempontból alapvetőnek érezzük annak hangsúlyozását, hogy felbontható prím csak „szokatlan” körülmények között jelenhet meg.*

Eme előzmények után bemutatjuk azt a félcsoportot, amely tartalmaz felbontható prímeket. A félcsoport alaphalmaza a természetes számok párjaiból álló $\mathbb{N} \times \mathbb{N}$ halmaz, a szorzást pedig a következőképpen definiáljuk:

$$(n_1, k_1)(n_2, k_2) := (n_1 + (n_2 \dot{-} k_1), k_2 + (k_1 \dot{-} n_2))$$

A definícióban szereplő műveleti jel a „pont-mínusz”, melynek jelentése

$$n \dot{-} k = \begin{cases} n - k & ha\ n \geq k \\ 0 & különben \end{cases}$$

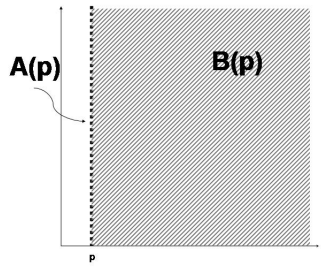
Hogy az így definiált algebrai struktúra egységelemes félcsoport, azt bemutattuk [2.5]-ben*.

Definíció (19) szerint (a, b) balról bontja (c, d)-t, ha található olyan (x, y), amellyel $(a, b)(x, y) = (c, d)$. A szorzás definíciójára nézve láthatjuk, hogy ehhez $c \geq a$ szükséges feltétel. Belátjuk, hogy ez elégséges is. Ha ugyanis $c \geq a$, akkor az $(x, y) = (b + c - a, d)$ választás megfelel. Tudniillik: $(a, b)(b + c - a, d) = (a + b + c - a - b, d + 0) = (c, d)$.

Asszociáltak tehát pontosan azok az (a, b), (c, d) párok, amelyekre $a = c$. Más szóval az asszociált osztályok az $\mathbb{N} \times \mathbb{N}$ függőlegesen egymás alatt álló rácspontjai.

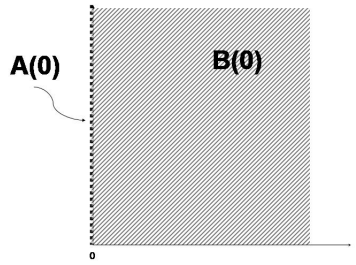
> Analóg módon: a *jobbról* bontás szükséges és elégséges feltétele, hogy $d \geq b$ legyen, és így az asszociált osztályok a rács vízszintesei. Ez utóbbi elrendezés különösen emlékeztet a vödrös-vizes interpretációra. A félsík a bontási tartomány, a félsíkot határoló (egyébként a félsíkhoz tartozó) egyenes pedig benne a víz. A balról bontást tanulmányozva fekvő vödröt látunk, a bontási tartomány jobbra esik az asszociáltsági tartományt jelentő függőleges egyenestől. A jobbról bontás vizsgálata ilyen szempontból szerencsésebb, mert ebben az esetben szó szerint vízszintesen helyezkedik el az asszociáltsági tartomány (azaz a „víz"). Az alábbi ábrán (*didaktikatörténeti* okból) most mégis a *balról* bontás helyzetét tüntetjük fel.

* A művelet a végtelen sorozatokat balra illetve jobbra toló operátorok modellezéséből jött létre. Ezeknek az operátoroknak az a sajátosságuk, hogy a jobbra csúsztatók „visszacsinálhatók", a balra csúsztatók viszont nem (kipotyognak a sorozatelemek). Ennek következtében a félcsoport jobb- és bal oldali egységei eltérnek; s ez a tulajdonság döntőnek bizonyult a felbontható prímeket tartalmazó példa megkonstruálásakor. Hangsúlyozzuk, hogy bár a szóbanforgó operátorok említése a matematikai irodalomban megtalálható, s ezek a források rámutatnak a jobb- és bal oldali egységekből képzett részfélcsoportok kvázidiszjunkt voltára (metszetük egyedül az egységelem), a természetes számpárokkal történő implementálás, és a felbontható prím céljára való felhasználás ötlete teljes egészében tőlünk származik.



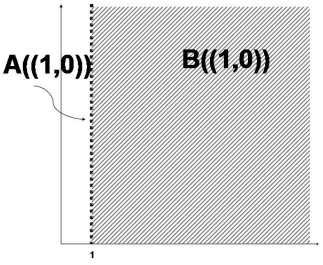
2.13. ábra ***A(p)*** **és** ***B(p)*** **elhelyezkedése** $\mathbb{N} \times \mathbb{N}$**-ben. Pontozott rácspontok a félsík bal szélén:** ***p*** **asszociáltsági tartománya; sraffozott rácspontok:** ***p*** **bontási tartománya**

Most számbavesszük a prímeket.



2.14. ábra **A** ***(0,0)*** **asszociáltjai és bontási tartománya**

Amint az ábráról látható, *a (0, 0)* univerzális bontó, bontási tartományának komplementere üres, tehát ***a (0, 0) triviális prím***.



2.15. ábra **Az** ***(1,0)*** **asszociáltjai és bontási tartománya**

Az *(1, 0)* bontási tartományának komplementere már nem üres: a *(0, n)* alakúakat tartalmazza. A *(0, n)*-alakúak viszont zárt komplexust alkotnak $\mathbb{N} \times \mathbb{N}$-ben: amint könnyen ellenőrizhető: $(0, n)(0, k) = (0, n+k)$. Tehát ***(1, 0)***, lévén, hogy a bontási tartományának a komplementere zárt, prím, s mivel e komplementer úgy zárt, hogy nem üres, ezért ***nemtriviális prím***.

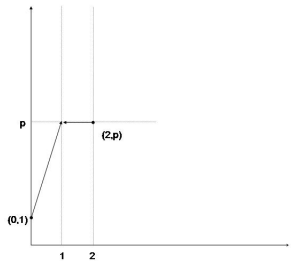
Természetesen ugyanígy nemtriviális prímek az *(1, 0)* asszociáltjai, az *(1, p)* alakú párok.

Tekintsük tehát az *(1, p)* alakú prímeket! Adunk rájuk egy felbontást:

$$(1, p) = (0, 1)(2, p)$$

Ebben a felbontásban sem *(0, 1)*, sem *(2, p)* nem asszociáltja *(1, p)*-nek, hiszen — emlékszünk —, asszociáltak azok, amelyeknek első koordinátájuk megegyezik. A szorzattá alakítás tehát *nem érdektelen*. *(1, p)* ezekszerint felbontható.

Figyeljük meg a bontás elhelyezkedését:



2.16. ábra *(1,p) = (0,1)(2,p)*

Emlékezzünk arra, hogy most egy *fekvő* „vödröt” látunk. (Ez azért van, mert *balról* bontást, *bal oldali* prímeket és felbonthatatlanokat tanulmányoztuk. A *jobbról* bontásnak *álló* vödrei vannak.) A vödör a pozitív abszcisszájú rácspontok halmaza. A víz a vödör fenekén az 1 abszcisszájú pontok halmaza, ők *(1, p)* asszociáltjai. A *(0, 1)* a vödrön kívüli szorzótényező a vödör alatt. Ő a szorzás bal oldali operandusa (a). A *(2, p)* a vödörben, de nem a vízben levő faktor. Ő a szorzás jobb oldali komponense (b). Pontosan úgy, ahogyan a „**Felbontható prím ábrájá**”-n láttuk a 85. oldalon.

Rámutatunk arra, hogy az *(1, p) = (0, 1)(2, p)* felbontásban *(0, 1)* egység. Ez azt illusztrálja, hogy ***nem az tesz érdektelenné egy felbontást, ha a szorzat egyik operandusa egység, hanem az, ha a szorzat egyik operandusa asszociált a szorzattal***. A „felbonthatatlan” fogalmának megalkotásakor annál is inkább érde-

mes az asszociáltakra, semmint az egységekre támaszkodni, mert így olyan struktúrákban is érvényesíteni tudjuk a definíciót, amelyekben *nincs egység*. E tekintetben [2.3. 83. o.] szóhasználatát követjük. Kiss Emil egyébként a felbontást érdektelennek nevezi akkor is, amikor az egyik tényező egység, természetesen „szokásos" gyűrű környezetben[*].

Fenti modellünk lehetőséget ad egy figyelemreméltó következtetésre. Ismeretes, hogy a kvaterniók szorzása *nem kommutatív*. Ennélfogva a **Tétel (13)** nem alkalmazható a Lipschitz-egészek esetében. (Így nevezzük az $a+bi+cj+dk$ alakú kvaterniókat, ahol $a, b, c, d \in \mathbb{Z}$.) Ennek ellenére kimondható

Tétel (14)

A Lipschitz-egészek körében a prímek felbonthatatlanok.

Bizonyítás: A bizonyítás a Lipschitz-egészek normanégyzetére[*] és annak multiplikativitására támaszkodik. Amint az az irodalomban számos helyen megtalálható, $\xi = a+bi+cj+dk$ Lipschitz-egész $N(\xi)$ normanégyzete az $a^2+b^2+c^2+d^2$ természetes szám. Látható az is, hogy $N(\xi)$ pontosan akkor 0, amikor $\xi = 0$. Végül a multiplikativitás azt jelenti, hogy $N(\xi\zeta) = N(\xi)N(\zeta)$. Ennek ismeretében állíthatjuk, hogy a szorzásnak olyan „visszanyúlása" a vödörből a vízbe, mint amilyennel az iménti példában találkoztunk nem képzelhető el. A normanégyzet multiplikativitása ugyanis garantálja, hogy az asszociáltaknak egyenlő legyen a normanégyzete. (Kölcsönösen bontják egymást: a bontást jelentő szorzásokra a normanégyzeteket felírva az egyenlőség adódik.) Tekintsünk tehát egy π Lipschitz-prímet! A $B(\pi)$ bontási tartományban, az $A(\pi)$ asszociáltsági tartományon kívül csak olyan Lipschitz-egészek lesznek találhatók, amelyeknek a normanégyzete *nagyobb*, mint π-é. Ezeket *bármilyen* nem zérus Lipschitz-egésszel szorozva (mely-

[*] Kiss az egységelemes integritási tartományt nevezi szokásos gyűrűnek [2.3. 48. o.].

[*] A „normanégyzet" szóhasználatról v. ö.: ** lábjegyzet a 107. oldalon!

nek normanégyzete ugyebár legalább 1) *nem kaphatunk* olyan szorzatot, amely $A(\pi)$-be esne. □

Figyeljük meg, hogy a bizonyítás logikája „a szorzás mindig nyújt" alapgondolatra támaszkodik. Egy Lipschitz-egész nyolcadmagával (asszociáltjaival) ül egy szférán (hipergömbön), melynek sugara az ő normája. Amint megszorozzuk őt egy másik nem zérus Lipschitz-egésszel, a szorzat csakis a tényezők szféráin kívülre, az origótól távolabbra kerülhet — azt mondhatjuk, hogy „semmilyen szorzás nem hoz vissza". Ez a tény önmagában elegendő a prímek felbonthatatlanságának igazolására.

A felbonthatatlanok prímtulajdonságáról

Ha visszatekintünk „**A prím tilalmi helyzete**" (83. o.) illetve „**A felbonthatatlan tilalmi helyzete**" c. ábrákra (83. o.), látjuk, hogy ha az ab szorzatot szimbolizáló pont a vödörben van, de a víz fölött, akkor csak a prím tilalma sérül, a felbonthatatlanságé nem, vagyis könnyen lehet, hogy egy „szorzótáblában" (értsd: egy grupoidban) lesznek olyan felbonthatatlanok, amelyek nem prímek.

Az algebratankönyvek lényegében az $\{(a, b) \mid a, b \in \mathbb{Z}\}$ alakú párok felett az $(a, b)(c, d) = (ac + kbd, ad + bc)$ szorzással definiált egységelemes félcsoportot veszik alapul. Ezekről a modellekről — és arról, hogy mit reprezentálnak — részletesebben szóltunk [2.6]-ban. Ott ráirányítottuk a figyelmet, hogy negatív k értékek mellett aránylag egyszerű analízis adható, és $k < -1$ esetén nem prím felbonthatatlanok lépnek fel. [2.7. 104. o.] a $k = -5$ és [2.8. 121. o.] a $k = -3$ esetben mutat példát nem prím felbonthatatlanra.

A félcsoportok körében egyszerű példákkal szolgálni. Például:

	0	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	3	3	1
2	0	4	0	2	0
3	0	1	0	3	0
4	0	4	2	2	4

M16 félcsoport Cayley-táblája

M16 félcsoportban 0 zéruselem, 2 kétoldali prím, 3 jobb oldali prím, 4 bal oldali prím. A prímek felbonthatatlanok, de **felbonthatatlan az 1 is, jóllehet nem prím** (bontja $2 \cdot 2$-t anélkül, hogy bontaná 2-t). Ráadásul a felbonthatatlanság minden esetben kétoldali. Az egyedüli felbontható elem a 0. Felhívjuk a figyelmet, hogy nincs univerzális bontó, vagyis egyik prím sem triviális; ugyanígy, mert nincs izolált elem, egyik felbonthatatlanság sem triviális.

Fontos látni, hogy amennyiben nem ragaszkodunk a gyűrűkörnyezethez, félcsoportban egyszerű véges példa máris adható. A bontás, az asszociáltság, a prím, a felbonthatatlan — ezek a fogalmak már a grupoidok körében is kifogástalanul definiálhatók. Azért indokolt mégis a félcsoportot választani terepnek, mert az asszociativitás nagyon mély elvárás, és az oktatómunkában csak fennakadást okozna, ha a kifejezéseket elborítanák a zárójelek. Azonkívül a nemasszociatív írásmódra való koncentrálás elvonná a figyelmet a lényegtől. A félcsoport ezenkívül biztosítja a bontás tranzitivitását, amely szintén nagyon kézenfekvő elvárás. Folyománya továbbá, hogy az asszociált osztályok (az izoláltak kivételével) csakugyan osztályozni fogják az elemeket. Ezeken kívül azonban további engedmény nem szükséges.

Mint fentebb említettük, a páros számok halmaza a szorzással kiváló félcsoport számtalan megfontolandó jelenség tanulmányozása céljára. Válasszuk a $|^P$ szimbólumot az „osztható a párosban” reláció jelölésére! Ezekszerint pl.

$$2 \,|^P\, 6 \cdot 10$$

hiszen $2 \cdot 30 = 6 \cdot 10$. Ugyanakkor se $2 \,|^P\, 6$ se $2 \,|^P\, 10$ nem áll fenn, hiszen nincsenek olyan páros számok, amelyekkel a 2-t megszo-

rozva akár 6-ot, akár 10-et kapnánk. 2 tehát a párosban ***nem prím***. Nyilvánvaló ugyanakkor, hogy felbonthatatlan, méghozzá triviálisan, hiszen nem áll elő szorzatként. Lehet mondani, hogy az ***M16*** véges félcsoport Cayley-táblájának kezelése túlságosan elvont matematikai hozzáállást igényel, de a páros számos példát egy általános iskolás is megérti.

További didaktikai lehetőségek

Idézzük fel relációsémánkat a 78. oldalról! A prímtulajdonság illetve a felbonthatatlanság definiáló tulajdonsága egy

$$\forall a, b \in M : c \mathcal{R} ab \Rightarrow (c \mathcal{R} a \vee c \mathcal{R} b)$$

logikai kifejezésben öltött testet. Ennek a formulának a és b a szabad változói, és maga a formula éppen c-ről mond valamit. (Amikor $\mathcal{R} = \angle$, akkor azt, hogy c prím, amikor $\mathcal{R} = \cong$, akkor azt, hogy c felbonthatatlan.) Úgy lehetne összefoglalni a formula jelentését, hogy a szorzat — c-re vonatkoztatott — viselkedéséből következtetünk a tényezők viselkedésére. Azt fogjuk vizsgálni, hogy — ellenkező irányban — a tényezők viselkedéséből lehet-e a szorzat viselkedésére következtetni. Mielőtt azonban a tartalmi jelentésre térnénk, fontoljuk meg: tisztán logikailag, formálisan hogyan lehet ezt az implikációt az ellenkező irányban olvasni. Arra jutunk, hogy egyenértékű a

$$\forall a, b \in M : \left(\overline{c \mathcal{R} a} \,\&\, \overline{c \mathcal{R} b}\right) \Rightarrow \overline{c \mathcal{R} ab}$$

formulával. Ez pedig olvasható $\forall a, b \in M : (c \mathcal{S} a \,\&\, c \mathcal{S} b) \Rightarrow c \mathcal{S} ab$ olvasatban, hiszen ehhez nem kell egyéb, mint $\mathcal{S}$-t $\mathcal{R}$ ellentettjének tekinteni.

Ez a formáció egyébként ésszerű is, és feltételezhető, hogy a hallgatóság ezt is várja. Míg a szorzat valamely tulajdonságából következtetünk (legalább) ***az egyik*** szorzótényező ugyanolyan tulajdonságára, addig ***mindkét*** tényező valamilyen viselkedéséből remélünk következtetni a szorzat azonos viselkedésére.

Tegyünk egy próbát, írjuk be S helyére ismert relációinkat (tekintve, hogy $\cong$ szimmetrikus reláció, a vele képzett sort csak egyszer szerepeltetjük):

$$\forall a, b \in M : (c \angle a \,\&\, c \angle b) \Rightarrow c \angle ab$$

$$\forall a, b \in M : (a \angle c \,\&\, b \angle c) \Rightarrow ab \angle c$$

$$\forall a, b \in M : (c \cong a \,\&\, c \cong b) \Rightarrow c \cong ab$$

Az első és a harmadik trivialitásnak tűnik — c-re nézve ezért nem mond semmit. A második viszont rendkívül szokatlan lenne: nem felel meg semmilyen intuitív elvárásunknak.

Ám lehetséges, hogy a formulával nem is c-ről kellene mondani valamit! Hanem a és b ***viszonyáról***. Lehet, hogy így majd mond is valamit a dolog.

$$\forall c \in M : (c \angle a \,\&\, c \angle b) \Rightarrow c \angle ab$$

$$\forall c \in M : (a \angle c \,\&\, b \angle c) \Rightarrow ab \angle c$$

$$\forall c \in M : (c \cong a \,\&\, c \cong b) \Rightarrow c \cong ab$$

A formula első változata ebben a formában is semmitmondó. A harmadik sor azt mondja, hogy a és b asszociált osztályainak metszete a szorzat asszociáltjaiba esik: $A(a) \cap A(b) \subseteq A(ab)$. Ez az állítás vagy triviális, vagy használhatatlanul erős követelmény. Már a félcsoportkörnyezet garantálja, hogy az asszociált osztályok diszjunktak legyenek. Ennélfogva vagy az a helyzet, hogy $A(a) = A(b)$, vagy az, hogy $A(a) \cap A(b) = \varnothing$. Utóbbi esetben az állított tartalmazás nem mellbevágó közlés, az előbbi esetben viszont a formula mondanivalója az, hogy az asszociált osztályok zártak a szorzásra. Ez azért szokatlan lenne. Mondjuk példaképpen az egészszámok szorzása esetében $\{5, -5\}$ egy asszociált osztály. Nem várjuk el, hogy pl. az $5 \cdot (-5)$ szorzat ide essen…

Hanem a

$$\forall c \in M : (a \angle c \,\&\, b \angle c) \Rightarrow ab \angle c$$

feltétel már érdekesnek tűnik. Ez azt mondja, hogy az M-beli komplexusokra nézve

$$B(a) \cap B(b) \subseteq B(ab)$$

Rámutatunk arra, hogy a fordított irányú tartalmazás ($B(ab) \subseteq B(a) \cap B(b)$) — kommutatív félcsoportokban — evidens, a most bemutatott irány viszont ott sem az. A kettő együttes fennállása

$$B(a) \cap B(b) = B(ab)$$

-t eredményezi, ami a-nak és b-nek egy különleges viszonyából fakad. Ezt a viszonyt $\perp$ relációjellel — az ortogonalitás avagy merőlegesség jelével — jelöljük. Ezen a módon, csak formai jegyekből kiindulva sikerül a ***relatív prím*** fogalmát bevezetni.

Hasonló definíciós lehetőségek kínálkoznak a ***legnagyobb közös bontó*** illetve a ***legkisebb közös bontott*** bevezetésére:

$$LNKB(a, b) := \{x \mid x \angle a \;\&\; x \angle b \;\&\; (y \angle a \;\&\; y \angle b) \Rightarrow y \angle x\}$$
$$LKKB(a, b) := \{x \mid a \angle x \;\&\; b \angle x \;\&\; (a \angle y \;\&\; b \angle y) \Rightarrow x \angle y\}$$

Ezek a definíciók teljesen szokásosak, és a matematikatanítás így használja őket. Hangsúlyozni azt kívánjuk, hogy tanulmányozásukhoz nem szükséges például egységelemes integritási tartományban lennünk. Illusztrációképpen bemutatjuk az ***M16***-os példa (92. o.) legnagyobb közös bontóinak és legkisebb közös bontottjainak táblázatait:

	0	**1**	**2**	**3**	**4**
0		1, 3	2, 4	1, 3	2, 4
1	1, 3	1, 3		1, 3	
2	2, 4		2, 4		2, 4
3	1, 3	1, 3		1, 3	
4	2, 4		2, 4		2, 4

M16 bal oldali legnagyobb közös bontói

	0	**1**	**2**	**3**	**4**
0		1, 4	2, 3	2, 3	1, 4
1	1, 4	1, 4			1, 4
2	2, 3		2, 3	2, 3	
3	2, 3		2, 3	2, 3	
4	1, 4	1, 4			1, 4

M16 jobb oldali legnagyobb közös bontói

	0	1	2	3	4
0					
1		1, 3		1, 3	
2			2, 4		2, 4
3		1, 3		1, 3	
4			2, 4		2, 4

M16 bal oldali legkisebb közös bontottjai

	0	1	2	3	4
0					
1		1, 4			1, 4
2			2, 3	2, 3	
3			2, 3	2, 3	
4		1, 4			1, 4

M16 jobb oldali legkisebb közös bontottjai

Ahol a cellák üresek, ott üreshalmazt kell érteni.

Érdekes és mély tanulmányozást kínál annak megválaszolása, hogy az asszociált osztályok milyen körülmények között adnak konzisztens osztályozást (tehát mikor lehet művelettáblának tekinteni az *LNKB / LKKB*-táblázatokat), milyen algebrai tulajdonságokkal rendelkező műveletek jönnek létre ilyenkor; létrejön-e valamilyen háló, teljesül-e disztributivitás.

> Bizonyítás nélkül közöljük: *LNKB / LKKB* definíciójából azonnal következik, hogy *LNKB(a, b)* illetve *LKKB(a, b)* elemei asszociáltak. (Pl. $c, d \in LNKB(a, b) \Rightarrow c \cong d$.) Tranzitív bontású grupoidban, így félcsoportban az *LNKB / LKKB* képhalmazai és az asszociált osztályok egybeesnek. (Ez azt jelenti, hogy $c \cong d \;\&\; c \in LNKB(a, b) \Rightarrow d \in LNKB(a, b)$.) Mindkettő asszociatív és az azonos oldaliak kölcsönösen disztributívak egymásra.
> (A műveleti tulajdonságok tárgyalásakor pl. *LNKB(a, LNKB(c, d))*-t akként kell értelmezni, hogy ha $a \in M$ és $H \subseteq M$, akkor $LNKB(a, H) := \{x \mid x \in LNKB(a, h), h \in H\}$.)

Végül didaktikai megfontolásaink közé tartozik még annak megemlítése, hogy a felbonthatatlanság klasszikusan az $f = ab \Rightarrow (f \cong a) \vee (f \cong b)$ implikációval kerül definiálásra. Ez a forma azonban nem fejezi ki az általunk elvárt „felbonthatatlan az, akinek az asszociáltsági tartományának a komplementere zárt” paradigmát (l. 79. o.!). Olyan esetekben, amikor az asszociáltság nem reflexív adódhatnak eltérések, de ezek a didaktikai folyamatot nem fogják megakasztani — ellenben a prím és a felbonthatatlan for-

mailag egységes definiálása sokat segíthet a két fogalom megértésében.

HT-rendszer — egy kísérlet prímek felderítésére

Definíció és példák

Ahogyan azt [2.9]-ben bemutattuk, a prímekkel (prímszámokkal) kapcsolatos didaktikai törekvésünk végülis az, hogy a hallgató a prímet, mint az éppen vizsgált struktúra atomi építőkövét (*generátorát* — l. ezzel kapcsolatban bővebben: [2.6]!) ismerje meg és tárja fel. Megfontolásaink szerint nem elegendő a prímet úgy szemlélni, hogy »íme egy elem, el tudom-e dönteni, hogy prím-e vagy sem«. (Természetesen olykor ez sem csekély feladat!) Meggyőződésünk szerint a prímfogalom akkor rögzül helyesen, ha a hallgató szeme előtt bontakozik ki az algebrai struktúra elemeiből, elemei közül az a néhány, amely tovább már nem analizálható, ugyanakkor a struktúra műveletével képes létrehozni az alaphalmaz összes elemét. Definiálunk tehát ebből a célból egy **algebrai struktúrát**.

Definíció (28)

Egy M grupoid egy $h : M \to M$ és egy $t : M \to M$ függvénnyel és egy $K \subseteq M$ („különlegesek”) részhalmazzal **HT-rendszert** alkot, ha $\forall\, x,\, y \in M$ esetén teljesülnek az alábbiak:

A1. $x = h(x)t(x)$

A2. $h(h(x)) = h(x)$

A3. $h(xy) = \begin{cases} h(x) & \text{,ha } x \notin K \\ h(y) & \text{,ha } x \in K \end{cases}$

A4. $t(xy) = \begin{cases} t(x)y & \text{,ha } x \notin K \\ t(y) & \text{,ha } x \in K \end{cases}$

A struktúrában K lehet üres halmaz. Az $M \setminus K$ halmazt alkalomadtán N-nel („normális elemek”) fogjuk jelölni.

Példák

HT1. példa: Ha a M-ben vannak bal oldali egységelemek (B), és veszünk egy tetszőleges $b \in B$ bal oldali egységelemet, akkor a $h(x) = b$, $t(x) = x$ választás és bármely $K \subseteq B$ megfelelő.

Megjegyzés: Ha h konstans, akkor a 2. és a 3. axióma automatikusan teljesül, bármi is K.

HT2a. példa: Ha a grupoid szorzása az $xy = x$ szorzás, akkor a $h(x) = t(x) = x$ választás megfelelő, és $K = \emptyset$.

HT2b. példa: Ha a grupoid szorzása az $xy = x$ szorzás, akkor a $h(x) = x$, $t(x) = t$ választás megfelelő, és $K = \emptyset$.

HT3a. példa: Ha a grupoid szorzása az $xy = y$ szorzás, akkor a $h(x) = t(x) = x$ választás megfelelő, és $K = M$.

HT3b. példa: Ha a grupoid szorzása az $xy = y$ szorzás, akkor a $h(x) = h$, $t(x) = x$ választás megfelelő, és $K = M$.

HT4. példa: $(\mathbb{N},+)$ félcsoporton vezessük be az alábbi függvényeket: h legyen az előjelfüggvény, azaz $h(0) = 0$, és $h(n) = 1$, ha $n > 0$ valamint $t(n)$ legyen $n \dot{-} 1$, azaz $t(0) = 0$, és $t(n) = n - 1$, ha $n > 0$. A K halmaz legyen $\{0\}$! Ezzel HT-rendszert kaptunk.

HT5. példa: V véges ábécé V^* sorozathalmaza az egymásmelléírás (konkatenáció) műveletével, a *head* és a *tail* függvényekkel valamint a $K = \{\lambda\}$ halmazzal. (Ez

a példa a HT-rendszer „ősmintája” és „keresztapja”.)

HT6. példa: Legyen $b,\ c \neq b \in M$ a grupoid két kitüntetett eleme! Vezessük be a grupoidon az alábbi szorzást:

$$xy := \begin{cases} x & \text{ha } x \neq b \\ y & \text{ha } x = b \end{cases}$$

b tehát egyfajta bal oldali egységelemként viselkedik. A többi elem esetében a szorzás hasonló a (HT2a)–(HT2b) példában említettekhez. h legyen az identitás, legyen $K = \{b\}$, és definiáljuk t-t az alábbiak szerint:

$$t(x) := \begin{cases} b & \text{ha } x = b \\ c & \text{ha } x \neq b \end{cases}$$

Belátható, hogy ezzel a definícióval HT-rendszert kaptunk.

Álljon itt a fenti konstrukcióhoz egy konkrét példa! Legyen $M = \{1, 2, 3\}$, a szorzás Cayley-táblája legyen az alábbi:

	1	**2**	**3**
1	1	2	3
2	2	2	2
3	3	3	3

M17 félcsoport

Látható, hogy $b = 1$. Ennek megfelelően $K = \{1\}$, h az identitás, válasszuk c-t 2-nek, t értékei ekkor táblázatban ábrázolva a következők lesznek:

x	1	2	3
t(x)	1	2	2

Ellenőrizzük az axiómákat!

(**A1**) teljesül, mert $1 = h(1)t(1) = 1 \cdot 1 = 1$; $2 = h(2)t(2) = 2 \cdot 2 = 2$; $3 = h(3)t(3) = 3 \cdot 2 = 3$.
(**A2**) teljesül, mert az identitás idempotens.
(**A3**) teljesüléséhez elegendő annyit vizsgálni, hogy az xy szorzat első tényezője (x) b-vel (1-gyel) egyenlő-e. Ha igen, akkor (**A3**) mindkét oldalán y áll; ha nem, akkor pedig x.
(**A4**) teljesüléséhez nézzük végig a lehetséges 9 szorzatot:

$t(1 \cdot 1) = t(1) = 1$ $\quad$ $t(1 \cdot 1) = t(1) = 1$
$t(1 \cdot 2) = t(2) = 2$ $\quad$ $t(1 \cdot 2) = t(2) = 2$
$t(1 \cdot 3) = t(3) = 2$ $\quad$ $t(1 \cdot 3) = t(3) = 2$
$t(2 \cdot 1) = t(2) = 2$ $\quad$ $t(2 \cdot 1) = t(2) \cdot 1 = 2 \cdot 1 = 2$
$t(2 \cdot 2) = t(2) = 2$ $\quad$ $t(2 \cdot 2) = t(2) \cdot 2 = 2 \cdot 2 = 2$
$t(2 \cdot 3) = t(2) = 2$ $\quad$ $t(2 \cdot 3) = t(2) \cdot 3 = 2 \cdot 3 = 2$
$t(3 \cdot 1) = t(3) = 2$ $\quad$ $t(3 \cdot 1) = t(3) \cdot 1 = 2 \cdot 1 = 2$
$t(3 \cdot 2) = t(3) = 2$ $\quad$ $t(3 \cdot 2) = t(3) \cdot 2 = 2 \cdot 2 = 2$
$t(3 \cdot 3) = t(3) = 2$ $\quad$ $t(3 \cdot 3) = t(3) \cdot 3 = 2 \cdot 3 = 2$

A definíció feltételrendszerének függetlensége

Kézenfekvő a kérdés, hogy (**A1**)–(**A4**) csakugyan axiómarendszer-e. Az ellentmondás-mentességet a bemutatott példák igazolják. Fennáll azonban a függetlenség kérdése: nem lehetséges-e, hogy valamelyik „axióma” (a többi háromból) levezethető? (Ekkor ugyanis a szóbanforgó állítás nem lenne axióma, hanem tétel.)

Állítjuk tehát, hogy

Tétel (15)

Az (**A1**)–(**A4**) feltételrendszer független.

Bizonyítás:

Az (**A1**) axióma függetlensége:

Legyen M a természetes számok halmaza a szorzással, h is, t is az azonosan 1 függvény és $K = M$. Ekkor (**A2**)–(**A4**) teljesül, de (**A1**) nem.

Az (**A2**) axióma függetlensége:

Tekintsünk egy tetszőleges $|M| > 1$ halmazt, és definiáljuk rajta az $xy := y$ szorzást! Válasszuk t-t az identitásnak ($t(x) := x$) és legyen $K = M$. Ha megvizsgáljuk az (**A1**), (**A3**), (**A4**) axiómákat, azt látjuk, hogy azok h megválasztásától függetlenül teljesülnek. De mert M-nek legalább 2 eleme van, h választható úgy, hogy ne legyen idempotens, pl. $M = \{a, b\}$ esetén legyen $h(a) = b$ és $h(b) = a$. Ez azt jelenti, hogy (**A1**), (**A3**), (**A4**) fennáll, de (**A2**) nem.

Az (**A3**) axióma függetlensége:

Legyen $|M| > 1$ halmazon annak művelete bármilyen idempotens művelet (pl. egy U halmaz 2^U részhalmazai a metszettel) — azzal a kikötéssel, hogy legyen olyan két (x és y) M-ben, hogy $xy \neq x$. h is, t is legyen az identitás, K legyen üres! Mint könnyen látható, (**A1**), (**A2**) és (**A4**) teljesül, de (**A3**) nem.

Az (**A4**) axióma függetlensége:

Tekintsük pl. a természetes számok halmazát a szorzással! h legyen az azonosan 1 függvény, t legyen az identitás, és legyen $K = M$. Ekkor (**A1**)–(**A3**) teljesül, de (**A4**) nem. □

Néhány tétel

A HT-rendszer használatával kapcsolatosan kimondunk néhány könnyen bizonyítható tételt:

Tétel (16)

K elemei bal oldali egységelemként viselkednek, azaz:
$x \in K \Rightarrow xy = y$.

Bizonyítás:

$xy = h(xy)t(xy) = h(y)t(y) = y$. □
Speciálisan: $xx = x$.
Ezzel azt is bizonyítottuk, hogy ***K* zárt *M*-ben**.

Tétel (17)

Jelölje H a h által előállított képet M-ben: $H := h(M)$. Másrészt legyen G h fixpontjainak halmaza, azaz $G := \{x \mid h(x) = x\}$. Ekkor $G = H$.

Bizonyítás:

(a) $G \subseteq H$ nyilvánvaló;
(b) $x \in H \Rightarrow \exists y : h(y) = x$, így az (**A2**) axióma miatt: $h(x) = h(h(y)) = h(y) = x$. □

Tétel (18)

Legyen $T := t(M)$ és $L := \{x \mid t(x) = x\}$. Nyilvánvaló, hogy $L \subseteq T$, mint, ahogy az is, hogy általában $L \neq T$, a $T \setminus L$ ugyanis többnyire nem üres. Ezt az (5) példa illusztrálja, ahol $T = M$ és $L = K$. Állítjuk, hogy ***L* zárt *M*-ben**.

Bizonyítás:

(a) $x \notin K$. Ekkor: $t(xy) = t(x)y = xy$.
(b) $x \in K$. Ekkor: $t(xy) = t(y) = y = xy$. □
Felhasználtuk a **Tétel (16)**-ot.

Tétel (19)

$x \in L \setminus K \Rightarrow xy \in L$.

Bizonyítás:

$t(xy) = t(x)y = xy$. □

A fenti tételek közül egyre (**Tétel (19)**) akkor lesz szükség, amikor azt vizsgáljuk, hogy a HT-rendszer elemein definiálható-e valamilyen hosszúság. Hosszúságon egy olyan számhozzárendelést értünk, amely rendelkezik a $len(xy) = len(x) + len(y)$ tulajdonsággal. Ennek definiálásakor játszik szerepet a **Tétel (18)**-ban definiált L halmaz. A t fixpontjain ugyanis célszerű a len értéket 0-nak definiálni, más elemeken pedig a $len(x) = len(t(x)) + 1$ rekurziót alkalmazni. Ez a definíció azonban nem mindig működik, mert a t nem feltétlenül „húz be” minden elemet L-be.

Diákköri kutatási feladatnak is alkalmas azt vizsgálni, hogy egy ilyen definíció milyen feltételek mellett működőképes.

HT-rendszer különböző struktúrákban

Csoportban

Be fogjuk látni, hogy h konstans. Vezessük be a következő jelöléseket! A csoport egységeleme legyen e, $h(e)$-t jelöljük h-val, $t(e)$-t pedig t-vel. Végül a ht szorzat jele legyen k. Először tételezzük fel, hogy K üres! Ekkor:

$$\forall x \in M : h(x) = h(ex) = h(e) = h$$

vagyis h konstans az egész csoporton. Másrészt:

$$\forall x \in M : x = h(x)t(x) = ht(x) \Rightarrow t(x) = h^{-1}x$$

Most tekintsük azt az esetet, amikor K nem üres! Legyen először $x \in K$, s tekintsük h és t értékeit x-en:

$$h(x) = h(xe) = h(e) = h$$
$$t(x) = t(xe) = t(e) = t$$

Ebből látható, hogy h is t is konstans K-n, amiből azonnal adódik, hogy $|K| \leq 1$, hiszen $\forall x \in K : x = h(x)t(x) = h(e)t(e) = ht = k$.

Másrészt, ha $x \neq k$, (azaz $x \in N$) akkor

$$h = h(e) = h(xx^{-1}) = h(x)$$

miatt h az egész csoporton konstans: $h(x) = h$. Így $t(x) = h^{-1}x$.

Ekkor viszont

$$h^{-1}k = t(k) = t(ke) = t(e) = h^{-1}$$

miatt $k = e$.

Összegezve: **Csoporton HT-rendszer csak a $h(x) = a$, $t(x) = a^{-1}x$ függvényekkel és $K = \{e\}$ vagy $K = \varnothing$ halmazzal képezhető.**

Egységelemes félcsoportban

Láthatóan, ha a grupoid egységelemes félcsoport, $|K| \leq 1$ akkor is fönnáll, de h nem feltétlenül konstans az egész félcsoporton.

Kommutatív struktúrákban

Ha a grupoid kommutatív, a $h(xy) = h(yx)$ egyenlőségből és az $x, y \in$ illetve $\notin K$ relációk vizsgálatából azt kapjuk, hogy $h(K) = k$ és $h(M\backslash K) = n$, illetve $h(xy) = k \Leftrightarrow x \in K \,\&\, y \in K$. Minden egyéb esetben $h(xy) = n$.

Ha $x, y \in K$, akkor $t(y) = t(xy) = t(yx) = t(x)$ miatt t is konstans K-n, ahonnan ismét $|K| \leq 1$ adódik.

Prímek származtatása HT-rendszerben

Most kimondjuk a HT-rendszer bevezetésének célját képező tételt:

Tétel (20)

Ha egy HT-rendszerben $p \in H$, akkor p prím.

Bizonyítás:

(a) $p \in K$ eset: p bont minden elemet, mert $pa = a$ miatt a $px = a$ egyenlet mindig megoldható, azaz p triviálisan prím.

(b) $p \notin K$ eset: Álljon fenn, hogy $p \angle ab$, azaz $px = ab$. Ekkor

$$p = h(p) = h(px) = h(ab) = \text{vagy } h(a) \text{ vagy } h(b)$$

Legyen pl. $p = h(a)$, ekkor $a = h(a)t(a) = pt(a)$ miatt $p \angle a$. A $p = h(b)$ esetben pedig $p \angle b$. □

A tétel megfordítása nem érvényes: Csoportban minden elem (triviálisan) prím, de — mint láttuk — $|H| = 1$.

A HT-rendszer alkalmazásának didaktikai célja

Ha a grupoidon sikerül HT-rendszert létrehozni (amihez sok feltételnek kell teljesülnie, pl. hogy a grupoid minden eleme előálljon szorzatként), akkor a h függvény fixpontjai prímelemeket „mutatnak ki". Ezek között vannak triviális prímek, ezek $H \cap K$ elemei, és vannak (vagy lehetnek) $H \setminus K$ halmaznak olyan elemei, amelyek „valódi" prímek: a struktúra valódi alapvető építőkövei. A HT-rendszer tehát a grupoid elemeinek esetleges *belső struktúrájának vizsgálata nélkül* fedi fel a köztük levő atomiakat. Didaktikai szempontból érdekes vállalkozás figyelemmel kísérni egy algebrai struktúra elemei belső szerkezetének ilyen irányú feltárását. Például a HT4. példában (98. o.) $H = \{0, 1\}, K = \{0\}$. A HT-rendszer vizsgálata azt mutatja, hogy a természetes számok, mint struktúraelemek, úgy szerveződnek, hogy az összeadás hozza létre őket összeadással létre nem hozható „atomokból". Ezek között a bonthatatlan atomok között van a K-beli 0, amely valóban atomi elem, de „impotens" abban az értelemben, hogy a struktúrát belőle összeadással (a grupoid műveletével) felépíteni nem lehet. Van ugyanakkor az 1, a „valódi", a „potens" atom, amelyből a természetes számok egész halmaza az összeadás révén csakugyan fölépül.

Kitekintés

Mindeddig a grupoidokra, félcsoportokra fókuszáltunk, ám természetesen nem szabad elfelejteni, hogy a prímfogalom eredetileg gyűrűkben jött létre, és az igazán mély problémák ott vetődnek fel. Illusztrációként bemutatunk egy fogalomkört, amellyel komoly kutatási program indítható.

Definíció (29)

Legyen $(R,+,\cdot)$ gyűrű; prímeknek értelemszerűen a *szorzás* prímjeit fogjuk nevezni (hiszen $(R,+)$ Abel-csoport, ami azt jelenti, hogy az összeadásra nézve R minden eleme triviális prím). Azt mondjuk, hogy $p \in R$ prím **ikerprím**, ha $\exists p_1, p_2 \in R\setminus\{0\}$ prímek úgy, hogy $p = p_1 + p_2$.

A természetes számok körében hagyományosan a (3, 5), (5, 7), (11, 13) stb. *párokat* szokás ikerprímeknek nevezni. A most adott definíció ebben a számkörben a megszokott párok közül a *nagyobbat* nevezi annak.

Az egészszámok körében valamivel érdekesebb a helyzet, mert pl. 7 + (-7) = 0 miatt a 0-t ikerprímnek kell tekinteni. (Emlékeztetünk arra, hogy a 0 *nem triviális* prím!) Ha ez didaktikai zavart okoz, a definíciót ebben az irányban finomítani kell. (Mondjuk úgy, hogy p-t is $R\setminus\{0\}$-ból kelljen választani.)

Véges gyűrűkben is érdekes lehet az analízis. Triviális, de megfontolásra érdemes példát szolgáltatnak a véges testek: ezekben a struktúrákban minden nemzérus elem triviális prím, ennélfogva minden nemzérus elem ikerprím is. Nemtriviális példa is adható ugyanakkor, ahogy erre példa mondjuk a 8-as maradékgyűrű: ebben prím az 1, 2, 3, 5, 6, 7 elem, és például 1 + 2 = 3.

Érdemes felhívni azonban arra a figyelmet, hogy a fenti példában a hat prím közül csak a 2 és a 6 nemtriviális, s az ő esetükben 2 + 2 = 6 + 6 = 4 és 2 + 6 = 0, vagyis csupán a nemtriviális prímek nem adnak ikerprímet.

Érdekes és szép tanulmányozást kínálnak viszont a Gauss-egészek. Mint ismeretes (l. pl. [2.10]) Bolyai János a Gauss-prímeket három osztályba sorolta, úgymint:

A: $\pm 1 \pm i$

B: $\{p = \pm(4n+3) \mid n \in \mathbb{N}$ és p természetes prím$\}$

C: $\{a + bi \mid a, b \in \mathbb{Z}, a \neq 0, b \neq 0, p = a^2 + b^2$ és p természetes prím$\}$

Ha a Gauss-egészek körében próbálunk ikerprímet keresni, azonnal látjuk, hogy azonos osztályú prímek összege mindig osztható 2-vel, ezért nem lehet prím. Tűzzük ki tehát magunk elé, hogy keresünk egy A-osztályú és egy B-osztályú prímet, melyek összege C-osztályú prím[*]! Az összeg normanégyzetét[**] kell vizsgálnunk, mégpedig abból a szempontból, hogy lehet-e prímszám. A normanégyzet az A-osztályú prím lehetséges előjelválasztásai szerint $(p \pm 1)^2 + 1$ lesz, ahol p a B-osztályú prím abszolút értéke. Ez a mennyiség, figyelembe véve, hogy $p = 4n + 3$

$$(p \pm 1)^2 + 1 = \begin{cases} (4n+4)^2 + 1 \\ (4n+2)^2 + 1 \end{cases}$$

— ha ez a kifejezés (természetes) prím, akkor C-osztályú ikerprímet találtunk a Gauss-prímek körében. Arra nézve, hogy lehet-e ezzel a módszerrel *végtelen sok* ikerprímet találni, ebben az esetben is csak azt mondhatjuk, hogy nem tudjuk. Ha $4k^2 + 1$ végtelen sokszor lesz prím, akkor minden bizonnyal. Sajnos azonban egyelőre egyetlen (másodfokú) polinomról sem tudjuk, hogy felvesz-e végtelen sokszor prím értéket[***].

A 2. fejezet tézisei

- A *deduktív* gondolkodás alapvető eszköze a komplex struktúrák analízise, szerkezeti elemeik feltárása. Már a filozófia kezdeteitől fogva megfogalmazódott a kérdés: melyek a legalapvetőbb, **tovább nem bontható**, már nem analizálható építőkövek. Ezeknek az **atomnak** nevezett objektumoknak a felkutatását modellezzük algebrai struktúrákban.

[*] A többi lehetséges kombináció hasonló eredményre vezet.

[**] Az $N(a + bi) = a^2 + b^2$ hozzárendelés elnevezésekor a normanégyzet szót részesítjük előnyben. L. ezzel kapcsolatban [2.6]!

[***] Pálfy Péter Pál szíves közlése.

- Az atomot kézenfekvő mint **felbonthatatlant** azonosítani. Matematikadidaktika-történeti okból ugyanakkor a **prím** fogalma is meghonosodott. A prím az *elsődlegest* jelenti, a kifejezés tehát az *induktív* gondolkodásmód terméke. A két megnevezés — jóllehet a prímfogalom és felbonthatatlanság fogalma korántsem azonos — még a középiskolai matematikatanításban is szinonimaként szerepel.
- Bár a „prím” és a „felbonthatatlan” különböznek, a kettő között **mély fogalmi analógiák** vannak, amelyek a definíciók megfogalmazásakor formai értelemben is tükröződnek. Mi törekedtünk jelen dolgozatban olyan **új szóhasználattal** élni, amelyből ezek az összefüggések kiolvashatók.
- A „prím” és a „felbonthatatlan” fogalmak megalkotásához **nem szükséges a gyűrű**, mint algebrai struktúra: **elegendő a félcsoport**, sőt, a legalapvetőbb definíciókat a grupoidok körében is kimondhatjuk.
- E fogalmak megkülönböztetéséhez *nincs szükség felsőfokú ismeretekre*: az **egészszámok** és a **páros egészszámok** szorzásának elsajátítása után a különbség már az általános iskolai matematikaanyag keretében is megvilágítható.
- Didaktikai céljukat tekintve is különös gonddal vezettük be tehát a **bontás** és **asszociáltság** fogalmakat ügyelve arra, hogy az *oszthatóság*, mint közismert fogalom és terminológia megalapozatlan asszociációkat ne támasszon.
- Különösen a felbonthatatlanságfogalom esetében érezzük fontosnak, hogy az általunk bevezetett szóhasználat **a lehető legegyszerűbb algebrai struktúrákban is alkalmazható** legyen: például az olyanokban is, amelyekben *nincs egység(elem)*.
- Megragadtuk a **triviális prím** illetve **felbonthatatlan** fogalmakat — rámutatva arra, hogy

formális logikai úton miként lehet bemutatni őket.

- Fejezetünk első eredménye a **prímek és felbonthatatlanok viszonyának vizsgálata**, amelynek eredményeképpen egy alkalmasan választott egységelemes félcsoportban sikerült **felbontható prímeket** bemutatni. Ez *új, tőlünk származó didaktikai eredmény*.
- Algebrai struktúrát (**HT-rendszer**) konstruáltunk a prímek (és a felbonthatatlanok) vizsgálata céljából. A struktúra egy **tőlünk származó axiómarendszerre** támaszkodik, amelynek ellentmondás-mentességét és függetlenségét ki is mutattuk.
- Bebizonyítottuk azt a HT-rendszerekre vonatkozó alapvető **tételt**, mely szerint a HT-rendszer egyik függvényének értékkészletében prímek állnak elő. Ilyen értelemben a HT-rendszer **prímek generátoraként** viselkedik.
- Kitekintésként **alternatív definíciót** adtunk az **ikerprím** fogalmára, amellyel a definíció teret nyer olyan esetekben is, amikor a prímelemek szomszédossága (távolsága) nem számszerűsíthető.

Ciklikus halmazok

Bevezetés a 3. fejezethez

Mottó: *Hej, Morzsa, hogy örülnél te most ennek!* [3.1]

Objektumorientált programozási nyelvek oktatása során közkeletű példa a *halmaz* objektum bemutatása, és annak tanulmányozása. Az osztály kipróbálása során a programozási nyelvtől függően különböző hibajelenségek lépnek fel, amikor egy halmazt saját elemévé akarunk tenni.

Ismeretes, hogy a saját magukat nem tartalmazó halmazok halmazának nemlétét illusztráló bizonyítás közkeletű neve *Russell-paradoxon*. A bizonyítás szerint amennyiben létezik az $S = \{ H \mid H \notin H \}$ halmaz, akkor nem tudunk válaszolni arra a kérdésre, hogy $S \in S$ vagy $S \notin S$ áll-e fenn, mert mindkettő ellentmondásra vezet. Matematikatörténeti érdekesség, hogy ezt a leleményt miért nem *Cantor-paradoxonnak* nevezzük, hiszen *Cantor* ugyanezt a gondolatmenetet használja tételében, mely szerint minden végtelennél van nagyobb végtelen.

És valóban: A halmaz és hatványhalmaza sohasem lehet azonos számosságú. Tételezzük fel ugyanis, hogy létezik egy $f : H \rightarrow 2^H$ bijektív függvény. Tekintsük ekkor H azon a elemeit, amelyekre $a \notin f(a)$ fönnáll, és jelöljük H eme részhalmazát S-sel. Tekintve, hogy $S \subseteq H$, azaz $S \in 2^H$, és mert f bijektív, lennie kell egyértelműen egy $x \in H$ elemnek, amelyre $f(x) = S$. Vizsgáljuk ezután x és S viszonyát. Ha föltesszük, hogy $x \in S$, akkor x rendelkezik az S-t definiáló tulajdonsággal, azaz $x \notin f(x)$, tehát $x \notin S$, ez pedig ellentmondás. Ha viszont föltesszük, hogy $x \notin S$, akkor ezzel azt mondtuk, hogy $x \notin f(x)$, vagyis $x \in S$; ami ismét ellentmondás. Lévén, hogy a $z \rightarrow \{z\}$ hozzárendeléssel H kölcsönösen egyértelműen leképezhető 2^H egy valódi részhalmazára, és az előbb beláttuk, hogy H és 2^H számossága egyenlő nem lehet, ebből az következik, hogy 2^H számossága nagyobb, mint H-é.

> Figyeljük meg, hogy ebben a bizonyításban nincs szó arról, hogy S üreshalmaz-e vagy sem. Ahogyan az sem merül fel, hogy S egyenlő-e H-val vagy sem.

Fentiek mutatják, hogy *Cantor* sémája pontosan a *Russell-paradoxont* követi (avagy fordítva: *Russell* követte *Cantort*). Mindenesetre tény, hogy ezek a felismerések vezettek az ún. „naiv halmazelmélet" feladásához, és a halmazelmélet axiomatizálásának igényéhez.

Itt mindjárt ki kell jelentenünk, hogy a *Zermelo–Fraenkel* néven ismert axiómarendszer (ZF) nem engedi meg, hogy egy halmaz önmaga eleme legyen: A ZF szerint $H \in H$ nem lehetséges.

Legyen ugyanis $H \in H$. Ekkor a **páraxióma** miatt létezik $\{H\}$. Nyilvánvaló, hogy $\{H\}$ nem üres. Ekkor a **regularitás axiómája** szerint kell lennie olyan elemének, amely diszjunkt tőle. Mivel nincs más eleme, csak H, kell, hogy $\{H\} \cap H = \varnothing$ legyen. Csakhogy $H \in H$ és $H \in \{H\}$, tehát $\{H\} \cap H \neq \varnothing$.

> A fenti bizonyítás csak a $H \in H$ (ún. *szimplán ciklikus*) esetet zárja ki, de a ZF egyéb axiómáinak felhasználásával belátható, hogy a ZF hosszabb ciklusokat is kizár. Pl., ha feltételezzük, hogy $A \in B$ és $B \in A$, akkor ismét a páraxióma miatt létezik $\{A, B\}$, mely nem üres, és a regularitás axiómája miatt kell lennie egy tőle diszjunkt elemének. De ez nem lehet A, mert $A \cap \{A, B\} = B$, és nem lehet B sem, mert $B \cap \{A, B\} = A$. Véges vagy megszámlálható hosszúságú ciklusok ehhez hasonlóan, az **unióaxióma** felhasználásával, teljes indukciós gondolatmenettel zárhatók ki.

A további vizsgálat céljából ezért egyelőre megkerüljük a ZF-et, pontosabban igyekszünk arra válaszolni, hogy a ZF egyes axiómái miként illeszthetők be rendszerünkbe. Jelen fejezet ezt az eljárást azzal illusztrálja, hogy a ZF axiómái közül a ***Meghatározottsági axióma***, a ***Részhalmaz-axióma*** és a ***Páraxióma*** beillesztésével kapcsolatban tartalmaz megfontolásokat.

A ZF egyes axiómáinak felsorolása és elnevezése az irodalomban gyakran eltér.

Tehát eszerint az mondjuk, hogy C ***ciklikus*** *halmaz*, ha $C \in C$, (C ilyenkor ***szimplán ciklikus***) illetve, ha van az $\{A_i\}$ halmazoknak egy olyan (akár megszámlálhatóan végtelen) lánca, amelyre $C \in A_1 \in A_2 \in \ldots \in C$. A ciklikus halmazok ábrázolása nem oldható meg az $\{a, b, \{\alpha, \beta, \ldots\}, \ldots\}$ technikával, hiszen a halmaz ilyen eljárással való „kiterítése" (linearizálása) végtelen jelsorozatot eredményezne. Nyilvánvaló következmény: *Ciklikus halmaz nem lehet üres*.

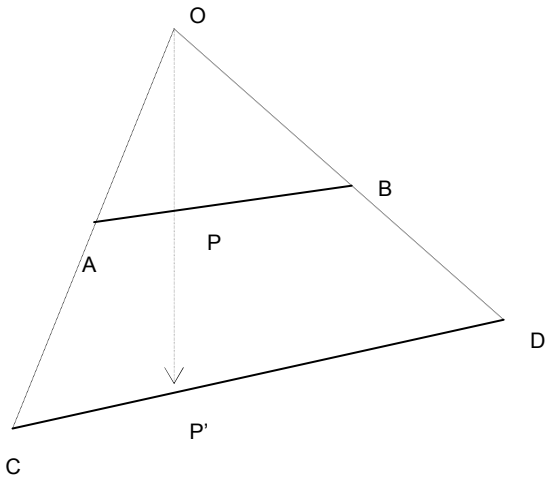
Mit mondhatunk a $\boldsymbol{C} = \{C \mid C \in C\}$ halmazról? Azt vizsgáljuk ezzel, hogy a szimplán ciklikus halmazok halmaza (szimplán) ciklikus-e. Ismeretes a Russell-paradoxon révén, hogy $\boldsymbol{C}$ komplementere nem létezik, de $\boldsymbol{C}$ ettől még igenis létezik, és sem a $\boldsymbol{C} \in \boldsymbol{C}$, sem a $\boldsymbol{C} \notin \boldsymbol{C}$ feltételezés nem vezet ellentmondásra.

Filozófiánk

Fel kell tennünk a kérdést, vajon miért vezet „*paradoxonra*" a ciklikus halmazok felőli elmélkedés. Kultúrtörténeti értelemben a paradoxon ($\pi\alpha\rho\alpha$- előtag = mellett, párhuzamban + $\delta o\xi\alpha$ = hit, vélemény, elképzelés, gondolkodás) olyan történet, tanítás, amely mélyebb megfontolásra, elgondolkodásra késztet azáltal, hogy valami meglepőt, megdöbbentőt, esetleg hihetetlent közöl. Jézus példabeszédei például rendre alkalmazzák ezt az eszközt: Boldogok, akik sírnak; a szegény asszony két fillérje többet ér, mint a gazdag ember nagyvonalú adománya; ha valaki első akar lenni, legyen a legutolsó, mindenkinek a szolgája és így tovább. Ezek az állítások nem „hülyeségek", nem is hamisak, sőt, mély igazságokat fejeznek ki, a szokatlan bennük csupán az, hogy mondanivalójukat a meghökkentés eszközével juttatják kifejezésre.

Lényeges hangsúlyozni, hogy jelen összefüggésben *nem tekintjük paradoxonnak* azt az állítást, amely azzal váltja ki a meghökkenést, hogy téves. Rendes körülmények között ilyen állítás hallatán az emberek először csakugyan meghökkennek, majd elgondolkodnak, belátják, hogy a közlés hamis, és napirendre térnek. Ennek a folyamatnak nem tulajdonítunk didaktikai jelentőséget. Még akkor sem, ha csakugyan vannak közkeletű tévedések, amelyeket gyomlálni tanácsos. Ezt a törekvést azonban a didaktika közvetlen látóköréből kívül esőnek érezzük. Fontos tény, hogy a hamis állítással kapcsolatos didaktikai értékelés nem függ attól, hogy az állítás hamis voltát belátni könnyű vagy nehéz. Paradoxonnak tehát minden esetben *igaz* állítást fogunk nevezni, amely azonban olyan szokatlan vagy meglepő megvilágításban hozza kifejezésre mondanivalóját, hogy hallgatóságát eddig bejáratlan gondolati utak megtételére ösztönzi.

A modern paradoxonok (esetleg a szerzők szándékától függetlenül vagy éppen annak ellenére) ilyen matematikadidaktikai eredményt érnek vagy érhetnek el. A *Banach–Taski-paradoxon* például bemutat egy olyan darabolási eljárást, amellyel egy gömbből két ugyanakkora gömböt lehet csinálni. A szerzők szándéka annak bemutatása volt, hogy ez lehetetlenség, az infinitezimális darabolás ilyen képtelenségre vezet. Érdekes: 1924-ben, amikor a paradoxont publikálták, mindenki tisztában volt azzal, hogy az 1 cm-es és a 2 cm-es szakasz „ugyanolyan hosszú”, hiszen egy egyszerű centrális vetítéssel az egyik minden pontja egy-egyértelműen a másik egy megfelelő pontjába átvihető (**3.1**. ábra).



3.1. ábra

Valahogy mégis, amikor *Banach* és *Tarski* ugyanezt nem hosszúsággal, hanem térfogattal mutatta ki, megdöbbenést váltott ki; sőt, a szerzők ezt abban a reményben tették, hogy ezzel az általuk felhasznált axiomatikus apparátus (nevezetesen a kiválasztási axióma) érvényességét meg fogják cáfolni. Nem ez történt, a paradoxon azonban azt a célt elérte, hogy hallatán a hosszúságról, területről és térfogatról illetve ezek egybevágóságáról mélyebben fogunk gondolkodni.

> Érdemes megjegyezni, hogy a Banach–Tarski-féle átdaraboló eljárás irgalmatlanul bonyolult. A két szerző ugyanezt az eredményt érte volna el, ha a gömböt bármely középpontból $\sqrt[3]{2}$ együtthatóval vetíti: ekkor is kétszer akkora térfogatú gömb jön létre. Ebben a példában viszont nincs semmi hókuszpókusz, azaz a várt eredményt nem képes kiváltani.

Vegyük észre, hogy a paradoxiális hatás matematikai eszközökkel meg sem ragadható! Szubjektív megítélés kérdése, hogy ki mit érez eléggé szokatlannak ahhoz, hogy az elébe táruló (esetleg) meglepő igazságot paradoxonnak lássa. Példa lehet erre a ***Yablo* paradoxonja** [3.4] néven elhíresült gondolatmenet:

Yablo paradoxonja sokféle interpretálásban forog közkézen, mi a végtelen 0/1-sorozat modelljét választjuk. A feladat az, hogy 0-kból és 1-esekből végtelen sorozatot kell készíteni, a szabály pedig az, hogy a sorozat egy adott pozíciójába 1-es kerül, ha tőle jobbra kizárólag csak 0-k állnak, egyébként 0. Rövid meggondolás után rájövünk, hogy ilyen sorozat nincs.

Van, aki ezt úgy fogadja, hogy ilyen sorozat nincs és kész. Ha a feladatot végiggondoljuk, azt kapjuk, hogy olyan *végtelen* sorozatot kellene készítenünk, amely csupa 0-ból áll, kivéve az *utolsó* pozíciót: ott áll egy 1-es. Minthogy *végtelen* sorozatnak nincs *utolsó* pozíciója, a feladat értelmetlen. Fából vaskarika. Az ilyen ember számára a Yablo-paradoxon nem paradoxon. Van viszont, aki úgy látja, hogy a feladat eléggé értelmesen volt megfogalmazva ahhoz, hogy úgy tűnjön, teljesíthető. Hogy mégsem teljesíthető, paradox hatást vált ki a szemlélőben.

Tehát a ciklikus halmaz léte vagy nemléte ugyanígy a fent bemutatott értelemben válik paradoxszá — már akinek azzá válik. A világról alkotott képünk egyrészt teljesen jól elfogad kategóriákat, amelyben önmaguk, az illető kategóriák is helyet kapnak. A fogalmak fogalma maga is fogalom, és ugyanígy vagyunk a legtöbb elvont dologgal. Matematikai eszköztárunkban mindennapos használatba vesszük a hatványhalmazokat, ezek a halmazok halmazokat tartalmaznak elemként. Mármost tehát miért is lenne képtelenség, hogy valamely halmaz önmagát tartalmazza?

Másrészt nagyon megszokott és biztonságos (vagy annak vélt) matematikai támaszaink vannak: pl. a természetes számok tulajdonságai, a végesség és a végtelenség fogalma és így tovább. Elsőre talán nem lehet észrevenni, és a paradoxon éppen itt kezd el „dolgozni”: hogy tudniillik a ciklikus halmaz feltételezése (avagy óvatlan beengedése) halomra dönti ezeket az otthonos épületeket. Miért?

A Peano-axiómák alapfogalma — mint ismeretes — a rákövetkezés. N halmaz rákövetkezője pedig (legalábbis a megszokott interpretáció szerint) az $N \cup \{N\}$ halmaz. Ezzel a generátorral elegendő az üreshalmazt axiomatikusan feltételezni (hogy tudniillik létezik), aztán a „motort” csak be kell indítani, és máris előttünk áll a természetes számok halmaza. Igen ám, de mi a helyzet akkor, ha valamelyik N esetében előadódhatna,

hogy $N \in N$? Nos, ekkor $N \cup \{N\} = N$, azaz a rákövetkezés megáll. Vagy ismét csak a rákövetkezés fogalmához tartozó bizonyosságunk az, hogy különböző halmazoknak a rákövetkezője is különböző. (Matematikusnyelven szólva a rákövetkezés invertálható hozzárendelés.) Igen ám, de mi a helyzet akkor, ha megengedjük pl. az $A = \{B\}$ és $B = \{A\}$ helyzetet? (A és B nem szimplán, de ciklikus halmazok.) Ekkor A és B rákövetkezője egyaránt $\{A, B\}$ lesz, azaz különböző halmazok rákövetkezője azonos.

Mélyen ül a matematikai gondolkodásban a következő gondolatmenet is: Véges az a halmaz, amely nem végtelen. Végtelen pedig az a halmaz, amely ekvivalens valamely valódi részhalmazával. Most legyen pl. $A = \{A, B\}$. Ha valakinek ekkor feltennénk a kérdést, hogy hány eleme is van A-nak, azt válaszolná, hogy kettő. Csakhogy $A \in A$ miatt $\{A\} \subseteq A$, és mivel A-n kívül A-nak van még más eleme is, $\{A\} \subset A$. Az $A \leftrightarrow A$ bijekció (az identitás) evidens módon $\{A\} \leftrightarrow A$ bijekcióvá tehető, azaz az A ekvivalens egy valódi részhalmazával. Ennélfogva A végtelen halmaz. Felkavaró dolog, hogy az, ami kettőnek (végesnek) látszik, arról „kiderül" hogy végtelen. Pedig ugye, mennyire természetes az, hogy az 12 óra után mindig 1 óra következik, azaz minden óra után van következő óra. A láncolat *ilyen értelemben* végtelen. Az óra *számlapján* ennek ellenére csak 12 (véges sok) szám látható.

Éppen az ezekkel a kérdésekkel való szembesítés fog — várakozásunk szerint — a kívánt matematikadidaktikai eredményhez vezetni. Hogy tudniillik, ha valaki a ZF axiómarendszer híve lesz, tudhassa, hogy ezt a döntést miért hozza, más szóval a választást kellően megbecsülje; ugyanakkor szembesüljön azzal is, hogy korrekt módon lehet a ZF-fel ellentétes univerzumokat konstruálni, amelyek — meglehet — a valóság egy más, eddig ismeretlen szeletét modellezik a matematikai gondolkodás számára.

Ciklikus halmaz „gyártása" nem triviális feladat. Egyszerű lenne azt mondani, hogy bármely A halmazból ciklikus halmaz lesz, ha A-t elemként felvesszük A-ba. Csakhogy az eljárás időzítésével gond van; ennek végiggondolását az Olvasóra bízzuk. A probléma abból fakad, hogy a halmazzal kapcsolatban él bennünk egy olyan eszme, hogy annak elemei mintegy „legyárthatók" legyenek. Ez azonban nem feltétlenül kell, hogy így legyen. Tekintsük ezért most a következő megközelítést!

Az alapvető jelölések

Beszéljünk — az esetleges félreértések elkerülése végett — egyelőre csak *entitásokról*, azaz „dolgokról”, amelyekről nem akarjuk megmondani, hogy micsodák. Csak annyit akarunk leszögezni róluk, hogy *vannak*.

Most egy igen komoly gondolati ugrás következik, amelyet sajnos nem lehet elkerülni, pl. a *Halmos*-féle *Elemi halmazelmélet* [3.3] sem kerüli el: elkezdünk beszélni egy ezen entitások közötti *relációról*. Ez azért nagyon merész ugrás, mert a reláció rendkívül bonyolult fogalom (egy Descartes-szorzat részhalmaza), hogyha a klasszikus úton kívánjuk bevezetni. Próbáljuk meg tehát teljesen formálisan felfogni a dolgot: lesz egy *jel*, amelyet két entitás közé írva használunk, és az így keletkezett jelsorozatnak az lesz az *értelme*, hogy a két entitás között ez a bizonyos viszony fönnáll. A jel, amelyet használni fogunk, így néz ki:

$$\in$$

Amikor a jelet olvassuk, az „*eleme*” szót ejtjük ki. Az entitásokat jelölő betűkkel együtt pl. egy ilyen jelsorozat képződhet:

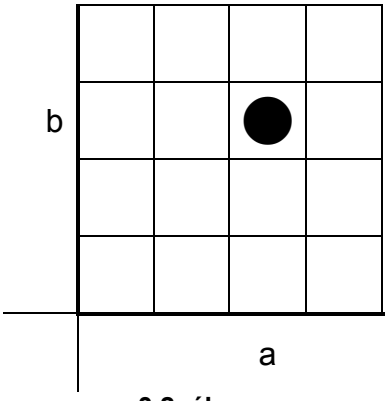
$$a \in b$$

Ezt a jelsorozatot úgy olvassuk, hogy „*á eleme bé[nek]* ”. (A magyar -nak/-nek toldalékot a gördülékenyebb kiolvasás kedvéért szükség esetén használjuk.)

Szeretnénk itt felhívni a figyelmet egy fontos jelölésbeli körülményre. A halmazelméleti irodalom a világosabb olvashatóság kedvéért az $a \in B$ tipográfiát részesíti előnyben. Ezzel azt sugallja, hogy az elem és a halmaz különböző típusok: lám, az elemeket kis-, a halmazokat pedig nagybetűvel írjuk. Ennek az iskolának az a kiindulópontja, hogy az elemek illetve a halmazok *vannak*, és azt vizsgálja, hogy egy eleve létező a elem és egy eleve létező B halmaz között fönnáll-e vajon az, hogy $a \in B$. Természetesen ez is nagyon alkalmas megközelítés, és a tapasztalat azt mutatja, hogy didaktikailag megfelelő is. Mi most azonban abból indulunk ki, hogy *csak egyforma „típusú” (azaz nem tipizált) entitások* léteznek, és egy adott entitás éppen azáltal válik halmaz-

zá, hogy az $\in$ reláció jobb oldalán áll. Az $a \in b$ íráskép tehát egyrészt azt tükrözi, hogy b halmaz, másrészt pedig azt, hogy a ebben a vonatkozásban (!) elem. Természetesen egy esetleges másik $c \in a$ vonatkozásban a halmaz.

Az entitások közötti $\in$ reláció ábrázolása céljából az alábbi koordinátarendszert választjuk:



3.2. ábra

A vízszintes tengelyen helyezzük el az $\in$ jel bal-, míg a függőleges tengelyen a jobboldalára eső entitásokat. Azt, hogy a és b entitás között az $\in$ reláció fönnáll a megfelelő cellában elhelyezett koronggal érzékeltetjük (**3.2**. ábra). A cellák ilyen kitöltését „bekorongozás”-nak fogjuk hívni.

Axiómák / Szóhasználat

I. Vannak entitások, amelyek között axiomatikusan értelmezzük az $\in$ relációt.
II. Ha $a \in b$ fönnáll, akkor azt mondjuk, hogy a (ebben a vonatkozásban) elem, b pedig halmaz.
III. Létezik olyan entitás, amely sohasem áll az $\in$ reláció jobb oldalán.

A III. posztulátum az *üreshalmaz* létezését mondja ki, és mint az alábbi megjegyzésben látni fogjuk, hajlani kényszerülünk arra a következtetésre, hogy üreshalmaz csak egy van. Ezt megelőlegezve, bevezetjük az üreshalmaz jelét: $\varnothing$.

Az üreshalmaz unicitására vonatkozó előbbi megjegyzésünk annak a törekvésnek az eredménye, hogy a halmazelmélet lehetőleg minden, de ha nem is minden, akkor is minél több tulajdonságát viszontlássuk jelen modellünkben. Abban pedig ismeretes a halmazok közötti $\subseteq$ tartalmazási reláció, amely szerint $A \subseteq B$ pontosan akkor áll fenn, ha A minden eleme eleme B-nek is. (Logikai írásmóddal: $(A \subseteq B) \Leftrightarrow (\forall x : (x \in A) \Rightarrow (x \in B))$) Erre a fogalomra támaszkodik a halmazok egyenlősége: $(A = B) \Leftrightarrow ((A \subseteq B) \,\&\, (B \subseteq A))$. Szavakkal: a halmazok akkor és csak akkor egyenlők, ha kölcsönösen tartalmazzák egymást (részhalmazként). *Halmos* ezt ***Meghatározottsági axiómának*** hívja, a ZF-ben az ***Egyenlőség*** vagy az ***„Extenzionalitás" axiómájának*** olvassuk. Ennek a definíciónak pedig az a következménye, hogy *csak egyetlen üreshalmaz létezik*.

Ha az eddigiek figyelembevételével fogunk neki „cellarácsot" rajzolni az $\in$ reláció ábrázolása céljából, a következőket bocsáthatjuk előre:

1. A leendő reláció képe (azaz a függőleges tengelyre eső vetülete) fogja megadni a rendszerben szereplő halmazokat.
2. Ha egy entitás nem jelenik meg relációs képként, akkor az az entitás *elem*.
3. Kell legyen a rácsban üres sor. (Ez lesz ugyanis az *üreshalmaz* ábrázolása.)
4. Nem lehet a rácsban két teljesen egyformán bekorongozott sor (mert akkor azok azonos halmazok).
5. Ha egy korongozás megfelel, akkor a sorok összes permutációja megfelel. Az üreshalmazt rögzíteni fogjuk (a legalsó sorban), ennek megfelelően az egyes axiómáknak megfelelő mintázatok száma mindig osztható lesz $(n-1)!$-sal.

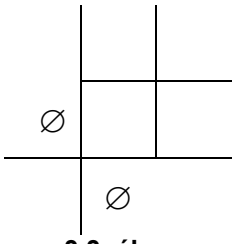
6. Hogy az egyenértékű sorpermutációk közül egy reprezentánst rögzíthessünk, mindig azt a permutációt fogjuk választani, amelyben a sorok alulról felfelé szigorúan monoton növekszenek.
7. Hogy a feni 6. pontban megfogalmazott követelménynek legyen értelme, a soroknak értéket kell adnunk. Egy valahogyan bekorongozott sor értéke a korongok, mint bináris 1-es számjegyek által meghatározott természetes szám lesz. Technikai okból a bitek helyiértékét fordítva rögzítjük: a bal szélen áll az 1-es helyiérték. Ennek megfelelően pl. az 1010 bitsorozat értéke 5 nem pedig 10.

Azt kapjuk, hogy a fenti 6. pont szerint rendezett sorokkal felállított sakktáblasoraink hossza $n-1$, terjedelme 2^n-1, eszerint a szigorúan monoton rendezett sakktáblák száma $\binom{2^n-1}{n-1}$*.

A modellek

Tételezzük fel ezek után, hogy egyetlen entitásunk van, és vizsgáljuk meg, hogy milyen univerzumok készíthetők ebből a készletből!

A III. posztulátum miatt ennek az egyetlen entitásnak az üreshalmaznak kell lennie, és a fenti 3. megjegyzés következtében a rendelkezésre álló egyetlen cellát nem lehet bekorongozni. Az egyetlen entitásból készíthető egyetlen univerzum tehát az alábbi (**3.3**. ábra):

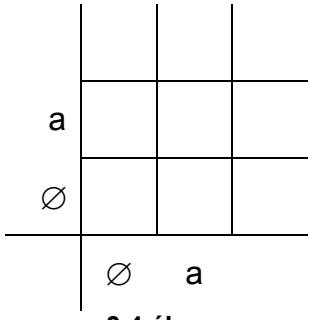


3.3. ábra

* A sorozat első öt értéke 1, 3, 21, 455, 31465.

Ebben az univerzumban tehát egyetlen entitás létezik, az $\varnothing$, és ő elem.

Mielőtt fölrajzolnánk a két entitásból álló lehetséges univerzumokat, emlékeztetünk arra, hogy az üreshalmaz számára kötelező üres sor mindig a legalsó lesz, ennek megfelelően az üreshalmaz mindkét tengelyen a legelső helyen szerepel. Vegyünk tehát két entitást, mint már tudjuk, ebből az egyiknek az $\varnothing$-nak kell lennie, a másik legyen a. Először rajzoljunk „vaktérképet” (**3.4**. ábra)…

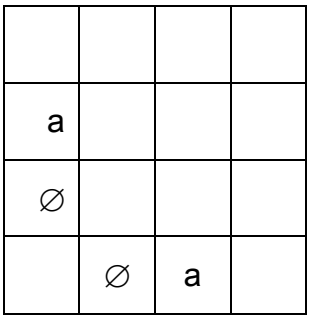


3.4 ábra

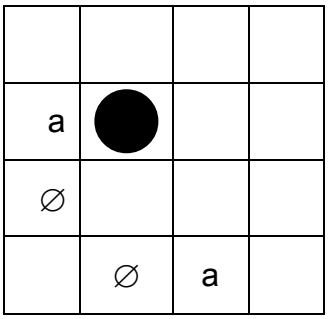
… és vizsgáljuk meg, hogy ebben hányféle korongozás készíthető!

> Mint kijelentettük, hogy az üreshalmazt a relációban *minden esetben a legalsó sorban* (és ezzel az első oszlopban) fogjuk elhelyezni, és ezzel az általánosságot nem szorítjuk meg. Más elrendezésekből sor- és oszlopcserékkel ez a helyzet elérhető.

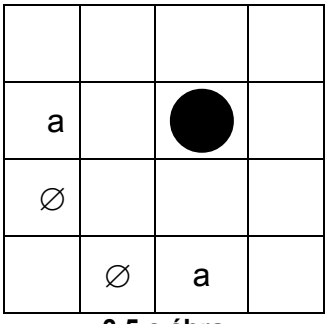
Az alsó sornak tehát üresen kell maradnia, a felső sor két cellája esetében pedig szabadon dönthetünk, hogy teszünk-e korongot vagy sem. Ennek megfelelően arra gondolhatunk, hogy négy ilyen univerzum létezik, mégpedig:



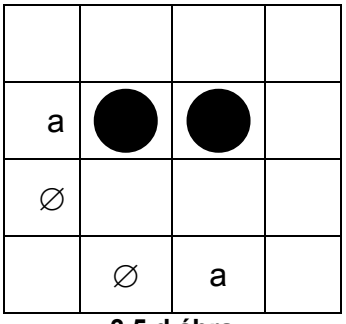
3.5.a ábra



3.5.b ábra



3.5.c ábra



3.5.d ábra

Nézzük!

A **3.5.a** jelű univerzummal az a „baj”, hogy két egyforma sor van benne. Márpedig a korábban tett 4. megjegyzés szerint „nem lehet a rácsban két teljesen egyformán bekorongozott sor”. A **3.5.a** univerzumnak ez a problematikája egy nagyon érdekes következtetésre vezet: ***NINCS MÁS ELEM, CSAKIS AZ ÜRESHALMAZ***.

A **3.5.b** univerzum megfelel klasszikus elvárásainknak: Van benne egy üreshalmaz, és egy a halmaz, amelynek egyetlen eleme van, mégpedig az üreshalmaz. Leírva: $a = \{\varnothing\}$.

> Közbevetőleg: A **3.5b** univerzumban az a halmaz *prímhalmaz* is. (L. az **M10**-es példát a(z) 75. oldalon!)

A **3.5.c** példával érkeztünk el oda, amit ennek a cikknek a bevezetőjében taglaltunk. A **3.5.c** univerzumban egy üreshalmaz és egy szimplán ciklikus halmaz (a) található. Végülis: íme, itt van, megkonstruáltuk, „legyártottuk”. Nem olyan módon, ahogyan ezt korábban megszoktuk, de teljesen korrekt gondolatmenettel.

Vizsgálható, tanulmányozható. Itt is megemlítjük, hogy a egyúttal prímhalmaz is.

Végül a **3.5.d** univerzum az üreshalmaz mellett egy ugyancsak szimplán ciklikus, de már nem prím a halmazt mutat be. A **3.5.d** univerzum illusztrálja egyébként azt a bevezetőben említett helyzetet, hogy egy halmaz, amely „ránézésre" kételeműnek látszik, valójában végtelen. Arra jutottunk, hogy

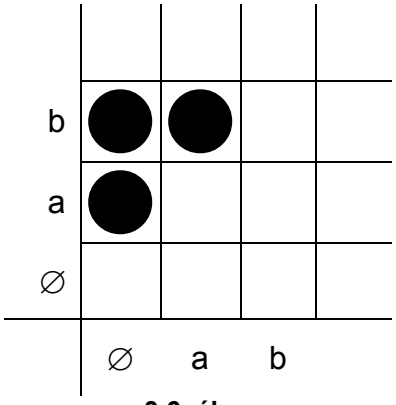
Korollárium (11)

Egy ciklikus halmaz vagy prímhalmaz vagy végtelen halmaz.

A fenti gondolatmenet ezt az eredményt csak szimplán ciklikus halmazra mutatta be, de induktív következtetéssel bármely ciklikus halmazra belátható. További meggondolást igényel, hogy esetleg nem *minden* ciklikus halmaz végtelen-e, azaz a prímhalmazok is nem végtelenek-e a ciklikus halmazok körében. Ha ugyanis a a fenti példa szerinti végtelen (nem prím) ciklikus halmaz, és $b = \{a\}$, akkor b egyfelől prímhalmaz ugyan, de a $\subset$ reláció tranzitivitása folytán van neki végtelen részhalmaza, és ebből arra következtethetünk, hogy b is végtelen. A **3.5.c**-as példa azonban arra mutat, hogy van valódi prímhalmaz is a ciklikus halmazok körében, olyan, amelynek a „magja" az üreshalmaz. A mag fogalmát most nem definiáljuk. A kérdést — amelyet inkább filozofikusnak érzünk — elnapoljuk. A most kimondott korollárium mindenesetre igaz.

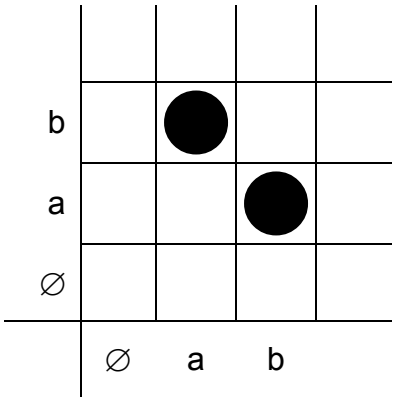
Mielőtt a három entitásból álló univerzumokra térnénk, számoljunk! Hány univerzum készíthető n entitásból? Mint korábban (120. o.) bemutattuk, n elemből $\binom{2^n - 1}{n-1}$, azaz $n = 3$ esetén 21 rendezett (összesen 42, amelyből 21 rendezetlen) univerzum készíthető.

Nézzünk akkor az említett 21-ből néhányat! Például (**3.6**. ábra):



3.6. ábra

Íme, egy meglehetősen "tisztességes" univerzum! Mit tudunk mondani róla? $a = \{\varnothing\}$, $b = \{\varnothing, a\} = \{\varnothing, \{\varnothing\}\}$. Más — szintén elterjedt — jelölésmóddal: $a = \{\{\}\}$, $b = \{\{\},\{\{\}\}\}$. Ez utóbbi emlékeztet a természetes számok *Peano*-féle rákövetkezési módszerrel történő előállítására. Az ábra a 0, az 1 és a 2 természetes számokat ábrázolja. Fontos észrevétel (és ezután bizonyos fokig természetes), hogy az ábrázolt reláció szigorú teljes rendezés. Azaz az $\in$ reláció itt **tranzitív**. Felvetődhet, hogy az a körülmény, hogy a reláció irreflexív is, garantálja-e, hogy a rendszerben nincs ciklikus halmaz. Lássuk ezért a következő példát (**3.7**. ábra):



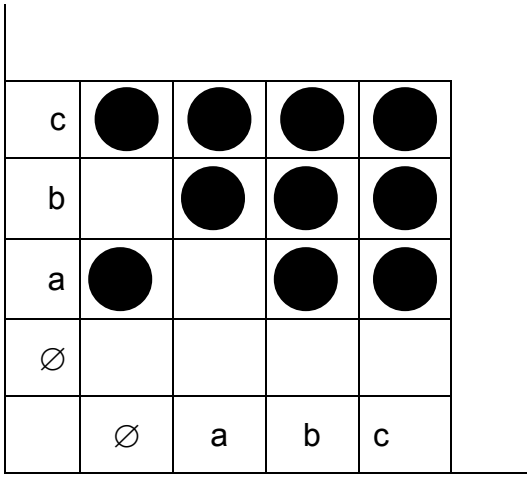
3.7. ábra

Ebben a példában az üreshalmaz mellett két ciklikus halmazt látunk: a is b is ciklikus (prímhalmaz is), de ***nem szimplán cikli-***

kus egyik sem. Holott maga a reláció irreflexív. Az irreflexivitás csak azt jelenti, hogy nincs szimplán ciklikus halmaz a rendszerben.

> Aki figyelembe veszi a relációk hatványozását, észreveheti, hogy a reláció *négyzete* (majd minden páros *hatványa*) már igenis tartalmaz elemeket az identitásrelációból, azaz *nem irreflexív*. **Ha a relációban nincs ciklikus halmaz, akkor a reláció minden hatványa irreflexív.**

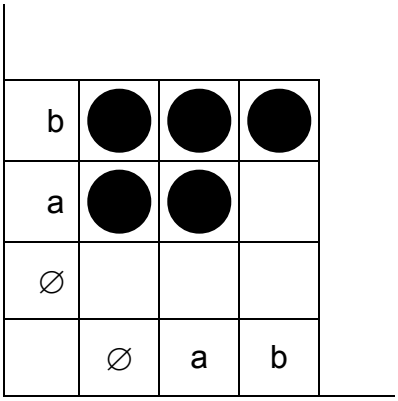
Minden halmazrendszert definiáló konstrukcióban nyilvánvalóan törekszünk arra, hogy a halmazelméletben megszokott halmazműveletekre nézve *zárt* rendszert kapjunk. A **3.6**-os példa a *metszetre és az unióra zárt* — a komplementerképzésre nézve azonban nem. (A komplementerképzésre zártság igen-igen erős kritérium lenne.) A **3.7**-es példa zárt a metszetre, az unióra azonban nem.



3.8. ábra

A **3.8**-as egy metszetre nem zárt példa. (Érdekes didaktikai tapasztalatokat lehet szerezni azzal, ha a hallgatóságnak azt a feladatot adjuk, hogy hozzanak létre metszetre nem zárt univerzumot három entitásból. Három megoldás van, de érdemes tanulmányozni az utánuk való „nyomozást”.)

Nézzünk a három entitásból építkező univerzumra még egy — egyelőre utolsó — példát (**3.9**. ábra):



3.9. ábra

Érdekesség, hogy ez is tranzitív rendszer, metszetre és unióra zárt; csak az üreshalmazra vonatkozó megszorítás miatt (hogy tudniillik kell lennie egy üres sornak, és emiatt nem lehet reflexív) nem rendezés. a is, b is szimplán ciklikus halmazok.

A ZF egyes axiómái ebben a sémában

Haladjunk *Halmos* sorrendjében!

A meghatározottság axiómája

Ekkor első a **meghatározottsági axióma**: ez nekünk is posztulátumunk volt, úgy interpretálódott ebben a sémában. hogy a cellarácsban nem lehet két egyforma sor.

A részhalmaz-axióma

A *Halmosnál* másodikként következő **részhalmaz-axióma** abban a formában, ahogy ő közli, a ZF-ben nem szerepel. Ennek ellenére nyilvánvaló, hogy a mi modellünkben ez a követelmény azt jelenti, hogy ha a cellarácsban szerepel egy sor, akkor minden olyan sornak is szerepelnie kell benne, amely e sorból elhagyással nyerhető. Eszerint az **3.3**-as, a **3.5.b**-s és a **3.5.c**-s példa „jó”, a **3.5.d**-s viszont nem. Talán meglepő, de a **3.6**-os és a **3.7**-es példa közül épp a **3.6**-os a nem jó, míg a **3.7**-es jó. (A **3.6**-os tartalmazza $\{\varnothing,\{a\}\}$-t, de nem tartalmazza $\{\{a\}\}$-t. A **3.7**-es viszont csak egyelemű halmazokat tartalmaz, illetve az üreshalmazt, tehát ebből a szempontból jó.)

Leegyszerűsítve úgy fogalmazhatunk, hogy az axióma megköveteli, hogy a rendszer legyen *„részhalmazra zárt”*. Azaz, ha $A \subseteq B$ és B benne van a rendszerben, akkor legyen benne A is. Ez a követelmény radikálisan csökkenti a szóbajöhető univerzumok számát. Az 1×1-es cellarácsban továbbra is egy helyes kitöltés van, de a 2×2-esben 3 helyett már csak 2, a 3×3-asban pedig 42 helyett már csak 6. A 4×4-es cellarácsban pedig a 2730 variációból mindössze 60 marad. Az alábbi táblázat (**3.10**. ábra) jobb szélső oszlopa számítógépes programmal végzett számlálás eredménye.

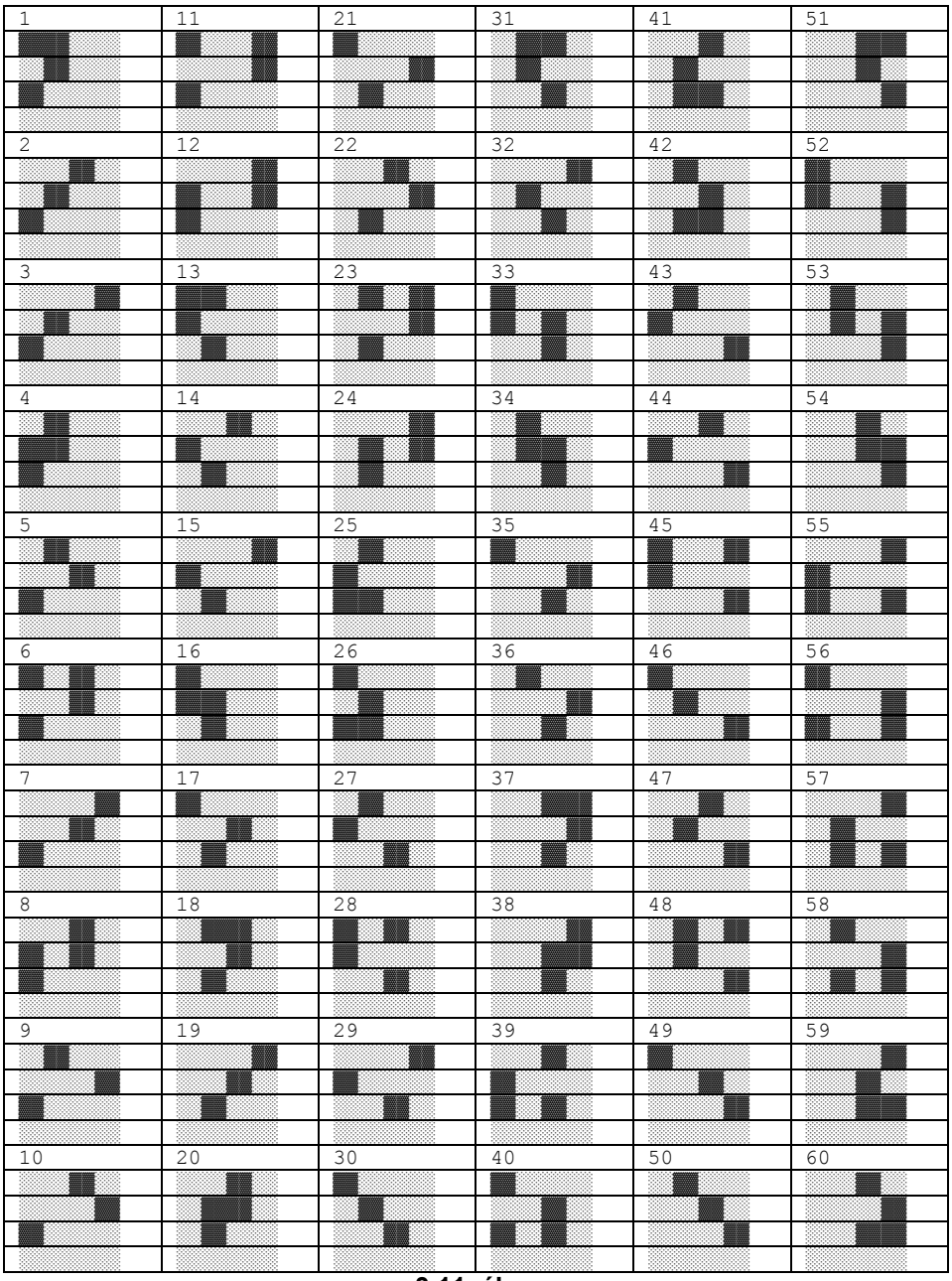
n	Univerzumok száma a Részhalmaz-axióma nélkül	Rendezett univerzumok száma a Részhalmaz-axióma nélkül	Univerzumok száma a Részhalmaz-axiómával	Rendezett univerzumok száma a Részhalmaz-axiómával
1	1	1	1	1
2	3	3	2	2
3	42	21	6	3
4	2730	455	60	10
5	755160	31465	840	35
6	843461640	7028847	18720	156
7	3721953186000	5169379425	559440	777
8	64522032005970000	12801990477375	22196160	4404
9	4400002888500990000000	109127055766394000	1092631680	27099
10	1184554667948240000000000000	3264315112291230000000	65768371200	181240
11	126361961219909000000000000000000000	34821969031059600000000000	4703596128000	1296185
12	535741093974606000000000000000000000000	13421443952786900000000000000000	393785778355200	9865164

3.10. ábra

A fenti táblázatban az első oszlop az *OEIS* (*Sloane*) sorozattárban **A145984**-es illetve a harmadik oszlop **A156972**-es azonosító alatt szerepel.

Hogyan halad ez a számsor? Vegyük észre, hogy ha egy k-elemű halmaz található a rendszerben, akkor kell lennie 2^k különböző halmaznak — ezek ugyanis az ő részhalmazai. Ennélfogva egy $n \times n$-es rácsban legföljebb olyan k esetében lehet k helyen satírozva bármely sor, ahol $2^k \leq n$ (azaz legföljebb $[log_2 n]$-elemű halmazok lehetnek a rendszerben). Ez azt jelenti, hogy 1 entitás mellett csak az üreshalmaz lehetséges (mint láttuk), 2 entitás

mellett csak egyelemű halmazok vannak (ezért nem volt jó a **3.5.d**-es példa), 3 entitás mellett is csak egyelemű halmazok fordulhatnak elő; a 4-es modellben már lehetnek kételemű halmazok is... és így tovább. Egy k-elemű sor pedig azonnal maga után vonja részhalmazait — szám szerint 2^k-2-t (tudniillik ő maga és az üreshalmaz már ott van). Így pl. a 4 $\times$ 4-es modellben egy 2-elemű halmaz mellett mindjárt megjelenik még kettő: pl. $\{a, b\}$ mellett $\{a\}$ és $\{b\}$. Álljon itt illusztrációképpen a 60 db részhalmazra zárt 4 $\times$ 4-es modell (**3.11**. ábra):



3.11. ábra

Mindjárt megemlítjük, hogy a részhalmazra zártság a metszetre vonatkozó zártságot maga után vonja: sőt, erősebb feltétel annál. (A **3.9**-es példa metszetre zárt, de részhalmazra nem.)

Mint láttuk, ezekben a modellekben a maximális elemszám 2 (lévén, hogy $[log_2 4] = 2$), és minden kételemű halmaz jelenléte

megkövetel — az üreshalmazon kívül — további kettőt. Egy kételemű halmaz kerülhet bármely sorba, kivéve a legalsót, azaz a sort 3-féleképpen ($n–1$-féleképpen) lehet kiválasztani. Adott sorban pedig egy kételemű halmazt 6-féleképpen lehet elhelyezni. (Ez n alatt a k.) Végül a két részhalmazt a fennmaradó két sorban kétféleképpen lehet elhelyezni. (Ez a szám — tudniillik a 2 — az $n–2$ alatt a $k–1$ eredménye.)

Ez a gondolatmenet természetesen csak az $n = 4$ esetben világítja meg a 60-as eredményt, a magasabb n-ekre vonatkozóan nem mond semmit. Alább ezzel kapcsolatban néhány megfontolást teszünk. (L. a terminológiával kapcsolatosan: a(z) 119. oldalon olvasható előrebocsátott szempontokat!)

A feladat átfogalmazása ekkor: Hányféleképpen lehet korongokat helyezni egy $n \times n$ cellából álló sakktáblára, ha az alábbi szabályokat kell figyelembe venni:

1. a legalsó sor mindig legyen üres
2. nem lehet a táblán két egyformán „bekorongozott” sor
3. ha egy sor fönt van a táblán, akkor fönn kell lennie minden olyan sornak, amely e sorból akárhány korong elvételével keletkezik

Az alábbi észrevételeket tesszük:

A Ha a sorokat alulról felfelé számozzuk 1-től kezdődően, akkor a k. sorban elhelyezhető korongok maximális száma $[log_2 k]$. (A szögletes zárójel az *egészrészt* jelenti.) Valóban: Ha fönt van egy k-korongos sor a táblán, akkor a (3) szabály miatt minden valódi részhalmaza is fönt van. A valódi részhalmaz, mint szám, mindig kisebb, mint maga a halmaz (hiányzik belőle legalább egy bit). Mivel a valódi részhalmazok a(z) 119. oldalon előrebocsátott 6. megállapodás miatt a halmaz *alatti* sorokban kell, hogy elhelyezkedjenek, a sor alatt kell lennie $2^k–1$ sornak. Ebből következik, hogy $n \geq 2^k$, azaz $k \leq [log_2 n]$.

B A választott interpretálásban az (1) szabály automatikusan teljesül. Valóban: Az 1. sorban —

mivel $[\log_2 1] = 0$ — nem lehet korong, azaz a legalsó sor mindig üres.

C A választott interpretálásban az (2) szabály automatikusan teljesül. Valóban: A 6. előrebocsátott megállapodás szerint a reprezentáns szigorúan monoton növekvő számsorozatot jelent, abban nem lehet két egyforma korongmintázat.

E megfontolások segítségével olyan számítógépes algoritmust készíthetünk, amely „belátható idő alatt”[♣] leszámolja a lehetséges kirakások számát — a **3.10**-es ábra táblázata szerint 12-ig. A sorozat ezzel együtt mély és rejtélyes marad. A számítógépes algoritmus csakugyan leszámlálja a sorozat elemeit (jelen esetben 12-ig), de explicit képlettel egyelőre nem szolgálhatunk[*].

A páraxióma

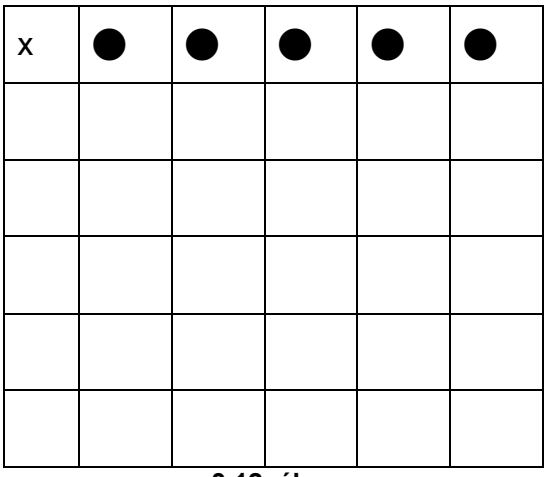
A Halmos-féle sorrendet követve a páraxióma következik. Ez azt mondja ki, hogy bármely két halmazhoz létezik olyan halmaz, amelynek e kettő eleme: $\forall a, b\, \exists c : a \in c \,\&\, b \in c$. Vizsgáljuk meg eddigi univerzumainkat a páraxióma teljesülése szempontjából!

Amint könnyen ellenőrizhető, az egyetlen entitásból létrehozott egyetlen univerzum (120. o.) nem teljesíti a páraxiómát. Hasonló vizsgálatot követően arra jutunk, hogy első univerzumunk, amely ezt a kritériumot teljesíti a **3.5.d**-s példa.

Könnyen belátható, hogy egy véges sok entitásból álló univerzum teljesíti a páraxiómát, ha van benne teli sor (**3.12**. ábra):

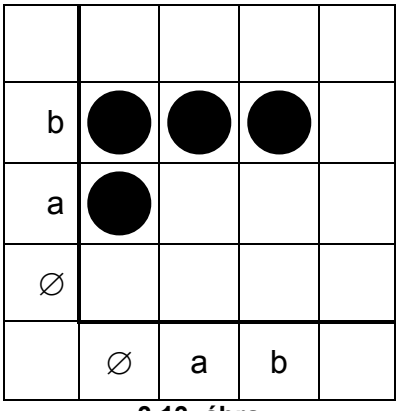
[♣] Számítógéptípustól és operációs rendszertől valamint a választott programozási nyelvtől függően a futásidő lehet néhány másodperc vagy néhány óra. (Pl. Microsoft Windows XP Professional 5.1.2600 SP 3 operációs rendszerben Intel Celeron D, 3066 MHz processzorral, 512 MB PC3200 DDR SDRAM-mal PHP 5.2.3 nyelven írt algoritmus futásideje n = 10 esetén 6,9 mp; n = 11 esetén 48,8 mp; n = 12 esetén 468 mp [csaknem nyolc perc!]. 12-nél nagyobb n-ekre a futásidő kivárhatatlanul megnövekszik.)

[*] A szerző ezúton köszöni *Suller Andrásnak* a programozás terén nyújtott hathatós segítségét.



3.12. ábra

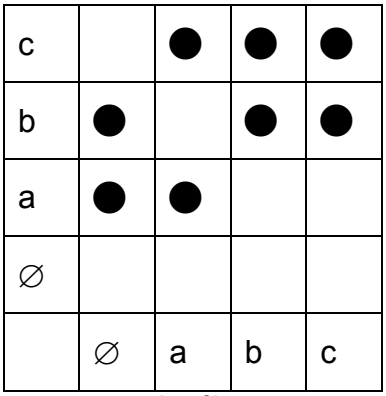
Ha ugyanis x halmaz az univerzum összes entitását tartalmazza (és így saját magát is), akkor annak bármely két entitását tartalmazza. Ezzel a páraxióma kielégül. Ha szánunk rá néhány percet, könnyen megállapítható, melyek a páraxiómát kielégítő univerzumok három entitásból. Például az alábbi (**3.13**. ábra) ilyen:



3.13. ábra

Összesen 12 megfelelő univerzumot fogunk találni, amelyből 6 rendezett, 6 rendezetlen. Mindegyik megoldás tartalmaz teli sort, azaz három entitásig a teli sor megléte a páraxióma teljesülésének szükséges feltétele is.

A szükségesség azonban ezt követően nem áll fenn. A páraxiómának a 4 entitásból készíthető 455 rendezett* univerzum közül 101 tesz eleget, ám e 101-ből 10-ben nincs teli sor. Például tekintsük az alábbi 4×4-es bekorongozást (**3.14**. ábra):



3.14. ábra

Abban az esetben, amikor van a táblán teli sor (és ekkor ez nyilván a legfölső a rendezettség miatt), könnyű megmondani a lehetséges korongozások számát: a legalsó sor üres, a legfölső sor tele van, a közbülső $n-2$ sorba pedig 1-től 2^n-2-ig eshetnek számok. (Emlékezzünk rá: egy sorbeli korongozást egy számmal azonosítottunk: a korongok az 1-es bitek.) A lehetséges korongozások száma ezen feltételek mellett tehát $\binom{2^n-2}{n-2}$. Ez a formula $n=1$-re értelmetlen (és csakugyan: az egyetlen üreshalmazból álló univerzum nem is teljesíti a páraxiómát), $n>1$ esetén néhány értéke pedig:

* A kényelem kedvéért ezt követően csak a rendezett univerzumokat vesszük számba.

n	Teli sort tartalmazó korongozások száma: $\binom{2^n-2}{n-2}$	Teli sort nem tartalmazó korongozások száma:	Összesen
2	1	0	1
3	6	0	6
4	91	10	101
5	4060	1620	5680
6	557845	550258	1108103
7	244222650		
8	351427189575		
9	1708447057008120		
10	28718314770890600000		

3.15. ábra

Arra törekedve, hogy a teli sort nem tartalmazó korongozások számát megadjuk — tehát a nehéz kérdésre választ adjunk — a következő feladatot tűzzük ki:

Feladat: Álljon egy tábla r sorból és c oszlopból. A korongozás fogalma a szokásos. Keressük az összes olyan korongozás számát, amely megfelel az alábbi feltételeknek:

(A) A tábla nem tartalmazhat üres sort.
(B) A tábla nem tartalmazhat teli sort.
(C) A tábla alsó sorától felfelé szigorúan monoton rendezett. (A rendezettség alatt a bevezetett fogalmat értjük: a korongozást bináris számnak olvassuk, és az így kapott számokra nézve legyenek a sorok alulról fölfelé szigorúan monoton rendezettek.)
(D) A tábla bármely két oszlopához legyen található olyan sor, amelyben a kiválasztott két oszlopban van korong.

A feltételnek eleget tevő táblázatok számát keressük. Jelöljük ezt a számot $f(r, c)$-vel!
A feladatot vizsgálva $f(r, c)$ értékeire a következő eredmények adódnak (**3.16**. ábra):

r \ c	3	4	5	6	7	8	9
3	1	10	65	350	1701	7770	34105
4	3	99	1620	20100	216573	2149749	
5	3	434	18913	550258			
6	1	1114	138410	9625729			
7	0	1860	715245				
8	0	2120	2785970				
9	0	1684	8527365				
10	0	935					
11	0	358					
12	0	91					
13	0	14					
14	0	1					
15	0	0					

3.16. ábra

Könnyű meggondolni, hogy ha akár a sorok, akár az oszlopok száma kisebb, mint 3, akkor nincs megoldás.

Belátható az is, hogy ha $r > 2^c - 2$, akkor sincs megoldás.

A tábla kitöltött értékeit programmal számoltuk le, explicit képlettel egyelőre nem szolgálhatunk. Van azonban egy **nagyon erős hipotézisünk**: A tábla $r = 3$ sorában a másodfajú *Stirling-számok* ($\sigma(n, k)$) közül a $k = 4$ sorozat található, egész pontosan: $f(3, c) = \sigma(c + 1, 4)$. (Lásd az *OEIS* sorozattár **A000453**-as elemét!)

A feladat megfogalmazásából világos, hogy $f(r, c)$ miként lesz segítségünkre. A táblázat kiemelt cellái ($f(r, r+1)$) éppen a páraxiómáról szóló feladat megoldásait szolgáltatják.

A 3. fejezet tézisei

- A „*Ciklikus halmazok*” fejezetben **új matematikadidaktikai, oktatás-módszertani ter-**

minológiát és szempontokat vezettünk be.

- Megfogalmaztunk egy „filozófiát” a paradoxonokkal kapcsolatosan, és bemutattuk **a paradoxiális hatás didaktikai lehetőségeit**.
- E téma bizonyos elemeit általános iskolás szakkörben is előadtuk. A fogalmak ***nem igényelnek komoly matematikai előképzettséget***.
- Célul az úgynevezett „ciklikus” halmazok kezelését tűztük ki, megállapítva velük kapcsolatban **néhány új szempontú matematikai állítást**.
- Véges **„univerzumokat” hoztunk létre** amelyek a Zermelo–Fraenkel-axiómarendszer egyes axiómáinak eleget tesznek; mégpedig sorrendben: a **meghatározottsági**, a **részhalmaz**- illetve a **páraxióma** követelményeinek.
- Azok az „univerzumok”, amelyeket e fejezetben sorra vettünk, teljesen természetesen és közérthetően állnak elő, és megvannak a maguk szabályai. Szabályosságaik, mint több helyen is láttuk, ***igen mély matematikai összefüggésekhez*** vezethetnek.
- Az „univerzumok” előállítása során a „**bekorongozásnak**” elnevezett eljárást alkalmaztuk, amelynek segítségével **számossági megfontolásokat** tettünk.
- Rámutattunk, hogy a téma akár ***a felsőoktatásban, sőt, önálló kutatási témaként*** is szerepet kaphat. Mint fogalomalkotási gyakorlat ugyanakkor a középiskolában, sőt, akár általános iskolában is felhasználható.

Összefoglalók

Magyar nyelvű összefoglaló

Tizenkilenc éves, felsőoktatásban illetve középiskolában szerzett tapasztalattal valamint a most befejezett PhD-hallgatói ku-ta-tó-mun-ka keretében egy féléven át tartott „különleges” ma-te-ma-ti-kaóráknak tanulságaképpen — amely utóbbiakról részletesen lásd [0.1] — a szigorú fogalmi megalapozást véljük célravezető di-daktikai módszernek.

Több kísérlet átgondolása és lehetőségek felmérése után három te-rületet választottunk, amelyeken keresztül a szigorú fogalmi meg-alapozás lehetőségét kívánjuk bemutatni. E három terület a következő:

- A közrefogás / elválasztás / folytonosság fogalomköre — ezzel kapcsolatosan naiv nyelvhasználati reflexek is rögzülnek már a beszédtanulás során, s e pontatlanságok nem küszöbölődnek ki automatikusan; szisztematikus átgondolásra van szükség.
- A prímek / felbonthatatlanok fogalma — ez a terület megjelenik már az általános iskolában is, és a középiskolai oktatásban jelentős szerepet kap. Rendkívül mély és megoldatlan problémái miatt ugyanakkor a legmagasabb szintű matematikaoktatásban is folyamatosan jelen van.
- Halmazelméleti fogalmaink — bár már korábban is találkozunk ezzel a diszciplínával és szóhasználatát alkalmazzuk is — csak a felsőoktatásban válnak megalapozottá. A ciklikus halmazokkal kapcsolatos problémakör nehézségeit jól megvilágítják azok a kutatási tapasztalatok, amelyekről programfejlesztők számolhatnának be például a Novell fejlesztése során: az egymásba ágyazott felhasználói csoportok engedélyezése milyen elméleti nehézségek felmerüléséhez vezetett a szoftverfejlesztésben.

A területek kiválasztása, illetve az eredmények tárgyalása során azt az elvet tartottuk szem előtt, hogy *a matematikadidaktika szerepe nem ér véget az általános- és a középiskolai oktatásban*. Matematikadidaktikai megfontolásokat szabad és kell is tenni a felsőfokú matematikai képzésben is. Az itt bemutatandó eszközök e célt is jól szolgálhatják.

A közrefogás / elválasztás fogalomkör területén végzett axiomatikai vizsgálatok során felállítottunk egy **axiómarendszert**, amely így ebben a formában *tőlünk származik*, és támaszkodik *Euklei-dész* axiómáira valamint *Pash* és *Veblen* hasonló kutatási területen alkalmazott összeállítására. Az elvégzett oktatási kísérlet illetve az axiómarendszerrel végiggondolt megfontolások azt mutatják, hogy ez az axiómarendszer csakugyan jól ragad meg valóságosnak érzett viszonyokat és szemléletes. Igen jól kezelhető véges modelleket ad, amelyek kitűnő oktatási segédletnek bizonyulhatnak. Az elemszámokból álló, így keletkező *sorozatok* igen mély összefüggéseket is mutatnak, és további tudományos kutatás tárgyai is lehetnek.

A prímfogalom megalapozása érdekében a szokásos *gyűrűkörnyezettől elszakadva* a lehető legegyszerűbb algebrai struktúrákat (*grupoidok*) vettük igénybe a vizsgálathoz. A kísérleti oktatás valamint a további didaktikai megfontolások is azt támasztják alá, hogy a **félcsoportkörnyezet** a legalkalmasabb a fogalom. Bevezettünk egy új **terminológiát** (*bontás*), amellyel elő lehet segíteni az oszthatóságtól való elvonatkoztatást. Ugyanebben a tárgyban megadtunk ismét egy **axiómarendszert** (*HT-rendszer*), amellyel prímek generálására (felkutatására) nyílik lehetőség.

Végül a halmazelméleti fogalmak megalapozásával foglalkozó kutatási területen a következő didaktikai lépéseket alkalmaztuk:

- Olyan közismert fogalmak, mint a közösségi portálok felhasználásával bemutattuk a *Russell-paradoxonnak* nevezett problémát.
- Az elemkénti tartalmazásnak, mint relációnak *Descartes*-féle koordinátarendszer celláiban történő bemutatására kialakítottuk a **bekorongozásnak** elnevezett eljárást.
- A *Zermelo–Fraenkel-axiómarendszer* egyes axiómáinak lépésenkénti bevezetésével megfogalmaztuk a követelményeknek megfelelő „bekorongozási” feladatot.
- A feladatnak eleget tevő véges modellek *elemszámát* vizsgáltuk.
- Rámutattunk a ciklikus halmaz jelenlétének lehetőségére, illetve arra, hogy a Russell-féle paradoxonban említett halmaz létrehozására miért nem nyílik lehetőség — ezzel mintegy feloldva a probléma axiómajellegét.

Jelen disszertáció a következő kutatási eredményeket mutatja be:

- Az **elválasztási rendszer** fogalmának bevezetése, axiómarendszerének (nyílt és zárt változatban való) fölállítása, a változatok tanulmányozása.
- **Véges modellek** (részbeni) feltérképezése, ábrázolásuk, elemszámokkal kapcsolatos vizsgálatok.
- **Eljárások bemutatása elválasztási rendszerek generálására** — ideértve az elválasztási rendszerekből származtatott további elválasztási rendszereket is —, annak **bizonyítása**, hogy a származtatási eljárások elválasztási rendszert adnak.
- Néhány további, az elválasztási rendszerekkel kapcsolatos **tétel** felállítása és **bizonyítása**.
- A **folytonosság** *Dedekind*- illetve *Cantor*-féle megközelítésének didaktikai szempontból is jól felhasználható **interpretálása** elválasztási rendszerekben.
- Annak megmutatása, hogy a *Dedekind*- és a *Cantor*-féle tulajdonság **független** egymástól.
- A **szomszédosság**, az **intervallum**, az **egyenes** fogalmának interpretálása ebben az axiomatikai környezetben.
- Definíciós lehetőségek megadása a **nyílt halmazok** fogalmának megragadására, az **erős** és **gyenge** nyíltság definiálása, kezdeményezés az értelmezés topológiai következményeinek vizsgálatára.
- A **bontás**, mint didaktikailag új terminológia bevezetése.
- A **bonthatósági** és **asszociáltsági** relációk definiálása, tulajdonságaik elemzése általában vett *grupoidokon* illetve *félcsoportokon*.
- A **prím** és a **felbonthatatlan** definiálása, a definíciók közötti **formai összhang** megteremtése.
- A **prímek felbonthatatlanságának** illetve a **felbonthatatlanok prímtulajdonságának** mély és alapos vizsgálata.
- A „kommutatív félcsoportban a prímek felbonthatatlanok” **tétel kimondása és bizonyítása**.
- **Példa** bemutatása olyan egységelemes félcsoportra, amelyben **felbontható prímek** találhatók.
- A **legnagyobb közös bontó** és a **legkisebb közös bontott** fogalmának bevezetése, az általuk kialakuló **hálószerkezet** felvázolása.

- A **HT-rendszernek** nevezett algebrai struktúra definiálása, axiómái függetlenségének bizonyítása, további tanulmányozása, néhány kisebb **tétel** kimondása és bizonyítása.
- Prímek generálására vonatkozó **tétel** kimondása és bizonyítása HT-rendszerben.
- Az **ikerprím** újradefiniálása a fogalomnak a természetes számokénál tágabb értelmezhetősége érdekében. Az új értelmezés bemutatása a *Gauss-prímek* körében.
- A *Russell-paradoxon* elemzése során magának a paradoxonnak a **didaktikai értelmezése**, a **ciklikus halmaz** fogalmi rögzítése.
- Halmazelméleti alapfogalmak vizsgálata céljából a **bekorongozásnak** elnevezett eljárás bevezetése, didaktikai erejének bemutatása.
- A *Zermelo–Fraenkel*-féle axiómarendszer három axiómájának lépésenkénti **bevezetése a modellbe**, a bevezetésnek a modellre gyakorolt hatásának vizsgálata, a modellek **elemszámára** vonatkozó megfontolások megtétele.
- Kitekintés és javaslat **önálló kutatási témák** továbbvitelére mindhárom területen.

Summary in English

Having taught for nineteen years in the higher education and in high schools, and, in addition, having got the to give a half year in an eighth-year elementary school as member of a "special" math program for gifted children (about which we publicized in detail. See [0.1]) — we feel the axiomatic foundations of several mathematical concepts, as the better didactic method.

After thinking about several attempts and explore ways we chose three areas through which we present the possibility of the strictest conceptual foundation. These three areas are:

- The concepts of embrace, separation, and continuity — related which there are fixed naïve language using reflexes also at the early language learning, and these inaccuracies are not eliminated automatically; we need a systematic consideration.
- The concepts of primes and irreducibles — this area there appears even in elementary school and it gains a signifi-

cant rule in high school. Because of their extraordinarily deep and unresolved problems they have a permanent attendance also in university teaching.

- Our theoretical concepts about set theory — although we meet them earlier and we use their nomenclature — become fixed only in the higher education. The heaviness of the concepts of cyclic sets are illuminated by the research experiences about which the Novell program developers could report: what a number of theoretical difficulties there appeared when they allowed nested groups of users.

At the selection of areas, and discussion of the results we kept in mind the principle that the role of mathematical didactic methods does not end in the elementary and secondary education. Mathematical didactic considerations may and should be done also in the upper level of mathematical training. The tools presented here can serve this purpose well.

When investigating the concepts of embrace and separation we set up a system of axioms, so that originates from me in this form, and relies on the axioms of *Euclid*, *Pash*, *Veblen* and other compilations used on similar areas of research. The axiom system can formulate the following ideas:

- The border points and internal points separate.
- The embrace is a symmetric relation.
- Any section can be continued.
- The embraced point is not allowed to leave the position of between the embracing points.

The educational experiments carried out and the considerations thought about the axiom system show that this axiom system catches just as well realistic conditions, and it is clear. It gives very easy to use finite models and they could prove to be an excellent teaching aid. The numerical analysis of the resulting series shows some very deep correlations, and it can be also target of other scientific researches.

In order to substantiate the concept of primes we detached from the usual ring environment and we used as simple algebraic structures as groupoids for the investigation. The experimental teaching as well as further considerations bear out that the semigroup is the most suitable environment for testing the concept We introduced a new terminology (*splitting*), which can facilitate the abstraction of the authority of division. In the same object we

introduced an axiom system (called *HT-system*), by which we generate primes.

Finally, on the research area establishing set-theoretic concepts, the following didactic steps were used:

- Using as well-known concepts such as social networking, we presented the problem called *Russell's* paradox.
- To show the relation of element containing in the cells of a Cartesian coordinate system, we have developed the procedure named "coining".
- With the step by step introduction of some axioms of the *Zermelo-Fraenkel* axiom system we formulated the requirements of the "coining" task.
- We studied the number of finite models obeying the task.
- We pointed out the possibility of the presence of cyclic sets, as well as the lack of possibility to create a set that is in *Russell's* paradox — having quasi dissolved the axiomatic nature of the problem.

This dissertation reports on the following results:

- The introduction of the concept of separation system, building an axiom system (open and closed versions), the study of variations.
- (Partial) mapping of finite models, pattern analysis, element number related studies.
- Presentation of procedures generating separation systems — including when the separation system is derived from earlier separation systems — having proven that the derivation procedures provide separation system.
- Having set up and proven some additional theorems related to the separation systems.
- Setting up an interpretation — useful also from the didactic point of view — of the continuity, so in *Dedekind's* as in *Cantor's* approach in separation systems.
- Pointing out that the *Dedekind's* and *Cantor's* properties are independent.
- Interpretation of the concept of the adjacency, of the interval, of the line in context of this axiomatical environment.

- Giving options to define the concept of open sets, the definition of strong and weak openness, initiative to test the topological interpretation of the consequences.
- Introducing the concept of *splitting* as a didactically new terminology.
- The definition of splitablity and associate relations, analysis of their properties taken on usual groupoids and semi groups.
- The definition of prime as well as of irreducible; creating between the both definitions a formal concordance.
- A deep and thorough investigation of the irreducibility of primes as well as the prime properties of irreducibles.
- Having expressed and proven the theorem as: “primes in commutative semi groups are irreducible”.
- Demonstrating an example of a semi group equipped with a unit in which it is possible to find reducible primes.
- Introducing the concepts of the greatest common splitter so as of the least common split; outlining the lattice construct established by them.
- Definition of the algebraic structure called HT-system; having proven the independency of its axioms; further investigations on it; having set up and proven some smaller theorems.
- Expressing and proving the theorem about generating primes in HT-systems.
- Redefinition of twin primes aiming to expand the competency of the definition onto areas wider than the natural numbers. An illustration of the new concept in the field of the *Gauss*-primes.
- Accompanying the *Russell’s* paradox giving an absolute concept of paradox at all; conceptual fixing the idea of cyclic sets.
- Aiming to the investigation of basic concepts of the set theory, having introduced a procedure, called “coining”; and, having shown its didactic power.
- A step by step introduction of three axioms of the *Zermelo-Fraenkel* axiom system; investigating the impact of the introduction onto the model; expressing considerations about element order of the several models.
- Outlook and proposals are taken for forwarding independent research projects in all the three areas.

Irodalom

[0.1] Egy tehetséggondozó program tapasztalatai / Csabay Károly == Új Pedagógiai Szemle

[1.1] Lukács evangéliuma 4. fejezet, 30. vers

[1.2] Vorlesungen über neuere Geometrie / Moritz Pasch. - Leipzig : Teubner, 1882.

[1.2a] Vorlesungen über neuere Geometrie / Moritz Pasch, Max Dehn. - Berlin : Springer, 1926.

[1.3] Gesammelte mathematische Werke / Richard Dedekind ; Herausgegeben von Robert Fricke, Emmy Noether [and] Öystein Ore. - Braunschweig : Druck und Verlag von Friedrich Vieweg & Sohn Akt.-Ges. - 23 cm. -Errata (Druckfehlerverzeichnis) included in vol. 3. - 1. Band. - 1930. - 397 p. - JFM 56.0024.05. - 2. Band. - 1931. - 442 p. - JFM 57.0036.01. - Zbl 0001.38501. - 3. Band. - 1932. - 508 p. - JFM 58.0042.09. - Zbl 0004.33701 Bibliographical footnotes

[1.4] Ueber unendliche, lineare Punktmannichfaltigkeiten. 5. Fortsetzung / Georg Cantor == Mathematische Annalen, Band XXI., 1883., pp. 545-591.

[1.5] A geometriák alapjai / H. S. M. Coxeter ; [ford. Sztrókay Kálmán]. - Budapest : Műszaki Kiadó, 1973; [Szeged] : Szegedi Ny. - 470 p. : ill. ; 24 cm

[1.6] A system of axioms for geometry. / Veblen, Oswald == TRANSACTIONS OF THE American Mathematical Society, vol. 1904/3, pp. 343-384.

[1.7] Projective Geometry. / By OSWALD VEBLEN and JOHN WESLEY YOUNG. - Volume I. - Boston : Ginn and Company, 1910. - x + 342 p.

[1.8] Axiomatikai vizsgálatok / Csabay Károly. - 2006. november 8-án, a Magyar Tudomány Napja alkalmából elhangzott konferencia-előadás prezentációja

[1.9] Elemek / Euklidész. - [Budapest] : Gondolat, 1983.

[2.1] Magyar népi tréfa. Közli: A magyar észjárás / Karácsony Sándor ; [sajtó alá rend., az utószót és a jegyzeteket írta Lendvai L. Ferenc]. - 2. jav., bőv. kiad. - Bp. : Magvető, 1985. - 561 p., [1] t. : ill. ; 17 cm. - (Magyar hírmondó) , 216. o.

[2.2] Egy gimnáziumi csoporttal lefolytatott kísérlet eredményei — Egy sorozatfajta elemzése / Csabay Károly. - MIDK2009-konferencia-előadás

[2.3] Bevezetés az algebrába / Kiss Emil. - Budapest : Typotex, 2007. - XVII, 717 p. : ill. ; 24 cm. - (Elméleti matematika)

[2.4] A prímfogalom általánosításából adódó didaktikai lehetőségek / Csabay Károly. - 2009. október 10-én, doktorandusznapon elhangzott konferencia-előadás

[2.5] Egy félcsoport bemutatása / Csabay Károly — Daragó József. - Megjelenés alatt a Polygonnál

[2.6] Prime / Csabay Károly — Daragó József. - HTTPS://DOCS.GOOGLE.COM/OPEN?ID=0B-TKH6Ox7FWwVjUxBFPFMk5PBGs

[2.7] Algebra / Fuchs László. - Budapest : Tankönyvkiadó, 1991. - 264 p.

[2.8] Algebra / Schmidt Tamás. - Budapest : Tankönyvkiadó, 1978. - 277 p.

[2.9] „HT-rendszer” — egy új lehetőség az építőkövekre bontás bemutatására / Csabay Károly. - 2010. január 23-án elhangzott MIDK-konferencia-előadás

[2.10] Kétszáz éve született Bolyai János / Kiss Elemér == KöMaL, 2002. november, pp. 457.-466.

[2.11] Absolute Algebra IV — Prime and Primary Ideals / Paul Lescot, 2011.

[3.1] Viccbeli szegény ember merengése a csontok felett, miután megette a kutyáját.

[3.2] Russell paradoxon szögekkel és spárgákkal / András Ferenc. - 2003. - Kézirat

[3.3] Elemi halmazelmélet / P. R. Halmos ; Halmazelméleti feladatok / L. E. Sigler. - Bp. : Műszaki Kvk., 1981. - 199 p. : ill. ; 25 cm

[3.4] Paradox without Self-Reference / Yablo, Stephen. - http://www.mit.edu/~yablo/pwsr.pdf