Fried Ervin

ALGEBRA II.

Algebrai struktúrák

Nemzeti Tankönyvkiadó

ALGEBRA II.
Algebrai struktúrák

Fried Ervin

ALGEBRA II.

Algebrai struktúrák

Nemzeti Tankönyvkiadó, Budapest

Felsőoktatási tankönyv

A könyv az Oktatási Minisztérium támogatásával,
a Felsőoktatási Pályázatok Irodája által lebonyolított
Felsőoktatási Tankönyv- és Szakkönyv-támogatási Pályázat keretében jelent meg.

Bírálók

Dr. Csákány Béla
egyetemi tanár

Dr. Ágoston István
egyetemi docens

A mű más kiadványban való részleges vagy teljes felhasználása, utánközlése, illetve sokszorosítása
a jogutód engedélye nélkül tilos!

ISBN 963 19 2512 9

© Fried Ervin, Nemzeti Tankönyvkiadó Rt., Budapest, 2002, jogutód Fried Katalin 2013

Nemzeti Tankönyvkiadó Rt.
A kiadásért felel: Pálfi József vezérigazgató
Raktári szám: 42 549/II
Felelős főszerkesztő: Palojtay Mária
Felelős szerkesztő: Balassa Zsófia
Műszaki szerkesztő: Görög Istvánné
A kötetet TEX szedőrendszerben gondozta: Fried Katalin
Terjedelem: 35,75 (A/5) ív
Első kiadás, 2002

TARTALOM

Előszó
(és használati javaslat 9

Első rész: Alapfogalmak 13
1. Halmazelméleti alapfogalmak 13
1.1. Halmazok 13
1.2. Reláció és függvény 16
1.3. Részbenrendezés, elrendezés, jólrendezés 18
1.4. Ekvivalenciareláció, partíció, függvény 22
1.5. Számosság 24
2. Általános algebrai alapfogalmak 27
2.1. Művelet, algebrai struktúra, típus 27
2.2. Részalgebrák 29
2.3. Izomorfizmus, homomorfizmus 31
2.4. Kongruenciareláció, faktorstruktúra, direkt szorzat 34
2.5. Néhány speciális típusú algebra 37
3. Részbenrendezett halmazok felhasználása az algebrában 40
3.1. A maximumfeltétel 40
3.2. Lezárás és Galois-kapcsolat 42
3.3. Hálók 46
3.4. Algebrai hálók reprezentálása 51

Második rész: Csoportok 56
4. Félcsoportok 56
4.1. Félcsoport definíciója és elemi tulajdonságai 56
4.2. Szabad félcsoportok 59
4.3. Félcsoportok speciális elemekkel 63
4.4. Szabad félcsoportok speciális faktorai 67
4.5. Faktorfélcsoportok invertálással 67

5. Csoportok 72
5.1. A csoport ekvivalens definíciói 72
5.2. Komplexusok, műveletek komplexusokkal 75
5.3. Részcsoportok 77
5.4. Mellékosztályok; elem és csoport rendje 78
5.5. Invariáns részcsoportok 82
5.6. Faktorcsoport, homomorfizmus-, izomorfizmustételek 87
5.7. Csoportok direkt szorzata 89
5.8. Véges Abel-csoportok 93
5.9. Speciális részcsoportok és normálosztók 101
5.10. Sylow-részcsoportok 108
5.11. Néhány speciális csoport 111
5.12. Szabad csoportok 115
6. Feloldhatóság 117
6.1. Normállánc 118
6.2. Feloldhatóság 122
6.3. Permutációcsoportok 125
6.4. Csoport-előállítás permutációcsoportokkal 131
6.5. A szimmetrikus csoport kompozícióláncai 134
6.6. Az S_n automorfizmuscsoportja 138
6.7. Lineáris transzformációk csoportja 141

Harmadik rész: Kommutatív gyűrűk 150
7. Kommutatív gyűrűk 150
7.1. Gyűrűk definíciója és elemi tulajdonságai 150
7.2. Részgyűrűk, ideálok 154
7.3. Hányadosgyűrű, lokális gyűrűk 158
7.4. Noether-gyűrű, polinomgyűrű 164
7.5. Egyértelmű felbontás 168
7.6. Karakterisztika és prímtest, egyszerű testbővítés 176
7.7. Műveletek ideálokkal, felbontási tétel 179
7.8. Ideálok gyökei 183
8. Kommutatív testek 187
8.1. Algebrai testbővítés 187
8.2. Felbontási test, algebrai lezárt 189
8.3. Véges testek 193
8.4. Hibajavító kódok 196
8.5. Szeparábilis bővítés, tökéletes test 198
8.6. Transzcendens bővítések 200
8.7. Normális bővítés 206

8.8. A klasszikus Galois-elmélet főtétele ... 208
8.9. Gyökjelekkel való megoldhatóság ... 212
8.10. Konkrét polinomtípusok megoldhatósága ... 220
8.11. A geometriai szerkeszthetőség algebrai elmélete ... 226
8.12. Az egységgyökök kiszámítása ... 229

Negyedik rész: Algebrák ... 237

9. Modulusok ... 237
9.1. Moduluselméleti alapfogalmak ... 237
9.2. Unitér modulusok ... 240
9.3. Az R-homomorfizmusok csoportja ... 241
9.4. Diagramok ... 248
9.5. Kapcsolatok az algebrai topológiával ... 250
9.6. A Hom_R funktor ... 253
9.7. Modulusok tenzorszorzata ... 261
9.8. Összefüggések $\otimes$ és Hom között ... 267

10. Algebrák ... 268
10.1. Egész elemek kommutatív gyűrűk felett ... 268
10.2. Dedekind-gyűrűk ... 271
10.3. Algebrai egészek $\mathbb{Q}$ felett ... 276
10.4. Féligegyszerű gyűrűk ... 281
10.5. Algebrák, csoportalgebra ... 285
10.6. A Jacobson-radikál ... 293
10.7. Algebrák valósan zárt testek felett ... 297

Ötödik rész: Egyéb algebrai struktúrák ... 311

11. Általános algebrák ... 311
11.1. A kifejezések algebrája ... 311
11.2. Szabad algebrák ... 314
11.3. Azonosságokkal definiálható osztály ... 318
11.4. Szubdirekt előállítás ... 325

12. Hálók ... 329
12.1. Hálók mint algebrai struktúrák ... 329
12.2. Disztributív hálók ... 338
12.3. Moduláris hálók ... 347
12.4. Atomos hálók és Boole-hálók ... 351
12.5. Kongruenciahálók ... 356

13. Rendezett csoportok és testek 357
13.1. Részbenrendezett csoportok 357
13.2. Rendezett testek 359
14. Relációalgebrák, algebrai logika 366
14.1. Relációalgebrák 366
14.2. 0–1 mérték, ultraszorzat (prímszorzat) 369
15. Kategóriák 375
15.1. Objektumok és morfizmusok 375
15.2. Funktorok 379
15.3. Kategóriák realizációja 384

Betűrendes mutató 389
Irodalomjegyzék 399

ELŐSZÓ
(és használati javaslat)

Ez a tankönyv a NEMZETI TANKÖNYVKIADÓ gondozásában 2000-ben megjelent ALGEBRA I. című tankönyv folytatása. Ennek megfelelően elsődlegesen az Eötvös Loránd Tudományegyetem másodéves matematikus és alkalmazott matematikus hallgatói számára készült, e szakoknak a tematikáját követi; vagyis a különböző (absztrakt) algebrai struktúrákkal foglalkozik. E könyv anyagának és módszereinek a tanulmányozásához megfelelő alapot ad az első kötet; noha annak ismerete itt nem feltétlenül szükséges. Igaz, hogy egyes tételeket itt nem bizonyítunk be ismételten.

Ez a könyv bevezető jellegű, tehát egyik struktúrafajtát sem vizsgálja részletesebben. Bevezető jellegű algebrajegyzet és -tankönyv Magyarországon (is) igen sok van; ezekről az irodalomjegyzékben adunk tájékoztatást. A felsoroltak mindegyike más és más felfogásban tárgyalja a fenti tananyagot, ezért nem lehet ezen tankönyveket rangsorolni; tulajdonképpen jól kiegészítik egymást. Ez a tankönyv az 1980-ban megjelent *Általános algebra* c. tankönyvem pótlására készült, amelynek legutóbbi kiadása is elfogyott. Tekintettel arra, hogy az idézett tankönyvhöz képest itt is lényeges változtatásokat éreztem szükségesnek, ezért nem tartottam volna jónak a fenti tankönyv újabb – lényegében változatlan – kiadását. Nem változtattam a könyv „szellemén", a tananyagot is főleg bővítettem. Igen lényeges különbség található a két könyv szerkezetében.

Az egész kötetet öt nagyobb részre osztottam fel. Az első résznek a címe: Alapfogalmak. Ide soroltam azokat a fogalmakat és ismereteket, amelyek egyik későbbi struktúrafajtához sem kapcsolhatók külön. Ennek következtében az itteni fogalmak nincsenek is konkrét példákkal megvilágítva.

Célszerű, hogy az első rész tüzetes átolvasása csak akkor történjen meg, ha valahol később ezekre az ismeretekre szükség van. Ezt utalások, illetve a nevek jelzik. Az algebrában is, mint bármely matematikai ágazatban az okoz gondot, hogy a fogalmak csak a példák után érthetők meg, viszont a példák megadásánál szükség van a pontos fogalmakra. (Ezért szokták a jobb képességű hallgatók egy-egy tárgy lehallgatása után azt mondani, hogy most kellene ismét felvenni ezt a tárgyat.)

A második rész olyan struktúrákkal foglalkozik, amelyek egyetlen kétváltozós művelet segítségével definiálhatók; nevezetesen egy rövid félcsoport-elméleti bevezetés után a csoportelmélettel. A harmadik rész tárgya a kommutatív gyűrűk elmélete. Itt a polinomgyűrűk megértését célzó rész, valamint az egyenletekkel foglalkozó (és ehhez kapcsolódó) részek szerepelnek. A negyedik rész témája az algebrák (az ilyen nevű algebrai struktúrák). Itt a modulusok általánosabb elmélete van (hagyatkozva az első kötetbeli ismeretekre). Az algebrák fontosságát az adja, hogy ezek vektorterek és gyűrűk is egyszerre; és igen sok fontos struktúra algebra. A kommutatív esetben az algebrai egészek, a nemkommutatív esetben

a csoportalgebrák vizsgálata a leglényegesebb pont. Az ötödik rész címe: egyéb algebrai struktúrák. Ez a kaleidoszkópszerű „színes forgatag” olyan témákat tartalmaz, amelyek egyrészt a már tárgyalt struktúrák „mögé” tekintenek, másrészt kapcsolatot teremtenek „nem algebrai” ágakkal.

E könyvben sokkal több feladat szerepel, mint az *Általános algebra* c. tankönyvemben. Ezek a feladatok részben az idézett könyv megírása óta eltelt idő „oktatási termékei”, részben e kötet írásakor keletkeztek. Nagyszámú hasznos és igen jó feladat található a TANKÖNYVKIADÓ gondozásában 1988-ban megjelent és BÁLINTNÉ SZENDREI MÁRIA, CZÉDLI GÁBOR és SZENDREI ÁGNES készítette *Absztrakt algebrai feladatok* című példatárban. Igyekeztem, hogy az itteni feladatanyagnak ne legyen átfedése a fenti példatárral; nem biztos, hogy ez maradéktalanul sikerült. A feladatok az egyes alfejezetek után következnek, illetve amikor kevés feladat adódott, vagy a feladatok megoldásához a későbbi anyag ismerete is szükséges volt, akkor e feladatok több alfejezet után szerepelnek együtt. A feladatok nagy része az anyag megértését szolgálja, de szerepelnek komolyabb gondolkozást megkívánó feladatok is. Ezt külön nem jeleztem. (Kérem, aki a kötetek bármelyikében hibát talál, észrevételét jelezze e-mailben, a `fried.algebra@cs.elte.hu` címen. A talált hibák javítása – lehetőleg naprakészen – megtalálható lesz az internet `http://www.math.elte.hu/fried.algebra` oldalán.)

(Itt említem meg, hogy az első kötetben a rezultánsnál elírás történt: a 296. és 297. oldalon a_n^n és b_k^k helyesen a_n^k és b_k^n.)

Ebben a könyvben ■ jelöli a bizonyítások és □ jelöli a definíciók és a megjegyzések végét.

Remélem, hogy ezt a tankönyvet is sikerrel használhatják más szakok és más egyetemek elsősorban matematikus szakra járó, de egyéb matematikát – mindenekelőtt algebrai módszereket – tanuló egyetemi hallgatói is.

Mint az első kötetben is említettem, egyetlen könyv (de az internet sem) pótolhatja az élő előadás élményét. A matematikát csak úgy lehet megtanulni, ha (lehetőleg aktívan) nyomon követjük a gondolkodásmódot, az esetleges hibákat; és a tételeket, a fogalmakat és a bizonyításokat *in statu nascendi* (a születés pillanatában) láthatjuk. Semmi sem pótolhat egy vitát az előadóval. Az írott segédanyagra az ismeretek felfrissítésekor van szükség. Ettől függetlenül célszerűnek tartom azt, hogy a tankönyv a közölt tananyagon kívül lehetőleg gondolkozni is tanítson és magyarázzon. Természetesen ehhez szükséges, hogy a fogalmak, tételek és a bizonyítások (eltekintve néhány hosszadalmas és mechanikus bizonyítástól) mind megtalálhatóak legyenek a tankönyvben.

Az itt szereplő fogalmak és tételek nem csak az elméleti és az alkalmazott matematika egyéb területeiről származnak, hanem gyökerük számos esetben az algebrán belül van. Ennek ellenére általában lemondtam e fogalmaknak a motivációjáról, mert ez az egész tárgyalást igen hosszadalmassá és esetleg érthetetlenebbé tenné.

Köszönetnyilvánítás. E könyv készítésével kapcsolatban is szeretném hálámat kifejezni azoknak, akik velem a matematikai gondolkozásmódot megismertették és megszerettették. Így NEUKOMM GYULA gimnáziumi tanáromnak, GEHÉR ISTVÁN egyetemi diáktársamnak, FUCHS LÁSZLÓ, RÉNYI ALFRÉD, PÉTER RÓZSA és mindenekfelett TURÁN PÁL egyetemi tanáraimnak. Hálával tartozom diákjaimnak és tanítványaimnak, akik állandó javító célzattal bírálták munkáimat; és akiktől ugyancsak nagyon sokat tanultam. Ezeknek a diákoknak a száma olyan nagy, hogy őket felsorolva óhatatlanul kimaradna jó néhány, akiket nem szeretnék megbántani. Ezért inkább egyetlen nevet sem írok ide; ők úgyis tudják, hogy

róluk van szó. Hálával tartozom algebrista kollégáimnak, akik jelenlétükkel erősítették a magyar algebrista közösséget.

Vannak, akik a könyv második kötetének a közvetlen megjelenését is elősegítették. Hálával és köszönettel tartozom két lektoromnak, név szerint CSÁKÁNY BÉLÁNAK és ÁGOSTON ISTVÁNNAK, akik magukra vállalták az átnézés keserveit, számos értelemzavaró hibától mentve meg a könyvet. Ha hiba maradt benne, az nem az ő munkájukat, hanem az enyémet minősíti.

Hálával tartozom a könyv előállításában való részvételéért FRIED KATALINNAK a tördelésért, a Nemzeti Tankönyvkiadóban PALOJTAY MÁRIÁNAK és BALASSA ZSÓFIÁNAK, akik a könyvet gondozták. Hálával tartozom az anyagi háttér biztosításáért a SZÉCHENYI PROFESSZORI ÖSZTÖNDÍJNAK, valamint a **T 029525** számú OTKA-nak. Végül, de nem utolsósorban hálával tartozom feleségemnek, HAY ERZSÉBETNEK, az erkölcsi háttér biztosításáért, türelméért és a könyv átolvasásában nyújtott segítségéért.

Budapesten a 2002. évben

Fried Ervin

ELSŐ RÉSZ
ALAPFOGALMAK

Az algebra tárgyát röviden a következőképpen fogalmazhatnánk meg: műveletekkel ellátott halmazok vizsgálata. Noha ez a meghatározás csak durván tükrözi a valóságot, arra azonban felhívja a figyelmet, hogy az algebrai vizsgálatokban igen lényeges szerepet játszanak a halmazelméleti alapfogalmak. Ennek megfelelően az első részben először halmazelméleti alapfogalmakat vizsgálunk. Ezután az algebrai alapfogalmakra térünk rá. Végezetül a részbenrendezett halmazoknak olyan vizsgálata szerepel, amely az algebrában igen fontos.

1. Halmazelméleti alapfogalmak

Ennek a fejezetnek a legnagyobb része már ismert fogalmak átismétlése és rendszerezése. Egyedül a jólrendezéssel kapcsolatos tételek újak. (Egyes esetekben szemléltetés végett később definiált fogalmak is szerepelnek, de akkor ezek már az első kötetben is felléptek.)

1.1. Halmazok

Nem célunk, és nem is lehet itt célunk az, hogy szigorú halmazelméleti megalapozást nyújtsunk. Arra törekszünk csupán, hogy ismertessük azokat a fontosabb halmazelméleti fogalmakat és összefüggéseket, amelyeket majd felhasználunk. Lényegében az úgynevezett „naiv halmazelméletet” tárgyaljuk, és bizonyos szemléletes tényeket a későbbiekben is „gátlástalanul” felhasználunk. Egy ponton térünk el a naiv halmazelmélettől: bevezetjük az osztály fogalmát is. Erre ugyanis bizonyos algebrai vizsgálatoknál szükségünk lesz. A halmazelmélet két alapvető fogalma az *osztály* és az *elemének lenni*. Az osztály fogalmára azért van szükség, hogy olyan nagy összességeket is megengedhessünk, amelyek más összességnek nem lehetnek elemei. Ennek megfelelően, *ha az A osztály eleme a B osztálynak (jelben: $A \in B$), akkor A halmaz*. Ha a fenti kapcsolat nem áll fenn, ezt $A \notin B$ fogja jelölni (*A nem eleme B-nek*). *Két osztály pontosan akkor egyenlő, ha elemeik ugyanazok.*

Az alábbiakban csak halmazokra mondjuk ki állításainkat, de ezek jó része igaz az osztályokra is. A halmazok egyenlőségére vonatkozó állítás alapján minden halmaz megadható elemeivel. Ezt formailag a következőképpen tesszük. Ha mód van rá, akkor kapcsos

zárójelen belül felsoroljuk a halmaz elemeit, vagy addig folytatjuk a felsorolást, amíg világosan nem látható, hogy mik a halmaz elemei. Például:

$$\{1, 5, 13\} \quad \text{vagy} \quad \{2, 4, 6, \ldots\}, \quad \text{vagy} \quad \{1, 4, 9, 16, \ldots\}.$$

Az első halmaz minden elemét felsoroltuk, a második halmaz elemei nyilván a páros természetes számok, a harmadiké pedig a négyzetszámok.

Amennyiben ilyen felsorolás nem adható meg, vagy nagyon kényelmetlen volna, akkor a zárójelen belül egy függőleges vonalat húzunk, amelynek a bal oldalán olyan elemek állnak, amelyek közül a halmaz elemei kikerülnek, jobb oldalán pedig azt az „utasítást" írjuk le, amelynek alapján a halmaz elemeit „kiválasztjuk". Így

$$B = \{x \mid x \in A\}$$

azt jelenti, hogy $B = A$. Mint látható, *a halmazokat nagy latin betűkkel fogjuk jelölni.* Noha a halmazok elemei is halmazok, általában *a halmazok elemeinek a jelölésére kis latin betűket használunk.*

Egy halmaz elemei között nincsenek megegyezők. Amennyiben ez előfordulhat, akkor halmaz helyett *rendszerről* beszélünk. (Például egy lineárisan összefüggő vektorrendszerben ugyanaz a vektor többször is szerepelhet.) A rendszer is kifejezhető a halmazelméleti alapfogalmak segítségével (ennek a pontos mikéntjére a függvények tárgyalásánál térünk ki). A halmazjelölés bemutatott formái rendszerekre is alkalmazhatók.

Tényként fogadjuk el, hogy létezik olyan halmaz, amelynek nincsenek elemei. Mivel minden halmazt egyértelműen meghatároznak az elemei, ezért csak egyetlen ilyen halmaz van: ezt *üres halmaznak* nevezzük és a $\emptyset$ jellel jelöljük.

Megjegyezzük, hogy az üres halmaz „léte" nélkül a többi alaptulajdonságból nem lehetne következtetni arra, hogy léteznek halmazok; míg az üres halmazból már végtelen sok halmazt tudunk „konstruálni" a következőképpen:

$$\emptyset, \quad \{\emptyset\}, \quad \{\emptyset, \{\emptyset\}\} \quad \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \quad \ldots$$

Az itt felsorolt halmazok nemcsak különbözőek, hanem elemszámuk $(0, 1, 2, 3, \ldots)$ is egyre növekszik. (Feltesszük, hogy egyetlen halmaz sem eleme önmagának.)

A halmazok között az „elemének lenni" kapcsolaton kívül létezik egy másik igen fontos kapcsolat:

Az A halmaz *része* vagy *részhalmaza* a B halmaznak, ha az A minden eleme a B halmaznak is eleme. E kapcsolatot $A \subseteq B$ jelöli. Ha emellett $A \neq B$, akkor *valódi részről* beszélünk (jelben: $A \subset B$). Minden halmaznak része az üres halmaz.

Az A és B halmazok $A \cup B$ *egyesítését* és $A \cap B$ *metszetét* a következőképpen értelmezzük:

$$A \cup B = \{x \mid x \in A \text{ vagy } x \in B\}, \qquad A \cap B = \{x \mid x \in A \text{ és } x \in B\}.$$

Ha $A \cap B = \emptyset$, akkor azt mondjuk, hogy A és B *idegen* vagy *diszjunkt* halmazok.

Beszélhetünk több halmaz egyesítéséről vagy metszetéről is, ehhez azonban szükségünk van az *indexezésre*. Ez tulajdonképpen egy függvény, ami egy I úgynevezett *indexhalmaz* minden i eleméhez hozzárendel egy A_i halmazt. (A függvényt definiálhatjuk a halmazelmélet egyéb fogalmaival, mi azonban definiálatlan alapfogalomnak fogjuk tekinteni.)

Az $\{A_i \mid i \in I\}$ halmazrendszer egyesítését, illetve metszetét a következőképpen értelmezzük:

$$\left\{\bigcup A_i \mid i \in I\right\} = \{x \mid \text{legalább egy } i \in I \text{ mellett } x \in A_i\},$$

$$\left\{\bigcap A_i \mid i \in I\right\} = \{x \mid \text{minden } i \in I \text{ mellett } x \in A_i\}.$$

Ha kétértelműség nem lép fel, akkor az $\bigcup A_i$, illetve a $\bigcap A_i$ jelölést használjuk. Ha az $\{A_i \mid i \in I\}$ halmazrendszer pontosan a B halmaz elemeiből áll, akkor $\left\{\bigcup A_i \mid i \in I\right\}$ helyett az $\left\{\bigcup A \mid A \in B\right\}$ jelölés is szerepelhet.

Egy $\{A_i \mid i \in I\}$ halmazrendszer *idegen*, illetve *páronként idegen*, ha $\bigcap A_i = \emptyset$, illetve bármely különböző $i, j \in I$ esetén $A_i \cap A_j = \emptyset$.

Az A halmaz $P(A)$ *hatványhalmazán* az A halmaz részhalmazainak halmazát értjük:

$$P(A) = \{B \mid B \subseteq A\}.$$

Az A halmaz *partícióján* vagy *osztályozásán* az A halmaz részhalmazainak olyan rendszerét értjük, amelyek az A halmazt „egyrétűen lefedik”. Más szóval $\pi \subseteq P(A)$ partíció, ha π különböző elemei páronként idegenek és $\left\{\bigcup B \mid B \in \pi\right\} = A$. Felhívjuk a figyelmet arra, hogy definíciónk szerint π elemei a „felsorolásban” többször is szerepelhetnek.

Az A és B halmazok $A \setminus B$ *különbségén* azoknak az A-beli elemeknek a halmazát értjük, amelyek nem elemei B-nek. Így $A \setminus B = \{x \mid x \in A \text{ és } x \notin B\}$. Amennyiben $B \subseteq A$, akkor azt mondjuk, hogy $A \setminus B$ *a B-nek az A-ra vonatkozó komplementuma*. Ha A valamilyen természetes módon rögzítve van, akkor egyszerűen a B *komplementumáról* beszélünk; ezt $\overline{B}$ jelöli. Világos, hogy $\overline{B}$ komplementuma B.

Az A és B halmaz *szorzatát* vagy *Descartes-szorzatát*

$$A \times B = \{(a, b) \mid a \in A \text{ és } b \in B\}$$

definiálja. E halmaz elemei tehát elempárok. Hasonló elv alapján értelmezhetők a *többtényezős szorzatok* is. Például:

$$A \times B \times C \times D = \{(a, b, c, d) \mid a \in A, b \in B, c \in C, d \in D\}.$$

A szorzatot általában $\left\{\prod A_i \mid i \in I\right\}$ jelöli, ahol az I *indexhalmaz* nem feltétlenül véges. E szorzat egy-egy elemét $(\ldots, a_i, \ldots)$ vagy valami hasonló fogja jelölni. A fenti esetben az a_i neve a szereplő elem *i-edik komponense*. Felhívjuk a figyelmet arra, hogy a többtényezős szorzat nem a kéttényezős szorzat ismétlése; $A \times B \times C$ elemei elemhármasok, míg $(A \times B) \times C$ elemei olyan elempárok, amelyeknek az első komponense is elempár. (Természetesen létezik közöttük egy „természetes bijekció”.)

Ha egy szorzat minden tényezője ugyanaz a halmaz, akkor *hatványról* beszélünk. Az A halmaz n-tényezős hatványát A^n jelöli ($n > 1$ természetes szám). Az $n = 1$ esetben definíció szerint legyen $A^1 = A$, ha pedig $n = 0$, akkor ugyancsak definíció szerint legyen $A^0 = \{\emptyset\}$.

1.2. Reláció és függvény

A relációkat igen általánosan lehet definiálni. Mi itt elsősorban csak speciális típusú (ún. binér) relációkkal foglalkozunk. Ezeket használják a leggyakrabban, és nekünk is főleg csak ezekre lesz szükségünk.

Az (A, B) halmazpáron értelmezett (kétváltozós) relációnak vagy A és B közötti megfeleltetésnek nevezzük az $A \times B$ halmaz tetszőleges ϱ részhalmazát. Az $A \neq B$ esetben *heterogén*, míg $A = B$ esetén *homogén* relációról beszélünk. Az utóbbi esetben azt mondjuk, hogy ϱ *reláció az A halmazon.*

(Általában, az A halmazon értelmezett n-változós reláción az A^n egy részhalmazát értjük.)

Ha $(a, b) \in \varrho$, akkor azt mondjuk, hogy *a és b relációban állnak (egymással).* Ezt a következőképpen szokták még jelölni:

$$\varrho(a, b), \qquad \text{illetve} \qquad a \varrho b.$$

(Megjegyezzük, hogy 0-változós relációt nem értelmezünk, egyváltozós reláció az A halmaz egy részhalmaza; többváltozós reláció esetén csak az $(a_1, \ldots, a_n) \in \varrho_n$ jelölést használjuk.)

Az (A, B) halmazpáron értelmezett relációk halmaza nyilvánvalóan $P(A \times B)$. E halmaz jelölésére $B = A$ esetén az $R(A)$ jelölést fogjuk használni. Az $A \times A$ halmazt *teljes* (vagy *univerzális*) *relációnak* nevezzük. Egy $\varrho \in R(A)$ reláció ($A \times A$-beli) $\overline{\varrho}$ komplementerét ϱ *komplementer relációjának* nevezzük. A teljes reláció komplementere az *üres reláció*, amit ugyancsak $\emptyset$ jelöl. Igen fontos egy A halmaz *diagonális relációja*, amit

$$\Delta(A) = \{(a, a) \mid a \in A\}$$

definiál.

Egy $\varrho \in P(A \times B)$ reláció ϱ^{-1} *inverzét* a következőképpen értelmezzük:

$$\varrho^{-1} = \{(b, a) \mid a, b \in \varrho\}.$$

Könnyen igazolhatók az alábbi összefüggések:

$$\overline{(\overline{\varrho})} = \varrho, \qquad (\varrho^{-1})^{-1} = \varrho, \qquad (\overline{\varrho})^{-1} = \overline{(\varrho^{-1})}, \qquad (\Delta^{-1}) = \Delta.$$

Bizonyos esetekben értelmezhetjük *relációk kompozícióját* vagy *szorzatát.* Ha $\varrho \in P(A \times B)$ és $\sigma \in P(B \times C)$, akkor kompozíciójukat a

$$\varrho \circ \sigma = \{(a, c) \mid \text{létezik olyan } b \in B, \text{ amelyre } (a, b) \in \varrho \text{ és } (b, c) \in \sigma\}$$

összefüggés definiálja.

1.1. Tétel. *A relációk szorzata asszociatív.*

Bizonyítás. Legyen adva az előzőeken kívül még egy $\tau \in P(C \times D)$ reláció. Ha $(a, d) \in (\varrho \circ \sigma) \circ \tau$, akkor létezik olyan $c \in C$, amelyre $(a, c) \in \varrho \circ \sigma$ és $(c, d) \in \tau$. Az első összefüggésből következik, hogy létezik olyan B-beli b, amelyre $(a, b) \in \varrho$ és $(b, c) \in \sigma$. Ekkor viszont a most adott b-re $(a, b) \in \varrho$ mellett $(b, d) \in \sigma \circ \tau$ is igaz, a fent talált $c \in C$ tulajdonságai alapján. Így pedig $(a, d) \in \varrho \circ (\sigma \circ \tau)$ is teljesül. Hasonlóképpen bizonyítható a $\varrho \circ (\sigma \circ \tau) \subseteq (\varrho \circ \sigma) \circ \tau$ összefüggés is; amiből azonnal adódik a két reláció egyenlősége. ■

Könnyen igazolhatók az alábbi összefüggések:

$$\emptyset \circ \varrho = \varrho \circ \emptyset = \emptyset, \qquad \Delta \circ \varrho = \varrho \circ \Delta = \varrho, \qquad (\varrho \circ \sigma)^{-1} = \sigma^{-1} \circ \varrho^{-1},$$

feltéve, hogy a felírt kompozíciók elvégezhetők (Δ a „megfelelő” $\Delta(A)$-t jelöli).

Ha $\varrho \in R(A)$ és $B \subseteq A$, akkor $\varrho|_B = \varrho \cap B^2$ a ϱ-nak a B-re való *megszorítása*. Ha $B \subseteq A$, $\sigma \in R(B)$, $\varrho \in R(A)$ és σ a ϱ-nak B-re való megszorítása, akkor ϱ a σ-nak (egy) A-ra való *kiterjesztése*.

Az alábbiakban homogén relációk néhány fontos tulajdonságát vezetjük be.

A ϱ reláció *reflexív*, ha $\Delta \subseteq \varrho$ (azaz minden $a \in A$ elemre $a\varrho a$).

A ϱ reláció *irreflexív*, ha $\Delta \cap \varrho = \emptyset$ (azaz $a\varrho a$ sohasem teljesül).

A ϱ reláció *szimmetrikus*, ha $\varrho^{-1} \subseteq \varrho$ (azaz $a\varrho b$ esetén $b\varrho a$ is igaz). Ezzel ekvivalensek a $\varrho \subseteq \varrho^{-1}$ és $\varrho^{-1} = \varrho$ feltételek is.

A ϱ reláció *antiszimmetrikus*, ha $\varrho \cap \varrho^{-1} \subseteq \Delta$ (azaz $a\varrho b$ és $b\varrho a$ együttesen csak $a = b$ esetén teljesülhet).

A ϱ reláció *szigorúan antiszimmetrikus*, ha $\varrho \cap \varrho^{-1} = \emptyset$ (azaz $a\varrho b$ és $b\varrho a$ sohasem teljesülhet egyszerre).

A ϱ reláció *trihotom*, ha $\{\varrho, \varrho^{-1}, \Delta\}$ partíció (azaz bármely $a, b \in A$ elemre $a\varrho b$, $b\varrho a$ és $a = b$ közül pontosan az egyik teljesül).

A ϱ reláció *tranzitív*, ha $\varrho \circ \varrho \subseteq \varrho$ (ez azt jelenti, hogy ha $a\varrho b$ és $b\varrho c$, akkor $a\varrho c$ is teljesül).

A fenti fogalmakra a gráfelméletben egyéb elnevezések is használatosak. Így, tetszőleges (homogén) relációt *irányított gráfnak* neveznek. Ha a reláció irreflexív, akkor *hurokmentes gráfról* van szó. Szimmetrikus reláció esetén *irányítatlan*, míg irreflexív és szimmetrikus reláció esetén *irányítatlan hurokmentes* gráfról beszélünk. Sok esetben az irányítatlan jelzőt nem szokták kitenni.

Az algebrában is igen fontos a *függvény* (*leképezés*) fogalma. A függvényeket a halmazelméleti fogalmak segítségével is lehet értelmezni, de – mint az előző pontban említettük – kényelmesebb számunkra, ha *a függvényeket is definiálatlan alapfogalomnak tekintjük*. Minden φ függvényhez tartozik két halmaz, a $D(\varphi)$ értelmezési tartomány és az $R(\varphi)$ értékkészlet. E kapcsolatot a következőképpen jelöljük:

$$\varphi : D(\varphi) \to R(\varphi) \qquad \text{vagy} \qquad D(\varphi) \overset{\varphi}{\to} R(\varphi).$$

$D(\varphi)$ tetszőleges a elemének a φ függvény „megfelelteti” az $R(\varphi)$ egy egyértelműen meghatározott b elemét. E kapcsolatot a következőképpen jelölhetjük:

$$b = \varphi(a), \qquad \text{vagy} \qquad \varphi : a \mapsto b, \qquad \text{vagy} \qquad (a, b) \in \varphi.$$

Felhívjuk a figyelmet arra, hogy a második jelölésnél a nyílnak „talpa” van; ezzel különböztetjük meg attól a jelöléstől, ami az értelmezési tartomány és az értékkészlet között szerepel. A harmadik jelölés arra akar rámutatni, hogy *a függvény speciális relációnak tekinthető*.

Egy $\varphi \in A \times B$ reláció akkor és csak akkor tekinthető függvénynek, ha:

1. *Minden $a \in A$ elemhez van olyan $b \in B$, hogy $(a, b) \in \varphi$.*

2. *Ha $(a, b_1), (a, b_2) \in \varphi$, akkor $b_1 = b_2$.*

A továbbiakban *egy függvény és a neki megfeleltetett reláció között nem teszünk különbséget*.

Azonnal látható, hogy a fenti 1. és 2. tulajdonságok bármelyike megmarad relációk szorzata esetén is. Ennek következménye: *két függvény relációszorzata is függvény*.

A függvények esetében beszélünk ezek *függvényszorzatáról* (*függvénykompozíciójáról*) is, amely éppen fordított sorrendben végezhető, mint a relációszorzás. Legyen $\varphi : A \to B$ és $\psi : B \to C$ két függvény. Ezek $\varphi \circ \psi$ relációszorzata azokból az (a, c) párokból áll, amelyekre alkalmas $b \in B$ elemmel $(a, b) \in \varphi$ és $(b, c) \in \psi$. Mivel itt függvényekről van szó, ezért b felírható $\varphi(a)$, c pedig $\psi(b)$ alakban, vagyis felírható a $c = \psi(\varphi(a))$ összefüggés. A kapott függvénykompozíció szokásos jelölése $\psi\varphi$, vagy $\psi \cdot \varphi$, vagy $\psi \circ \varphi$.

Érdemes jól az emlékezetünkbe vésni, hogy ha $\varphi : A \to B$ és $\psi : B \to C$ függvények, akkor $\varphi \circ \psi$ ezek relációszorzatát, míg $\psi \circ \varphi$ függvényszorzatukat jelöli.

Legyen $\varphi : A \to B$ tetszőleges függvény. Az A halmaz egy C részhalmaza esetén $\varphi(C)$-vel jelöljük a $\{\varphi(x) \mid x \in C\}$ halmazt. Ha speciálisan $C = A$, akkor az $\mathrm{Im}(\varphi) = \varphi(A)$ jelölést fogjuk használni. Az $\mathrm{Im}(\varphi)$-t a φ *képhalmazának* nevezzük. Ha $\mathrm{Im}(\varphi) = B$, akkor azt mondjuk, hogy φ *szürjekció* vagy *szürjektív* függvény (magyarul *ráképezés* is használatos).

A $\varphi : A \to B$ függvény φ^{-1} inverz relációja általában nem függvény. Ez a reláció mégis igen fontos. Ha D tetszőleges részhalmaza B-nek, akkor a $\varphi^{-1}(D) = \{x \in A \mid \varphi(x) \in D\}$ halmazt, amely A-nak részhalmaza, a D *teljes inverz képének* nevezzük. A $D = \{b\}$ esetben a $\varphi^{-1}(b)$ jelölést is fogjuk használni. Ha $\varphi^{-1}(b)$-nek bármely B-beli b esetén legfeljebb egy eleme van, akkor azt mondjuk, hogy φ *injekció* vagy *injektív függvény*. Látható, hogy egy φ függvény pontosan akkor injekció, ha $\varphi(a_1) = \varphi(a_2)$ esetén $a_1 = a_2$ is teljesül.

Nyilvánvalóan igaz, hogy *injekciók függvényszorzata injekció*, és *szürjekciók függvényszorzata szürjekció*.

Egy függvényt *bijekciónak* nevezünk, ha injekció és szürjekció: Világos, hogy az injekciók és szürjekciók függvényszorzatára az előzőekben kimondottak alapján, *bijekciók függvényszorzata bijekció*.

Végül megemlítjük, hogy az indexezés úgy adható meg egy $\varphi : I \to P(A)$ függvénnyel, hogy az $i \in I$ elemhez a $\varphi(i) = A_i$ halmazt rendeljük hozzá. Ezzel egyszersmind a halmazrendszereket is le lehet írni, hiszen az A_i és A_j elemek akkor is megegyezhetnek, ha $i \neq j$.

A fentiekben „egyváltozós” függvényekről beszéltünk, de szükség van *többváltozós függvényekre* is. Ezek azonban nem okoznak elvi gondot, mert egy többváltozós függvény nem más, mint a direkt szorzaton értelmezett egyváltozós függvény.

1.3. Részbenrendezés, elrendezés, jólrendezés

Egy halmazon értelmezett relációk között két olyan típus is van, amely számunkra igen fontos. Ezek egyike a részbenrendezés, a másik az ekvivalenciareláció.

Egy ϱ relációt részbenrendezésnek nevezünk, ha reflexív, antiszimmetrikus és tranzitív.

Egy σ relációt szigorú részbenrendezésnek nevezünk, ha irreflexív, szigorúan antiszimmetrikus és tranzitív.

1.2. Tétel. *Ha ϱ részbenrendezés és σ szigorú részbenrendezés egy A halmazon, akkor $\varrho \setminus \Delta$ szigorú részbenrendezés, és $\sigma \cup \Delta$ részbenrendezés. Ezen felül érvényes a $(\varrho \setminus \Delta) \cup \Delta = \varrho$ és a $(\sigma \cup \Delta) \setminus \Delta = \sigma$ összefüggés.*

Bizonyítás. $\varrho \setminus \Delta$ irreflexív és $\sigma \cup \Delta$ reflexív, tetszőleges ϱ és σ reláció esetén. Ha $(a, b) \in \varrho \setminus \Delta$, akkor $a \neq b$, amiből ϱ antiszimmetriája miatt $(b, a) \notin \varrho$. Így $\varrho \setminus \Delta$ sem tartalmazza (b, a)-t, amiből adódik a szigorú antiszimmetria. Ha $(a, b) \in \sigma$, akkor $(b, a) \notin \sigma$. Így e két pár mindegyike csak úgy lehet eleme $\sigma \cup \Delta$-nak, ha Δ-nak eleme, vagyis tényleg antiszimmetrikus relációt kaptunk.

Tegyük most fel, hogy $(a, b), (b, c) \in \varrho \setminus \Delta$. Ekkor ϱ tranzitivitásából $(a, c) \in \varrho$ következik. Mivel $\varrho \setminus \Delta$ szigorúan antiszimmetrikus, ezért $c \neq a$; és így $(a, c) \in \varrho \setminus \Delta$. Ezzel $\varrho \setminus \Delta$ tranzitivitását bizonyítottuk. Tegyük most fel, hogy (a, b) és (b, c) elemei $\sigma \cup$ $\cup \Delta$-nak. Ha mindketten σ-nak is elemei, akkor a tranzitivitásból következik, hogy (a, c) is eleme σ-nak. Ha egyikük eleme σ-nak, a másik pedig Δ-beli, akkor (a, c) megegyezik az (a, b) és (b, c) valamelyikével, és így ugyancsak σ-beli. Amennyiben pedig mindketten Δ-beliek, akkor (a, c) is az. Eszerint (a, c) mindig eleme $\sigma \cup \Delta$-nak, ami bizonyítja a tranzitivitást.

Az utolsó két állítás azonnal következik abból, hogy $\Delta \subseteq \varrho$ és $\sigma \cap \Delta = \emptyset$. ■

A most bizonyított tétel szerint bármely részbenrendezés egyértelműen meghatároz egy szigorú részbenrendezést, és viszont. Ha egy halmazon adott egy rögzített részbenrendezés, akkor ezt a $\leq$ jel fogja jelölni. A megfelelő szigorú részbenrendezésre pedig a $<$ jelet fogjuk használni.

Érdemes megjegyezni, hogy a ϱ részbenrendezéssel együtt ϱ^{-1} is az. A $\leq$ és $<$ relációk inverzét, megfelelően, $\geq$ és $>$ fogja jelölni.

A részbenrendezésre *tipikus példát* adnak egy halmaz részhalmazai, amelyek között a reláció a tartalmazás. Valóban, a H halmaz tetszőleges A részhalmazára $A \subseteq A$; a H halmaz A és B részhalmazaira $A \subseteq B$ és $B \subseteq A$ csak úgy állhatnak fenn, ha $A = B$; s ha a H halmaz A, B és C részhalmazaira $A \subseteq B$ és $B \subseteq C$ igaz, akkor $A \subseteq C$ is teljesül. Azt, hogy ez a példa tipikus, úgy értjük, hogy minden részbenrendezés „elképzelhető” mint egy halmaz bizonyos részhalmazai között fennálló tartalmazási reláció. Tekintsük ugyanis a H halmaznak egy $\leq$ részbenrendezését. Feleltessük meg a halmaz tetszőleges a elemének a $H_a = \{x \mid x \leq a\}$ halmazt. Ez a megfeleltetés visszafelé is egyértelmű, hiszen $H_a = H_b$ azt jelenti, hogy $a \leq b$ és $b \leq a$, ami csak $a = b$ esetén teljesülhet. Ha mármost $a \leq b$, akkor a tranzitivitás miatt $H_a \subseteq H_b$; míg $H_a \subseteq H_b$-ből a definíció szerint következik $a \leq b$.

Ha az A halmazon adott a $\leq$ részbenrendezés, akkor ehelyett azt is mondhatjuk, hogy $\langle A; \leq \rangle$ *részbenrendezett halmaz.*

Ha $B \subseteq A$, akkor a $\leq$ részbenrendezésnek a B-re való megszorítását is ugyanígy fogjuk jelölni. $\langle B; \leq \rangle$ nyilvánvalóan szintén részbenrendezett halmaz. Az így kapott részbenrendezést *indukált részbenrendezésnek* nevezik.

Legyen B az $\langle A; \leq \rangle$ részbenrendezett halmaz tetszőleges részhalmaza. Ha $a \in B$ olyan, hogy B-ben nincs az a-nál kisebb elem (azaz $x < a$ esetén $x \notin B$), akkor azt mondjuk, hogy a a B-nek egy *minimális eleme.* (Világos, hogy egy tetszőleges, részbenrendezett halmaz bármely véges részhalmazának van minimális eleme.) Ha az $a \in B$ elem a B halmaz minden, tőle különböző eleménél kisebb, akkor a a B-nek *legkisebb eleme.* A szigorú antiszimmetria következtében egy részhalmaznak a legkisebb eleme (ha van ilyen)

egyértelmű. (Legkisebb elem általában még véges részbenrendezett halmazok esetében sem létezik.) Analóg módon definiálhatjuk egy részhalmaz *maximális elemeit*, illetve *legnagyobb elemét*. Ezek nem mások, mint a szóban forgó részhalmaz minimális elemei, illetve a legkisebb eleme, ha az eredeti részbenrendezés helyett ennek inverzét tekintjük.

Tekintsük az $\langle A; \leq \rangle$ részbenrendezett halmaz egy tetszőleges B részhalmazát. Ha valamely $x \in A$-ra minden $b \in B$ esetén teljesül $x \leq b$, akkor azt mondjuk, hogy x *alsó korlátja* B-nek. Hasonlóan, ha valamely A-beli y-ra minden B-beli b esetén $b \leq y$ teljesül, akkor y *felső korlátja* B-nek. A B alsó korlátjainak a halmazát $L(B)$, felső korlátjainak a halmazát $U(B)$ jelöli. Ha az $L(B)$ halmaznak van egy u legnagyobb eleme, akkor azt mondjuk, hogy u a B-nek *legnagyobb alsó korlátja*. (Ez tehát azt jelenti, hogy u alsó korlátja B-nek és B bármely x alsó korlátja esetén $x \leq u$ – azaz u felső korlátja B alsó korlátainak.) A B részhalmaz legnagyobb alsó korlátját $\bigwedge\{b \mid b \in B\}$ fogja jelölni. ($b \in B$ helyébe bármely más olyan meghatározás írható, amelyik megadja, hogy mely b elemeket kell figyelembe venni.) Hasonlóképpen az előzőekhez, lehetséges, hogy van az $U(B)$ elemei között egy v legkisebb elem, amit a B *legkisebb felső korlátjának* nevezünk, és $\bigvee\{b \mid b \in B\}$-vel jelölünk ($v$ tehát felső korlát és a felső korlátok alsó korlátja).

Két elem, a és b legnagyobb alsó, illetve legkisebb felső korlátját $a \wedge b$, illetve $a \vee b$ is fogja jelölni.

Most egy fontos speciális esetre térünk rá:

Az $\langle A; \leq \rangle$ részbenrendezett halmazt *rendezett*, *elrendezett* vagy *teljesen rendezett* halmaznak nevezünk, ha a megfelelő $<$ reláció trihotom.

Megjegyezzük, hogy egy elrendezett halmaz minden részhalmaza is elrendezett az indukált részbenrendezésnél.

Az elrendezett halmazok további specializálását adja a következő definíció:

Az $\langle A; \leq \rangle$ részbenrendezett halmaz *jólrendezett*, ha minden nemüres részhalmazának van legkisebb eleme. Jólrendezett halmazok esetén tehát bármely kételemű részhalmaznak is van legkisebb eleme; amiből következik, hogy jólrendezett halmaz teljesen rendezett.

Tetszőleges $\langle A; \leq \rangle$ elrendezett halmaz esetén a b elemet az a elem *rákövetkezőjének* nevezzük, ha $a < b$ és bármely $x > a$ esetén $b \leq x$. Jólrendezett halmazokban minden a elemnek van rákövetkezője, ha a nem a halmaz legnagyobb eleme, nevezetesen az $\{x \mid x > a\}$ részhalmaz legkisebb eleme.

Igen fontos bizonyítási segédeszközt ad az

1.3. Jólrendezési tétel. *Minden halmaz jólrendezhető.* ■

A halmazelmélet többi axiómájával a jólrendezési tétel összeegyeztethető, de az is összeegyeztethető, hogy a jólrendezési tétel nem igaz. A mai algebrai vizsgálatoknál általában a jólrendezési tétel igazságát szokták feltenni. A jólrendezési tételt azért nem nevezzük axiómának, mert az úgynevezett *kiválasztási axiómából* szokták bizonyítani (pontosabban, azzal ekvivalens). A kiválasztási axióma „lényegében" azt mondja ki, hogy *nemüres halmazok bármely rendszerének minden eleméből egyszerre kiválasztható azoknak egy-egy eleme*.

A következőkben a jólrendezési tétel néhány olyan formáját (illetve következményét) mutatjuk be, amelyeket az algebrai vizsgálatoknál szoktak alkalmazni.

1. Transzfinit indukció

Ha egy „értelmesen megfogalmazott formula” érvényes az $\langle A; \leq \rangle$ jólrendezett halmaz első elemére és érvényes minden olyan a elemre, amelynél kisebbekre is érvényes, akkor az A halmaz minden elemére is érvényes. (Látható, hogy ez a teljes indukció általánosítása.) A transzfinit indukció tulajdonképpen nem átfogalmazása a jólrendezési tételnek, hanem olyan bizonyítási módszer, amely a jólrendezett halmazokon érvényes. Felhasználhatóságát az biztosítja, hogy minden halmaz jólrendezhető. A transzfinit indukció érvényessége azonnal következik a jólrendezett halmazokra. Tekintsük ugyanis azoknak az elemeknek a halmazát, amelyekre a tekintett formula nem igaz. Ha ennek a részhalmaznak volna első eleme, arra a feltétel szerint igaz volna a formula. Így e halmaznak nincs első eleme; ami a jólrendezettség alapján azzal ekvivalens, hogy e részhalmaz üres. Így a formula valóban érvényes a halmaz minden elemére.

Abban az esetben, amikor a természetes számok „természetes” rendezését tekintjük, akkor speciális esetként a *teljes indukciót* nyerjük. A transzfinit indukció segítségével definiálni is lehet fogalmakat. Ilyen esetben *transzfinit rekurzióról* beszélünk.

2. Zorn-lemma

A Zorn-lemma megfogalmazásához néhány fogalomra van szükségünk. Egy részbenrendezett halmaz valamely részhalmazát láncnak nevezzük, ha az az indukált részbenrendezésnél teljesen rendezett. Mint tetszőleges részhalmaznál, egy x elem felső korlátja a C láncnak, ha minden $c \in C$ esetén $c \leq x$ teljesül. Egy $\langle A; \leq \rangle$ részbenrendezett halmazt *induktívnak* nevezünk, ha minden $C \subseteq A$ láncnak létezik (A-beli) felső korlátja. A Zorn-lemma azt mondja ki, hogy minden induktív halmazban van (legalább egy) maximális elem. Abban a speciális esetben, amikor a vizsgált részbenrendezett halmaz elemei egy halmaz bizonyos részhalmazai, akkor az induktivitás azt jelenti, hogy a vizsgált részhalmazok bármely növő láncának egyesítését tartalmazza a szóban forgó részhalmazok egyike. Ez gyakran maga az egyesítés.

A Zorn-lemma ilyen speciális esete használható fel annak a bizonyítására, hogy egy vektortér minden alterének van direkt kiegészítője. Tekintsük azokat az altereket, amelyeknek az adott altérrel való metszete egyedül a nullvektorból áll. Ezek egy induktív halmazrendszert alkotnak. A Zorn-lemma miatt van tehát közöttük maximális. E maximálisok bármelyikéről könnyen belátható, hogy az adott altérnek direkt kiegészítője lesz.

3. Teichmüller–Tukey-lemma

Ennek kimondásához a véges jellegű tulajdonság definiálására van szükség. Egy halmaz részhalmazaira definiált tulajdonságot véges jellegűnek nevezünk, ha egy részhalmaznak pontosan akkor van meg ez a tulajdonsága, ha ennek minden véges részhalmaza ilyen tulajdonságú. A lemma szerint egy halmaz bármely, adott véges jellegű tulajdonsággal rendelkező részhalmazai között van maximális.

A Teichmüller–Tukey-lemma felhasználásával bizonyítható például, hogy bármely vektortérben létezik bázis. Tekintsük ugyanis a vektortérnek a lineárisan független vektorrendszereiből álló részhalmazait. A lineáris függetlenség, definíció szerint, véges jellegű. Létezik tehát maximális lineárisan független rendszer, amiről azonnal belátható, hogy bázis.

A felsorolt állítások ekvivalenciáját nem bizonyítjuk. A részbenrendezésre vonatkozó, itt felsorolt eredmények az algebrában segédeszközként használatosak. A részbenrendezésnek az algebrával való szorosabb kapcsolatára a későbbiekben még vissza fogunk térni.

1.4. Ekvivalenciareláció, partíció, függvény

Egy Θ relációt ekvivalenciarelációnak nevezünk, ha reflexív, szimmetrikus és tranzitív.

Az ekvivalenciarelációk igen szoros kapcsolatban állnak a partíciókkal. Elsőként ezt a kapcsolatot írjuk le.

Az A halmazon értelmezett tetszőleges ϱ relációhoz hozzárendelhetünk egy A/ϱ halmazrendszert a következőképpen:

Legyen tetszőleges $a \in A$ esetén $H_a = \{x \in A \mid x \varrho a\}$. Az A/ϱ halmazrendszer pedig álljon az összes különböző H_a alakú halmazból.

1.4. Tétel. *Ha Θ ekvivalenciareláció, akkor A/Θ osztályozás.*

Bizonyítás. Azonnal látható, hogy a megadott részhalmazok lefedik az A halmazt. A reflexivitás miatt ugyanis bármely A-beli a elem benne van H_a-ban, tehát a megadott részhalmazok valamelyikében.

Az egyrétűség kimutatására célszerű a szimmetriát és a tranzitivitást átfogalmazni a megadott részhalmazok „nyelvére”:

1. Ha $a \varrho b$, akkor $b \varrho a$. Azaz, ha $a \in H_b$, akkor $b \in H_a$.

2. Ha $a \varrho b$ és $b \varrho c$, akkor $a \varrho c$. Más szóval, ha $a \in H_b$ és $b \in H_c$, akkor $a \in H_c$.

Ha tehát $x \in H_a \cap H_b$, akkor $x \in H_a$ miatt $a \in H_x$, amit összevetve az $x \in H_b$ feltétellel azonnal adódik, hogy $a \in H_b$. Persze ekkor $b \in H_a$ is teljesül; és így $H_a \subseteq H_b$, valamint $H_b \subseteq H_a$, ami bizonyítja az egyrétűséget. ■

Megjegyezzük, hogy A/ϱ nemcsak ekvivalenciareláció esetén lehet osztályozás. Ha például egy kételemű halmazon két elem pontosan akkor van relációban, ha különböznek, akkor ugyancsak osztályozást nyerhetünk a fenti módon.

Az előbbi tétel azonban mégis megfordítható, de csak annyiban, hogy minden osztályozás meg *tud* határozni egy ekvivalenciarelációt.

1.5. Tétel. *Tetszőleges $\pi \subseteq P(A)$ osztályozáshoz létezik pontosan egy olyan $\varrho = \varrho[\pi]$ ekvivalenciareláció, amelyre $\pi = A/\varrho$.*

Bizonyítás. Legyen $\pi \subseteq P(A)$ tetszőleges. Ehhez a következőképpen rendelünk hozzá egy $\varrho = \varrho[\pi]$ relációt: Legyen $a \varrho b$, ha van olyan $H \in \pi$, amelyre $a, b \in H$.

Ez a reláció definíció szerint szimmetrikus. Ha π elemeinek egyesítési halmaza A, akkor minden elem benne van egy ilyen részhalmazban, tehát ϱ reflexív. Ha π elemei diszjunktak, akkor $a \varrho b$ és $b \varrho c$ azt jelenti, hogy ezek π ugyanazon elemében vannak, ezért ϱ tranzitív. Eszerint ϱ ekvivalenciareláció. Az A/ϱ osztályozásnál a és b pontosan akkor kerülnek egy osztályba, ha $a \varrho b$, azaz, ha a és b ugyanabban a π szerinti osztályban voltak.

Ha ϱ és σ különböző ekvivalenciarelációk, akkor van olyan $a, b \in A$, hogy $(a, b) \in \varrho$, de $(a, b) \notin \sigma$ (vagy fordítva). Ekkor viszont A/ϱ esetében van olyan osztály, amelynek a és b mindegyike eleme, de A/σ-nál nincs. ■

A következőkben az ekvivalenciarelációnak, illetve az osztályozásnak a függvényekkel való szoros kapcsolatát mutatjuk meg.

1.6. Tétel. *Tetszőleges* $\varphi : A \to B$ *függvény esetén*
$\operatorname{Ker}(\varphi) = \{(a_i, a_j) \in A \times A \mid \varphi(a_i) = \varphi(a_j)\}$ *ekvivalenciareláció.*

Bizonyítás. $\varphi(a) = \varphi(a)$ miatt $\operatorname{Ker}(\varphi)$ reflexív. Az egyenlőség szimmetriája bizonyítja a reláció szimmetriáját, és tranzitivitása a reláció tranzitivitását. ■

A $\operatorname{Ker}(\varphi)$ relációt a φ függvény *magjának* nevezzük.

1.7. Tétel. *Tetszőleges* $\varphi : A \to B$ *esetén teljesül:*

$$A/\operatorname{Ker}(\varphi) = \{\varphi^{-1}(b) \in P(A) \mid b \in B\}.$$

Bizonyítás. Az $A/\operatorname{Ker}(\varphi)$ osztályozásában – mint láttuk – a_i és a_j pontosan akkor esik egy osztályba, ha a $\operatorname{Ker}(\varphi)$ relációban állnak; azaz akkor, ha $\varphi(a_i) = \varphi(a_j)$. Így egy osztály valóban a $\varphi^{-1}(b)$ elemeiből áll, ahol $b \in B$. (Megengedtük, hogy egy-egy osztályt többször is felsoroljunk.) ■

1.8. Tétel. *Tetszőleges* $\varphi : A \to B$ *függvény esetén az* $\operatorname{Im}(\varphi)$*-re értelmezett* $b \mapsto \varphi^{-1}(b)$ *függvény bijekció, amely* $\operatorname{Im}(\varphi)$*-t* $A/\operatorname{Ker}(\varphi)$*-re képezi.*

Bizonyítás. (A fenti függvény természetesen a B-nek csak az $\operatorname{Im}(\varphi)$-beli b elemeire van értelmezve, mert egyébként $\varphi^{-1}(b)$ üres.) Mivel $b \in \operatorname{Im}(\varphi)$ egyértelműen meghatározza $\varphi^{-1}(b)$-t, ezért valóban függvényt kaptunk. Tekintettel arra, hogy φ függvény, ezért a kapott függvény injektív. Mivel $A/\operatorname{Ker}(\varphi)$ minden eleme fellép képként, ezért e függvény bijektív is. ■

Noha tetszőleges függvény egyértelműen meghatározza a magját, e kapcsolat nyilván nem fordítható meg. A létrehozott osztályozásból nem lehet megmondani, hogy a halmaz elemeit eredetileg hova képeztük le; csupán annyit tudunk, hogy bizonyos elemeknek a képe megegyezett-e vagy sem. Azt azonban bebizonyítjuk, hogy minden ekvivalenciareláció előállítható egy alkalmas függvény magjaként.

1.9. Tétel. *Legyen* Θ *az* A *halmaz tetszőleges ekvivalenciarelációja, és legyen* $H_a = \{x \in A \mid x \Theta a\}$. *Ekkor* Θ *a magja annak a* $\varphi : A \to A/\Theta$ *függvénynek, amely minden* a *elemhez* H_a*-t rendeli.*

Bizonyítás. Az A/Θ definíciójánál láttuk, hogy $(a, b) \in \Theta$ pontosan akkor teljesül, ha $H_a = H_b$. A $\operatorname{Ker}(\varphi)$ definíciója szerint $(a, b) \in \operatorname{Ker}(\varphi)$ pontosan akkor igaz, ha $\varphi(a) = \varphi(b)$. A tételben megadott φ függvény definíciója szerint a két feltétel ugyanazt jelenti, így a két ekvivalenciareláció megegyezik. ■

Egy A halmazon értelmezett relációk az $A \times A$ részhalmazai. Ennek megfelelően a részhalmazok részbenrendezése a relációk részbenrendezését is adja. Ezt a részbenrendezést célszerű pontosan megfogalmazni:

1.10. Definíció. Legyenek $\varrho, \sigma \in R(A)$ (azaz binér relációk az A halmazon). Azt mondjuk, hogy ϱ kisebb-egyenlő σ (jelben $\varrho \leq \sigma$), ha tetszőleges $a, b \in A$ esetén az $a \varrho b$ feltételből $a \sigma b$ következik. □

Tekintettel arra, hogy ez pontosan az $R(A)$ részhalmazaira adott részbenrendezés, ezért a tulajdonságait nem kell újra bizonyítani.

Mivel egy halmaz részbenrendezése részhalmazain is részbenrendezést hoz létre, ezért a most megadott részbenrendezés az ekvivalenciarelációkat is (természetes módon) részbenrendezi. Ezáltal az osztályozásokat is részbenrendeztük; mivel az ekvivalenciarelációk és osztályozások egyértelműen meghatározzák egymást. Azonnal látható az alábbi

1.11. Tétel. *Az osztályozásokra a binér relációk részbenrendezésének megfelelő rendezés a következőt jelenti:*

Az A halmaz $\pi_1, \pi_2 \subseteq P(A)$ osztályozásaira $\pi_1 \leq \pi_2$ pontosan akkor teljesül, ha π_1 minden eleme részhalmaza a π_2 valamelyik elemének. ■

1.12. Tétel. *Legyen adva két függvény: $\varphi : A \to B$ és $\psi : A \to C$. Ha φ szürjektív és* Ker $(\varphi) \leq$ Ker (ψ)*, akkor létezik pontosan egy olyan $\sigma : B \to C$ függvény, amelyre $\psi = \sigma \circ \varphi$.*

Bizonyítás. Mint rendszerint, itt is az unicitás (egyértelműség) bizonyítása egyszerűbb.

Ha a kívánt σ függvény létezik, akkor tetszőleges $a \in A$ mellett $\sigma(\varphi(a)) = \psi(a)$ teljesül; azaz csak $\sigma : \varphi(a) \mapsto \psi(a)$ lehet.

Ezek után csupán azt kell belátni, hogy most egy függvényt definiáltunk. A φ függvény szürjektivitása miatt B minden eleme $\varphi(a)$ alakú, így σ minden B-beli elemhez hozzárendel egy C-beli (hiszen $\psi(a) \in C$) elemet. Azt kell még belátni, hogy valóban csak egyetlen elemet rendel hozzá. Ez azért nem triviális, mert több A-beli elemnek is lehet ugyanaz a B-beli elem a képe. Tegyük fel tehát, hogy $\varphi(a_1) = \varphi(a_2)$. Ez azt jelenti, hogy a_1 és a_2 a Ker (φ)-nél ugyanabba az osztályba esnek. A két függvény magjára vonatkozó feltétel szerint ekkor e két elem Ker (ψ)-nél is ugyanabba az osztályba esik, tehát $\psi(a_1) = \psi(a_2)$. ■

1.5. Számosság

A halmazelmélet osztályokkal való felépítése CANTOR nevéhez fűződik. E felépítés esetén a halmazok osztályában is értelmezhető reláció, akkor is, ha ennek „elemei" nem feltétlenül halmazok. Ezt nem részletezzük itt; hanem „úgy teszünk", mintha ez is halmaz volna.

A halmazok között egy nyilvánvaló ekvivalenciarelációt lehet létesíteni: Az A és B halmazok ekvivalensek, ha létezik egy $A \to B$ bijekció. Világos, hogy két véges halmaz pontosan akkor ekvivalens, ha ugyanannyi elemük van, és egyetlen véges halmaz sem ekvivalens valódi részhalmazával.

Végtelen halmazoknál ez nem igaz: a pozitív egész számok halmaza ekvivalens a pozitív páros számok halmazával, mint ezt például az $n \mapsto 2n$ bijekció mutatja. Az viszont végtelen halmazokra is igaz, hogy:

tetszőlegesen adott A és B halmazok esetén vagy egy $\varphi : A \to B$, vagy egy $\psi : B \to A$ injekció létezik.

Ennek bizonyítása végett tekintsük azokat a $\varrho \subseteq A \times B$ relációkat, amelyek esetében minden A-beli elem legfeljebb egy B-beli elemmel és minden B-beli elem legfeljebb egy A-beli elemmel áll relációban (azaz ϱ bijekció az A-nak egy A' és B-nek egy B' részhalmaza között). Ilyen reláció létezik, például ilyen az üres reláció. A relációknak ez a tulajdonsága nyilván véges jellegű, hiszen ha egy reláció nem ilyen, akkor definíció szerint egy kételemű részrelációja sem ilyen. A Teichmüller–Tukey-lemma szerint tehát létezik maximális az ilyen tulajdonságú relációk között, ami bijekciót létesít egy $A_1 \subseteq A$ és egy $B_1 \subseteq B$ részhalmaz között. Ha ezek valódi részhalmazok, azaz létezik $a' \in A \setminus A_1$ és $b' \in B \setminus B_1$, akkor a relációt az (a', b') párral bővítve egy nagyobb ugyanilyen tulajdonságú relációt kapnánk, a maximalitással ellentétben. Ezért vagy $A_1 = A$, vagy $B_1 = B$. Az első esetben a reláció egy $A \to B$, a másodikban egy $B \to A$ injekciót hoz létre.

Mivel injekciók szorzata injekció, ezért így egy reflexív és tranzitív relációt nyertünk, amely – mint fentebb láttuk – nem részbenrendezés, hiszen létezhet $\varphi : A \to B$ és $\psi : B \to A$ injekció, anélkül, hogy ezek bármelyike bijekció volna. Megmutatjuk azonban, hogy ebben az esetben létezik egy $\chi : A \to B$ bijekció is.

Álljon $B_0 \subseteq B$ azokból az elemekből, amelyek nem $\varphi(a)$ alakúak ($a \in A$). Legyen $A_0 = \psi(B_0)$, majd $i \in \mathbb{N}$ mellett $B_i = \varphi(A_{i-1})$ és $A_i = \psi(B_i)$. Legyen $A' = \bigcup\{A_i \mid i \in \mathbb{N}_0\}$ és $B' = \bigcup\{B_i \mid i \in \mathbb{N}_0\}$, továbbá $A'' = A \setminus A'$ és $B'' = B \setminus B'$. Könnyen belátható, hogy a $\chi(a) = \begin{cases} \varphi(a), & \text{ha } a \in A'' \\ \psi^{-1}(a), & \text{ha } a \in A' \end{cases}$ megfeleltetés valóban bijekció.

Ezáltal valóban egy részbenrendezést kaptunk, ahol az egyenlőség szerepét a halmazok ekvivalenciája veszi át. Sőt, mi több, azt is láttuk, hogy ez egy teljes rendezés, amelyben A „megelőzi" B-t, ha nem ekvivalensek, és létezik egy $\varphi : A \to B$ injekció. Azt mondjuk, hogy az ekvivalens halmazok *egyenlő számosságúak*, és ha A és B nem ekvivalensek, de létezik egy $\varphi : A \to B$ injekció, akkor A *kisebb számosságú*, mint B.

Ebben a részbenrendezésben elöl állnak a véges halmazok; első az üres halmaz, majd az egyelemű, kételemű stb. halmazok következnek.

Megmutatjuk, hogy e sorozatnak nincs „vége", minden halmaznál van nagyobb számosságú halmaz.

Bármely A halmaz $P(A)$ hatványhalmazának a számossága nagyobb, mint az A számossága.

Bármely A halmaz esetén a $\varphi(a) \to \{a\}$ ($a \in A$) leképezés egy $\varphi : A \to P(A)$ injekciót létesít. Azt kell tehát megmutatni, hogy a két halmaz nem ekvivalens. Ha A üres, akkor $P(A)$ egyelemű; ha A egyelemű, akkor $P(A)$ kételemű; ezekben az esetekben tehát nem létezik bijekció. Egyébként elegendő azt belátni, hogy egy $\varphi : A \to P(A)$ injektív leképezés soha sem lehet szürjektív.

Ha mindig $a \in \varphi(a)$ lenne, és φ szürjektív volna, akkor csak $\varphi(a) = \{a\}$ lehet, hiszen ezek a részhalmazok csak ekkor léphetnének fel képként. Ekkor viszont az A-nak a, b különböző elemeire $\{a, b\} \notin \mathrm{Im}(\varphi)$, azaz φ valóban nem volna szürjektív. Egyébként van olyan $a \in A$, amire $a \notin \varphi(a)$. Álljon $B \subseteq A$ az összes ilyen elemből. Ha $b \notin B$, akkor B definíciója szerint $b \in \varphi(b)$, és így $\varphi(b) = B$ lehetetlen, mert $b \notin \varphi(b)$. Ha viszont $b \in B$, akkor B definíciója szerint $b \notin \varphi(b)$, ezért nem lehet $\varphi(b) = B$.

A legkisebb végtelen számosság az egész számok számossága. Ezt a számosságot *megszámlálhatónak* (pontosabban *megszámlálhatóan végtelennek*) nevezik. A valós számok számossága *kontinuum*. Az itt elfogadott axiómák nem döntik el, hogy van-e e két számosság között más is.

Feladatok

1. Mutassuk meg, hogy ha (feltevésünkkel ellentétben) egy halmaznak önmaga eleme, akkor létezik egy végtelen $A_1 \ni A_2 \ni \ldots$ halmazsorozat.

2. Bizonyítsuk be, hogy a halmazok egyesítése és metszete asszociatív művelet. Mutassuk meg, hogy véges sok halmaz egyesítése (metszete) leírható páronkénti egyesítés (metszet) segítségével.

3. Legyenek $\varphi : A \to B$ és $\psi : B \to C$ függvények. Mutassuk meg, hogy a $\psi\varphi$ függvényszorzat nem más, mint $(\varphi^{-1} \circ \psi^{-1})^{-1}$, ahol $\circ$ a relációszorzat.

4. Az A halmazon értelmezett relációk közti részbenrendezést mint $A \times A$ részhalmazainak a tartalmazás szerinti részbenrendezését értelmeztük. Értelmezzük ennek alapján relációk metszetét és egyesítését.

5. Definiáltuk relációk tulajdonságait: reflexivitás, irreflexivitás, szimmetria, antiszimmetria, szigorú antiszimmetria, trihotómia. Döntsük el, ezek közül melyik marad meg egyesítésnél, illetve metszetnél.

6. Legyen $\varphi : A \to B$ és $\psi : B \to C$ két függvény. Bizonyítsuk be, hogy ha a $\psi\varphi$ függvény injektív, akkor φ is az, ha szürjektív, akkor ψ is az. Mutassunk példát arra, hogy a szorzat bijektivitásából egyik tényező bijektivitása sem következik.

7. Mutassuk meg, hogy egy halmaz relációi körében akármennyinek létezik egyesítése és metszete. Mutassuk meg, hogy ugyanez érvényes e halmaz ekvivalenciarelációira is. Mutassuk meg, hogy a metszet mindkét esetben ugyanaz, de az egyesítés nem.

8. Legyen $\varrho \in R(A)$. Bizonyítsuk be, hogy $\varrho \subseteq \varrho \cup \varrho^{-1}$, s ez utóbbi szimmetrikus, és a legszűkebb ϱ-t tartalmazó szimmetrikus reláció.

9. Legyen $\varrho \in R(A)$. Bizonyítsuk be, hogy ϱ része a $\varrho \cup (\varrho \circ \varrho) \cup (\varrho \circ \varrho \circ \varrho) \cup \ldots$ relációnak, amely tranzitív, és a legszűkebb ϱ-t tartalmazó tranzitív reláció.

10. Mutassuk meg, hogy $R(A)$ elemeinek bármely halmazához található egy őket tartalmazó legkisebb ekvivalenciareláció.

11. Definiáljuk a $\varrho, \sigma \in R(A)$ relációkra a $\varrho \star \sigma$ háromváltozós relációt úgy, hogy $(a, b, c) \in \varrho \star \sigma$ akkor és csak akkor, ha $(a, b) \in \varrho$ és $(b, c) \in \sigma$. Mutassuk meg, hogy nem minden háromváltozós reláció írható ilyen alakba, és lehet találni olyan, a fentiektől különböző ϱ_1, σ_1 relációkat, amelyekre $\varrho_1 \star \sigma_1 = \varrho \star \sigma$.

12. Mutassuk meg, hogy bármely háromváltozós ϱ_3 reláció „előállítható” olyan σ kétváltozós relációként, amelyben egy pár első eleme olyan pár, amelyek egy ϱ_3-tól függő ϱ kétváltozós relációban vannak, a második elem pedig egy ugyancsak ϱ_3-tól függő egyváltozós relációban. (Előállítható az azt jelenti, hogy létesíthető egy természetes bijekció köztük.)

13. Bizonyítsuk be, hogy a racionális számok halmaza megszámlálható.

14. Bizonyítsuk be, hogy az algebrai számok halmaza is megszámlálható (algebrai számok az egész együtthatós nemnulla polinomok gyökei).

15. Bizonyítsuk be, hogy egy megszámlálható halmaz hatványhalmaza kontinuum számosságú.

16. Bizonyítsuk be, hogy a valós függvények halmazának a számossága ugyanakkora, mint egy kontinuum számosságú halmaz hatványhalmazáé.

2. Általános algebrai alapfogalmak

Az alábbiakban olyan alapvető fogalmak szerepelnek, amelyek már az első kötetben „naiv" módon előfordultak. A csoportok és gyűrűk tárgyalásánál az alábbiakban ismertetett tételek precíz kimondása és bizonyításuk ismerete elmellőzhető; de a mélyebb megértéshez szükséges. Első olvasásnál elegendő csak akkor visszalapozni ezekre a részekre, ha utalunk valamire, ami itt szerepel. A fogalmak tisztán látása végett olvasás közben célszerű ezeket a számokból, polinomokból, vektorokból vagy lineáris transzformációkból álló struktúrák esetére megvizsgálni.

2.1. Művelet, algebrai struktúra, típus

Mint már említettük, az algebrai vizsgálatok tárgya: műveletekkel ellátott halmazok. Bizonyos esetekben meg szokták engedni az üres halmazt is. Mi általában csak nemüres halmazokkal foglalkozunk. Ha A nemüres halmaz, akkor az A-n értelmezett műveletek A bizonyos elemeihez az A egy-egy általuk jól meghatározott elemét rendelik hozzá. Ezt szabatosan a következő módon értelmezzük:

2.1. Definíció. Tetszőleges A nemüres halmaz és $n \geq 0$ egész szám esetén bármely $f : A^n \to A$ függvényt az A-n értelmezett n-változós műveletnek nevezünk. □

A leggyakoribb esetben $n \leq 2$. Az $n = 2$ esetben azt mondjuk, hogy f *bináris művelet*. Ilyen például a számok, polinomok, függvények stb. körében az összeadás vagy szorzás. Az $n = 1$ esetben *unáris műveletről* beszélünk. Unáris művelet például, ha minden számhoz hozzárendeljük a negatívját, vagy a 0-tól különböző számok halmazában minden számhoz a reciprokát. De unáris művelet az is, amikor minden természetes számhoz hozzárendeljük a rákövetkezőjét, vagy például a 2-vel való osztásakor keletkező maradékát. Ugyancsak unáris műveletet kapunk, ha egy K test feletti $\mathcal{V}$ vektortérben minden $\mathbf{u}$ vektorhoz a $c\mathbf{u}$-t rendeljük hozzá, rögzített $c \in K$ mellett ($f_c : \mathbf{u} \mapsto c\mathbf{u}$). Végül, az $n = 0$ esetben *nullváltozós* vagy *nulláris műveletről* beszélünk. Mivel A^0-nak egyetlen eleme van, ezért egy nulláris művelet az A halmaz egy elemének a kijelölését jelenti. Ilyen például az egész számok között a 0 vagy az 1 kijelölése.

Ha az A halmazon értelmezett algebrai struktúráról beszélünk, akkor ezt úgy értjük, hogy az A halmazon kívül még bizonyos műveletek is adottak. E műveletek halmaza határozza meg az algebrai struktúrát.

2.2. Definíció. Algebrai struktúrán (vagy általános algebrai struktúrán) olyan $\mathfrak{A} = \langle A; F \rangle$ halmazpárt értünk, ahol A nem üres, és minden $f \in F$ elemhez található egy

$n(= n(f))$ nemnegatív egész szám, amelyre f az A-n értelmezett n-változós művelet. Az A halmazt az $\mathfrak{A}$ tartóhalmazának nevezzük. □

Egy-egy algebrai struktúra „szerkezete" tehát erősen függ attól is, hogy milyen műveletek tartoznak hozzá. E műveletekről a legkevesebb, amit mondhatunk, az, hogy hány változósak. Ha például az egész számok körében az összeadást, szorzást, egy szám negatívjának a vételét és a 0 kijelölését tekintjük műveletnek, akkor a változószámok rendre: $(2, 2, 1, 0)$. Nemnegatív egészeknek egy ilyen rendszere megadja, hogy a szóban forgó algebra milyen „típusú". Célszerű azonban a kétváltozós műveletek között valamilyen különbséget tenni; legalább annyit, hogy az egyiknek a neve az „első", a másiké a „második" kétváltozós művelet. Ezért abból fogunk kiindulni, hogy adott a „műveleti neveknek" egy M halmaza és minden műveleti névről eleve tisztáztuk, hogy mennyi a változószáma. Azaz, minden műveleti névhez hozzárendeltünk egy nemnegatív egész számot.

2.3. Definíció. Típusnak nevezünk egy $\tau : M \to \mathbb{N}_0$ függvényt, ahol $\mathbb{N}_0$ a nemnegatív egész számok halmaza. Az M (esetleg üres) halmaz elemeit műveleti neveknek hívjuk.

Az $\langle A; F\rangle$ algebrát τ típusúnak nevezzük, ha létezik M-nek F-re való bijekciója, amelynél ha az M-beli f-nek f_A felel meg, és $\tau(f) = n$, akkor $f_A : A^n \to A$. (Ha τ típusú algebráról beszélünk, a szóban forgó bijekciót rögzítve gondoljuk, s ha félreértésre nem ad okot, akkor M és F elemeit ugyanúgy jelöljük – tehát a fenti f_A helyett f-et írunk.) f_A neve az f-nek A-beli realizációja. □

Legyen például $M = \{E, R, \ddot{O}, S\}$; $\tau(E) = 0, \tau(R) = 1, \tau(\ddot{O}) = \tau(S) = 2$. Legyen továbbá $A = \mathbb{N}$ a természetes számok halmaza és $F = \{1, ', +, \times\}$, ahol 1 az „egynek mint természetes számnak a kijelölése", $'(n) = n'$ az n rákövetkezője, $+(a, b) = a + b$ (az összeadás), $\times(a, b) = a \times b$ (a szorzás). Ekkor $\langle A; F\rangle$ τ típusú algebra a következő megfeleltetésnél: $E \to$ egy, $R \to$ rákövetkezés, $\ddot{O} \to$ összeadás, $S \to$ szorzás (a bijekció inverze az, hogy minden szónak megfeleltetjük az első betűjét).

Sok esetben a típust természetes számok egy sorozatával adjuk meg. Ha adott az $(n_1, n_2, \ldots, n_i, \ldots)$ (esetleg véges) sorozat, akkor ez a következő típust határozza meg:

$$M = \{\text{első név, második név, } \ldots, i\text{-edik név, } \ldots\}$$

azzal a τ függvénnyel, amelyre

$$\tau : \text{első név} \to n_1, \quad \tau : \text{második név} \to n_2, \ldots, \quad \tau : i\text{-edik név} \to n_i, \ldots .$$

A fenti példa esetében a típus a $(0, 1, 2, 2)$ sorozattal is megadható.

A 2.3. definíció alapján egy-egy algebrai struktúrának nincs egyértelműen meghatározott típusa. A műveleti nevek „megváltoztatása" ugyanis eleve egy másik τ függvényt jelent. Ezen úgy lehet segíteni, hogy az ilyen módon egymásból kapható típusokat nem különböztetjük meg. Ennek jogosságához mindenekelőtt be kell látni, hogy a nevek megváltoztatása ekvivalenciareláció a típusok között.

2.4. Tétel. *Legyen $\tau_1 : M_1 \to \mathbb{N}_0$ és $\tau_2 : M_2 \to \mathbb{N}_0$ két típus. Vezessük be továbbá a $\tau_1 \sim \tau_2$ relációt, amely pontosan akkor álljon fenn, ha létezik olyan $\mu : M_1 \to M_2$ bijekció, amelyre $\mu \circ \tau_2 = \tau_1$. A bevezetett reláció ekvivalenciareláció; és minden algebrának – ekvivalenciától eltekintve – egyértelmű típusa van.*

Bizonyítás. Tetszőleges $\tau : M \to \mathbb{N}_0$ típus esetében az M-nek önmagára való identikus τ leképezésére $\mu \circ \tau = \tau$, így a reláció reflexív. Ha μ bijekció, akkor $\mu^{-1} \circ \mu$ identitás.

Így $\mu \circ \tau_2 = \tau_1$ esetén $\mu^{-1} \circ \mu \circ \tau_1 = \mu^{-1} \circ \tau_2 = \tau_2$, amiből a szimmetria is következik, hiszen bármely bijekció inverze is bijekció. Ha a μ és ν bijekciókra $\mu \circ \tau_2 = \tau_1$ és $\nu \circ \tau_3 = \tau_2$, akkor $(\mu \circ \nu) \circ \tau_3 = \tau_1$ biztosítja a tranzitivitást, mert két bijekció szorzata is az. Így tényleg ekvivalenciarelációt kaptunk.

Tegyük most fel, hogy az $\langle A; F \rangle$ algebra típusa τ_1 is és τ_2 is. Ez azt jelenti, hogy léteznek olyan $\sigma_1 : M_1 \to F$ és $\sigma_2 : M_2 \to F$ bijekciók, amelyeknél tetszőleges $m_i \in M_i$ esetén $\sigma_j(m_i)$ változószáma $\tau_j(m_i)$ ($j \in \{1, 2\}$). Mivel F elemeinek a változószáma egyértelmű, ezért bármely $m \in M_1$ esetén $\tau_2(\sigma_2^{-1}(\sigma_1(m))) = \tau_1(m)$. Eszerint e függvényekre $(\sigma_1 \circ \sigma_2^{-1}) \circ \tau_2 = \tau_1$; amiből a két típus ekvivalenciája következik, mert bijekció inverze bijekció és két bijekció szorzata is bijekció. ■

Felhívjuk a figyelmet arra, hogy egy algebrában különböző műveleti neveknek is lehet ugyanaz a realizációja.

A továbbiakban néhány további alapvető algebrai fogalom ismertetésére térünk rá.

2.2. Részalgebrák

Tetszőleges algebrai struktúrának tekinthetjük olyan „részeit”, amelyek az eredetivel egyező típusú algebrák. Ez így még túl laza kapcsolatot jelent. Például az egész számok az összeadással (2) típusú algebra; ennek része a pozitív egészek, amelyek a szorzással ugyancsak (2) típusú algebra. De hiába kétváltozós mindkét művelet, mégis érezzük, hogy az utóbbi algebra az előbbinek nem „igazán” része. Ehhez az kellene, hogy a részben a műveletek ne csak ugyanannyi változószámúak, hanem ugyanazok legyenek. Ez természetesen így nem lehetséges, hiszen különböző halmazokon értelmezett műveletek nem lehetnek azonosak. Ennek áthidalására szolgál:

2.5. Definíció. Az $\mathfrak{A}' = \langle A'; F' \rangle$ algebrát a τ típusú $\mathfrak{A} = \langle A; F' \rangle$ algebra részalgebrájának nevezzük, ha az alábbiak teljesülnek:

(1) $\mathfrak{A}'$ is τ típusú.

(2) A' részhalmaza A-nak.

(3) Ha f_A, illetve $f_{A'}$ az f műveleti név A-beli, illetve A'-beli realizációja, akkor $f_{A'}$ az f_A-nak az A'-re való megszorítása. □

A 2.5. definíció szerint egy részalgebrán először műveleteket kellene értelmezni, és utána kellene megnézni, hogy a definíció feltételei teljesülnek-e. Konkrét esetekben azonban ehelyett azt szoktuk megnézni, hogy egy részhalmaz az *eredeti* műveletekre – pontosabban ezek megszorítására – nézve algebra-e. Ez az eljárás mindig alkalmazható.

2.6. Tétel. *Legyen $\mathfrak{A} = \langle A; F \rangle$ tetszőleges, τ típusú algebra, és legyen A' az A-nak részhalmaza. Tetszőleges $f \in F$ esetén jelölje f' az f-nek mint relációnak az A'-re való megszorítását, és legyen $F' = \{f' \mid f \in F\}$. Ha F' minden eleme művelet az A'-n, akkor $\mathfrak{A}' = \langle A'; F' \rangle$ részalgebrája az $\mathfrak{A}$-nak, és minden egyes f' annak a műveleti névnek az $\mathfrak{A}'$-n való realizációja, amelyiknek az $\mathfrak{A}$-beli realizációja a megfelelő f.*

Megfordítva, minden részalgebra a fenti módon állítható elő.

Bizonyítás. Nem megy az általánosság rovására, ha feltesszük, hogy maga F egyszersmind a műveleti nevek halmaza is. Mivel bármely $f \in F$ esetén f' és f változószáma megegyezik, ezért a 2.5. definíció (1) feltétele teljesül. A (2) feltétel teljesülését eleve megköveteltük. A (3) feltétel teljesülése pedig az F' konstrukciója alapján nyilvánvaló. ■

Érdemes részletesebben megnézni, mit jelent az, hogy a részalgebrán a műveletek az eredetieknek megszorításai. Legyen például $f \in F$ egy kétváltozós művelet, és legyenek $a, b \in A'$. A művelet definíciója szerint ekkor van egyetlen olyan $c \in A$, amelyre $f(a, b) = c$. Relációalakban felírva: $((a, b), c) \in f$. Mivel az f-nek f' megszorítása művelet A'-n, és $a, b \in A'$, ezért van olyan egyértelmű $d \in A'$, amelyre $((a, b), d) \in f'$. Mivel f' az f-nek megszorítása, ezért $((a, b), d) \in f$ is teljesül, és a művelet tulajdonságai szerint ebből $d = c$ adódik. Más szóval $(a, b) \in A'$ esetén $f(a, b) \in A'$ is teljesül. Erre a tulajdonságra mint a részalgebra műveleti zártságára fogunk utalni. Emlékeztetünk rá, hogy eredendően nem kívántuk meg, hogy a művelet eredménye a részalgebrán ugyanaz legyen.

A részalgebrák műveleti zártsága alapján a részalgebrát úgy tekinthetjük, mintha az eredeti algebra műveletei volnának rajta értelmezve. Noha ez pontatlan, nem okoz félreértést. Ilyenkor az $\langle A; F\rangle$ egy-egy részalgebráját $\langle A'; F\rangle$ jelöli ($A' \subseteq A$).

Ha $\mathfrak{A}' = \langle A'; F\rangle$ az $\mathfrak{A} = \langle A; F\rangle$ részalgebrája, azaz $A' \subseteq A$, akkor ezt $\mathfrak{A}' \leq \mathfrak{A}$ jelöli. Az $A' \neq A$ esetben az $\mathfrak{A}' < \mathfrak{A}$ jelölést is használni fogjuk.

2.7. Tétel. *Egy $\mathfrak{A}$ algebra részalgebrái a $\leq$ relációra részbenrendezett halmazt alkotnak, amelynek $\mathfrak{A}$ a legnagyobb eleme.*

Bizonyítás. A reflexivitás nyilvánvaló, ugyanúgy, mint az, hogy $\mathfrak{A}$ a legnagyobb elem. Az antiszimmetria azért igaz, mert a halmazok tartalmazására is igaz; és a műveletek megszorítása egyértelmű. A tranzitivitás abból következik, hogy ha először A'-re, majd utána ennek egy A'' részhalmazára szorítunk meg egy műveletet, ugyanazt kapjuk, mintha rögtön A''-re szorítanánk meg. ■

Egy algebra részalgebrái között tehát van legnagyobb. Legkisebb viszont általában nincs. A következő tétel arra ad választ, hogy mikor van egy algebra bizonyos részalgebráinak legnagyobb alsó korlátja.

2.8. Tétel. *Legyen $\{\mathfrak{A}_i = \langle A_i; F\rangle \mid i \in I\}$ az $\mathfrak{A} = \langle A; F\rangle$ algebra részalgebráinak egy halmaza. Akkor és csak akkor létezik e halmaz $\mathfrak{A}' = \langle A'; F\rangle = \bigwedge(\mathfrak{A}_i \mid i \in I)$ legnagyobb alsó korlátja, ha $A^\star = \left\{\bigcap A_i; i \in I\right\}$ nem üres, és ekkor $A' = A^\star$.*

Bizonyítás. A részalgebrákon megadott részbenrendezés definíciója szerint A' minden egyes A_i-nek részhalmaza, és nem üres. Így $A^\star$ nem lehet üres. Ha ez teljesül, akkor viszont tetszőleges n-változós $f \in F$ műveletre és $a_1, \ldots, a_n \in A^\star$ elemekre bármely $i \in I$ esetén $f(a_1, \ldots, a_n) \in A_i$, tehát $f(a_1, \ldots, a_n) \in A^\star$. Ezért $\langle A^\star; F\rangle$ részalgebra; és nyilvánvalóan a megadott részalgebrának legnagyobb alsó korlátja. ■

Előfordulhat, hogy bizonyos részalgebrák tartóhalmazának a közös része az üres halmaz. Az a céltól függ, hogy az egyöntetűség kedvéért megengedjük-e az üres halmazon értelmezett algebrákat. Ennek ugyanis nemcsak előnye, de hátránya is van.

A fenti tételnek a felhasználásával beláthatjuk, hogy egy algebra részalgebrái bármely halmazának mindig van legkisebb felső korlátja. Ehhez előkészületül egy másik tételt bizonyítunk be, amelyre a későbbiekben szintén szükségünk lesz.

2.9. Tétel. *Legyen B az $\mathfrak{A} = \langle A; F\rangle$ algebra tartóhalmazának tetszőleges, nemüres részhalmaza. Ekkor van az $\mathfrak{A}$-nak olyan legkisebb $\mathfrak{A}' = \langle A'; F\rangle$ részalgebrája, amelynek tartóhalmaza tartalmazza B-t. Ezt a részalgebrát a B generálta részalgebrának, vagy B generátumának nevezzük; tartóhalmazát $[B]$-vel fogjuk jelölni.*

Bizonyítás. Mivel $B \subseteq A$, ezért van olyan részalgebra, amelynek tartóhalmaza tartalmazza B-t, nevezetesen maga $\mathfrak{A}$ ilyen. Tekintsük azokat az $\mathfrak{A}_i = \langle A_i; F\rangle$ részalgebrákat, amelyekre $B \subseteq A_i$. Mivel B nem üres, ezért a 2.8. tétel szerint létezik az $\mathfrak{A}' = \langle A'; F\rangle = \bigwedge(\mathfrak{A}_i \mid B \subseteq A_i)$ részalgebra. Erre a részalgebrára nyilván $A' = \left\{\bigcap A_i \mid B \subseteq A_i\right\}$. Így $B \subseteq A'$; és mivel $\mathfrak{A}'$ a szóban forgó részalgebrák mindegyikének alsó korlátja, ezért valóban a legkisebb B-t tartalmazó részalgebra. ■

Noha $A' = \left\{\bigcap A_i \mid B \subseteq A_i\right\}$, mégsem igaz, hogy A' mindig megegyezne B-vel. A metszetben ugyanis a B-t tartalmazó részhalmazok közül csak olyan fordul elő, amely egyúttal valamelyik részalgebrának a tartóhalmaza is.

2.10. Tétel. *Egy algebra részalgebrái bármely halmazának mindig van legkisebb felső korlátja a részalgebrák között.*

Bizonyítás. Jelölje B az adott részalgebrák tartóhalmazainak az egyesítését. A 2.9. tétel szerint éppen a B generálta részalgebra lesz a legkisebb felső korlát. ■

2.11. Definíció. Egy algebra tartóhalmazának egy B részhalmazát generátorrendszernek nevezzük, ha a B generálta részalgebra az adott algebra. Ha a B-nek nincs olyan, nála kisebb részhalmaza, amely generátorrendszer, akkor B minimális generátorrendszer. Ha egy algebrának van véges sok elemből álló generátorrendszere, akkor az algebrát végesen generáltnak nevezzük, ha egyetlen elemből álló is van, akkor pedig ciklikusnak. □

2.3. Izomorfizmus, homomorfizmus

Az algebrák között egy nagyon „bő” osztályozást lehet megadni úgy, hogy egy osztályba soroljuk a megegyező típusú algebrákat. Ez az osztályozás olyan algebrákat is „ugyanannak” tekint, amelyekben a műveletek teljesen másképpen végezhetők, de véletlenül minden változószámra éppen ugyanannyi műveletük van. Egy másik „azonosítási” lehetőség az, ha megegyeznek abban az értelemben, hogy tartóhalmazaik is egyenlők és minden műveleti név esetében mindkét algebrában ugyanazt a realizációt adtuk meg. Ez az osztályozás viszont túl szűk. Világos ugyanis, hogy egy algebra „szerkezete” nem változik meg attól, hogy az elemeit „más színűre festjük”, és egyszersmind a műveleteket is másképpen jelöljük. Az ilyen kapcsolatban álló algebrákat „szerkezetileg azonos”-nak kell tekinteni. Ennek az azonosságnak a megfogalmazásához szükség van a művelettartó leképezés fogalmára.

2.12. Definíció. Legyen $\mathfrak{A} = \langle A; F_A \rangle$ és $\mathfrak{B} = \langle B; F_B \rangle$ két, azonos típusú algebra és $\varphi : A \to B$ egy függvény. Azt mondjuk, hogy $\varphi : \mathfrak{A} \to \mathfrak{B}$ (vagy $\varphi : A \to B$) műveletartó leképezés, ha bármely megfelelő f_A és f_B műveletpárra (vagyis ugyanannak az f műveleti névnek A-beli és B-beli realizációjára) teljesül a

$$\varphi(f_A(a_1, \ldots, a_n)) = f_B(\varphi(a_1), \ldots, \varphi(a_n))$$

összefüggés, ahol $n(= \tau(f))$ a műveletek változószáma. (Nullváltozós műveletek esetén a műveletartás azt jelenti, hogy a művelet által A-ban kijelölt elem képe a megfelelő művelet által B-ben kijelölt elem.) □

A jelölés formailag egyszerűsíthető, ha a több változó jelenlétét egy előzőleg bevezetett jelöléssel „eltüntetjük". Ez a következőképpen történik: Legyen $\varphi : A \to B$ tetszőleges függvény. Jelölje $n \in \mathbb{N}$ esetén $\varphi^n : A^n \to B^n$ azt a függvényt, amit

$$\varphi^n(a_1, \ldots, a_n) = (\varphi(a_1), \ldots, \varphi(a_n))$$

definiál, míg φ^0 legyen az egyelemű halmaz egyetlen önmagára való leképezése.

Egyszerű behelyettesítéssel látható, hogy φ műveletartása azzal ekvivalens, hogy minden f műveleti névre teljesül:

$$\varphi \circ f_A = f_B \circ \varphi^{\tau(f)}.$$

Ez az összefüggés jól szemléltethető a következő *kommutatív diagrammal*:

$$\begin{array}{ccc} A^n & \xrightarrow{f_A} & A \\ {\scriptstyle \varphi_n}\downarrow & & \downarrow{\scriptstyle \varphi} \\ B^n & \xrightarrow{f_B} & B \end{array}$$

A felírt összefüggés azt fejezi ki, hogy ezen a diagramon a bal felső sarokban álló A^n-ből kiindulva, a nyilak mellett felírt függvényeket egymás után alkalmazva bármelyik úton haladunk is, végeredményül mindig ugyanazt a függvényt kapjuk.

2.13. Definíció. A műveletartó leképezést homomorfizmusnak nevezzük. Ha a leképezés injektív, szürjektív vagy bijektív, akkor – megfelelően – injektív, szürjektív, illetve bijektív homomorfizmusról beszélünk. A bijektív homomorfizmus neve izomorfizmus.

Egy algebra önmagába való homomorfizmusát endomorfizmusnak, önmagára való izomorfizmusát automorfizmusnak nevezzük. □

Érdemes felfigyelni arra, hogy definíció szerint az endomorfizmus nem feltétlenül szürjektív, míg az izomorfizmus mindig szürjektív.

2.14. Tétel. *Homomorfizmusok szorzata homomorfizmus. Ha mindkét homomorfizmus injektív, szürjektív, illetve bijektív, akkor a szorzatuk is az. Izomorfizmusnak – mint függvénynek – az inverze is izomorfizmus.*

Bizonyítás. Mivel leképezésekre az analóg állítás igaz, ezért elegendő azt belátni, hogy ha $\varphi : A \to B$ és $\psi : B \to C$ a megfelelő algebrákon műveletartó, akkor $\psi\varphi : A \to C$ ugyancsak műveletartó. Ennek kimutatására válasszunk ki tetszőlegesen egy f

műveleti nevet, és legyen $\tau(f) = n$. A művelettartás szerint $\varphi \circ f_A = f_B \circ \varphi^n$ és $\psi \circ f_B = f_C \circ \psi^n$. A függvényszorzás asszociativitását és a nyilvánvaló $(\psi \circ \varphi)^n = \psi^n \circ \varphi^n$ összefüggést figyelembe véve, a következőket kapjuk:

$$(\psi \circ \varphi) \circ f_A = \psi \circ (\varphi \circ f_A) = \psi \circ (f_B \circ \varphi^n) = (\psi \circ f_B) \circ \varphi^n = (f_C \circ \psi^n) \circ \varphi^n =$$
$$= f_C \circ (\psi^n \circ \varphi^n) = f_C \circ (\psi \circ \varphi)^n,$$

ami bizonyítja $\psi \circ \varphi$ művelettartását.

Tekintsünk végül egy $\varphi : A \to B$ izomorfizmust. Legyen egy n-változós f műveleti névnek f_A az A-beli és f_B a B-beli realizációja. Legyen továbbá $f_B(b_1, \ldots, b_n) = b_0$. A bijektivitás következtében minden $1 \leq i \leq n$ indexre egyértelműen meghatározott az $a_i = \varphi^{-1}(b_i)$ elem. Az $a_0 = f_A(a_1, \ldots, a_n)$ elemre a művelettartás miatt $b_0 = \varphi(a_0)$, azaz $a_0 = \varphi^{-1}(b_0)$ teljesül, ami φ^{-1} művelettartását biztosítja. ■

Az a most belátott tény, hogy valamilyen matematikai „struktúrafajta” esetében a bijektív homomorfizmus inverze is az, egyáltalában nem magától értetődő. Ez „reláció-struktúrák” esetében általában nem is igaz. Tekintsünk például két kételemű részbenrendezett halmazt: egyik legyen a $\{0, 1\}$, a $0 \leq 0 < 1 \leq 1$ relációval, a másik az $\{a, b\}$ halmaz az $a \leq a$ és $b \leq b$ relációval. A $\varphi(a) \to 0$, $\varphi(b) \to 1$ összefüggéssel megadott függvény bijektív és relációtartó. Ezzel szemben inverze nem tartja meg a relációt, hiszen $a = \varphi^{-1}(0) < \varphi^{-1}(1) = b$ nem igaz.

2.15. Definíció. Ha létezik egy $\varphi : \mathfrak{A} \to \mathfrak{B}$ izomorfizmus, akkor azt mondjuk, hogy $\mathfrak{A}$ és $\mathfrak{B}$ izomorfak. Ennek jele: $\mathfrak{A} \cong \mathfrak{B}$. Ha $\varphi : \mathfrak{A} \to \mathfrak{B}$ szürjekció, akkor $\mathfrak{B}$-t az $\mathfrak{A}$ homomorf képének nevezzük. □

2.16. Tétel. *Adott típusú algebrák osztályában az izomorfizmus ekvivalenciarelációt határoz meg.*

Bizonyítás. Az identikus leképezés nyilvánvalóan izomorfizmus, és így a fenti reláció reflexív. A 2.14. tétel szerint egy bijektív homomorfizmus inverze is izomorfizmus, ezért a fenti reláció szimmetrikus. Végül, a tranzitivitás közvetlen folyománya a 2.14. tételben szereplő első állításnak, hiszen izomorfizmusok szorzata is izomorfizmus. ■

A 2.16. tétel azt fejezi ki, hogy az izomorf algebrákat bizonyos értelemben azonosnak tekinthetjük. Ez a „bizonyos értelem” a szóban forgó algebrák belső szerkezete. Izomorf algebrákban ugyanis a megfelelő műveletek hasonló módon hatnak. Csupán a műveleteket figyelve, nem tudunk különbséget tenni az izomorf algebrák között. Tekintettel arra, hogy az algebrai struktúrák vizsgálatakor a műveletek játsszák a központi szerepet, ezért izomorf algebrák belső szerkezetét nem is akarjuk megkülönböztetni. Ez azonban nem jelenti azt, hogy két izomorf algebra mindig, minden szempontból azonosnak tekinthető. Tekintsük például az $a + b\sqrt{2}$ alakú számok halmazát, ahol a, b egész számok. Ezek a valós számok összeadására és szorzására nézve egy $(2, 2)$ típusú algebrát alkotnak. Könnyen belátható az is, hogy az $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ megfeleltetés ennek az algebrának egy önmagával való izomorfizmusa. Az egymásnak megfeleltetett elemeket azonban nyilvánvalóan nem azonosíthatjuk, mert akkor például $\sqrt{2}$ és $-\sqrt{2}$ megegyeznének, ami képtelenség.

2.4. Kongruenciareláció, faktorstruktúra, direkt szorzat

Mint a halmazelméleti bevezető részben láttuk, minden függvény meghatároz egy ekvivalenciarelációt, ez meg egy osztályozást, amely bizonyos értelemben egyértelműen meghatározza a függvény hatását az értelmezési tartományon. A következőkben azt nézzük meg, hogy milyen ekvivalenciarelációt és milyen osztályozást kapunk, ha a függvény homomorfizmus.

2.17. Definíció. Az $\mathfrak{A} = \langle A; F\rangle$ algebra tartóhalmazán megadott Θ ekvivalenciarelációt kongruenciarelációnak vagy kongruenciának nevezzük, ha bármely n-változós $f \in F$ műveletre az

$$(a_1, b_1), \ldots, (a_n, b_n) \in \Theta$$

feltételből

$$(f(a_1, \ldots, a_n),\ f(b_1, \ldots, b_n)) \in \Theta$$

következik. □

Ha egy ϱ relációra hasonlóképpen értelmezzük ϱ^n-t, mint a függvények esetében, akkor a feltétel szerint $((a_1, \ldots, a_n), (b_1, \ldots, b_n)) \in \Theta^n$. A Θ reláció tehát pontosan akkor kongruenciareláció, ha f^2 úgy képezi le az $A^n \times A^n$ halmazt az $A \times A$ halmazra, hogy emellett Θ^n képe része legyen Θ-nak, azaz, ha $f^2(\Theta^{\tau(f)}) \subseteq \Theta$.

Érdemes felfigyelni arra, hogy nulláris műveletekre a következmény triviális, hiszen Θ eleve reflexív.

2.18. Tétel. *Ha a $\varphi : \mathfrak{A} \to \mathfrak{B}$ leképezés homomorfizmus, akkor az általa indukált reláció kongruenciareláció. Ezt a kongruenciarelációt is* Ker (φ)*-vel jelöljük.*

Bizonyítás. Legyen $(a_1, b_1), \ldots, (a_n, b_n) \in \text{Ker}\ (\varphi)$, és legyen f az $\mathfrak{A}$-nak tetszőleges, n-változós művelete. Ez azt jelenti, hogy bármely $1 \leq i \leq n$ indexre $\varphi(a_i) = \varphi(b_i)$. A művelettartás alapján ebből $\varphi(f(a_1, \ldots, a_n)) = \varphi(f(b_1, \ldots, b_n))$ következik, ami azt jelenti, hogy $(f(a_1, \ldots, a_n),\ f(b_1, \ldots, b_n)) \in \text{Ker}\ (\varphi)$. ■

2.19. Definíció. Az $\mathfrak{A} = \langle A; F\rangle$ algebra tartóhalmazának egy π osztályozását (a műveletekkel) kompatibilis osztályozásnak nevezzük, ha $\mathfrak{A}$ bármely n-változós f műveletéhez és π bármely $A_1, \ldots, A_n$ elemeihez létezik a π osztályozásnak olyan A' eleme, hogy valahányszor $a_i \in A_i$ $(i = 1, \ldots, n)$, mindannyiszor teljesül $f(a_1, \ldots, a_n) \in A'$.

Ezt az osztályt $A' = f(A_1, \ldots, A_n)$ jelöli, mivel csak az f művelettől és az $A_1, \ldots, A_n$ osztályoktól függ. □

2.20. Tétel. *Ha Θ az $\mathfrak{A} = \langle A; F\rangle$ algebrának egy kongruenciarelációja, akkor A/Θ kompatibilis osztályozás.*

Bizonyítás. Nulláris műveletekre a kompatibilitás triviális. Legyen $f \in F$ tetszőleges, n-változós művelet $(n > 0)$, és legyenek $A_1, \ldots, A_n \in A/\Theta$. Legyenek továbbá $a_i \in A_i$ $(i = 1, \ldots, n)$ adott elemek és A' az A/Θ-nak az $f(a_1, \ldots, a_n)$-et tartalmazó eleme. Válasszunk most tetszőleges $b_i \in A_i$ $(i = 1, \ldots, n)$ elemeket. Ezekre – A/Θ definíciója szerint – fennáll, hogy $(a_i, b_i) \in \Theta$. A kongruenciareláció definíciója alapján tehát

$(f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)) \in \Theta$. Ismét figyelembe véve A/Θ definícióját, $f(b_1, \ldots, b_n) \in A'$ adódik. ■

A következő tételben azt mutatjuk meg, hogy miképpen kaphatunk kompatibilis osztályozásból homomorfizmust.

2.21. Tétel. *Legyen π az $\mathfrak{A} = \langle A; F\rangle$ algebra tartóhalmazának egy kompatibilis osztályozása. Az $\mathfrak{A}$ algebra tetszőleges n-változós f műveletéhez rendeljük hozzá azt a π elemein értelmezett f' ugyancsak n-változós műveletet, amelyre $f'(A_1, \ldots, A_n) = f(A_1, \ldots, A_n)$, és jelölje F' ezeknek a műveleteknek a halmazát. Ekkor $\mathfrak{B} = \langle \pi; F'\rangle$ az $\mathfrak{A}$-val egyező típusú algebra és minden egyes f' az őt definiáló f-nek megfelelő művelet. Az a $\varphi : A \to \pi$ úgynevezett természetes leképezés, amely minden elemnek az őt tartalmazó osztályt feleltei meg, egy $\varphi : \mathfrak{A} \to \mathfrak{B}$ szürjektív homomorfizmus, amelyre $\pi = A/\operatorname{Ker}(\varphi)$.*

Bizonyítás. A 2.19. definíció szerint minden egyes f' valóban művelet, és változószáma nyilván megegyezik az őt definiáló f műveletével. Így valóban egy $\mathfrak{A}$-val azonos típusú algebrát kaptunk, ahol f' és f ugyanannak a műveleti névnek a realizációjaként tekinthető. A φ leképezés definíciója szerint szürjektív és $\pi = A/\operatorname{Ker}(\varphi)$ a függvényekre látottak alapján (1.9. tétel) igaz. Ha f egy n-változós művelet, akkor π kompatibilitása következtében, φ definíciója szerint fennáll a $\varphi(f(a_1, \ldots, a_n)) = f'(\varphi(a_1), \ldots, \varphi(a_n))$ egyenlőség. Így φ valóban homomorfizmus. ■

2.22. Definíció. Ha Θ az $\mathfrak{A} = \langle A; F\rangle$ algebrának tetszőleges kongruenciarelációja, akkor a 2.20. tételben szereplő $\mathfrak{A}/\Theta = \langle A/\Theta; F'\rangle$ algebrát az $\mathfrak{A}$ (Θ szerinti) faktoralgebrájának (vagy faktorának) nevezzük. □

A függvények vizsgálatakor láttuk, hogy $A/\operatorname{Ker}(\varphi)$ és $\operatorname{Im}(\varphi)$ között természetes módon bijekció létesíthető. Most azt fogjuk megmutatni, hogy ez a bijekció homomorfizmus esetében izomorfizmus.

2.23. Tétel. *Legyen φ az $\mathfrak{A} = \langle A; F_A\rangle$ algebrának a $\mathfrak{B} = \langle B; F_B\rangle$ algebrába való homomorfizmusa. Ekkor $\mathfrak{B}' = \langle \operatorname{Im}(\varphi); F\rangle \leq \mathfrak{B}$, és az* 1.8. *tételben megadott $b \mapsto \varphi^{-1}(b)$ bijekció izomorfizmus $\mathfrak{B}'$ és $\mathfrak{A}/\operatorname{Ker}\varphi$ között.*

Bizonyítás. A φ művelettartása miatt $\operatorname{Im}(\varphi)$ zárt a $\mathfrak{B}$-beli műveletekre, és így valóban részalgebrát kapunk. A megadott leképezésről már láttuk, hogy bijekció. Legyen az n-változós f műveleti név realizációja $\mathfrak{A}$-ban, $\mathfrak{B}'$-ben és $A/\operatorname{Ker}(\varphi)$-ben rendre f_A, f_B és f'_A. Ha $f_A(a_1, \ldots, a_n) = a_0$, akkor a művelettartás miatt $f_B(b_1, \ldots, b_n) = b_0$, és $f'_A(A_1, \ldots, A_n) = A_0$, ahol $b_i = \varphi(a_i)$ és $a_i \in A_i$ $(i = 0, 1, \ldots, n)$. Ez azt jelenti, hogy $A_i = \varphi^{-1}(\varphi(a_i))$ $(i = 0, 1, \ldots, n)$, és ezek az elemek kielégítik az

$$f'_A(\varphi^{-1}(\varphi(a_1)), \ldots, \varphi^{-1}(\varphi(a_n))) = \varphi^{-1}(\varphi(a_0)) = \varphi^{-1}(f_B(\varphi(a_1), \ldots, \varphi(a_n)))$$

összefüggést, tehát a művelettartás is igaz. ■

Megemlítjük még, hogy minden homomorfizmus kapcsolatot létesít a két megfelelő algebra részalgebrái, illetve kongruenciarelációi között, de erre majd később térünk vissza.

A homomorfizmusokról szóló eredmények befejezéséül bebizonyítjuk az 1.12. tétel algebrákra vonatkozó megfelelőjét:

2.24. Tétel. *Legyen adva a* $\psi : \mathfrak{A} \to \mathfrak{C}$ *és a szürjektív* $\varphi : \mathfrak{A} \to \mathfrak{B}$ *homomorfizmus úgy, hogy* $\mathrm{Ker}\,(\varphi) \leq \mathrm{Ker}\,(\psi)$. *Ekkor létezik pontosan egy olyan* $\sigma : \mathfrak{B} \to \mathfrak{C}$ *homomorfizmus, amelyre* $\psi = \sigma \circ \varphi$.

Bizonyítás. Az 1.12. tétel szerint σ egyértelmű és létezik. Most tehát csak annyit kell belátni, hogy ha φ és ψ homomorfizmusok, akkor σ is az. Tekintsük evégett az n-változós f műveleti név megfelelő realizációit, legyenek ezek f_A, f_B és f_C. Ha $\mathfrak{B}$-ben $f_B(b_1, \ldots, b_n) = b_0$ és az $a_i \in \mathfrak{A}$ elemekre $\varphi(a_i) = b_i$ $(i = 0, 1 \ldots, n)$, akkor σ definíciója szerint $\sigma(b_i) = \psi(a_i)$ $(i = 0, 1, \ldots, n)$, ami bizonyítja a művelettartást. ■

Az eddigiekben mindig egyetlen algebrából „készítettünk" egy újabb algebrát (részalgebra, faktoralgebra). A következőkben olyan konstrukcióról lesz szó, amikor több algebrára is szükség van.

2.25. Definíció. Legyenek adva az azonos típusú $\mathfrak{A}_i = \langle A_i; F_i \rangle$ algebrák. Ezek $\mathfrak{A} = \prod \mathfrak{A}_i$ direkt szorzatának tartóhalmaza az $A = \prod A_i$ halmaz. Ha az f műveleti név $\mathfrak{A}_i$-beli realizációja az f_i n-változós művelet, akkor az f-nek $\mathfrak{A}$-beli f' realizációját az

$$f'((\ldots, a_i^{(1)}, \ldots), \ldots, (\ldots, a_i^{(n)}, \ldots)) = (\ldots, f_i(a_i^{(1)}, \ldots, a_i^{(n)}), \ldots)$$

összefüggés definiálja, ahol $a_i^{(j)} \in \mathfrak{A}_i$. Az $\mathfrak{A}_i$ algebra a szorzat i-edik komponense. □

A direkt szorzat elemei tehát vektoroknak tekinthetők, ahol az i-edik helyen álló elemet az i-edik algebrából vettük, a műveleteket pedig komponensenként végezzük (az i-edik komponensben természetesen az i-edik algebra megfelelő műveletével). Sok esetben célszerű a direkt szorzatnak egy másik, „absztraktabb" definícióját használni.

Ez a definíció az alábbi tételből olvasható ki, amely megadja, hogy bizonyos függvények halmaza izomorf a fent definiált direkt szorzattal. Ezért a direkt szorzat fenti definíciója helyett a következő tételben megadott függvényhalmazt is tekinthetjük a megadott algebrák direkt szorzatának.

2.26. Tétel. *Legyenek az* $\mathfrak{A}_i = \langle A_i; F_i \rangle$ *algebrák* $\tau : M \to \mathbb{N}_0$ *típusúak, ahol* i *egy* I *indexhalmaz elemein fut végig, és legyen* $\sigma_i : M \to F_i$ *az a bijekció, amely minden műveleti névhez a realizációját rendeli* $(i \in I)$. *Legyen továbbá* $\mathbf{A}$ *azoknak az* $\mathbf{a} : \mathbb{N}_0 \to \bigcup\{A_i \mid i \in I\}$ *függvényeknek a halmaza, amelyekre* $\mathbf{a}(i) \in A_i$ *és* $\mathbf{F}$ *azoknak az* $\mathbf{f} = \sigma(f)$ *függvényeknek a halmaza, amelyekre*

$$(\mathbf{f}(\mathbf{a}_1, \ldots, \mathbf{a}_n))(i) = f_i(\mathbf{a}_1(i), \ldots, \mathbf{a}_n(i)), \qquad (i \in I,\ f \in M),$$

ahol $f_i = \sigma_i(f)$ *és* $n = \tau(f)$. *Ekkor* $\langle \mathbf{A}; \mathbf{F} \rangle$ *is* τ *típusú algebra, és* $\sigma : M \to \mathbf{F}$ *bijekció, amely minden műveleti névhez a realizációját rendeli hozzá. Az*

$$\mathbf{a} \mapsto (\ldots, \mathbf{a}(i), \ldots)$$

megfeleltetés az $\langle \mathbf{A}; \mathbf{F} \rangle$ *algebrát izomorf módon képezi le a* $\prod \mathfrak{A}_i$ *direkt szorzatra.* (Ez a bijekció egyébként halmazok esetében is létezik.)

Bizonyítás. A tétel állításából minden nyilvánvaló, kivéve a leképezés művelettartása. Ez viszont azonnal következik az **f** és a 2.25. definícióban megadott f' függvények értelmezéséből. ■

Ugyancsak azonnal látható:

2.27. Tétel. *A* $\pi_i : \mathbf{a} \mapsto \mathbf{a}(i)$ *megfeleltetés a direkt szorzatnak az* i*-edik komponensre való szürjektív homomorfizmusa, amit* i*-edik projekciónak nevezünk.* ■

Megjegyzések. 1. A direkt szorzat 2.26. tételben megadott formájának az az előnye, hogy a „komponenseket" nem kell „sorba rakni". Ez lehetőséget ad a direkt szorzat egyszerűbb kezelésére. Ezzel szemben nem elég szemléletes. Éppen ezért általában a sorozatokkal megadott leírást fogjuk használni.

2. A direkt szorzatból nyilvánvalóan elhagyhatóak az egyelemű komponens algebrák. Egyelemű, vagy *triviális algebra* minden típus esetében létezik; egyszerűen tekintünk egy egyelemű halmazt, és ezt az elemet tekintjük minden művelet eredményének. Természetesen egy vizsgált algebraosztályban nem feltétlenül van benne az adott típusú egyelemű algebra (például nem létezik egyelemű test). Egyelemű adott típusú algebra lényegében (azaz izomorfizmustól eltekintve) egy van. □

A későbbiekben majd szó lesz a direkt szorzat fontos részalgebráiról és faktoralgebráiról is.

2.5. Néhány speciális típusú algebra

A legfontosabb, legklasszikusabb algebratípusok a gyűrűk (mert a „számkörök" általában gyűrűt alkotnak) és a csoportok (amelyek bizonyos struktúrák leírásánál lépnek fel). Az első esetben kettő, a második esetben egy kétváltozós művelet szerepel. Algebrai szempontból – a fontosságtól eltekintve is – a struktúrák leírásánál a műveletek száma és azok *aritása* (változószáma) a meghatározó.

Egy-egy algebra annál „gazdagabb", minél több művelet van benne értelmezve. A műveletek aritása mutatja ezek bonyolultságát. Ha kevés és viszonylag kis aritású művelet szerepel, akkor az algebra „túl egyszerű"; amennyiben a műveletek száma és azok aritása nagy, akkor az algebra – rendszerint – túlságosan bonyolult és csak igen speciális esetben takar fontos struktúrát. A csoportok és gyűrűk ebből a szempontból „középen" állnak.

Algebrai leírás szemszögéből a legegyszerűbb az olyan algebra, amelyikben egyáltalán nincs is értelmezve semmiféle művelet. Ezek az algebrák a halmazok, amelyekről a műveletek alapján semmit nem lehet mondani. Valamivel többet lehet mondani olyan algebrákról, amelyekben vannak ugyan műveletek, de ezek mind nullváltozósak. Mivel egy nullváltozós művelet egy-egy elem kijelölését jelenti, ezért ezeket az algebrákat úgy nevezik, hogy halmazok, kijelölt elemekkel. Elég meglepő, de valami hasznuk még ezeknek az algebráknak is van. Az elemek kijelölése ugyanis biztosítja, hogy ezeket minden egyes részalgebra tartalmazza. Ennek következtében részalgebrák metszete soha sem lehet üres. A fenti gondolatmenetben sehol nem használtuk ki, hogy egyéb művelet nincs az algebrában. Így:

2.28. Tétel. *Ha egy algebrában van nullváltozós művelet, akkor részalgebrái bármely halmazának van metszete. Ebben az esetben létezik az algebrának legkisebb részalgebrája, amelyet az üres halmaz generálta részalgebrának tekintünk.* ■

A fenti eredményhez nem szükséges, hogy legyen nullváltozós művelet. Triviális példaként megemlítjük az egyelemű halmazt, amelyen bármely akárhány változós műveletnek egyértelműen csak a halmaz egyetlen eleme lehet az eredménye. Ennek az algebrának egyetlen részalgebrája önmaga, akkor is, ha nem definiálunk rajta nullváltozós műveletet.

Megemlítjük, hogy a kijelölt elemek megegyezhetnek akkor is, ha más-más művelet jelöli ki őket. Ez nem akadályozható meg például akkor, ha az algebrának egy homomorf képét tekintjük. Részalgebrában azonban ezek az elemek csak akkor eshetnek egybe, ha az eredetiben is megegyeztek.

Ha az algebrában minden művelet legfeljebb egyváltozós, akkor unáris algebrákról beszélünk. Ha egy unáris algebrában az unáris műveletek száma 1, akkor azt mondjuk, hogy ez monounáris algebra.

Egy monounáris algebra lényegében egy igen speciális, irányított gráf. Ezeknek a vizsgálatára nem térünk ki. Megjegyezzük, hogy a nem monounáris unáris algebrák szerkezete lényegesen bonyolultabb a monounárisokénál.

A következőkben megadunk egy tulajdonságot, amely az unáris algebrákat megkülönbözteti a többitől. Ezt legegyszerűbben a színezett irányított gráfok nyelvén írhatjuk le. Ha az $\langle A; F\rangle$ unáris algebrának tekintjük egy $a \in A$ elemét és egy $f \in F$ műveletét, akkor húzzunk egy nyilat, amely a-ból indul és $f(a)$-ba mutat ($a \to f(a)$). Ezt a nyilat még ki is „színezzük”: azt mondjuk, hogy a „színe” f ($a \overset{f}{\to} f(a)$). Így egy színezett, irányított gráfot kapunk. Nevezzük az A halmaz a és b elemét ekvivalensnek, ha a-ból el lehet jutni b-be színezett „úton”, a nyilak irányításának figyelembevétele nélkül. Így egy ekvivalenciarelációt kapunk. Az indukált osztályozás osztályait a gráf *komponenseinek* nevezik. Azonnal látható, hogy minden egyes A_i komponens egy részalgebra tartóhalmaza. Az eredeti algebra természetesen meghatározza az összes $\langle A_i; F\rangle$ részalgebrát. Ez azonban fordítva is igaz. Tetszőleges $f \in F$ esetén megadható, miképpen hat f az A-n (vagy A^0-on, ha f nulláris), ugyanis f értelmezési tartománya az A_i-k egyesítési halmaza. Ha fordítva, az $\langle A_i; F\rangle$ algebrákból indulunk ki, akkor tehát egyértelműen értelmezhető egy algebra, amelynek tartóhalmaza az eredeti tartóhalmazok egyesítése, és a műveleteket már egyértelműen meghatározza az a feltétel, hogy az eredeti algebrák ennek részalgebrái. Ha viszont a műveletek között van nem unáris – legyen például f kétváltozós –, akkor az f műveletet A_1-re és A_2-re megszorítva ebből nem határozható meg $f(a_1, a_2)$.

Az unáris algebrákon túlmenő legegyszerűbb esetben pontosan egy kétváltozós művelet létezik.

2.29. Definíció. Azokat az $\langle A; F\rangle$ algebrákat, amelyekben F egyetlen kétváltozós műveletből áll, grupoidoknak nevezzük.

A grupoidokra felsorolunk néhány példát. Mindegyik esetben legyen a tartóhalmaz $\mathbb{N}$, a pozitív egész számok halmaza. Öt műveletet definiálunk, amelyek ($\mathbb{N} \times \mathbb{N}$)-et képezik le $\mathbb{N}$-re. Legyen $\ddot{O}(a, b) = a+b$; $S(a, b) = a \cdot b$; $L(a, b) =$ az a és b legnagyobb közös osztója; $K(a, b) = [(a + b)/2]$ ($[a]$ az a valós szám egész részét jelöli); $F(a, b) = a \times b^2$.

$$\langle \mathbb{N}; \{\ddot{O}\}\rangle, \qquad \langle \mathbb{N}; \{S\}\rangle, \qquad \langle \mathbb{N}; \{L\}\rangle, \qquad \langle \mathbb{N}; \{K\}\rangle, \qquad \langle \mathbb{N}; \{F\}\rangle$$

a definíció szerint grupoid.

Ha vizsgáljuk ezt az öt algebrát, akkor igen nehéz volna róluk bármi „közöset” is megállapítani – attól eltekintve, hogy a tartóhalmaz mindig $\mathbb{N}$. E ténynek az az oka, hogy a

fenti öt művelet teljesen másképpen viselkedik, teljesen más „szabályszerűségeknek” tesz eleget. Ha a jól ismert „műveleti azonosságokat” nézzük, akkor láthatjuk, hogy az első három például asszociatív, de a többi nem az. A harmadik és a negyedik eleget tesz egy furcsa azonosságnak ($L(a, a) = K(a, a) = a$), aminek a másik három nem. Az első négy példában a kommutativitás mindenütt fennáll, de már az F műveletre ez sem teljesül.

A fenti meggondolás alapján arra a következtetésre juthatunk, hogy célszerű adott típusú algebráknak mindig egy-egy olyan osztályát vizsgálni, amelyeknek valami más közös tulajdonságuk is van. Általában – de nem mindig – ez a közös tulajdonság az lesz, hogy a műveletekre bizonyos „azonosságok” teljesülnek. A következőkben ezt mindig konkrétan vizsgáljuk, és csak később definiáljuk pontosan.

Ez a követelmény a tényleges struktúrák vizsgálatakor is felmerül. Egy-egy struktúráról ugyanis annál többet lehet mondani, minél több tulajdonságát ismerjük. Márpedig egy-egy struktúra szerkezetéről messze nem eleget árul el az, ha tudjuk, milyen típusú.

A következő részben majd olyan fontos algebrákkal foglalkozunk, amelyek definiálhatók egyetlen kétváltozós művelet segítségével.

Feladatok

1. Mikor különbözik az egyelemű tartóhalmazon két műveleti név realizációja?

2. Mutassuk meg, hogy tetszőleges (nemüres) halmazon bármilyen típusú algebra értelmezhető.

3. Legyen $\mathfrak{Z} = \langle A; f \rangle$ egy (2) típusú algebra, ahol $f(a, b) = a$. Bizonyítsuk be, hogy A minden részhalmaza egy részalgebra tartóhalmaza.

4. Legyen $\mathfrak{Q} = \langle A, q \rangle$ egy (3) típusú algebra, ahol $q(a, a, c) = a$, és $q(a, b, c) = c$, ha $a \neq b$. Határozzuk meg $\mathfrak{Q}$ összes részalgebráját.

5. Általánosítsuk az előző két feladatot.

6. Mutassuk meg, hogy ha egy algebra tartóhalmazának minden részhalmaza egy részalgebra tartóhalmaza, akkor részalgebrák egyesítésének a tartóhalmaza megegyezik az egyes részalgebrák tartóhalmazának az egyesítésével.

7. Mutassuk meg, hogy az előző feladat következménye akkor is igaz, ha az algebra műveletei egyváltozósak, noha nem minden részhalmaz tartóhalmaza valamely részalgebrának.

8. Mutassuk meg, hogy az egyelemű halmaznak egyetlen részalgebrája és egyetlen kongruenciarelációja van.

9. Mutassuk meg, hogy a 4. feladatban definiált $\mathfrak{Q}$ algebrának pontosan két kongruenciarelációja van, ha a tartóhalmaz legalább kételemű.

10. Mutassuk meg, hogy a 3. feladatban definiált $\mathfrak{Z}$ algebrának minden ekvivalenciarelációja kongruenciareláció.

11. Jelölje $\mathbb{Q}$ a racionális számok halmazát, + az összeadást és $\times$ a szorzást. Határozzuk meg $\langle \mathbb{Q}; \{+\} \rangle$ és $\langle \mathbb{Q}; \{+, \times\} \rangle$ összes kongruenciarelációit.

Definíció. Egy $\mathfrak{A} = \langle A; R\rangle$ párt relációstruktúrának nevezünk, ha R az A halmazon értelmezett relációk halmaza. Egy $\varphi : A \to B$ leképezés (reláció)homomorfizmus, ha relációtartó, azaz, ha a ϱ n-változós „relációnév" A-beli ϱ_A és B-beli ϱ_B realizációjára $(a_1, \ldots$ $\ldots, a_n) \in \varrho_A$ esetén $(\varphi(a_1), \ldots, \varphi(a_n)) \in \varrho_B$ teljesül. □

Relációstruktúrák esetében a 2.5. definíció szerint kapott részstruktúra neve *feszített részstruktúra*. $\mathfrak{B}$ az $\mathfrak{A}$ relációalgebra részstruktúrája, ha a $\mathfrak{B}$-beli relációk $\mathfrak{A}$-ban is teljesülnek.

12. Bizonyítsuk be a 2.14. tétel állítását – az utolsó kivételével – (reláció)részstruktúrákra is.

13. Mutassuk meg, hogy egy relációhomomorfizmus esetében a kép részstruktúra, de nem mindig feszített részstruktúra.

14. Változtassuk meg a relációhomomorfizmus definícióját úgy, hogy izomorfizmus (azaz bijektív homomorfizmus) inverze is izomorfizmus legyen.

15. Határozzuk meg, hogy az előző feladatban javasolt változtatás esetén milyen $\mathfrak{B}$-re vonatkozó „következményei" vannak egy $\mathfrak{B} \to \mathfrak{A}$ homomorfizmusnak.

16. Definiáljuk az $\mathfrak{A}_i$ relációstruktúrák $\mathfrak{A} = \prod \mathfrak{A}_i$ direkt szorzatát. Melyik típusú homomorfizmus lesz a $\pi_i : \mathfrak{A} \to \mathfrak{A}_i$ természetes projekció?

3. Részbenrendezett halmazok felhasználása az algebrában

Az algebrai struktúrák vizsgálatában lényeges szerepet töltenek be a részstruktúrák és a kongruenciarelációk. Ezek mindegyikét természetes módon részben lehet rendezni. Ezeknek a részbenrendezéseknek több igen fontos tulajdonsága van. E tulajdonságok tetszőleges részbenrendezett halmazok esetén vizsgálhatók, ami által több konkrét esetben felhasználhatók. Tekintettel arra, hogy e vizsgálatokban lényegében semmiféle konkrét algebrai struktúra nem szerepel, ezért ezek a vizsgálatok a bevezetéshez sorolhatók. Ezzel szemben az itteni speciális vizsgálatok nehezebben „láthatók" konkrét utalások nélkül, ezért célszerű lehet az egyes tételeket csak akkor elolvasni, amikor azok felhasználásra kerülnek. A fentieknek megfelelően, most részbenrendezett halmazok tulajdonságaival foglalkozunk. A későbbiekben a kapott eredményeket átírjuk részhalmazrendszerekre, majd végül algebrai struktúrákra.

3.1. A maximumfeltétel

Algebrai struktúrák vizsgálatakor igen jelentős ezek részstruktúráinak vagy speciális típusú részstruktúráinak a vizsgálata. Gondolhatunk például egy csoport részcsoportjaira, egy vektortér altereire vagy egy lineáris transzformációnál szereplő invariáns alterekre. Az ilyen kapcsolatra vonatkozó sok alapvető eredmény esetében nem lényeges, hogy részstruktúrákról van szó; elegendő speciális részhalmazrendszerekkel foglalkozni. Ezen túlmenően,

elég csak annyit feltenni, hogy a részhalmazokat egy részbenrendezett halmaz – nevezetesen az adott halmaz hatványhalmaza – elemeinek tekintjük.

Mindenekelőtt a részbenrendezett halmazok egy igen egyszerű alapvető tulajdonságát fogalmazzuk meg, amely szükségtelenné teszi, hogy minden egyes tételt lényegében kétszer bizonyítsunk be.

A részbenrendezett halmazok dualitási elve. *Ha egy tétel minden részbenrendezett halmazra igaz, akkor igaz tételt nyerünk belőle, ha kisebb-egyenlő helyett mindenütt nagyobb-egyenlőt, illetve kisebb helyett mindenütt nagyobbat írunk.*

Ez az elv annak a triviális következménye, hogy – mint láttuk – a nagyobb-egyenlő mint reláció ugyancsak reflexív, antiszimmetrikus és tranzitív. Felhívjuk a figyelmet arra, hogy a helyettesítést nemcsak ott kell elvégezni, ahol szerepel a kisebb-egyenlő jel, hanem minden egyes olyan fogalmat, amelyet a kisebb-egyenlő reláció segítségével definiáltunk, az analóg fogalommal kell helyettesíteni.

3.1. Definíció. Egy $\langle P, \leq \rangle$ részbenrendezett halmaz elemeinek egy $x_0, x_1, \ldots, x_n, \ldots$ $\ldots$ rendszerét növő láncnak nevezzük, ha minden i indexre fennáll, hogy $x_i \leq x_{i+1}$. Ha minden i indexre $x_i < x_{i+1}$ teljesül, akkor szigorúan növő láncról beszélünk. Ha a fenti növő lánchoz van olyan n természetes szám, amelyre $n < i$ esetén $x_i = x_n$ igaz, akkor azt mondjuk, hogy a fenti lánc stabilizálódik. □

3.2. Definíció. Ha a $\langle P, \leq \rangle$ részbenrendezett halmaz bármely nemüres részhalmazának van maximális eleme, akkor azt mondjuk, hogy P-ben érvényes a maximumfeltétel.

A P-nek egy Q részhalmazát lefelé induktívnak nevezzük, ha abból, hogy Q tartalmazza az $x \in P$ elemnél nagyobb elemeket, következik, hogy $x \in Q$ (azaz minden olyan P-beli elemet tartalmaz, amelynek az összes P-beli felső korlátját tartalmazza). P-ben érvényes a lefelé menő indukció, ha önmaga az egyetlen lefelé induktív részhalmaza. □

Megjegyezzük, hogy ha P-ben érvényes a lefelé menő indukció, akkor a P halmazban van maximális elem. Ha ugyanis ilyen elem nem volna, akkor az üres halmaz is lefelé induktív volna. Ha viszont P-nek vannak maximális elemei, akkor ezek minden lefelé induktív Q részhalmazban benne lesznek, mert náluk nagyobb elem nem létezik.

A maximumfeltétel duálisára mint minimumfeltételre fogunk utalni. Ez tehát azt mondja ki, hogy a részbenrendezett halmaz minden részhalmazában van minimális elem. Ekkor a lefelé menő indukció helyébe a felfelé menő indukció lép. A természetes számok rendezett halmazára érvényes a minimumfeltétel, hiszen minden részhalmazának van legkisebb eleme. Itt a felfelé menő indukció pontosan a teljes indukciónak felel meg.

3.3. Tétel. *Tetszőleges $\langle P; \leq \rangle$ részbenrendezett halmazra ekvivalensek az alábbi feltételek:*

(1) *Minden szigorúan növő lánc véges.*

(2) *Minden növő lánc stabilizálódik.*

(3) *Érvényes a maximumfeltétel.*

(4) *Érvényes a lefelé menő indukció.*

Bizonyítás. Ciklikus bizonyítást adunk.

Tegyük fel, hogy (1) teljesül, és legyen $x_0, x_1, \ldots$ tetszőleges növő lánc. Definiáljuk az $y_0, y_1, \ldots$ növő láncot a következőképpen. Legyen $y_0 = x_0$. Ha $y_i = x_j$ már definiálva van, akkor legyen $y_{i+1} = x_k$, arra a legkisebb k indexre, amelyik j-nél nagyobb, és amelyikre $x_j < x_k$ teljesül. Az így definiált növő lánc, definíció szerint szigorúan növő, (1) szerint tehát véges. Így létezik olyan j index, hogy x_j után már ennél nagyobb eleme nincs a láncnak, azaz stabilizálódik.

Tegyük most fel, hogy a részbenrendezett halmaz minden növő lánca stabilizálódik, és tekintsük a P-nek egy tetszőleges, nemüres Q részhalmazát. Legyen x_0 a Q tetszőleges eleme és definiáljuk az $x_0, x_1, \ldots$ növő láncot úgy, hogy x_{j+1} legyen egy, az x_j-nél nagyobb Q-beli elem, ha ilyen létezik, s legyen egyenlő x_j-vel, ha ez maximális elem Q-ban. Ezáltal egy növő láncot definiáltunk, így (2) szerint stabilizálódik, tehát van olyan i index, amelyre $x_{i+1} = x_i$; ez éppen azt jelenti, hogy x_i a Q-nak egy maximális eleme.

Ezután azt tegyük fel, hogy P-ben teljesül a maximumfeltétel, és legyen Q a P-nek egy lefelé induktív részhalmaza. Ha Q nem egyezne meg P-vel, akkor a Q-nak (a P-beli) S komplementerében volna elem; a maximumfeltétel szerint tehát volna egy x maximális elem is. Az x maximalitása miatt minden x-nél nagyobb elem Q-ban van, ezért a Q-ra vonatkozó feltétel szerint ez is eleme volna Q-nak, ellentétben az x választásával. Így S üres, azaz P-ben érvényes a lefelé menő indukció.

Végül azt tegyük fel, hogy P-ben érvényes a lefelé menő indukció. Definiáljuk Q-t mint P azon x elemeinek a halmazát, amelyekre igaz, hogy minden olyan szigorúan növő lánc véges, amelynek x a legkisebb eleme. Ha y a P-nek egy olyan eleme, hogy minden, nála nagyobb elem Q-beli, akkor tetszőleges $y = x_0 < x_1 < \ldots$ szigorúan növő lánc véges, hiszen x_1 is Q-beli. Megmutattuk tehát, hogy Q induktív. A lefelé menő indukció alapján ez azt jelenti, hogy Q tartalmazza P minden elemét. Így minden szigorúan növő lánc véges, mert e lánc legkisebb (első) eleme is Q-ban van. ■

3.2. Lezárás és Galois-kapcsolat

A lezárás tulajdonképpen analízisbeli vagy inkább topológiai fogalom. Algebrai szempontból a lezárás bizonyos elemek generálta részstruktúrát jelent. Ennek megfelelően a zártság a részalgebra absztrakt definíciójának tekinthető. Ez a kép elősegíti a lezárásra vonatkozó definíciók és tételek megértését.

3.4. Definíció. A $\langle P; \leq \rangle$ részbenrendezett halmaznak egy $\varphi : P \to P$ leképezését lezárásnak nevezzük, ha az alábbiak teljesülnek:

(1) $x \leq \varphi(x) \quad (x \in P)$.

(2) $\varphi(\varphi(x)) = \varphi(x) \quad (x \in P)$.

(3) Ha $x \leq y$, akkor $\varphi(x) \leq \varphi(y) \quad (x, y \in P)$.

(4) Ha $x \leq \varphi(y)$, akkor $\varphi(x) \leq \varphi(y) \quad (x, y \in P)$.

A $\varphi(x)$ elemet az x elem lezártjának nevezzük. □

A fenti feltételek nem függetlenek, közülük némelyek már egyértelműen meghatározzák a lezárást:

3.5. Tétel. *Ha a* $\langle P; \leq \rangle$ *részbenrendezett halmaz egy* $\varphi : P \to P$ *leképezésére teljesül a* 3.4. *definícióbeli* (1) *és* (4) *feltétel, akkor* φ *lezárás.*

Bizonyítás. $x \leq y$ esetén az (1) tulajdonság szerint fennálló $y \leq \varphi(y)$, valamint a tranzitivitás felhasználásával azt kapjuk, hogy $x \leq \varphi(y)$. Ebből viszont (4) következtében $\varphi(x) \leq \varphi(y)$ adódik, ami bizonyítja a (3) tulajdonságot. Az (1) feltételt x helyett $\varphi(x)$-re alkalmazva azt kapjuk, hogy $\varphi(x) \leq \varphi(\varphi(x))$. Alkalmazzuk most a (4) tulajdonságot, x helyébe $\varphi(x)$-et és y helyébe x-et téve. A feltételi egyenlőtlenség ebben az esetben $\varphi(x) \leq$ $\leq \varphi(x)$, ami nyilvánvalóan teljesül. A (4) tulajdonság szerint ekkor $\varphi(\varphi(x)) \leq \varphi(x)$ is igaz. Ezt az előbb kapott egyenlőtlenséggel egybevetve, kapjuk a (2) alatti összefüggést. ■

A lezárás szokásos definíciójában vagy (1) és (4), vagy (1), (2) és (3) szerepel. Könnyen belátható, hogy (4) valóban következik a másik háromból.

Egy részbenrendezett halmaz esetén bármely lezárás egyértelműen meghatározható úgy is, hogy megadjuk a zárt elemeket, vagyis azokat, amelyek megegyeznek saját lezártjukkal.

3.6. Tétel. *Legyen* φ *egy lezárás a* $\langle P; \leq \rangle$ *részbenrendezett halmazon, és legyen* Q *a* $\varphi(y) = y$ *tulajdonsággal definiált, úgynevezett zárt elemek halmaza.* Q*-ra teljesül az alábbi összefüggés:*

(∗) *Ha* $x \in P$*, akkor létezik az* $x^* = \bigwedge\{y \mid y \in Q, y \geq x\}$ *elem; továbbá* $x^* \in Q$*.*

Ezenfelül érvényes az $x^* = \varphi(x)$ *egyenlőség is.*

Megfordítva, ha Q *egy olyan részhalmaz, amelyre a* (∗) *tulajdonság teljesül, akkor az* $x \to x^*$ *megfeleltetés lezárás. A* (∗) *tulajdonságú részhalmazok és a lezárások egyértelműen meghatározzák egymást.*

Bizonyítás. A (∗) tulajdonság helyett mindjárt azt bizonyítjuk be, hogy a $\varphi(x)$ elem zárt, és az x-nél nagyobb-egyenlő zárt elemek legnagyobb alsó korlátja. (A „bonyolult” definícióra a megfordításnál van szükség.) A zártság triviálisan igaz, hiszen a (2) tulajdonság éppen ezt mondja ki. A (4) tulajdonság következtében $\varphi(x)$ az összes szóba jövő zárt elemnek alsó korlátja; de maga is zárt lévén, csak a legnagyobb alsó korlát lehet.

Tegyük most fel, hogy a Q részhalmazra teljesül a (∗) tulajdonság. Mivel x a szóban forgó elemeknek alsó korlátja, míg x^* ezek legnagyobb alsó korlátja, ezért $x \leq x^*$. Ha $x \leq$ $\leq y^*$, akkor $y^* \in Q$ következtében y^* előfordul az x^*-ot definiáló kifejezés jobb oldalán, amiből $x^* \leq y^*$ következik. Így a definiált megfeleltetés valóban lezárás.

Végül azt kell még megmutatnunk, hogy a (∗) tulajdonságú részhalmazok és a lezárások egyértelműen határozzák meg egymást. $x^* = \varphi(x)$ következtében a zárt elemek halmazának a segítségével definiált lezárás megegyezik az eredetivel. Ha először egy (∗) tulajdonságú részhalmaz van adva, akkor a definiált lezárásban a zárt elemek azok lesznek, amelyekre $x^* = x$ teljesül. $x^* \in Q$ miatt ezek mind Q-beliek. Fordítva, ha $x \in Q$, akkor x^* definíció szerint egy olyan halmaz alsó korlátja, amely tartalmazza x-et, így $x^* \leq x$. Mivel a fordított irányú tartalmazás eleve teljesül, ezért ebben az esetben $x^* = x$, tehát x valóban zárt elem. ■

3.7. Definíció. Legyen $\langle P; \leq \rangle$ és $\langle Q; \leq \rangle$ két részbenrendezett halmaz. Egy $\alpha : P \to Q$ és $\beta : Q \to P$ leképezéspárt (P és Q közötti) Galois-megfeleltetésnek vagy Galois-kapcsolatnak nevezünk, ha az alábbi feltételek teljesülnek:

(1) Ha $x \leq y$ P-beli (Q-beli) elemek, akkor $\alpha(x) \geq \alpha(y)$ ($\beta(x) \geq \beta(y)$) teljesül.

(2) Bármely P-beli (Q-beli) x elemre fennáll az $x \leq \beta\alpha(x)$ ($x \leq \alpha\beta(x)$) összefüggés.

A $P = Q$ és $\alpha = \beta$ esetben homogén Galois-megfeleltetésről beszélünk. □

Megjegyzés. Galois-megfeleltetések általában úgy jönnek létre, hogy a szereplő P és Q halmazok diszjunktak. Érdekes módon éppen ez az eset visszavezethető a homogén Galois-megfeleltetésekre. Tekintsük ugyanis a P és Q halmazok egyesítési halmazát, és ezen vezessük be a $\leq$ relációt úgy, hogy $x \leq y$, ha mindkét elem P-beli vagy mindkettő Q-beli, és $x \leq y$ teljesül az eredeti részbenrendezésre. E reláció nyilvánvalóan részbenrendezés. Terjesszük ki az egyesítési halmazra az α leképezést úgy, hogy legyen $\alpha(x) = \beta(x)$ minden Q-beli x-re. Ezáltal az egyesítési halmaznak egy önmagába való leképezését nyerjük. Abból, hogy az eredeti két leképezés Galois-megfeleltetést létesített, azonnal következik, hogy az itt definiált kiterjesztésre fennáll a 3.7. definíció (1) és (2) feltétele is, ami biztosítja, hogy Galois-megfeleltetést nyertünk. □

A homogén Galois-megfeleltetés előnye az, hogy nem kell eseteket megkülönböztetni. Éppen ezért a továbbiakban ezeket fogjuk vizsgálni.

3.8. Tétel. *A $\langle P; \leq \rangle$ részbenrendezett halmaz bármely α (homogén) Galois-megfeleltetésére teljesülnek az alábbiak:*

(1) *Ha $x \leq y$ a P-nek tetszőleges elemei, akkor $\alpha\alpha(x) \leq \alpha\alpha(y)$.*

(2) *Bármely $x \in P$ elemre $\alpha\alpha\alpha(x) = \alpha(x)$.*

(3) *Tetszőleges $x, y \in P$ elemekre az $x \leq \alpha(y)$ és az $y \leq \alpha(x)$ feltételek ekvivalensek.*

(4) *Ha létezik az $u = \bigvee\{x \mid x \in H\}$ elem, akkor létezik a $\bigwedge\{\alpha(x) \mid x \in H\}$ elem is, és megegyezik $\alpha(u)$-val ($H \subseteq P$).*

Bizonyítás. (1) azonnal következik a 3.7. definíció (1) pontjának kétszeri alkalmazásával.

A definíció (2) pontja szerint $x \leq \alpha\alpha(x)$, amiből a definíció (1) pontja alapján $\alpha(x) \geq \alpha\alpha\alpha(x)$ következik. Másrészt, a definíció (2) pontját x helyett $\alpha(x)$-re alkalmazva, az $\alpha(x) \leq \alpha\alpha\alpha(x)$ összefüggéshez jutunk, amiből azonnal következik (2) is.

A definíció (1), majd (2) pontját figyelembe véve az $x \leq \alpha(y)$ feltételből $\alpha(x) \geq \alpha\alpha(y) \geq y$ következik. x és y szerepét felcserélve azonnal adódik a két feltétel ekvivalenciája; így (3) is igaz.

(4)-ben $u \geq x$ minden $x \in H$ elemre teljesül, így a definíció (1) pontja szerint $\alpha(u)$ a szóba jövő $\alpha(x)$ elemeknek alsó korlátja. Ha v ezeknek az elemeknek tetszőleges alsó korlátja, akkor a most bizonyított (3) összefüggés miatt $\alpha(v) \geq x$ teljesül a H tetszőleges x elemére. A legkisebb felső korlát tulajdonsága miatt tehát $\alpha(v) \geq u$ is igaz, amiből – ismét a most belátott (3) tulajdonság alapján – azonnal következik, hogy $v \leq \alpha(u)$. Így $\alpha(u)$ valóban a legnagyobb alsó korlát. ■

A következőkben megmutatjuk, hogy milyen szoros kapcsolat áll fenn a lezárás és a Galois-megfeleltetés között.

3.9. Tétel. *Legyen α egy Galois-megfeleltetés a $\langle P; \leq \rangle$ részbenrendezett halmazon. Ekkor $\alpha\alpha$ lezárás a P minden olyan Q részhalmazán, amely bármely x elemével együtt az $\alpha(\alpha(x))$ elemet is tartalmazza. Ezt a lezárást a fenti Galois-megfeleltetés indukálta lezárásnak nevezzük.*

Bizonyítás. A Galois-megfeleltetés (2) tulajdonsága miatt teljesül a lezárásra vonatkozó (1) feltétel. Ha $x \leq \alpha\alpha(y)$, akkor a 3.8. tétel szerint $\alpha\alpha(x) \leq \alpha\alpha\alpha\alpha(y) = \alpha\alpha(y)$, ami bizonyítja a (4) tulajdonságot. ■

3.10. Tétel. *Minden lezárást egy Galois-megfeleltetés indukál.*

Bizonyítás. Legyen φ egy lezárás a $\langle P; \leq \rangle$ részbenrendezett halmazon. Legyen Q a P-beli zárt elemek halmaza, és minden $x \in Q$ elemhez rendeljünk hozzá egy új x' elemet. Ezeknek az elemeknek a Q' halmazán definiáljunk egy részbenrendezést: $x' \leq y'$ pontosan akkor, ha $x \geq y$. A P és Q' részbenrendezett halmazok egyesítésén – mint részbenrendezett halmazon – definiálhatunk egy Galois-megfeleltetést: tetszőleges P-beli x-re legyen $\alpha(x) = (\varphi(x))'$, míg Q' elemeire legyen $\alpha(x') = x$. Könnyű számolással belátható, hogy ez valóban Galois-megfeleltetés, amely a P halmazon éppen az eredeti lezárást indukálja. ■

A Galois-kapcsolat jellemzően két halmaz részhalmazain lép fel. Pontosabban szólva, az egyik halmaz elemei „hatnak" a másik halmazon, és bizonyos esetekben ez a hatás jellemzően speciális (például lineáris transzformációk hatnak egy vektortéren, és a specialitás az, hogy a transzformáció egy vektort a nullvektorba visz). Ezt az esetet mutatjuk be az alábbiakban.

3.11. Definíció. Az (A, B) halmazpáron értelmezett tetszőleges ϱ reláció esetén jelölje $\varphi : P(A) \to P(B)$ azt a függvényt, amely az A bármely A_1 részhalmazához az A_1 összes elemével relációban álló elemek halmazát rendeli:

$$\varphi(A_1) = \{b \mid (a, b) \in \varrho \text{ bármely } a \in A_1 \text{ esetén}\}. \qquad \square$$

3.12. Tétel. *Legyen ϱ egy reláció az (A, B) halmazpáron. A $\varphi : P(A) \to P(B)$ és $\varphi^{-1} : P(B) \to P(A)$ függvények Galois-kapcsolatot létesítenek, ha a hatványhalmazon a részbenrendezést a tartalmazással adjuk meg.*

Bizonyítás. $(\varrho^{-1})^{-1} = \varrho$ miatt elég annak a kimutatása, hogy az A halmaz bármely $A_1 \subseteq A_2$ részhalmazára $\varphi(A_2) \subseteq \varphi(A_1)$ és $A_1 \subseteq \varphi^{-1}\varphi(A_1)$.

Ha $b \in \varphi(A_2)$, akkor bármely A_2-beli a elemre teljesül, hogy $(a, b) \in \varrho$, de ekkor ez fennáll A_1 összes elemére is, hiszen A_1 minden eleme A_2-nek is eleme. Így tehát $\varphi(A_2) \subseteq \varphi(A_1)$. Legyen most $a \in A_1$. A $\varphi(A_1)$ definíciója szerint ebben csak olyan b elemek vannak, amelyekre $(a, b) \in \varrho$. Ez azt jelenti, hogy $\varphi(A_1)$ tetszőleges b eleme mellett teljesül a $(b, a) \in \varrho^{-1}$ összefüggés, ami éppen azt jelenti, hogy $a \in \varphi^{-1}\varphi(A_1)$. ■

Erre a vektorterek esetében már láttunk példát, amikor az A_2 halmaz szerepét egy $\mathcal{U}$ vektortér játszotta, míg A_1 elemei az $\mathcal{U}$ lineáris transzformációi voltak. Ekkor a ϱ relációt az definiálta, hogy $\varrho(\alpha, \mathbf{u})$ pontosan akkor teljesül, ha $\alpha(\mathbf{u}) = \mathbf{o}$. Hasonló Galois-kapcsolat fog szerepelni a modulusok és algebrák esetében. Másféle Galois-kapcsolatot fogunk látni a testelméletben (pontosabban a Galois-elméletben), ahonnét az elnevezés is származik.

3.3. Hálók

Algebrai szempontból különlegesen fontosak azok az esetek, amikor részbenrendezett halmazokban minden véges halmaznak vagy amikor minden halmaznak van legkisebb felső, illetve legnagyobb alsó korlátja. Ugyanis ez a tulajdonsága megvan bármely algebra részalgebráinak mint részbenrendezett halmaznak. (Ilyen vizsgálatoknál célszerű megengedni az üres halmazon értelmezett részalgebrákat, amennyiben részalgebrák tartóhalmazának a közös részeként az üres halmaz is fellép.)

3.13. Definíció. Legyen $\langle L; \leq \rangle$ egy részbenrendezett halmaz. Ha L minden véges, nemüres részhalmazának létezik a legkisebb felső, illetve legnagyobb alsó korlátja, akkor azt mondjuk, hogy L egyesítés-, illetve metszetfélháló. Ha mindkét fajta korlátelem létezik, akkor hálóról beszélünk. □

Az üres halmaz felső, illetve alsó korlátjait külön kell definiálni, és általában nem fogjuk megkívánni, hogy ezek létezzenek. Ha a P részbenrendezett halmaznak tekintjük egy tetszőleges x elemét, ez az üres halmaz minden elemének felső korlátja, mert az üres halmaz bármely y elemére teljesül $y \leq x$, hiszen ilyen y elem nem létezik. Eszerint, ha az üres halmaznak létezik legkisebb felső korlátja, akkor az a részbenrendezett halmaz legkisebb eleme lesz. Hasonlóképpen a részbenrendezett halmaz legnagyobb elemét tekintjük az üres halmaz legnagyobb alsó korlátjának.

3.14. Definíció. Legyen $\langle L; \leq \rangle$ részbenrendezett halmaz. Ha létezik benne egy legkisebb (legnagyobb) elem, ezt az L nullelemének (egységelemének) nevezzük és 0-val (1-gyel) jelöljük. A nullelem (egységelem) az üres halmaz legkisebb felső (legnagyobb alsó) korlátja. □

3.15. Definíció. Ha az $\langle L; \leq \rangle$ részbenrendezett halmaz minden részhalmazának létezik legkisebb felső korlátja, akkor L-et teljes hálónak nevezzük. □

A 3.15. definíció tulajdonképpen teljes egyesítés-félhálót definiál. Megmutatjuk azonban, hogy az elnevezés mégis jogos, mert a feltételből az is következik, hogy bármely részhalmaznak van legnagyobb alsó korlátja. Legyen B az L egy A részhalmaza alsó korlátainak a halmaza, és legyen u a B legkisebb felső korlátja. Mivel az üres halmaznak van legkisebb felső korlátja, ezért létezik nullelem, ami minden elemnek alsó korlátja – így biztosan eleme B-nek. Ha $b \in B$ és $a \in A$, akkor $b \leq a$ miatt $u = \bigvee\{b \mid b \in B\} \leq a$ következik, és így $u \in B$. Továbbá, $b \leq u$ következtében u az A-nak legnagyobb alsó korlátja. Ha A üres, akkor $\bigvee\{x \mid x \in L\}$ az L egységeleme; és ez az üres halmaz legnagyobb alsó korlátja.

Egy algebra tartóhalmazának részhalmazai és az algebra részalgebrái is teljes hálót alkotnak. Itt egy részhalmaz generálta részalgebra tekinthető a részhalmaz „lezárásának”. Az alábbiakban ezt a képet vizsgáljuk „absztraktan”, részbenrendezett halmazokra (illetve hálókra).

3.16. Tétel. *Teljes hálón adott tetszőleges lezárás esetén zárt elemek legnagyobb alsó korlátja is zárt, és a zárt elemek teljes hálót alkotnak.*

Bizonyítás. Legyen φ egy lezárás az $\langle L; \leq \rangle$ teljes hálóban. Legyen A zárt elemekből álló halmaz, és legyen $a = \bigwedge\{x \mid x \in A\}$. Az $a \leq \varphi(x)(= x)$ összefüggésből a lezárás (4) tulajdonsága alapján $\varphi(a) \leq \varphi(x)$ következik, és így $\varphi(a)$ is alsó korlátja A-nak. Ezért kisebb-egyenlő a legnagyobb alsó korlátnál: $\varphi(a) \leq a$. A lezárás (1) tulajdonsága miatt tehát $\varphi(a) = a$. Így a zárt elemek halmazában bármely részhalmaznak van legnagyobb alsó korlátja, amiből a 3.15. definíció és a dualitás szerint következik állításunk. ■

Célszerű megjegyezni, hogy zárt elemek legkisebb felső korlátja nem feltétlen ugyanaz, mint az eredeti hálóban vett legkisebb felső korlát. Legyen például a részbenrendezett halmaz egy végtelen halmaz részhalmazainak a halmaza a tartalmazásra mint részbenrendezésre nézve. Egy részhalmaznak a lezártja legyen önmaga, ha a részhalmaz véges, míg végtelen részhalmazok lezártja legyen az egész halmaz. Ekkor végtelen sok, páronként diszjunkt véges halmaz legkisebb felső korlátja az egyesítésük (ami általában nem az egész halmaz), míg a zárt halmazok között a legkisebb felső korlát nyilván az egész halmaz.

3.17. Tétel (a 3.16. tétel kiegészítése)**.** *Ha φ az $\langle L; \leq \rangle$ teljes hálóban lezárás, és A zárt elemeknek egy halmaza, akkor ennek a zárt elemek közti legkisebb felső korlátja* $\varphi\left(\bigvee\{x \mid x \in A\}\right)$.

Bizonyítás. Legyen $a = \bigvee\{x \mid x \in A\}$, és legyen b az A legkisebb felső korlátja a zárt elemek közt. Ekkor b az A-beli elemek egy felső korlátja L-ben is, amiből $a \leq b = \varphi(b)$ következik. A lezárás (4) tulajdonsága szerint tehát $\varphi(a) \leq \varphi(b) = b$. Másrészt viszont, tetszőleges $x \in A$ mellett $x \leq a \leq \varphi(a)$ alapján az következik, hogy $\varphi(a)$ az A elemeinek egy felső korlátja a zárt elemek között, tehát $b \leq \varphi(a)$ is igaz. ■

3.18. Definíció. Az $\langle L; \leq \rangle$ teljes háló egy c elemét kompaktnak nevezzük, ha a következő tulajdonság teljesül:

Amennyiben L egy A részhalmazára $c \leq \bigvee\{x \mid x \in A\}$ teljesül, akkor létezik A-nak egy olyan véges B részhalmaza, amelyre igaz az analóg $c \leq \bigvee\{x \mid x \in B\}$ összefüggés. □

Ez az elnevezés a topológiából származik, de igen fontos a fogalom az algebrában is, ahol – mint látni fogjuk – a végesen generáltságot jelenti.

3.19. Tétel. *Egy teljes hálóban akkor és csak akkor érvényes a maximumfeltétel, ha minden eleme kompakt.*

Bizonyítás. Legyen $x_1, x_2, \ldots, x_n, \ldots$ az L teljes háló elemeinek egy növő lánca, és x e lánc elemeinek a legkisebb felső korlátja. Ha x kompakt, akkor a triviális $x \leq \bigvee\{x_i \mid i \in \mathbb{N}\}$ feltételből következik, hogy a lánc elemei közül már véges soknak a legkisebb felső korlátja is nagyobb-egyenlő x-nél. E felső korlát azonban nyilvánvalóan valamelyik x_i, amiből $x \leq x_i$ következik. Ez pedig csak úgy lehetséges, hogy a fenti lánc (legkésőbb x_i-nél) stabilizálódik.

Tegyük most fel, hogy érvényes a maximumfeltétel, és valamely H részhalmazra és egy x elemre $x \leq \bigvee\{y \mid y \in H\}$ teljesül. Tekintsük az L háló összes $y_\nu = \bigvee\{y \mid y \in H_\nu\}$

elemének a halmazát, ahol H_ν végigfutja a H összes véges részhalmazát. A maximumfeltétel miatt ezek között az elemek között létezik egy y_0 maximális, amely egy H_0 véges részhalmaz elemeinek a legkisebb felső korlátja. Mármost, a H tetszőleges y elemét a H_0-hoz hozzávéve, ismét véges részhalmazt kapunk, amiből y_0 maximalitása alapján $y \leq y_0$ következik. Így $x \leq y_0$ is igaz, ami bizonyítja x kompaktságát. ■

A 3.19. tételhez szükséges a háló teljessége. Például a természetes számok szokásosan rendezett halmaza háló ugyan, és minden eleme kompakt, ennek ellenére nem érvényes benne a maximumfeltétel. A tétel második felének a bizonyításában viszont látható, hogy ott a teljességre valójában nem volt szükség.

A következő tétel arra mutat rá, hogy véges sok végesen generált rész generátuma is végesen generált.

3.20. Tétel. *Teljes hálóban véges sok kompakt elem legkisebb felső korlátja is kompakt; a kompakt elemek egy nullelemes egyesítés-félhálót alkotnak.*

Bizonyítás. Legyen L teljes háló, és legyenek $x_1, \ldots, x_n$ az L kompakt elemei; legyen továbbá $x \in L$ ezeknek legkisebb felső korlátja. Tegyük fel, hogy $x \leq \bigvee\{y \mid y \in \in H\}$, ahol $H \subseteq L$. Ebből következik, hogy minden i-re teljesül az $x_i \leq \bigvee\{y \mid y \in H\}$ feltétel is. A kompaktság következtében tehát léteznek a H-nak olyan $H_1, \ldots, H_n$ véges részhalmazai, amelyekre fennáll az $x_i \leq \bigvee\{y \mid y \in H_i\}$ összefüggés. Ebből pedig azonnal kapjuk, hogy a H_i halmazok H' egyesítésére igaz az $x \leq \bigvee\{y \mid y \in H'\}$ reláció, ami H' végessége folytán éppen x kompaktságát jelenti. A tétel második állítása ebből már nyilvánvalóan adódik. ■

Most egy algebrai szempontból alapvető jelentőségű fogalmat vezetünk be.

3.21. Definíció. Egy teljes hálót kompaktul generáltnak vagy algebrai hálónak nevezünk, ha minden eleme előáll kompakt elemek legkisebb felső korlátjaként. □

Ez a fogalom azt a képet takarja, hogy egy algebra minden részalgebrája végesen generált részalgebrák egyesítése. Ez azért van így, mert minden művelet véges aritású.

Algebrai hálóban megadott tetszőleges lezárás kompakt elemei szoros kapcsolatban állnak az eredeti elemekkel:

3.22. Tétel. *Legyen φ egy lezárás az $\langle L; \leq \rangle$ algebrai hálón, és jelölje K a zárt elemek halmazát. A $\langle K; \leq \rangle$ háló minden kompakt eleme egy L-beli kompakt elem lezártja.*

Bizonyítás. Legyen a a K-nak egy kompakt eleme. Mivel L algebrai háló, ezért a felírható $a = \bigvee\{x \mid x \in C_a\}$ alakban, ahol C_a az a-nál kisebb-egyenlő L-beli kompakt elemek halmaza – sőt az is nyilván feltehető, hogy e halmaz az összes, a-nál kisebb-egyenlő L-beli kompakt elemet tartalmazza. A lezárásra vonatkozó elemi tulajdonságokból következik, hogy egyrészt $a \leq \bigvee\{\varphi(x) \mid x \in C_a\}$, másrészt $\bigvee\{\varphi(x) \mid x \in C_a\} \leq \varphi(\bigvee\{\varphi(x) \mid x \in \in C_a\})$. A 3.17. tétel szerint a jobb oldalon a fellépő K-beli $\varphi(x)$ elemek K-beli legkisebb felső korlátja áll. Az a elem K-beli kompaktsága alapján tehát létezik a C_a-nak olyan véges

D részhalmaza, amelyre $a \leq$ mint ezeknek a $\{\varphi(x) \mid x \in D\}$ elemeknek a K-beli legkisebb felső korlátja: $a \leq \varphi(\bigvee\{\varphi(x) \mid x \in D\})$. Másrészt a nyilvánvaló $\varphi(x) \leq a$ összefüggés miatt a jobb oldal legfeljebb akkora, mint a, így a két oldal meg is egyezik.

Legyen most $c = \bigvee\{x \mid x \in D\}$. Az $x \leq \varphi(x) \leq a$ összefüggés miatt $c \leq a$, és így $\varphi(c) \leq \varphi(a) = a$ is igaz. Másrészt $\varphi(c) \geq x$ következtében $\varphi(c) \geq \varphi(x)$ is teljesül (ahol $x \in D$ tetszőleges), ezért $\varphi(c) \geq \bigvee\{\varphi(x) \mid x \in D\}$ is igaz. Ebből viszont a lezárásra vonatkozó (4) tulajdonság szerint $\varphi(c) \geq \varphi(\bigvee\{\varphi(x) \mid x \in D\}) = a$, tehát $a = \varphi(c)$. A 3.20. tétel szerint viszont c az L-nek egy kompakt eleme. ■

A 3.22. tétel megfordítása nem igaz, azaz általában nem lesz minden kompakt elem lezártja kompakt (a zártak halmazában sem).

Ennek megmutatására legyen például a kiindulási háló a $[0, 1]$ zárt intervallum részhalmazainak a halmaza. Ez a tartalmazásra nézve algebrai hálót alkot, amelynek kompakt elemei a véges részhalmazok. Definiálunk egy lezárást a zárt halmazok megadásával: legyenek ezek a 0-t tartalmazó – szokásos értelemben vett – zárt intervallumok. A 3.6. tétel szerint valóban lezárást adtunk meg. A zárt halmazok hálójában azonban egyetlen kompakt elem van: az egyedül a 0-t tartalmazó halmaz. (Ne felejtsük el, hogy a 3.17. kiegészítés szerint ebben a hálóban a zárt intervallumok legkisebb felső korlátja nem az egyesítési halmazuk, hanem az ezt tartalmazó legkisebb zárt intervallum!)

Még az a feltétel sem elegendő, hogy a zárt elemek hálója is teljes háló legyen.

Tekintsük például a nemnegatív egészek halmazát, és az algebrai háló legyen e halmaz részhalmazainak a tartalmazásra vett hálója. Zártak legyenek a pozitív számokból álló véges halmazok és az egész halmaz. A zárt halmazok körében – nyilvánvalóan – éppen a végesek a kompaktak, hiszen az egész halmaz a végesek legkisebb felső korlátja, de nem felső korlátja véges soknak. Ezzel szemben az egész halmaz egy kompakt halmaz – nevezetesen az egyedül a 0-ból álló halmaz – lezártja.

Most egy szükséges és elégséges feltételt adunk arra, hogy a zárt elemek hálójában pontosan a kompaktak lezártjai legyenek zártak. Ezt a feltételt nem szokták használni; a „fontos” feltétel a 3.27. tételben fog szerepelni.

3.23. Tétel. *Legyen φ lezárás az $\langle L; \leq\rangle$ algebrai hálón, és legyen K a zárt elemek halmaza. Bármely L-beli kompakt elem lezártja pontosan akkor lesz kompakt elem a $\langle K; \leq\rangle$ hálóban, ha K minden eleme előáll K-beli kompakt elemek L-beli legkisebb felső korlátjaként. Ekkor $\langle K; \leq\rangle$ is algebrai háló.*

Bizonyítás. Tegyük fel először, hogy az L-beli kompakt elemek lezártja K-beli kompakt elem. Mivel L algebrai háló, ezért K tetszőleges a eleme felírható $a = \bigvee\{x \mid x \in C\}$ alakban, ahol $x \in C$ pontosan akkor, ha $x \leq a$ és x kompakt L-ben. A lezárás elemi tulajdonságaiból azonnal következik, hogy $a = \bigvee\{\varphi(x) \mid x \in C\}$ is teljesül; ami feltétel szerint a-nak éppen egy kívánt alakú előállítását adja.

Tegyük most fel, hogy K minden eleme előállítható a kívánt módon, és legyen $\varphi(a)$ az a (L-beli) kompakt elem lezártja. Ekkor $\varphi(a)$ is felírható K-beli kompakt elemek L-beli egyesítéseként: $\varphi(a) = \bigvee\{x \mid x \in C\}$, ahol C elemei K-beli kompakt elemek. Mivel $a \leq \varphi(a)$, és a az L-ben kompakt, ezért létezik a C-nek egy olyan véges D részhalmaza,

amelyre $a \leq \bigvee\{x \mid x \in D\}$ teljesül. Ebből viszont – a lezárás elemi tulajdonságait figyelembe véve – azonnal következik a $\varphi(a) = \varphi\left(\bigvee\{x \mid x \in D\}\right)$ összefüggés. A 3.17. kiegészítés szerint tehát $\varphi(a)$ véges sok K-beli kompakt elem K-beli legkisebb felső korlátja, a 3.20. tétel szerint tehát maga is kompakt K-ban.

Mivel esetünkben az L-beli legkisebb felső korlát triviálisan K-beli is, ezért K valóban algebrai háló. ■

Most térünk rá arra a fogalomra, amely az algebrai struktúrák részstruktúrahálójának leírásánál lényeges szerepet tölt be. Előkészületül egy másik fogalomra van szükség.

3.24. Definíció. Egy részbenrendezett halmazt (felülről) irányítottnak nevezünk, ha bármely kételemű részhalmazának van felső korlátja. Az alulról irányítottság ennek a duálisa. □

A részbenrendezés tranzitivitásából azonnal következik:

3.25. Tétel. *Felülről irányított, részbenrendezett halmazban bármely nemüres véges részhalmaznak van felső korlátja.* ■

3.26. Definíció. Ha egy algebrai hálóban értelmezett lezárásban zárt elemek felülről irányított részhalmazának legkisebb felső korlátja is zárt elem, akkor algebrai lezárásról beszélünk. □

3.27. Tétel. *Algebrai lezárásban kompakt elem lezártja a zárt elemek hálójában kompakt.*

Bizonyítás. Legyen φ algebrai lezárás az $\langle L; \leq\rangle$ algebrai hálóban, és tekintsük az a kompakt elem $\varphi(a)$ lezártját. Tegyük fel, hogy a zárt elemek K halmazában egy H halmaz elemeinek (K-beli) legkisebb felső korlátja $\varphi(a)$-nál nagyobb-egyenlő. Az 3.17. kiegészítés alapján ez azt jelenti, hogy $\varphi(a) \leq \varphi\left(\bigvee\{\varphi(x) \mid x \in H\}\right)$. Legyen $b = \bigvee\{\varphi(x) \mid x \in H\}$, és tekintsük az $y_\nu = \bigvee\{\varphi(x) \mid x \in H_\nu\}$ elemeket, ahol H_ν végigfut a H összes véges részhalmazán. Nyilvánvaló, hogy a $H_\lambda = H_\nu \cup H_\mu$ esetben $y_\lambda = y_\nu \vee y_\mu$ és így $\varphi(y_\lambda) \geq \geq \varphi(y_\nu) \vee \varphi(y_\mu)$; amiből azonnal következik, hogy a $\varphi(y_\nu)$ elemek irányított halmazt alkotnak. Az algebrai lezárás definíciója szerint tehát $c = \bigvee \varphi(y_\nu) \in K$. Az y_ν-k definíciójából azonnal következik, hogy $b = \bigvee y_\nu$. Így azt kapjuk, hogy $a \leq \varphi(a) \leq \varphi(b) \leq \varphi(c) = c$. Felhasználva a kompaktságát, azt nyerjük, hogy léteznek olyan $y_1, \ldots, y_n$ elemek, amelyekre $a \leq \bigvee\{y_i \mid 1 \leq i \leq n\}$. Legyen $H_i \subseteq H$ a megfelelő y_i elemet definiáló véges részhalmaz. A $H_0 = H_1 \cup \cdots \cup H_n$ véges részhalmazhoz tartozó y_0 elemre teljesül tehát $a \leq y_0$, illetve $\varphi(a) \leq \varphi(y_0) = \varphi(\bigvee\{\varphi(x) \mid x \in H_0\})$. ■

Egy példán mutatjuk meg, hogy a 3.27. tétel megfordítása nem igaz. Tekintsük egy végtelen halmaz összes részhalmazát. Ez a tartalmazásra nézve algebrai háló. Itt pontosan a véges részhalmazok kompaktak. Definiáljuk a lezárást úgy, hogy minden véges halmaz lezártja legyen önmaga, a végtelen halmazoké pedig az egész halmaz. Itt kompakt elem lezártja kompakt, de minden elem (nemcsak a zártak) előáll kompaktak legkisebb felső korlátjaként.

3.4. Algebrai hálók reprezentálása

A továbbiakban az algebrai hálóknak egy algebra részalgebrahálójával és más algebrai rendszerekkel való kapcsolatát mutatjuk meg. Elsődleges célunk annak a megmutatása, hogy az algebrai háló „lényegében" ugyanaz, mint egy algebra részalgebrahálója. Ez a fogalom pontosabban izomorfizmussal fogalmazható meg. Tekintettel arra, hogy az algebrák izomorfizmusa – mint már jeleztük – itt nem elegendő, ezért definiálni kell részbenrendezett halmazok izomorfizmusát:

3.28. Definíció. A $\langle P; \leq_P \rangle$ és $\langle Q; \leq_Q \rangle$ részbenrendezett halmazt egymással izomorfnak nevezzük, ha létezik olyan $\varphi : P \to Q$ bijekció, amelyre $a, b \in P$ esetén $a \leq_P b$ pontosan akkor teljesül, ha $\varphi(a) \leq_Q \varphi(b)$. □

3.29. Definíció. Egy egyesítés-félháló valamely H nemüres részhalmazát ideálnak nevezzük, ha bármely két elemével együtt azok legkisebb felső korlátja is H-ban van, továbbá $x \leq y \in H$ esetén $x \in H$ is teljesül. □

3.30. Definíció. Egy H halmaz részhalmazhálóján a $P(H)$ hatványhalmaz elemeinek a tartalmazásra – mint részbenrendezésre – alkotott hálóját értjük.

Egy $\mathfrak{A} = \langle A; F \rangle$ algebrai struktúra részalgebrahálóján az $\mathfrak{A}$ részalgebráinak a tartóhalmazok tartalmazására – mint részbenrendezésre – alkotott hálóját értjük. □

3.31. Tétel. *Egy H halmaz részhalmazai, a H-n értelmezett 0-elemes egyesítés-félháló ideáljai (neve ideálháló) és a H-n értelmezett tetszőleges algebra részalgebrái a H részhalmazhálójának egy-egy részhálóját alkotják. Ezek mindegyike algebrai háló.*

Tetszőleges $\langle L; \leq \rangle$ háló esetén ekvivalensek az alábbi állítások:

(1) $\langle L; \leq \rangle$ *algebrai háló.*

(2) $\langle L; \leq \rangle$ *izomorf egy algebrai háló algebrai lezárásában a zárt elemek hálójával.*

(3) $\langle L; \leq \rangle$ *izomorf egy halmaz részhalmazhálóján – mint algebrai hálón – adott lezárásban a zárt elemek hálójával.*

(4) $\langle L; \leq \rangle$ *izomorf egy algebrai struktúra részalgebrahálójával.*

(5) $\langle L; \leq \rangle$ *izomorf egy 0-elemes egyesítés-félháló ideálhálójával.*

Bizonyítás. Az öt állítás ekvivalenciáját ciklikusan bizonyítjuk; és a megfelelő lépésben mindig igazoljuk, hogy valóban hálókat kapunk (amennyiben ez nem lett volna előzőleg bizonyítva).

Azt, hogy bármelyik állítás következik a rákövetkezőből, úgy mutatjuk meg, hogy bebizonyítjuk, mindegyik állítás speciális esetként tartalmazza az előzőt. Csupán ott használjuk majd az izomorfizmust, amikor azt bizonyítjuk, hogy az első állításból következik az utolsó.

A 3.27. és a 3.23. tételek szerint, ha (2) teljesül, akkor (1) is fennáll.

Tekintsük most egy H halmaz $\langle P(H); \subseteq \rangle$ részhalmazhálóját. Mindenekelőtt megmutatjuk, hogy ez egy algebrai háló. Mivel $P(H)$ adott elemeinek közös része ezeknek az elemeknek a $P(H)$-beli legnagyobb alsó korlátja, ezért ez egy teljes háló. Legyen $A \subseteq H$ e hálónak egy kompakt eleme. Mivel $A \subseteq \bigvee\{\{a\} \mid a \in A\}$, a kompaktság alapján van

olyan véges $B \subseteq A$, amelyre $A \subseteq \bigvee\{\{a\} \mid a \in B\}$, azaz $A \subseteq B$, vagyis A véges. Megfordítva, legyen $A = \{a_1, \ldots, a_n\}$. Ha $A \subseteq \bigvee\{H_i \mid i \in I\}$, akkor minden egyes A-beli elem benne van legalább egy H_i-ben, mondjuk $a_i \in H_i$. Ekkor viszont $A \subseteq H_1 \cup \cdots \cup H_n$, tehát A valóban kompakt.

Az ezen értelmezett algebrai lezárási rendszer tehát (2) tulajdonságú.

Tekintsük most egy $\langle H; F\rangle$ algebra részalgebráit. A H részhalmazhálója algebrai háló. Tetszőleges $A \subseteq H$ részhalmaz lezártja legyen az A generálta $[A]$ részalgebra. Ahhoz, hogy a (3) tulajdonság feltételeit kielégítsük, a 3.26. definíció és a 3.27. tétel alapján elég megmutatni, hogy algebrai lezárást értelmeztünk. Az világos, hogy ez a megfeleltetés lezárás. Tekintsük részalgebrák irányított $\{\langle A_i; F\rangle \mid i \in I\}$ rendszerét. Ez a 3.25. tétel szerint azt jelenti, hogy bármely $i_1, \ldots, i_n \in I$ indexhez van olyan k index, amelyre $A_{i_j} \subseteq A_k$ $(1 \leq j \leq n)$. Legyen $f \in F$ n-változós művelet, és $a_1, \ldots, a_n \in \bigcup\{A_i \mid i \in I\}$. Feltehető, hogy $a_i \in A_i \subseteq A_k$; és így $f(a_1, \ldots, a_n) \in A_k$, hiszen A_k egy részalgebra tartóhalmaza. Tehát algebrai lezárást kaptunk, ami pontosan a (3) alatti tulajdonság.

(Érdemes felfigyelni a következőkre: a bizonyításban igen lényeges az, hogy a műveletek véges változósak. Tulajdonképpen az analízist is lehetne „algebrának tekinteni"; olyan algebrának, amelyben végtelen változós művelet van, hozzárendelve *bizonyos* sorozatokhoz határértéküket. Talán ez az a pillanat, amikor világosan látható, mi különbözteti meg az algebrai módszereket az analízisben vagy topológiában használtaktól.)

A következő lépésben egy 0-elemes egyesítés-félhálóból kell kiindulnunk. Feladatunk úgy értelmezni műveleteket, hogy pontosan az ideálok legyenek a részalgebrák. Ezáltal alkalmazni tudjuk a (4) tulajdonságot.

Legyen tehát $\langle S; \leq\rangle$ tetszőleges, 0-elemes egyesítés-félháló. Az S-ben először is bevezetünk egy $\vee$ kétváltozós műveletet (ezt egyesítésnek nevezzük), amely az a, b elempárhoz az $a \vee b$ legkisebb felső korlátjukat rendeli hozzá. Ezek után az S-nek minden a eleméhez külön-külön hozzárendelünk egy f_a egyváltozós műveletet, amelyet a következőképpen definiálunk:

$$f_a(x) = \begin{cases} a, & \text{ha} \quad a \leq x, \\ 0 & \text{egyébként.} \end{cases}$$

Egy ideál – definíció szerint – zárt az egyesítésre, s mivel az egyváltozós műveletek minden elemhez nála kisebb-egyenlő elemet rendelnek, így ezekre is. Ezért minden ideál részalgebrája a most definiált algebrának. Tegyük most fel, fordítva, hogy az S egy T részhalmaza részalgebra, azaz zárt ezekre a műveletekre. A kétváltozós műveletre való zártság azt jelenti, hogy T zárt az egyesítésre. Ha most $x \leq y \in T$, akkor $x = f_x(y) \in T$ miatt T-re teljesül az ideált definiáló másik feltétel is, így T valóban ideál.

Végül azt kell még bizonyítanunk, hogy bármely $\langle L; \leq\rangle$ algebrai háló izomorf egy nullelemes egyesítés-félháló ideálhálójával. Ezt az egyesítés-félhálót könnyen megtalálhatjuk, mert a 3.20. tétel szerint az L-beli kompakt elemek S halmaza nullelemes egyesítés-félháló. Ezt választjuk a bizonyításhoz. Olyan izomorfizmust kell definiálni, amely L elemei és S ideáljai között létesít bijekciót. A definíció egyszerűbben történhet, ha egy $\varphi : L \to P(S)$ függvényt definiálunk, és utána mutatjuk meg, hogy képként pontosan az ideálok lépnek fel. Legyen tehát

$$\varphi(a) = \{x \in S \mid x \leq a\}.$$

Ha $x, y \in S$, és $x, y \leq a$, akkor $x \vee y \in S$, és $x \vee y \leq a$. A részbenrendezés tranzitivitását is figyelembe véve azt kapjuk, hogy $\varphi(a)$ mindig ideál. ($0 \leq a$ miatt $0 \in \in \varphi(a)$.) Ugyancsak a tranzitivitás következtében világos, hogy ha $a \leq b$, akkor $\varphi(a) \subseteq \subseteq \varphi(b)$. Ezért φ rendezéstartó leképezés.

Tekintsük most az S egy tetszőleges I ideálját, és legyen $a = \bigvee\{x \mid x \in I\}$. Azonnal világos, hogy $I \subseteq \varphi(a)$, mert $x \in I$ esetén $x \leq a$. Tekintsük a $\varphi(a)$ ideál tetszőleges y elemét, amelyre tehát $y \leq a = \bigvee\{x \mid x \in I\}$. Mivel y kompakt, ezért van olyan véges $J \subseteq I$, amelyre $y \leq \bigvee\{x \mid x \in J\}$. Az ideáltulajdonság miatt $x_0 = \bigvee\{x \mid x \in J\} \in I$, és így $y \leq x_0$ alapján $y \in I$, azaz $I = \varphi(a)$.

Ha $\varphi(a) \subseteq \varphi(b)$, akkor b a $\varphi(a)$ elemeinek egy felső korlátja, s így $a \leq b$. Amennyiben $\varphi(a) = \varphi(b)$, akkor tehát $a = b$, ezért φ injektív. A kapott $a \leq b$ egyenlőtlenségből azt kapjuk, hogy φ^{-1} is relációtartó, tehát φ izomorfizmus. ■

3.32. Tétel. *Egy algebra részalgebráira akkor és csak akkor érvényes a maximumfeltétel, ha minden részalgebrája végesen generált (azaz van olyan véges részhalmaza, amely generálja).*

Bizonyítás. Mindenekelőtt vizsgáljuk meg, mikor kompakt egy $\mathfrak{A}$ algebra részalgebrahálójának egy $\mathfrak{B}$ eleme. Legyen B a $\mathfrak{B}$ tartóhalmaza, és tekintsük a $b_i \in B$ elemek generálta $\mathfrak{B}_i$ algebrákat. Ezek halmazelméleti egyesítése B minden elemét tartalmazza, így generátumuk tartalmazza $\mathfrak{B}$-t. Ha $\mathfrak{B}$ kompakt, akkor ezek közül véges soknak – mondjuk az $\mathfrak{B}_1, \ldots, \mathfrak{B}_r$ algebráknak – a generátuma tartalmazza $\mathfrak{B}$-t; ezért a véges $\{b_1, \ldots, b_r\}$ halmaz a $\mathfrak{B}$ generátorrendszere.

Fordítva, legyen $\{b_1, \ldots, b_r\}$ generátorrendszere $\mathfrak{B}$-nek. Tegyük fel, hogy az $\{\mathfrak{A}_i \mid i \in \in I\}$ algebrák generátuma tartalmazza $\mathfrak{B}$-t. Mivel a műveletek aritása véges, ezért minden egyes b_j-hez ($1 \leq j \leq r$) létezik véges sok $\mathfrak{A}_i$, amelyek generátuma tartalmazza a kiszemelt b_j elemet. Az összes ilyen $\mathfrak{A}_i$ generátuma tehát tartalmaz minden b_j elemet, tehát ezek $\mathfrak{B}$ generátumát. A kompaktság most már abból következik, hogy a figyelembe vett $\mathfrak{A}_i$ algebrák száma véges.

A tétel további része azonnal következik a 3.19. és a 3.31. tételből. ■

Célszerű megjegyezni, hogy a „részalgebra” fogalmába sok olyan dolog beleillik, amire először nem is gondolna az ember. Ha például az algebra műveletei közé bevesszük az algebrának bármilyen típusú endomorfizmusait (önmagába való homomorfizmusait), akkor különböző részalgebrafajtákat kapunk, amelyek mind algebrai hálót alkotnak a tartalmazásra nézve. Ez különösen a csoportoknál fontos, de hasonló speciális esetek kaphatók gyűrűk esetében is.

Megjegyzés. Érdemes tudni, hogy a 3.31. tétel (3) és (4) állításának az ekvivalenciája közvetlenül is bizonyítható. Azaz, ha adott a $\langle P(A); \leq \rangle$ hálóban egy algebrai lezárás, akkor könnyen konstruálható olyan algebra, amelynek részalgebrái pontosan a zárt halmazok. Evégett csak azt kell tenni, hogy bármely véges részhalmaz elemeiből előállítsuk a generátum minden elemét. Ezt a legegyszerűbben úgy tehetjük meg, hogy minden ilyen esetben egy-egy külön műveletet vezetünk be. Csak az az egy kérdés merül fel, hogy ez a művelet milyen értéket vegyen fel máshol, hogy „ne okozzon zavart”. Ezt úgy oldhatjuk meg, hogy minden más esetben valamelyik (pl. az első) helyen álló

elem legyen a függvényérték – hiszen ez mindig benne van a kérdéses elemek generálta részalgebrában, lévén azok egyike. Ezek után az eljárás a következő. Tetszőleges $a_1, \ldots, a_n$ elemekhez tekintjük az őket tartalmazó legkisebb zárt halmazt, és ennek bármely a_0 elemét. Minden ilyen $a_0, a_1, \ldots, a_n$ rendszerhez hozzárendelünk egy n-változós $f = f_{(a_0,a_1,\ldots,a_n)}$ műveletet úgy, hogy $f(a_1, \ldots, a_n) = a_0$ és minden más elem-n-esre legyen $f(b_1, \ldots, b_n) = b_1$. Az olvasóra bízzuk annak az ellenőrzését, hogy a részalgebrák valóban a zárt részhalmazok lesznek. □

A következőkben bizonyos relációkkal létrehozott igen fontos részalgebrákat vizsgálunk.

3.33. Tétel. *Legyen $\mathfrak{A} = \langle A; F\rangle$ tetszőleges algebrai struktúra. Értelmezhetők olyan műveletek az $A \times A$ halmazon, hogy a részalgebrák pontosan az A ekvivalenciarelációi, illetve az $\mathfrak{A}$ kongruenciarelációi legyenek.*

Bizonyítás. Az 3.32. tétel utáni megjegyzés gondolata alapján adjuk meg a műveleteket a két algebrában.

Az ekvivalenciarelációk esetében a következő műveleteket definiáljuk: Minden $a \in A$ elemhez hozzárendelünk egy r_a nullváltozós műveletet, amely az (a, a) elemet jelöli ki (r biztosítja a reflexivitást). Definiálunk egy s egyváltozós műveletet, amelyre $s : (a, b) \mapsto (b, a)$ (s tehát szimmetrizál). Definiálunk egy kétváltozós t műveletet a következőképpen. Legyen $t((a, b), (b, c)) = (a, c)$, míg $b \neq c$ esetén legyen $t((a, b), (c, d)) = (a, b)$ (t biztosítja a tranzitivitást). Világos, hogy az ezekre a műveletekre való zártság pontosan azt fejezi ki, hogy a megfelelő A-beli reláció reflexív, szimmetrikus és tranzitív.

Tegyük most fel, hogy adott az $\mathfrak{A}$ algebra, és úgy akarunk műveleteket definiálni, hogy éppen a kongruenciarelációk legyenek a részalgebrák. Mivel minden kongruenciareláció ekvivalenciareláció, ezért a fenti műveleteket meghagyjuk. Emellett minden $f \in F$ művelethez hozzárendelünk egy $f \times f$ műveletet a következőképpen: ha f n-változós, akkor legyen:

$$f \times f : ((a_1, b_1), \ldots, (a_n, b_n)) \mapsto (f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)).$$

Itt is könnyen látható, hogy ezekre a műveletekre való zártság éppen a műveletekkel való kompatibilitást fejezi ki. (A bizonyítás nem szorul változtatásra nullváltozós műveletek esetében sem.) ■

Az 3.32. és 3.33. tételekből azonnal adódik:

3.34. Következmény. *Egy halmaz ekvivalenciarelációi, illetve egy algebra kongruenciarelációi algebrai hálót alkotnak.* ■

Feladatok

1. Mutassuk meg, hogy akármilyen nagy számosságú részbenrendezett halmazban igaz lehet a maximumfeltétel.

2. Mutassuk meg, hogy a maximumfeltétel egy részbenrendezett halmazban akkor is igaz lehet, ha a halmazban akármilyen véges hosszúságú lánc található.

3. Mutassuk meg, hogy egy teljesen rendezett akármekkora számosságú halmazban is teljesülhet a maximumfeltétel. Milyen teljes rendezéssel ekvivalens a minimumfeltétel?

4. Mutassuk meg, hogy ha egy részbenrendezett halmazban a maximumfeltétel is és a minimumfeltétel is teljesül, akkor a halmazban minden lánc véges.

5. Mutassunk példát arra, hogy egy Galois-kapcsolatnál az $x \wedge y$ elem létezéséből nem következik az $\alpha(x) \vee \alpha(y)$ létezése.

6. Mutassunk példát arra, hogy ha egy részbenrendezett halmazban minden *nemüres* részhalmaznak van legkisebb felső korlátja, még az sem következik, hogy minden (nemüres) *véges* részhalmaznak van legnagyobb alsó korlátja.

7. Legyen $\mathcal{V}^*$ a K test feletti $\mathcal{V}$ véges dimenziós vektortér duális tere. Az $\alpha \in \mathcal{V}^*$ és $\mathbf{u} \in \mathcal{V}$ elemekre definiáljuk a $\varrho \in \mathcal{V}^* \times \mathcal{V}$ relációt úgy, hogy $(\alpha, \mathbf{u}) \in \varrho$ pontosan akkor, ha $\alpha(\mathbf{u}) = \mathbf{o}$. A $\mathcal{V}^*$ és a $\mathcal{V}$ részhalmazain melyek a ϱ-meghatározta Galois-kapcsolat zárt részhalmazai?

8. Bizonyítsuk be, hogy minden Galois-kapcsolat előáll mint egy reláció által meghatározott Galois-kapcsolat „része” (azaz létezik mindkét irányban relációtartó beágyazás a relációnál szereplő halmazok részhalmazaiba).

9. Legyen $P = Q = \langle \mathbb{Q}; \leq \rangle$. Bizonyítsuk be, hogy $\alpha(r) = \beta(r) = -r$ Galois-kapcsolatot létesít P és Q között. Mutassuk meg, hogy nincs olyan „reláció-meghatározta” Galois-kapcsolat, amely az itt szereplővel „izomorf” volna.

10. Mutassuk meg, hogy ha egy háló minden eleme kompakt, akkor minden nemüres részhalmaznak van legkisebb felső korlátja.

11. Mutassuk meg, hogy ha egy 0-elemes háló minden eleme kompakt, akkor a háló teljes.

12. Tekintsük egy tetszőleges végtelen halmaz részhalmazainak a tartalmazásra vett algebrai hálóját. A φ lezárás rendelje minden véges részhalmazhoz önmagát és minden végtelen részhalmazhoz az egész halmazt. Bizonyítsuk be, hogy ez nem egy algebrai lezárás, mégis minden kompakt elem lezártja is kompakt.

13. Bizonyítsuk be, hogy egy teljes háló részhálóin van olyan φ lezárás, amelyben a zárt elemek pontosan a teljes részhálók ($\langle K; \leq \rangle$ teljes részhálója az $\langle L; \leq \rangle$ teljes hálónak, ha $K \subseteq L$ és K teljes háló a $\leq$ részbenrendezésre).

Mutassunk példát arra, hogy φ nem algebrai lezárás.

14. Az egészek $\mathbb{Z}$ és a racionálisak $\mathbb{Q}$ gyűrűin vezessük be a következő relációt: $\varrho(n, r)$ pontosan akkor teljesül, ha $n \cdot r \in \mathbb{Z}$ ($n \in \mathbb{Z}$ és $r \in \mathbb{Q}$). Határozzuk meg a ϱ-definiálta Galois-kapcsolat zárt részhalmazait.

MÁSODIK RÉSZ
CSOPORTOK

Ebben a részben olyan algebrai struktúrákkal foglalkozunk, ahol van bináris művelet, de csak egy. A második fejezet végén láttuk, hogy ennyi információ nagyon keveset árul el az algebráról. Az igazán „érdekes" és fontos struktúrák esetében valami „többletet" is ki kell kötni. Ez legtöbbször valami „azonossággal" tehető meg; de igen sokszor találkozunk olyan kikötéssel, amely nemcsak hogy nem azonosság, de azonossággal nem is fejezhető ki. Ebben a részben az alapvető azonosság az asszociativitás.

4. Félcsoportok

Noha a félcsoportokra is számos alkalmazási lehetőség van, itt elsősorban a csoportok bevezetéseként kerülnek tárgyalásra. A csoportokban ugyanis sok olyan fogalom és következmény szerepel, amelyek kimondásához, illetve bizonyításához elég félcsoportokra hivatkozni. Tulajdonképpen minden csoport egyben speciális félcsoport is. A félcsoportok vizsgálata közben alapvető az azonosság fogalma. Ez a fogalom az első részben még nem szerepelt. Majd látni fogjuk, hogy az azonosság az algebra egyik sarkalatos (bár nem kizárólagos) fogalma.

4.1. Félcsoport definíciója és elemi tulajdonságai

Mindenekelőtt szükségünk lesz egy bináris művelet bizonyos tulajdonságaira, pontosabban néhány azonosságra.

4.1. Definíció. Legyen f egy, az A halmazon értelmezett bináris művelet. Azt mondjuk, hogy:

(1) f asszociatív, ha $f(f(a, b), c) = f(a, f(b, c))$,

(2) f kommutatív, ha $f(a, b) = f(b, a)$,

(3) f idempotens, ha $f(a, a) = a$

teljesül bármely $a, b, c \in A$ esetében. □

4.2. Definíció. Az $\langle A; F \rangle$ grupoidot félcsoportnak nevezzük, ha az F egyetlen (bináris) művelete asszociatív. □

Félcsoportok esetén a műveletet (félcsoport-)*szorzásnak*, (félcsoport-)*összeadásnak* vagy kompozíciónak szokták nevezni. Ennek megfelelően speciális műveleti jeleket is használnak. Ha szorzásról van szó, akkor vagy az $f(a,b) = a \cdot b$, vagy az $f(a,b) = ab$ jelölés, összeadás, illetve kompozíció esetén pedig az $f(a,b) = a + b$, illetve az $f(a,b) = a \circ b$ jelölés használatos. A félcsoportműveletet általában akkor szokták összeadásnak nevezni, ha a kommutativitás is teljesül rá.

Félcsoportok esetében a tartóhalmazt rendszerint S betűvel jelölik (az angol semigroup rövidítése), és – ha ez nem okoz félreértést – ugyanúgy jelölik a félcsoportot is. Mi is ezt a jelölést használjuk.

Ha S-ben a művelet az elemek egymás mellé írásával van jelölve, akkor az asszociativitás a jól ismert $(ab)c = a(bc)$ formát ölti.

Az asszociativitás többtényezős szorzatokra is teljesül.

4.3. Tétel. *Többtényezős szorzat eredménye független a zárójelezéstől.*

Bizonyítás:. Legyen b az $a_1, \ldots, a_n$ elemeknek ebben a sorrendben vett szorzata – valamilyen zárójelezés mellett. Kimutatjuk, hogy b megegyezik a $c = (\ldots((a_1a_2)a_3)a_4\ldots\ldots)a_n$ szorzattal. Ezt a szorzatot szabatosan rekurzív módon definiálhatjuk:

$$c_1 = a_1, \quad c_2 = c_1a_2, \quad \ldots, \quad c = c_n = c_{n-1}a_n.$$

A bizonyítást n-re vonatkozó teljes indukcióval végezzük. $n \leq 2$ esetén nincs mit bizonyítani, míg $n = 3$ esetén az állítás éppen az asszociativitást jelenti. Tegyük fel, hogy állításunk igaz minden, n-nél kevesebb tényezős szorzatra. A feltétel szerint $b = b_1b_2$, ahol b_1 az $a_1, \ldots, a_k$ elemeknek ebben a sorrendben vett szorzata és b_2 az $a_{k+1}, \ldots, a_n$ elemeknek ebben a sorrendben vett szorzata. Mivel $k \geq 1$, ezért b_2 – a teljes indukciós feltétel szerint – b_3a_n alakú, ahol b_3 az $a_{k+1}, \ldots, a_{n-1}$ elemeknek ebben a sorrendben vett szorzata (megengedve, hogy e szorzatban nincs is tényező, azaz b_3 fel se lép). Az asszociativitás miatt ekkor $b = b_1(b_3a_n) = (b_1b_3)a_n$, ahol b_1b_3 az $a_1, \ldots, a_{n-1}$ elemeknek e sorrendben felírt szorzata. Ugyancsak az indukciós feltétel szerint e szorzat a kívánt alakra hozható, azaz $b_1b_3 = c_{n-1}$, amivel egyszersmind a b elemet is a kívánt alakra hoztuk. ■

A 4.3. tétel következtében többtényezős szorzatban a zárójeleket nem szükséges kiírni. Ezt az elvet mi is követni fogjuk, kivéve azokban az esetekben, amikor azt akarjuk megmutatni, hogy a bizonyítás során az asszociativitást használjuk.

Az asszociativitáshoz hasonló eredmény mondható a kommutativitásra is.

4.4. Tétel. *Ha egy félcsoportban a szorzás kommutatív, akkor egy többtényezős szorzat eredménye nem függ a tényezők sorrendjétől.*

Bizonyítás. Három tényezőre az állítás könnyen ellenőrizhető. Négy tényező esetén az $(ab)(cd) = (ac)(bd)$ egyenlőséget bizonyítjuk:

$$(ab)(cd) = a(b(cd)) = a((bc)d) = a((cb)d) = (a(cb))d = ((ac)b)d = (ac)(bd),$$

a kommutativitás és az asszociativitás alapján. A 4.3. tétel és a most kapott azonosság biztosítják, hogy egy többtényezős szorzatban bármely két, egymás melletti tényező felcserélhető. Egymás melletti elemek cseréjével pedig nyilván bármelyik sorrendből bármelyik másik sorrend elérhető. ■

Félcsoportok esetében is lehet beszélni részstruktúráról, faktorstruktúráról és direkt szorzatról. Ezekről – a 2. fejezet eredményei alapján – csak annyit tudunk, hogy grupoidok. Megmutatjuk, hogy ezek is félcsoportok:

4.5. Tétel. *Egy S félcsoport minden részgrupoidja és faktorgrupoidja félcsoport. Félcsoportok (mint grupoidok) direkt szorzata is félcsoport.*

Hasonló eredmény igaz a kommutativitásra és az idempotenciára is.

Bizonyítás. Mivel az asszociativitás bármely három elemre igaz, ezért teljesül egy részgrupoid elemeire is.

Legyen $\varphi : S \to T$ *szürjektív* grupoidhomomorfizmus az S félcsoportról a T grupoidra. A szürjektivitás miatt T bármely a_1, b_1, c_1 elemeihez léteznek olyan $a, b, c \in S$ elemek, amelyekre $\varphi(a) = a_1$, $\varphi(b) = b_1$ és $\varphi(c) = c_1$. Mivel φ művelettartó, ezért az $(ab)c = a(bc)$ összefüggésből azonnal következik az $(a_1b_1)c_1 = a_1(b_1c_1)$ összefüggés.

Legyen $\mathbf{S}$ az $\{S_i | i \in I\}$ félcsoportok direkt szorzata a $\pi_i(\mathbf{S}) = S_i$ projekciókkal. Ekkor az $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbf{S}$ elemekre – a projekciók művelettartása alapján – $\pi_i(\mathbf{a}(\mathbf{bc})) = \pi_i((\mathbf{ab})\mathbf{c})$; amiből a direkt szorzat definícióját figyelembe véve következik az asszociativitás.

A kommutativitásra és idempotenciára vonatkozó eredmények hasonlóan bizonyíthatók, felhasználva, hogy ezeket a fogalmakat is azonosságok definiálják. ■

A fenti tétel alapján „jogos” a *részfélcsoport* és *faktorfélcsoport* elnevezés.

Félcsoportban be lehet vezetni a hatvány fogalmát.

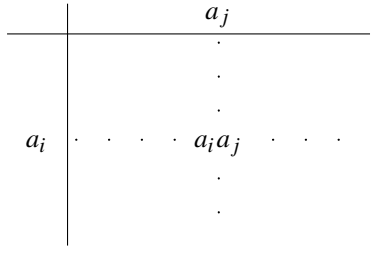
4.6. Definíció. Legyen a az S félcsoport egy tetszőleges eleme. Az a elem n-edik hatványát a következőképpen értelmezzük pozitív egész n-ekre: $n = 1$ esetén $a^1 = a$, $n \geq 2$ esetén rekurzívan definiáljuk a hatványt: $a^n = (a^{n-1})a$. □

4.7. Tétel. *Az S félcsoport egy a eleme által generált részfélcsoport elemei a-nak hatványai. Ez kommutatív félcsoport, amelyben az $a^n a^k = a^{n+k}$ és az $(a^n)^k = a^{nk}$ összefüggések teljesülnek. Az $n \to a^n$ megfeleltetés a pozitív egész számok additív félcsoportjának szürjektív homomorfizmusa a szóban forgó félcsoportra.*

Bizonyítás. A hatvány definíciója alapján az a elem hatványai benne vannak az a generálta részfélcsoportban. A 4.3. tételből azonnal következik az $a^n a^k = a^{n+k}$ összefüggés, mert a szorzat minden egyes tényezője az a elem. Ezek az elemek tehát már félcsoportot alkotnak az eredeti félcsoportbeli műveletre; így pontosan ezek a részfélcsoport elemei. Mivel ebben a félcsoportban nincs más elem, és a fenti azonosság teljesül, ezért a megadott leképezés szürjektív homomorfizmus, amelyben 1-nek az a elem felel meg. Az $(1n)k = nk$ összefüggés és a művelettartás bizonyítja a másik azonosságot, míg a kommutativitás nyilvánvaló, mert $a^n a^k = a^{n+k}$ és $n + k = k + n$. ■

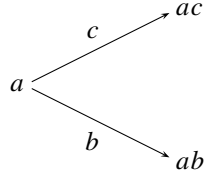
Véges félcsoportok esetében a műveleteket konkrétan meg lehet adni. Tulajdonképpen az eljárás tetszőleges véges grupoidra is elmondható, sőt sokszor alkalmazható. Ezért az alábbiakat grupoidokra mondjuk. A szorzás konkrét megadása történhet úgy, hogy minden egyes elempárra felírjuk a szorzat eredményét. Ezt legegyszerűbben egy táblázat, az úgynevezett *Cayley-táblázat* segítségével tehetjük meg. A táblázatnak annyi sora és annyi

oszlopa van, ahány eleme van a grupoidnak. Ha a grupoid elemeit valamilyen sorrendben felírtuk, akkor a táblázat i-edik sorába kívülre a grupoid i-edik (a_i) elemét írjuk, j-edik oszlopába felül a j-edik (a_j) elemet; ezek találkozási pontjába pedig szorzatukat, $a_i a_j$ sorrendben:



A Cayley-táblázatról azonnal leolvasható, hogy a grupoid kommutatív-e (a táblázat szimmetrikus-e), de igen nehéz belőle eldönteni az asszociativitást, vagyis azt, hogy a grupoid félcsoport-e.

A másik ábrázolási lehetőség a *Cayley-gráf*. E gráf szögpontjai a grupoid elemei. A gráf élei úgynevezett színezett irányított élek. Az élek ugyancsak a grupoid elemeivel vannak „színezve". A grupoid minden a eleméből pontosan egy b színű él indul ki, s ennek az élnek a végpontja az ab szögpont (fontos a sorrend).



A Cayley-gráfon elég nehezen ellenőrizhető a kommutativitás is, az asszociativitás is (bár lehet konkrét eljárást adni ezek ellenőrzésére), mégis nagyon sok helyen igen hasznosan alkalmazható.

4.2. Szabad félcsoportok

Mint láttuk, a félcsoportművelet asszociativitásából következtetni lehet az általános asszociativitásra. Ez lehetőséget adott arra, hogy a szorzás során a zárójeleket elhagyhassuk, ami lényeges könnyítés. Kérdés, hogy nem igaz-e valami más összefüggés is, ami további egyszerűsödéshez vezetne. Természetesen bizonyos speciális esetekben fennállhatnak valamilyen összefüggések; arra vagyunk azonban kíváncsiak, hogy léteznek-e *általános* összefüggések. Ha ezen a ponton kezdenénk el vizsgálni a félcsoportokat, akkor minden egyes félcsoportban minden lehetséges szorzatot fel kellene írni, és utána minden lehetséges párról (természetesen egy-egy félcsoporton belül) el kellene dönteni, hogy megegyeznek-e vagy sem. Ha például azt tapasztalnánk – ami nem igaz –, hogy minden félcsoportban bármely a és b elemre fennáll az $ab = ba$ összefüggés, akkor bebizonyítottuk volna, hogy a művelet mindig kommutatív. (Erre ellenpélda a legalább kételemű halmazon értelmezett egyváltozós függvények félcsoportja.)

Mindenekelőtt tisztázni kell azt is, hogy milyen összefüggésekre gondolunk. Összefüggésnek tekinthető az is, hogy két valamilyen módon képezett elem különbözik egymástól. Összefüggés az is, hogy az a és c elemekhez van olyan b elem, amelyre $ab = c$. Teljesen reménytelen ilyen „bonyolult" összefüggések általános érvényességét vizsgálni. Az alábbiakban csak olyan összefüggéseket tekintünk, amelyek két „különböző módon képzett" elemnek az egyenlőségét mondják ki. Az ilyen összefüggéseket *azonosságnak* nevezik.

A következő eszmefuttatás célja a 4.8. definíció indoklása.

Megtakarítható a munka nagy része akkor, ha tudunk találni egy olyan félcsoportot, amelyikben csak azok az összefüggések igazak, amelyek minden félcsoportban teljesülnek. Ilyen félcsoport természetesen nem létezhet, hiszen ebben a félcsoportban is lehetne találni olyan a, b és c elemeket, amelyekre $ab = c$ igaz, bár általában nem igaz, hogy bármelyik két elem szorzata bármely harmadikkal egyenlő. Gondoljunk azonban arra, hogy bizonyos elemekre természetesen igaz az $ab = c$ összefüggés, eleve azért, mert más elemekből így állítottuk őket elő – például az $a = x$, $b = yz$ és $c = x(yz)$ esetben. Éppen ezért azt sem kérdezhetjük, hogy minden elemre igaz-e a kiválasztott félcsoportban valami; csupán annyit nézhetünk, hogy *bizonyos elemekre* teljesül-e az összefüggés, de ezeket az elemeket úgy kell kiválasztani, hogy ne legyen köztük semmi *eleve adott* összefüggés. Ha tehát létezik ilyen $\langle A; F\rangle$ félcsoport, akkor nem az A halmaznak, hanem csak az A egy X részhalmazának az elemeiről kell megvizsgálni, hogy milyen összefüggés igaz reájuk. Nagyon kell azonban vigyázni arra, hogy az X elemei nehogy eleve előállíthatók legyenek az A bizonyos elemeiből. Ez ellen úgy védekezhetünk, hogy az A-t csak olyan elemekből alkotjuk meg, amelyeknek muszáj az A-hoz tartozniuk. Ez matematikailag pontosan azt jelenti, hogy X a fenti félcsoport generátorrendszere legyen.

Arra a megállapításra jutottunk tehát, hogy egy $\langle [X]; \cdot\rangle$ alakban megadott félcsoportot keresünk („$\cdot$" a félcsoportműveletet és $[X]$ az X generálta félcsoport tartóhalmazát jelöli) azzal a tulajdonsággal, hogy az X halmaz elemeire csak olyan összefüggések álljanak fenn, amelyek „minden félcsoportban" igazak. A továbbiakban ezt fogjuk pontosabban megfogalmazni.

Az egyszerűség kedvéért tegyük fel, hogy $X = \{x, y, z\}$, és próbáljuk meg valahol „realizálni" ezeket az elemeket; azaz tetszőleges S félcsoportokban vegyük fel az a, b, c elemeket és „álljon a az x helyett, b az y helyett és c a z helyett". Ha az X elemeiből újabb elemeket képezünk, akkor ezt az eljárást „leutánozhatjuk" az S félcsoportban is. Így xy-t az ab, $(yz)x$-et a $(bc)a$ stb. realizálja. Amennyiben az X elemei között semmiféle „szükségtelen" összefüggés nincs, akkor minden olyan esetben, amikor az X elemeiből kétféle módon képezett kifejezés megegyezik, megegyeznek az S félcsoport megfelelő elemei is. Ez azt jelenti, hogy a „leutánozás" *mindig egyértelmű megfeleltetés (leképezés).* Így az X halmazon „elkezdett" megfeleltetés folytatható az egész A halmazra, s mivel $A = [X]$, ezért a folytatás egyértelmű. Még egy dolgot fontos észrevenni, nevezetesen azt, hogy a szorzat képe – a „leutánozás" miatt – a képek szorzata lesz. Így a folytatás homomorfizmus. Az itt megállapított eljárást foglaljuk egybe az alábbi definícióban.

4.8. Definíció. Az $F_X = \langle [X]; \cdot\rangle$ félcsoportot az X generálta szabad félcsoportnak nevezzük, ha tetszőleges $S = \langle A; \cdot\rangle$ félcsoport esetén minden $\varphi : X \to A$ függvénynek létezik olyan egyértelmű $\psi : [X] \to A$ kiterjesztése, amely F_X-nek az S-re való homomorfizmusát adja.

Az X halmazt az F_X szabad generátorrendszerének, X elemeit pedig szabad generátoroknak nevezzük. Ha X-nek n darab eleme van, akkor az F_n jelölést is fogjuk használni. Egy félcsoportot szabad félcsoportnak nevezünk, ha van szabad generátorrendszere. □

Most belátjuk, hogy a szabad félcsoportok megfelelnek a kitűzött célnak:

4.9. Tétel. *Az F_n szabad félcsoport szabad generátorelemeire akkor és csak akkor teljesül egy összefüggés, ha ez az összefüggés bármely félcsoport bármely n darab elemére igaz.*

Bizonyítás. Ha az összefüggés „mindig" igaz, akkor természetesen igaz a szabad félcsoport generátorelemeire is.

Legyen most az adott szabad félcsoport felvett szabad generátorrendszere $\{x_1, \ldots, x_n\}$. Tegyük fel, hogy ezekből a szorzás segítségével kétféleképpen előállítunk egy-egy elemet, amelyeket jelöljön $f(x_1, \ldots, x_n)$ és $g(x_1, \ldots, x_n)$. Ezek egyenlősége azt jelenti, hogy F_n-ben $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$.

Tekintsük ezután egy tetszőleges S félcsoport $a_1, \ldots, a_n$ elemrendszerét (lehetnek azonosak is köztük). Ha az x_i-nek az a_i elemet feleltetjük meg, akkor a *művelettartó kiterjesztés során* az $f(x_1, \ldots, x_n)$ elemnek $f(a_1, \ldots, a_n)$, a $g(x_1, \ldots, x_n)$ elemnek pedig $g(a_1, \ldots, a_n)$ felel meg. A kiterjesztett megfeleltetésnél azonban egy elemnek csak egy képe van, a két S-beli elem tehát egyenlő; és így az összefüggés valóban fennáll. ■

A 4.9. tételből azonnal adódik az alábbi

Következmény. *Ha a $\varphi : X \to Y$ függvény injektív, szürjektív, illetve bijektív, akkor a kiterjesztett $\psi : F_X \to F_Y$ homomorfizmus is, megfelelően, injektív, szürjektív, illetve bijektív.* ■

A szabad félcsoportok hasznosságáról meggyőződtünk; csupán azt nem láttuk még be, hogy létezik is szabad félcsoport – ami nélkül az egész eredmény teljesen értelmetlenné válna.

4.10. Tétel. *Minden nemüres X halmazra létezik F_X.*

Bizonyítás. Az előállítás alapelve a következő: az általános asszociativitás következtében az X generálta szabad félcsoport elemeit úgy kaphatjuk meg, hogy ismételten szorzunk egy-egy X beli elemmel, jobbról. Először elkészítjük ezeket a „kifejezéseket", majd értelmezzük reájuk a szorzást – az asszociativitás figyelembevételével. Végül kimutatjuk, hogy X valóban szabad generátorrendszer.

Definiáljuk az $\{X_i | i \in \mathbb{N}\}$ halmazokat rekurzívan a következő módon: $X_1 = X$, $X_{n+1} = X_n \times X$ (direkt szorzat). Végezetül F_X tartóhalmaza legyen $\widehat{X} = \bigcup\{X_i | i \in \mathbb{N}\}$. Ha nagyon pontosak akarnánk lenni, akkor azt is be kellene látni, hogy az X_i halmazok páronként diszjunktak. Mi azonban ezt inkább elfogadjuk mint nyilvánvaló tényt.

(I) Az X_1 elemeit betűknek vagy 1 hosszúságú szavaknak nevezzük.

(II) Az X_n elemei n hosszúságú szavak. Ha $v \in X_{n+1}$, azaz $n + 1$ hosszúságú szó, akkor $v = (u, x)$, ahol $u \in X_n$ és $x \in X$. Az X_i halmazok diszjunktsága alapján v az u és x elemeket egyértelműen meghatározza. Ugyanezen oknál fogva egy u szó $\ell(u)$ hossza is egyértelműen meghatározott.

(III) Az u és v szavak $uv = u \cdot v$ szorzatát rekurzióval definiáljuk a következőképpen:

Ha $\ell(v) = 1$, akkor $v \in X$. Ebben az esetben legyen $uv = (u, v)$. Tegyük fel, hogy $\ell(v) = n \geq 2$ és a szorzat minden olyan esetre értelmezett, amikor a második tényező hossza kisebb, mint n.

$\ell(v) > 1$ miatt v egyértelműen felírható $v = (v_1, x)$ alakba, ahol $\ell(v_1) = n - 1$ és $x \in X$. A rekurzió alapján az $u_1 = uv_1$ szorzat definiált, és legyen $uv = (u_1, x)$.

Ezáltal egy grupoidot definiáltunk, amiről először is ki kell mutatni, hogy félcsoport, azaz bizonyítani kell a szorzás asszociativitását. Ezt a harmadik tényező hosszára vonatkozó teljes indukcióval bizonyítjuk.

Tekintsük az $(uv)w$ szorzatot. Ha $\ell(w) = 1$, akkor a szorzás definíciója szerint $u(vw) = (uv, w) = (uv)w$, tehát igaz az asszociativitás. Legyen most $\ell(w) = n$, és tegyük fel, hogy minden olyan szorzatra teljesül az asszociativitás, amelyben a harmadik tényező hossza $n - 1$. Feltétel szerint $w = (w_1, x)$, ahol $\ell(w_1) = n - 1$ és $x \in X$. A teljes indukciós feltevés és a szorzás definíciója alapján:

$$u(vw) = u(v(w_1, x)) = u((vw_1, x)) = (u(vw_1), x) = ((uv)w_1, x) = (uv)(w_1, x) = (uv)w.$$

Ugyancsak a szavak hossza szerinti teljes indukcióval bizonyítható triviálisan, hogy X generátorrendszer.

Tegyük fel végül, hogy adott az X halmaznak egy φ leképezése az S félcsoportba. Ez a leképezés csak egyféleképpen terjeszthető ki. Az 1 hosszúságú szavakra definíció szerint értelmezve van, s ha értelmezve van minden $n - 1$ hosszúságú szóra, akkor egy $u = (v, x)$ n hosszúságú szóra csak $\varphi(v) = \varphi(u)\varphi(x)$ lehetséges.

Tekintettel arra, hogy az (u, x) szó mind az u szót, mind az x betűt egyértelműen meghatározza, ezért a fenti módon egy egyértelmű leképezést definiáltunk. Most még a művelettartást kell bizonyítani. Ez a második tényező hosszára vonatkozó teljes indukcióval történik. Ha az uv szorzatban $\ell(v) = 1$, akkor a definíció szerint $\varphi(uv) = \varphi(u)\varphi(v)$. Legyen most $\ell(v) = n > 1$, és tegyük fel, hogy az állítás mindig igaz, ha a második tényező hossza $n - 1$. Ekkor a $v = (v_1, x)$ felírással:

$$\varphi(uv) = \varphi(u(v_1, x)) = \varphi((uv_1)x) = \varphi(uv_1)\varphi(x) = (\varphi(u)\varphi(v_1))\varphi(x) =$$

$$= \varphi(u)(\varphi(v_1)\varphi(x)) = \varphi(u)\varphi(v_1x) = \varphi(u)\varphi(v);$$

felhasználva a teljes indukciós feltételt és a szorzás asszociativitását mindkét félcsoportban. ■

A bizonyításban nem használtuk fel az általános asszociativitást. Ez a tulajdonság teljesül viszont minden szabad félcsoportban a generátorelemekre, a szorzás definíciója alapján. Így az általános asszociativitásra egy újabb (és teljesen kirészletezett) bizonyítást kaptunk.

Érdemes meggondolni a következőket. Az X halmaz által szabadon generált félcsoport elemei $x_1 \dots x_n$ alakú szavak (n a szó hossza), ahol a fellépő betűk nem feltétlenül különböznek. Két ilyen szó pontosan akkor egyenlő, ha ugyanolyan hosszúak és a megfelelő helyeken ugyanazok a betűk szerepelnek.

A továbbiakban a szabad félcsoportok egy felhasználási lehetőségéről szólunk. Ez a lehetőség a (Mealy-féle) automata. Ez az automaták következő elképzelésén alapszik. Egy automata minden őt érő „ingerre” belső állapotától függően valamilyen módon válaszol,

miközben belső állapota is megváltozik. Így egy automatához három halmaz tartozik: a bemenő jelek X halmaza, a kimenő jelek Y halmaza és az állapotok A halmaza. Emellett adott x bemenő jel és a állapot esetén az automata létrehoz egy $\lambda(a, x)$ kimenő jelet és az új $\delta(a, x)$ állapotba kerül. Pontosabban leírva:

4.11. Definíció. Egy (Mealy-) automata egy $(A, X, Y, \delta, \lambda)$ ötös, ahol A, X, Y halmazok, $\delta : A \times X \to A$ és $\lambda : A \times X \to Y$ függvények. □

Egy automata általában nemcsak egyetlen jelet kap, hanem egy-egy jelsorozatot. Legyen például az automata az a_0 „kezdő-" állapotban, és kapja az x_1 bemeneti jelet. Ekkor az $a_1 = \delta(a_0, x_1)$ állapotba kerül, miközben az $y_1 = \lambda(a_0, x_1)$ jelet adja ki. Ha most az x_2 bemenő jelet kapja, akkor ismét egy újabb ($a_2 = \delta(a_1, x_2)$) állapotba kerül, és kibocsátja az $y_2 = \lambda(a_1, x_2)$ jelet. Hasonlóan képezhető $a_3 = \delta(a_2, x_3)$ és $y_3 = \lambda(a_2, x_3)$ stb.

Végeredményben bármely $x_1x_2x_3\ldots$ bemenő jelsorozathoz hozzátartozik (tetszőlegesen rögzített kezdőállapot esetén) egy $y_1y_2y_3\ldots$ kimenő jelsorozat. Természetesen a kimenő jelsorozatban felléphetnek azonos betűk akkor is, ha a bemenő jelsorozatban csupa különböző betű szerepel. Mivel a jelsorozatokban zárójelek nincsenek, ezért a bemenő jelsorozatok az X generálta szabad félcsoport elemei, míg a kimenő jelsorozatok az Y generálta szabad félcsoportban vannak. Ennek megfelelően az automatákhoz hozzárendelhetők bizonyos félcsoport-leképezések (nem homomorfizmusok!), amelyek lényegében meghatározzák az automata működését.

Az automaták algebrai elmélete igen bőséges és a téma nem tartozik az általános algebrai alapismeretek közé, ezért tárgyalásukra e könyv keretein belül nem térünk ki.

4.3. Félcsoportok speciális elemekkel

4.12. Definíció. Az S félcsoport egy e elemét bal oldali (jobb oldali) neutrális elemnek nevezzük, ha minden S-beli a elemre $ea = a$ ($ae = a$) teljesül. Ha $e \in S$ mind bal oldali, mind jobb oldali neutrális elem, akkor neutrális elemnek nevezzük.

Az S félcsoport i eleme idempotens, ha $ii = i$. □

Világos, hogy bármelyik oldali neutrális elem idempotens.

Ha a félcsoportban multiplikatív írásmódot használunk, akkor a neutrális elem helyett szoktak *egységelemet* is mondani (hasonlóan használatos a *bal oldali*, illetve *jobb oldali egységelem* is).

Ha a félcsoportban additív írásmódot használunk, akkor (bal, jobb oldali) neutrális elem helyett használatos a *(bal, jobb oldali) nullelem* elnevezés is.

4.13. Tétel. *Ha e bal oldali és f jobb oldali neutrális eleme az S félcsoportnak, akkor $e = f$. Ha az S félcsoportnak van neutrális eleme, akkor S-ben nincs rajta kívül sem bal oldali, sem jobb oldali neutrális elem.*

Bizonyítás. Tetszőleges $a \in S$ mellett egyrészt $ea = a$, másrészt $af = a$ teljesül. A speciális $a = f$, majd $a = e$ választással az első esetben $ef = f$, míg a másodikban $ef = e$ adódik, amiből azt kapjuk, hogy $e = ef = f$. Ha e neutrális elem, akkor bal oldali neutrális

elem is, s ezért megegyezik minden jobb oldali neutrális elemmel. Hasonlóképpen meg kell azonban egyeznie minden bal oldali neutrális elemmel is, hiszen egyszersmind jobb oldali neutrális elem. ■

A 4.13. tételből triviálisan következik, hogy *egy félcsoportban legfeljebb egy neutrális elem van.* Multiplikatív írásmód esetén tehát legfeljebb egy egységelem létezik. Ha létezik egységelem, akkor azt mondjuk, hogy a félcsoport *egységelemes félcsoport.*

Most az egységelem duális fogalmáról lesz szó.

4.14. Definíció. Az S félcsoport egy u elemét bal oldali (jobb oldali) zéruselemnek nevezzük, ha minden S-beli a elemre $ua = u$ ($au = u$) teljesül. Ha $u \in S$ mind bal oldali, mind jobb oldali zéruselem, akkor zéruselemnek nevezzük. □

Világos, hogy bármelyik oldali zéruselem idempotens.

Könnyen összetéveszthető a nullelem és a zéruselem. Ezt elkerülendő, zéruselemről csak multiplikatív félcsoport esetén fogunk beszélni.

4.15. Tétel. *Ha egy félcsoportban van zéruselem, akkor az egyértelműen meghatározott.*

Bizonyítás. A bizonyítás gondolatmenete hasonló ahhoz, amit a 4.13. tétel bizonyításakor használtunk. Legyen ugyanis u és v az S félcsoport bal oldali és jobb oldali zéruseleme. Ekkor $u = uv$ (mert u bal oldali zéruselem) és $v = uv$ (mert v jobb oldali zéruselem), így $u = v$. Ezzel azt is bizonyítottuk, hogy egy félcsoportban, ha van bal oldali zéruselem is és jobb oldali zéruselem is, akkor ezek megegyeznek és nincs rajtuk kívül más bal oldali vagy jobb oldali zéruselem. ■

Ha az S félcsoportban van zéruselem, akkor *zéruselemes félcsoportnak nevezzük.*

A 4.13. tétel és a 4.15. tétel nem zárja ki annak a lehetőségét, hogy egy félcsoportban több „egyoldali" zéruselem vagy neutrális elem legyen. A következő példában megmutatjuk, hogy ez lehetséges is.

Tetszőleges, S nemüres halmazon értelmezhető úgynevezett *balzérus félcsoport*, az $ab = a$ művelettel. Ez nyilván grupoid, és egy akárhány tényezős szorzat eredménye mindig az első tényező, ami bizonyítja az asszociativitást. Világos, hogy egy *balzérus félcsoportban minden elem bal oldali zéruselem és minden elem jobb oldali egységelem.* (Hasonló módon definiálható a *jobbzérus félcsoport is.*)

Érdekes eredmény adódik a következő esetben is. Legyen a félcsoport tartóhalmaza $\{0, a, 1\}$, és a szorzást definiáljuk a következőképpen: 0 legyen zéruselem, 1 legyen egységelem és legyen $aa = a$. Ezzel minden szorzatot definiáltunk. Ha egy háromtényezős szorzatban valahol szerepel a 0, akkor a szorzat mindig 0 lesz. Ha 0 nem fordul elő, de szerepel az a, akkor a szorzat mindig a lesz. Végül, ha sem 0, sem a nem szerepel, akkor a szorzat 1. Ezzel beláttuk a szorzat asszociativitását. Ugyanez a meggondolás többet is mutat. Nevezetesen azt, hogy a félcsoportnak van két részfélcsoportja: $\{0, a\}$ és $\{a, 1\}$, és mindkettőben van zéruselem is, egységelem is. A zéruselemek rendre 0 és a, az egységelemek pedig a és 1. Azt láthatjuk tehát, hogy egy zéruselemes (egységelemes) félcsoportnak lehet olyan zéruselemes (egységelemes) részfélcsoportja, amelynek zéruseleme (egységeleme) különbözik az eredetitől. Mivel a részfélcsoport elemeinek önmagukat megfeleltetve nyilván a

részfélcsoportnak az egész félcsoportba való homomorfizmusát kaptuk, ezért eredményünket a következőképpen fogalmazhatjuk:

Zéruselemes (egységelemes) félcsoportok körében a zéruselem (egységelem) képe homomorfizmus esetén nem lesz feltétlenül a kép zéruseleme (egységeleme).

Szürjektív homomorfizmusnál azonban ilyen eset nem fordulhat elő.

4.16. Tétel. *Szürjektív homomorfizmusnál bal oldali zéruselem (egységelem) képe ismét bal oldali zéruselem (egységelem).*

Bizonyítás. Legyen $\varphi : S \to T$ szürjektív félcsoport-homomorfizmus. Tekintsük az S tetszőleges a, és a T tetszőleges b elemét. Mivel φ szürjektív, ezért létezik olyan $a_1 \in S$, amelyre $b = \varphi(a_1)$ teljesül. Ekkor $\varphi(a)b = \varphi(a)\varphi(a_1) = \varphi(aa_1)$. Ha a bal oldali zéruselem (egységelem), akkor $aa_1 = a$ ($aa_1 = a_1$), amiből $\varphi(a)b = \varphi(a)$ ($\varphi(a)b = \varphi(a_1) = b$) következik. ■

Sok olyan eset van azonban, amikor arra van szükségünk, hogy csak olyan homomorfizmusokat nézzünk, amelyeknél zéruselemnek, illetve egységelemnek a képe ismét zéruselem, illetve egységelem. Főleg az egységelem esete fontos. Nagyon könnyen elérhető, hogy egy homomorfizmus „tartsa" az egységelemet. Ezt úgy tehetjük meg, hogy az egységelemet műveletnek „nevezzük ki".

4.17. Definíció. Az $\langle M; \{1, \cdot\}\rangle$ algebrát monoidnak nevezzük, ha 1 nullváltozós művelet, $\langle M; \{\cdot\}\rangle$ félcsoport, és minden $a \in M$ esetén teljesül az $1a = a1 = a$ összefüggés. □

4.18. Tétel. *Monoidban az* 1 *elem egységelem; a monoidhomomorfizmus egységelemtartó.*

Bizonyítás. Az első állítás azonnal következik a monoid és az egységelem definíciójából és a 4.13. tételből. Ebből pedig következik a második állítás, tekintettel arra, hogy monoidhomomorfizmus tartja a nullváltozós műveletet is. ■

4.19. Definíció. Ha az M monoidban az a elemhez található olyan b (olyan c) elem, amelyre $ba = 1$ ($ac = 1$) teljesül, akkor azt mondjuk, hogy a-nak b balinverze (c jobbinverze). A $b = c$ esetben inverzelemről beszélünk, amelyet a^{-1}-gyel jelölünk. □

4.20. Tétel. *Ha egy monoid valamely elemének van mindkét oldali inverze, akkor ezek megegyeznek. Egy monoidban minden elem inverze egyértelműen meghatározott. Ha egy monoid valamelyik a elemének van egy b inverze, akkor b-nek is van inverze, nevezetesen a.*

Bizonyítás. A $ba = ac = 1$ feltételből $b = b1 = b(ac) = (ba)c = 1c = c$ következik, ami bizonyítja az első állítást. Ebből azonnal kapjuk, hogy az inverz egyértelműen meghatározott, mert az inverz balinverz is és jobbinverz is. Mivel a $ba = 1$ összefüggés azt is jelenti, hogy b az a balinverze és azt is, hogy a a b-nek jobbinverze, ezért még az is igaz, hogy egy elem balinverzének az eredeti elem jobbinverze. ■

4.21. Tétel. *Ha egy monoid a és b elemének c, illetve d balinverze (jobbinverze), akkor ab-nek egy balinverze (jobbinverze) dc.*

Bizonyítás. Ha $ca = db = 1$, akkor $(dc)(ab) = d(ca)b = d1b = db = 1$. A jobbinverzre vonatkozó állítás hasonlóképpen bizonyítható. ■

Az inverzelemek segítségével monoidokban is definiálható egy elem negatív kitevőjű hatványa.

4.22. Definíció. Az M monoid tetszőleges a elemére legyen $a^0 = 1$, és bármely n pozitív egész számra legyen $a^{-n} = (a^n)^{-1}$. □

Könnyen belátható a

4.23. Tétel. *Ha egy monoid valamelyik elemének van inverze, akkor ennek képe bármely rögzített monoidhomomorfizmusnál az adott elem képének az inverze.* ■

4.4. Szabad félcsoportok speciális faktorai

Szabad félcsoportokból minden félcsoport előállítható.

4.24. Tétel. *Minden félcsoport egy szabad félcsoport homomorf képe.*

Bizonyítás. Legyen G az S félcsoport tetszőleges generátorrendszere ($G = S$ is lehetséges). A G halmaz bármely g elemének önmagát megfeleltetve, egy $\varphi : G \to S$ leképezést kapunk, amely a 4.8. definíció szerint kiterjeszthető a G által szabadon generált F_G-nek egy S-be való homomorfizmusává. Mivel G generátorrendszer, ezért e homomorfizmus szürjektív. ■

A szabad félcsoportok segítségével lehetőség nyílik bizonyos összefüggéseknek (további azonosságoknak) eleget tevő félcsoportok leírására. A szabad félcsoportokban ugyanis egy ekvivalenciarelációt vezethetünk be azáltal, hogy megmondjuk, a képen mely elemeknek *kell* megegyezniök. Ez az ekvivalenciareláció meghatároz egy kongrueniarelációt; s ha a szerinte vett faktorfélcsoport eleget tesz a kívánalmaknak, akkor ez a megfelelő „szabad speciális félcsoport" lesz. (Azért kell megnézni, hogy a faktor eleget tesz-e a kívánalmaknak, mert a szabad félcsoportban általában először csak a generátorelemekre teszik fel a feltételek teljesülését – hátha elég.) A következőkben ezt mutatjuk meg néhány fontos példán.

Szabad kommutatív félcsoport

Tekintsük az X halmaz generálta szabad félcsoportot. Ennek homomorf képe lesz minden olyan kommutatív félcsoport is, amelynek van az X számosságánál nem nagyobb számosságú generátorrendszere. A kérdés az, hogy van-e ezek között „legnagyobb", azaz olyan, amelyiknek az összes többi már homomorf képe. Világos, hogy F_X minden kommutatív homomorf képében bármely két szó ugyanarra képeződik le, ha ezek csak a betűk sorrendjében különböznek egymástól. (Ez a fogalom teljesen pontosan is definiálható, de szemléletesen is világos. A pontos definícióra majd az általános algebrák vizsgálatakor

kerül sor.) Könnyen belátható, hogy az így definiálható reláció kongruenciareláció; s a szerinte vett faktorfélcsoport kommutatív. Ez a félcsoport tekinthető az X generálta félcsoportnak; és a fenti eljárás biztosítja, hogy valahányszor az X halmazt leképezzük egy kommutatív félcsoportba, e leképezés kiterjeszthető homomorfizmussá.

Hasonló elv alapján értelmezhetjük a *szabad idempotens*, illetve a *szabad idempotens kommutatív félcsoportot*. (*Idempotens félcsoport* egy olyan félcsoport, amelyben a művelet idempotens.)

Szabad monoid

Sokkal több gondot okoz a szabad monoidok definiálása. Erre kétféle lehetőség is kínálkozik, de egyik sem igazán kielégítő.

Az egyik az, hogy ugyanazt csináljuk, mint a szabad félcsoportok esetén, csak hozzáveszünk egy úgynevezett üres szót, amit 1 jelöl. Ennek a hossza nulla, és bármely szó mellé odaírva, a szóban nem történik változás.

A másik lehetőség, hogy az X generálta szabad M_X monoidot egy F_Y szabad félcsoport homomorf képének tekintjük, ahol $Y = \{1\} \cup X$. A homomorfizmushoz a következő osztályozást vezetjük be:

1. A betűk mind külön-külön osztályt alkotnak.

2. Tegyük fel, hogy az $n - 1$ hosszúságú szavak már osztályozva vannak, és legyen (u, x) tetszőleges, n hosszúságú szó. Az $u = 1$ esetben legyen (u, x) ugyanabban az osztályban, mint x. Ha u_1 az u-val egy osztályban levő, de u-nál rövidebb szó, akkor legyen (u, x) ugyanabban az osztályban, mint (u_1, x). Ha u-val egy osztályban nincs nála rövidebb szó és $x = 1$, akkor legyen (u, x) ugyanabban az osztályban, mint u. Végül, ha u-val egy osztályban nincs nála rövidebb szó és $x \neq 1$, akkor kerüljön (u, x) egy új osztályba.

Ha most minden osztályban kiválasztjuk a legrövidebb elemet, akkor ezek monoidot alkotnak, amelyet az X halmaz szabadon generál arra a szorzásra nézve, amelynél az eredeti szorzatnak mindig a legrövidebb alakját tekintjük. Ez a monoid lényegében megegyezik az első konstrukcióban adott monoiddal.

Ezeknél a konstrukcióknál nem tudjuk azonban biztosítani, hogy az egységelem képe mindig az egységelem lesz. Ez csak akkor sikerül, ha szürjektív homomorfizmust nézünk. Ez azt jelenti, hogy azért minden monoid egy szabad monoid homomorf képe lesz. A szabad monoid „minden igényt kielégítő” definiálása csak akkor fog sikerülni, ha az egységelemet nullváltozós műveletként tekintjük.

4.5. Faktorfélcsoportok invertálással

Célunk a csoportoknak mint olyan félcsoportnak a definiálása, amelyben minden elemnek van inverze. Induljunk ki egy X halmazból, amelyen egy megfeleltetés van értelmezve a következő tulajdonságokkal:

Az x elemnek megfeleltetett x' elem különbözik x-től és $(x')' = x$ teljesül minden X-beli x-re.

Az M_X szabad monoidon egy relációt vezetünk be:

Ha $u = vxx'w$ (ahol v vagy w, vagy mindkettő az üres szó is lehet), akkor vw az u egy rövidítése.

4.25. Definíció. Ha egy szónak nincs rövidítése, akkor rövidíthetetlennek nevezzük. Ha u_1 az u szóból rövidítések egymás utáni sorozatával előálló rövidíthetetlen szó, akkor u_1-et az u egy rövidített alakjának nevezzük. □

4.26. Tétel. *A szavak rövidített alakja egyértelmű.*

Bizonyítás. A szó hosszára vonatkozó teljes indukcióval bizonyítunk. A legfeljebb 1 hosszúságú u szavak esetén rövidítés nem lehetséges, így ezek önmaguknak a rövidített alakjai, s más rövidített alakjuk nincs. Legyen most u hossza $n > 2$, és tegyük fel, hogy minden, az n-nél rövidebb u_1 szónak létezik egyértelmű $r(u_1)$ rövidített alakja. Azt kell kimutatni, hogy ha u-ból rövidítések egymásutánjával kétféleképpen állítunk elő rövidíthetetlen szót, akkor ezek megegyeznek. Ha az u rövidíthetetlen, akkor az állítás triviálisan igaz. Legyen tehát $u = v_1xx'w_1 = v_2yy'w_2$, és a két rövidítéssorozat első lépéseként adódó szavak legyenek v_1w_1, illetve v_2w_2. A v_1 és v_2 hosszára az általánosság megszorítása nélkül feltehető $\ell(v_1) \leq \ell(v_2)$. Három esetet különböztetünk meg.

1. Ha $\ell(v_1) = \ell(v_2)$, akkor a két rövidítéssorozat első lépése megegyezik, s a kapott v_1w_1 szó két rövidített alakja egyúttal az u-nak a két rövidített alakja lesz. $\ell(v_1w_1) = n - 2$ figyelembevételével a teljes indukciós feltételből következik a két rövidített alak megegyezése.

2. Az $\ell(v_2) = \ell(v_1) + 1$ esetben $u = v_1xx'x''w_2$ (ahol $x'' = (x')'$), és a két rövidítéssorozat első lépése után a $v_1x''w_2$ és a v_1xw_2 szavakhoz jutunk. $x'' = x$ miatt e két szó megegyezik, és ezek után az előző esethez hasonlóan látható be az egyértelműség.

3. A fennmaradó esetben az eredeti szó $u = v_1xx'tyy'w_2$ alakú (t itt tetszőleges – esetleg az üres – szó lehet), és a két rövidítéssorozat első lépése után adódó szavak: $vtyy'w$, illetve $vxx'tw$. Mivel e szavak hossza $n - 2$, ezért mindegyiknek egyértelmű rövidített alakja van, amelyek megegyeznek az u-ból előállított két rövidített alakkal. Az indukciós feltevés szerint $n-2$ hosszúságú szavaknál bárhogyan kezdve a rövidítést, a kapott szó rövidített alakja az eredeti szó rövidített alakja lesz, amiből $r(vtyy'w) = r(vtw)$ és $r(vxx'tw) = r(vtw)$ következik. Mivel $\ell(vtw) = n - 4$, e szó rövidített alakja is egyértelmű, ami biztosítja, hogy u két rövidített alakja megegyezik. ■

A fenti igen hasznos eljárás menete ahhoz hasonlít, amikor egy ◊ jel tetejéről kétféle úton lefelé menve ugyanoda érünk. Ezt az eljárást a jel alapján *károlemmának* nevezik.

4.27. Tétel. *Két M_X-beli szó legyen Θ_G relációban, ha rövidített alakjuk megegyezik. Ekkor Θ_G kongruenciareláció, s a szerinte vett faktorfélcsoportban minden elemnek van inverze.*

Bizonyítás. A 4.26. tétel alapján a reláció jóldefiniált és reflexív. A reláció szimmetrikussága a definíció szimmetrikussága alapján nyilván teljesül. Ha az u, v, w szavak $r(u), r(v), r(w)$ rövidített alakjaira $r(u) = r(v)$ és $r(v) = r(w)$, akkor $r(u) = r(w)$, amiből a reláció tranzitivitása következik. Ha a rövidített alakokra $r(u_1) = r(u_2)$ és $r(v_1) = r(v_2)$ teljesül, akkor a rövidített alakok egyértelműsége szerint:

$$r(u_1v_1) = r(r(u_1)r(v_1)) = r(r(u_2)r(v_2)) = r(u_2v_2),$$

ami éppen azt jelenti, hogy a reláció kongruenciareláció.

Az utolsó állítás bizonyítására azt kell belátni, hogy minden u szóhoz létezik olyan u' szó, amelyre $r(uu')$ megegyezik az üres szóval. Ez az u' szó úgy keletkezik u-ból, hogy az u-beli betűket fordított sorrendben írjuk fel, és minden x betű helyére az x'-t tesszük. Állításunkat teljes indukcióval bizonyíthatjuk. Ha u egyetlen betűből áll, akkor a megfelelő szó az eredetileg hozzárendelt u' betű, és uu' valóban az üres szó. Ha az állítás igaz minden, n-nél rövidebb szóra, és $u = vx$ egy n hosszúságú szó, ahol $\ell(v) = n-1$, akkor az indukciós feltevés alapján $r(vxx'v') = r(vv')$ valóban az üres szó, vagyis $u' = x'v'$. ■

4.28. Tétel. *Vezessünk be az M_X-beli rövidíthetetlen szavak körében egy szorzást úgy, hogy u és v szorzata legyen az uv rövidített alakja. Minden rövidíthetetlen szónak megfeleltetve az M_X/Θ_G-beli képét, a most definiált grupoidnak az M_X/Θ_G-vel való izomorfizmusát kapjuk.*

Bizonyítás. A rövidített alak egyértelműsége folytán M_X/Θ_G minden osztályában pontosan egy rövidíthetetlen alak van; az adott megfeleltetés tehát bijekció. A 4.27. tétel szerint Θ_G kongruenciareláció. Így uv rövidített alakja éppen az u-t, illetve v-t tartalmazó osztályok szorzatában van; ami bizonyítja a művelettartást. ■

Feladatok

1. Mutassuk meg, hogy az alább felsorolt számok félcsoportot alkotnak mind az összeadásra, mind pedig a szorzásra nézve:

A racionálisak, a valósak, a komplexek; a természetes és az egész számok, a páros számok, és általában egy rögzített $n > 1$ egész számmal osztható számok. Ezek közül melyek monoidok?

2. Mutassuk meg, hogy az alábbi számok félcsoportot alkotnak a szorzásra, de nem alkotnak félcsoportot az összeadásra:

A páratlan számok, a 3-mal nem osztható számok, az $nk+1$ ($n > 1$ rögzített természetes szám), illetve az $5k \pm 1$ alakú számok.

3. Mutassuk meg, hogy egy vektortér lineáris transzformációi félcsoportot (monoidot) alkotnak mind az összeadásra, mind a szorzásra nézve.

4. Mutassuk meg, hogy egy halmaz önmagára való leképezései félcsoportot (monoidot) alkotnak a kompozícióra nézve.

5. Mutassuk meg, hogy egy algebra részalgebrái félcsoportot alkotnak a legkisebb felső korlát képzésére nézve. Mi a feltétele annak, hogy ez monoid legyen?

6. Bizonyítsuk be, hogy az n elemű ciklikus (egy elemmel generált) nem izomorf félcsoportok száma n.

7. Bizonyítsuk be, hogy a ciklikus szabad félcsoportnak minden $n \in \mathbb{N}$ esetén van olyan részcsoportja, amelyik nem generálható n-nél kevesebb elemmel.

8. Bizonyítsuk be, hogy az n elemmel szabadon generált félcsoport minden szabad generátorrendszere n elemű (és csak sorrendben térhet el az eredeti generátorrendszertől).

9. Bizonyítsuk be, hogy a véges, vagy megszámlálhatóan végtelen sok elemmel szabadon generált félcsoport tartóhalmazának számossága megszámlálható; a végtelen sok elemmel generálté megegyezik a generátorrendszer számosságával.

10. Bizonyítsuk be, hogy a két elemmel szabadon generált félcsoportnak van olyan részfélcsoportja, amelyik izomorf a megszámlálhatóan végtelen sok elemmel generált szabad részcsoporttal (azaz van benne olyan végtelen elemsorozat, amelyekből képezett szorzatok csak akkor egyenlők, ha ezeknek ugyanazon szorzatai).

11. Bizonyítsuk be, hogy az $\{x, y\}$ halmaz által szabadon generált kommutatív félcsoportnak azok az $x^i y^j$ elemei, amelyekre $i \geq 2j$, részfélcsoportot alkotnak.

12. Bizonyítsuk be, hogy a két elemmel szabadon generált kommutatív félcsoportnak van olyan részfélcsoportja, amelyik nem generálható véges sok elemmel.

13. Bizonyítsuk be, hogy az n elem által szabadon generált kommutatív félcsoport csak akkor tartalmaz a k elemmel szabadon generált kommutatív félcsoporttal izomorf félcsoportot, ha $k \leq n$. (Azaz bármely $n + 1$ eleme között „fennáll valamilyen összefüggés”.)

14. Bizonyítsuk be, hogy a két elemmel szabadon generált idempotens félcsoportnak hat eleme van. Mutassuk meg, hogy a véges sok elemmel generált szabad idempotens félcsoport nem mindig véges.

15. Bizonyítsuk be, hogy az n elemmel generált szabad idempotens kommutatív félcsoport elemeinek száma $2^n - 1$.

16. Mi a kapcsolat az idempotens kommutatív félcsoportok és a félhálók között?

17. Az a elemmel generált grupoid elemeinek felírásában háromféle jel szerepel: a, (és). Minden elemet egyértelműen meghatároz ezeknek az elemeknek a sorrendje (persze nem minden sorrend értelmes). E grupoid elemei tehát a három elemmel szabadon generált félcsoport elemeinek tekinthetők. A félcsoportokban a szorzás asszociatív, de a kapott grupoidban nem az. Mi ennek az oka?

18. Legyen A és B két, nemüres halmaz, és definiáljuk a többtényezős szorzatokat: Ha a szorzatban van A-beli elem, akkor az eredmény legyen az első A-beli tényező; amennyiben ilyen nincs, akkor legyen az eredmény az utolsó B-beli tényező. Bizonyítsuk be, hogy itt A minden eleme bal oldali zéruselem és B minden eleme bal oldali egységelem. Bizonyítsuk be, hogy ez idempotens félcsoport, de nem balzérus félcsoport.

19. Tekintsük egy adott test feletti adott méretű négyzetes mátrixokat. Ezek a szorzásra félcsoportot alkotnak. Határozzuk meg ennek olyan részfélcsoportjait, amelyek bal-, illetve jobbzérus félcsoportok.

20. Mutassuk meg, hogy mind a balzérus, mind a jobbzérus félcsoportok idempotens félcsoportok.

21. Mutassuk meg balzérus (jobbzérus) félcsoportokra a következőket:

(1) minden részhalmaza részfélcsoport,

(2) minden ekvivalenciareláció kongruenciareláció,

(3) minden köztük menő leképezés homomorfizmus,

(4) mindegyikük szabad balzérus (jobbzérus) félcsoport.

Mutassuk meg, hogy egy grupoid pontosan akkor balzérus vagy jobbzérus félcsoport, ha (1) és (2) teljesül.

22. Nevezzük az $\mathfrak{A} = \langle A; \cdot \rangle$ grupoidot öröklődőnek, ha minden részhalmaza részgrupoid (részalgebra). Bizonyítsuk be, hogy $\mathfrak{A}$ pontosan akkor öröklődő, ha minden *legfeljebb* kételemű részhalmaza részalgebra, azaz, ha $a, b \in A$ esetén $a \cdot b \in \{a, b\}$.

Vezessük be az öröklődő $\mathfrak{A}$ grupoid esetén a P (piros) és K (kék) relációkat: legyen $(a, b) \in P$, ha $a \cdot b = a$ és $(a, b) \in K$, ha $a \cdot b = b$. Az első relációt jelölje $a \to b$, a másodikat $a \dashrightarrow b$. Így egy „piros” és egy „kék” irányított gráfot kapunk.

Bizonyítsuk be az alábbiakat:

(1) Mindkét reláció reflexív.

(2) A két reláció közös része a diagonális reláció, egyesítésük a teljes reláció (azaz minden pár relációban van).

(3) $\mathfrak{A}$ pontosan akkor félcsoport, ha mindkét reláció tranzitív.

(4) $\mathfrak{A}$ pontosan akkor kommutatív, ha mindkét reláció szimmetrikus.

Tegyük fel, hogy egy A halmazon értelmezve van két (kétváltozós) reláció, P és K, amelyeket megfelelően $\to$ és $\dashrightarrow$ jelöl úgy, hogy ezekre a fenti (1) és (2) tulajdonság teljesül, és definiáljuk az $a \cdot b$ $(a, b \in A)$ műveletet úgy, hogy $a \cdot b = a$, ha $a \to b$ és $a \cdot b = b$, ha $a \dashrightarrow b$.

Bizonyítsuk be az alábbiakat:

(1) $\mathfrak{A} = \langle A; \cdot \rangle$ öröklődő grupoid.

(2) $\mathfrak{A}$ pontosan akkor félcsoport, ha mindkét reláció tranzitív.

(3) $\mathfrak{A}$ pontosan akkor balzérus (jobbzérus) félcsoport, ha P (K) a diagonális reláció.

23. Legyen $T(H)$ a H halmaz önmagába való leképezéseinek a kompozícióra való félcsoportja.

Határozzuk meg, hogy véges H esetén az alábbi részhalmazok közül melyik részfélcsoportja $T(H)$-nak:

(1) Amelyeknek a képe H-val egyenlő.

(2) Amelyeknek a képe valódi része H-nak.

(3) Amelyeknek a képe páratlan (páros) sok elemet tartalmaz.

(4) Amelyeknek a képe legfeljebb (legalább) k elemű ($k \leq |H|$).

(5) Amelyeknek a képe egy $H' \subset H$ részhalmazban van.

(6) Amelyek magjában minden osztály egyelemű.

(7) Amelyek magjában nem minden osztály egyelemű.

(8) Amelyek magjában minden osztály több mint egyelemű.

(9) Amelyek magjában minden osztálynak páros (páratlan) sok eleme van.

(10) Amelyek magjának osztályai tartalmazzák a H előre adott részhalmazait.

Határozzuk meg, hogy végtelen H esetén az alábbi részhalmazok közül melyik részfélcsoportja $T(H)$-nak:

(1) Amelyek képe az egész H.

(2) Amelyek képe csak véges sok elemet nem tartalmaz.

(3) Amelyek képe végtelen sok elemet tartalmaz.

(4) Amelyek képe csak véges sok elemet tartalmaz.

(5) Amelyek magjában minden osztály véges.

(6) Amelyek magjában van véges osztály.

(7) Amelyek magjában van végtelen osztály.

(8) Amelyek magjában minden osztály végtelen.

5. Csoportok

A csoport fogalma szerencsés és igen sok alkalmazást megengedő fogalom. A csoport volt az első olyan algebrai struktúra, amelyet absztrakt definícióval adtak meg. Jelentősége igen nagy a matematika számos fejezetében, sőt, például az elméleti fizikában is. Ezért van az is, hogy a csoportoknak nagyon sokféle definíciója ismeretes.

Első lépésként ezeket a definíciókat adjuk meg, és az adott definíciók ekvivalenciáját bizonyítjuk.

5.1. A csoport ekvivalens definíciói

A csoport fogalma annyival gazdagabb a félcsoporténál, hogy itt megkövetelik az egységelem létezését, továbbá azt is, hogy minden elemnek létezzék inverze. A fenti meghatározást tulajdonképpen definíciónak tekinthetnénk, de a félcsoportoknál látottak alapján a létezést kívánó feltételeket itt is célszerű műveletekkel biztosítani.

5.1. Definíció. A $\langle G; \{1, {}^{-1}, \cdot\}\rangle$ algebrai struktúrát – ahol 1 nullváltozós, $^{-1}$ egyváltozós és $\cdot$ kétváltozós művelet – csoportnak nevezzük, ha

(1) $\langle G; \{1, \cdot\}\rangle$ monoid;

(2) bármely G-beli a elemre $a^{-1} \cdot a = a \cdot a^{-1} = 1$ teljesül (a^{-1} jelöli azt az elemet, amelyet az egyváltozós művelet a-hoz hozzárendel).

Ha a $\langle G; \{\cdot\}\rangle$ félcsoport kommutatív, akkor azt mondjuk, hogy a csoport kommutatív vagy Abel-féle.

Ha a kétváltozós műveletet + jelöli, akkor additív, egyébként multiplikatív csoportról beszélünk. □

(Ha félreértést nem okoz, akkor a csoportokat is alaphalmazukkal fogjuk jelölni.)

A definíció alapján világos, hogy minden csoport egyszersmind félcsoport is, de olyan félcsoport, amelyben létezik neutrális elem, s erre nézve minden elemnek van inverze. A csoportfogalom ennél annyiban erősebb, hogy bármely csoporthomomorfizmus az egységelemet az egységelembe s az inverzelemet az inverzelembe kell hogy vigye. Mint a 4.16. tétel előtti példában láttuk, félcsoport-homomorfizmusnál az egységelem képe nem feltétlenül lesz a kép egységeleme. Amennyiben viszont megköveteljük, hogy inverzelem is létezzék, akkor ez a többlet biztosítja, hogy a félcsoport-homomorfizmusnál az egységelem képe a kép egységeleme és az inverzelem képe a kép inverzeleme lesz. (Egyébként ez az oka annak, hogy eredetileg sem az egységelemet, sem az inverzelemet nem művelettel definiálták, és a csoporthomomorfizmusnál is csak a szorzattartást tették fel – ugyanis erősebb feltételre nem volt szükség.) A következőkben az itt vázolt állítást fogjuk bebizonyítani. Ehhez azonban, előkészületül, be kell látni egy, a félcsoportokra vonatkozó tételt.

5.2. Tétel. *Egy G félcsoportra az alábbi állítások ekvivalensek:*

(I) *A félcsoportban létezik egy* 1 *egységelem és minden a elemnek létezik erre vonatkozó a^{-1} inverze (tehát minden $a \in G$ esetén teljesülnek az $1a = a1 = a$ és $a^{-1}a = aa^{-1} = 1$ összefüggések).*

(II) *G-ben egyértelműen megoldhatók az $ax = b$ és $ya = b$ egyenletek (tehát bármely $a, b \in G$ esetén létezik pontosan egy olyan G-beli c, illetve d, amelyre $ac = b$ és $da = b$ teljesül).*

(III) *G-ben megoldhatók az $ax = b$ és $ya = b$ egyenletek.*

(IV) *G-ben létezik egy 1 bal oldali egységelem, és minden G-beli a elemnek létezik a^{-1} bal oldali inverze (tehát minden $a \in G$ esetén teljesülnek az $1a = a$ és $a^{-1}a = 1$ összefüggések).*

Bizonyítás. Tegyük fel, hogy G-re teljesül (I). Ha $ac = b$, akkor $c = 1c = (a^{-1}a)c = a^{-1}(ac) = a^{-1}b$ miatt az $ax = b$ egyenletnek *csak* $a^{-1}b$ lehet a megoldása; és ez $a(a^{-1}b) = (aa^{-1})b = 1b = b$ alapján valóban megoldás. Hasonlóan látható be, hogy az $ya = b$ egyetlen megoldása ba^{-1}. Így (I) esetén valóban teljesül (II).

Ha (II) igaz, akkor (III) nyilvánvalóan igaz, mert ez (II)-nél annyiban gyengébb, hogy a megoldások egyértelműsége nincs kikötve.

Tegyük most fel, hogy (III) igaz, és legyen 1 az $ya = a$ egy megoldása. A feltétel szerint tetszőleges b-hez létezik olyan c, amelyre $ac = b$. Ebből viszont $1b = 1(ac) = (1a)c = ac = b$ következik, vagyis 1 bal oldali egységelem. Az $ya = 1$ megoldhatósága biztosítja a bal oldali inverzelem létezését. Így (III)-ból valóban következik (IV).

Végezetül tegyük fel, hogy (IV) teljesül. A feltétel szerint létezik bal oldali egységelem, legyen ez (illetve ezek egyike) 1. Tetszőleges, G-beli a elemnek legyen b (egy) balinverze és ennek a kiválasztott b-nek legyen c (egy) balinverze. Eszerint tehát $cb = ba = 1$. Ekkor

$$ab = 1(ab) = (cb)(ab) = c((ba)b) = c(1b) = cb = 1,$$

vagyis b az a-nak (1-re vonatkozó) jobbinverze is. Ebből

$$a1 = a(ba) = (ab)a = 1a = a$$

alapján következik, hogy 1 kétoldali egységelem, és így (I) is fennáll. ■

5.3. Következmény. *Ha egy félcsoportra az 5.2. tétel (valamelyik) feltétele teljesül, akkor a félcsoport egyetlen idempotens eleme az egységelem.*

Bizonyítás. Többet bizonyítunk, mégpedig azt, hogy egyetlen elemnek sem lehet „saját” bal vagy jobb oldali egységeleme. Tegyük fel ugyanis, hogy $ea = a$. Ekkor $1a = a$ miatt a (II) feltétel alapján $e = 1$ következik. (Jobb oldali egységelemre hasonló a bizonyítás.) Ha e idempotens, azaz $ee = e$, akkor a most bizonyított eredményt $a = e$-re alkalmazva, $e = 1$ következik. ■

A továbbiakhoz egy fogalomra van szükségünk.

5.4. Definíció. Ha az S félcsoport tetszőleges a, b és c elemeire az $ab = ac$ (illetve a $ba = ca$) feltételből $b = c$ következik, akkor azt mondjuk, hogy S-ben érvényes a bal oldali (jobb oldali) egyszerűsítési szabály. S-ben érvényes az egyszerűsítési szabály, ha S-ben mind a bal oldali, mind a jobb oldali egyszerűsítési szabály érvényes. □

5.5. Következmény. *Ha egy S félcsoportra teljesülnek az 5.2. tétel feltételei, akkor S-ben érvényes az egyszerűsítési szabály.*

Bizonyítás. Az állítás azonnal adódik a (II)-ben megkövetelt egyértelműségből. ■

5.6. Tétel. *Tegyük fel, hogy az S_1 és S_2 félcsoportokra teljesülnek az 5.2. tétel feltételei. Ekkor bármely $\varphi : S_1 \to S_2$ félcsoport-homomorfizmus az S_1 egységelemét az S_2 egységelemébe viszi; és ha $a \in S_1$, akkor a inverzének a képe az a képének az inverze lesz.*

Bizonyítás. S_1 egységeleme idempotens, tehát φ szorzattartása miatt a képe is idempotens. Az 5.3. következmény alapján tehát e kép az S_2 egységeleme. Ugyancsak a szorzattartást felhasználva kapjuk, hogy $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(1)$. Mivel $\varphi(1)$ az S_2 egységeleme, ezért $\varphi(a^{-1})$ a $\varphi(a)$-nak az egyik inverze. Mivel az inverz egyértelmű, ezért az inverz képe valóban a kép inverze. ■

Az 5.6. tétel biztosítja, hogy ha csak olyan félcsoportokat tekintünk, amelyekre az 5.2. tétel feltételei teljesülnek, akkor ezek körében az egységelemet is és az inverzelemet is úgy tekinthetjük, mintha műveletekkel választottuk volna ki őket.

Éppen ezért *csoportnak fogunk nevezni minden olyan félcsoportot is, amelyben létezik egységelem és minden elemnek létezik inverze.*

Az 5.2. tétel és az 5.5. következmény ebben a megfogalmazásban a következőképpen írhatók át:

5.7. Tétel. *Egy G félcsoport akkor és csak akkor csoport, ha az $ax = b$ és az $ya = b$ egyenletek (egyértelműen) megoldhatók, illetve akkor és csak akkor, ha létezik bal oldali egységelem és erre vonatkozóan minden elemnek létezik bal oldali inverze. Minden csoportban érvényes az egyszerűsítési szabály.* ■

Az 5.7. tétel azonnal két problémát vet fel. Az első kérdés az, hogy a feltételben szükséges-e az, hogy *bal oldali* egységelemet és *bal oldali* inverzelemet követeljünk meg. Nyilvánvaló az, hogy ha mind a két esetben *jobb oldali*-t mondunk, akkor ugyanígy látható be, hogy csoportot kapunk. Kérdés azonban, hogy a bal oldali egységelem és a jobb oldali inverzelem léte nem biztosítja-e azt, hogy a vizsgált félcsoport csoport. Könnyen látható, hogy ez nem így van. Bármely jobbzérus félcsoportban minden elem bal oldali egységelem és ezek bármelyikét szemeljük is ki, minden elemnek van jobb oldali inverzeleme – nevezetesen a kiszemelt bal oldali egységelem. Márpedig, ha a jobbzérus félcsoportnak legalább két eleme van, akkor ez nem lehet csoport a 4.13. tétel miatt.

A másik felmerülő kérdés az, hogy ha egy félcsoportban teljesül az egyszerűsítési szabály, akkor nem következik-e ebből az, hogy a szóban forgó félcsoport csoport. Azonnal látható, hogy ez nincs így. Tekintsük ugyanis a természetes számokat, az összeadással mint félcsoportművelettel ellátva. E félcsoportban nyilvánvalóan érvényes az egyszerűsítési szabály, és mégsem csoport. Egy nagyon fontos speciális esetben azonban mégis igaz az állítás:

5.8. Tétel. *Ha egy véges félcsoportban érvényes az egyszerűsítési szabály, akkor az csoport.*

Bizonyítás. Legyen $c_1, \ldots, c_n$ a félcsoport összes eleme, és tekintsük a félcsoport tetszőleges a elemét. Az $ac_1, \ldots, ac_n$ elemek természetesen ugyancsak elemei a félcsoportnak. Ha valamely szóba jövő i és j természetes számokra $ac_i = ac_j$, akkor az egyszerűsítési szabály következtében $c_i = c_j$ is teljesül. Eszerint a fent kapott kétényezős szorzatok a félcsoport különböző elemei. A végesség miatt ezek tehát a félcsoport összes elemei, s így a félcsoport bármely b eleméhez létezik olyan c elem, amelyre $ac = b$. A jobb

oldali egyszerűsítési szabályt is figyelembe véve kapjuk, hogy a félcsoport kielégíti az 5.2. tétel (III) feltételét – és így csoport. ■

A természetes számok additív csoportja igaz, hogy nem csoport, de azért elégíti ki az egyszerűsítési szabályt, mert egy csoportnak (az egészek additív csoportjának) a részfélcsoportja. Ez a tulajdonság általában is igaz:

5.9. Tétel. *Bármely csoport bármely részfélcsoportjában érvényes az egyszerűsítési szabály.*

Bizonyítás. Tegyük fel, hogy a vizsgált részfélcsoport a, b és c elemeire $ab = ac$. Ez az összefüggés természetesen a szóban forgó csoportban is igaz, s így az 5.5. következmény szerint $b = c$. A jobb oldali egyszerűsítési szabály hasonlóan bizonyítható. ■

Azt, hogy az 5.9. tétel sem fordítható meg (tehát van olyan félcsoport, amelynek minden részfélcsoportjában érvényes az egyszerűsítési szabály, mégsem csoport), Malcev bizonyította be az alábbi példával:

Tekintsük az $\{a, b, c, d, x, y, u, v\}$ generálta F szabad félcsoportot. Legyen Θ az a legszűkebb kongrueniareláció, amelynél $(ax, by), (au, bv), (cx, dy) \in \Theta$. Ha az $S = F/\Theta$ elemeit is a generátorhalmazból képezett szavakkal írjuk fel, akkor S-ben teljesülnek az $ax = by$, $au = bv$ és $cx = dy$ összefüggések. Belátható, hogy ezeknek az összefüggéseknek és a félcsoport-tulajdonságnak a felhasználásával nem kaphatjuk meg a $cu = dv$ összefüggést, azaz $cu \neq dv$. Az is kimutatható, hogy S-ben érvényes az egyszerűsítési szabály. Ezzel szemben S nem lehet egy csoport részfélcsoportja. Ekkor ugyanis a felírt egyenlőségekből

$$d^{-1}c = yx^{-1} = b^{-1}a = vu^{-1}, \qquad \text{azaz} \qquad cu = dv$$

következne, ami nem teljesül.

5.2. Komplexusok, műveletek komplexusokkal

Csoportok esetében igen sok tulajdonságot a csoport (tartóhalmaza) részhalmazainak segítségével lehet megfogalmazni. Ilyen esetekben a nemüres részhalmazokat *komplexusoknak* szokták nevezni. Mi is követjük ezt az elnevezést, és az alábbiakban a komplexusokra vonatkozó néhány tulajdonságot mutatunk be.

5.10. Definíció. Komplexusok körében a tartalmazást, az egyesítést és a metszetet (ha nem üres) úgy értelmezzük, mint a halmazok körében. Ha a csoportművelet szorzás, akkor diszjunkt komplexusok egyesítését összeadással jelöljük (+). Ha K és L két komplexus, akkor legyen ezek komplexusszorzata $KL = \{k\ell \mid k \in K, l \in L\}$, és az inverz $K^{-1} = \{k^{-1} \mid k \in K\}$. Jelölje továbbá aK az $\{a\}K$ komplexusszorzatot. □

5.11. Tétel. *Egy G csoport komplexusai a szorzásra nézve félcsoportot alkotnak, amelyek egységeleme az $\{1\}$ komplexus, zéruseleme G. Ha K, L, M a G csoport tetszőleges komplexusai, akkor*

(I) $(K \cup L)M = KM \cup LM$ *és* $M(K \cup L) = MK \cup ML$;

(II) $(K \cap L)M \subseteq KM \cap LM$ *és* $M(K \cap L) \subseteq MK \cap ML$;

(III) *ha* $K \subseteq L$, *akkor* $KM \subseteq LM$ *és* $MK \subseteq ML$;

(IV) $(K^{-1})^{-1} = K$ *és* $(KL)^{-1} = L^{-1}K^{-1}$;

(V) $(K \cup L)^{-1} = K^{-1} \cup L^{-1}$ *és* $(K \cap L)^{-1} = K^{-1} \cap L^{-1}$;

(VI) *ha* $K \subseteq L$, *akkor* $K^{-1} \subseteq L^{-1}$.

Ha K és L végesek, akkor

(VII) $\max(|K|, |L|) \leq |KL| \leq |K| \cdot |L|$, *továbbá*

(VIII) $|Ka| = |aK| = |K|$, *tetszőleges $a \in G$ esetén.*

($|X|$ az X halmaz számosságát jelöli.)

Bizonyítás. A szorzás asszociativitásából következik, hogy a komplexusok szorzása is asszociatív. $\{1\}$ és G nyilvánvalóan rendelkezik az egységelem, illetve a zéruselem tulajdonságaival. $(a^{-1})^{-1} = a$ és $(ab)^{-1} = b^{-1}a^{-1}$ bizonyítják a (IV) alatti tulajdonságokat. Az (V) és a (VI) alatti tulajdonságok nyilvánvalóak. Ezek következtében az (I), (II) és (III) alatti tulajdonságokra elegendő mindig az elsőnek a bizonyítása. (Például, ha a (III) alatti első állítás igaz, és $K \subseteq L$, akkor (VI) miatt $K^{-1} \subseteq L^{-1}$, (III) miatt $K^{-1}M^{-1} \subseteq L^{-1}M^{-1}$, amiből (IV) és (VI) alapján $MK = (K^{-1}M^{-1})^{-1} \subseteq (L^{-1}M^{-1})^{-1} = ML$ következik.) A (III) alatti első állítás nyilvánvalóan teljesül, amiből a metszet és az egyesítés definíciója szerint azonnal következik a (II) alatti első állítás, valamint a $(K \cup L)M \supseteq KM \cup LM$ összefüggés. Másrészt a $(K \cup L)M$ bármely eleme am alakú, ahol $a \in K \cup L$, azaz am vagy KM-nek, vagy LM-nek eleme, ami bizonyítja az (I) alatti első állítást is. (A (II) alatti állításokban nem írható fel egyenlőség, amit például úgy láthatunk be, hogy M-et G-nek, továbbá K-t és L-t diszjunktaknak választjuk.)

A (VII) alatti második egyenlőtlenség nyilvánvaló, amiből azonnal kapjuk, hogy $|aK| \leq |K|$ és $|Ka| \leq |K|$. Ebből viszont

$$|K| = |a^{-1}aK| \leq |aK| \qquad \text{és} \qquad |K| = |Kaa^{-1}| \leq |Ka|$$

következik; ami az előzővel együtt bizonyítja a (VIII) alatti összefüggéseket. Eszerint KL tartalmaz mind K-val, mind L-lel megegyező elemszámú halmazt, és így teljesül a (VII) alatti első egyenlőtlenség is. ■

A továbbiakban a csoportok részstruktúráit, a részcsoportokat fogjuk vizsgálni. Ezek számos tulajdonsága egyszerűen megfogalmazható a komplexusok segítségével.

5.3. Részcsoportok

A 2.5. definíciót, illetve a 2.6. tételt speciálisan csoportokra alkalmazva a részcsoport definíciójához jutunk. A részcsoportok esetében is, éppen úgy, mint a csoportoknál tettük, a részcsoport tartóhalmazát és a részcsoportot nem jelöljük különbözőképpen. Használjuk viszont a szokásos $\leq$ jelölést.

5.12. Definíció. A G csoport egy H komplexusa részcsoport ($H \leq G$), ha a következők teljesülnek:

(1) $1 \in H$;

(2) ha $a, b \in H$, akkor $ab \in H$;

(3) ha $a \in H$, akkor $a^{-1} \in H$. □

Mivel a csoport bármely komplexusáról feltettük, hogy nem üres, ezért könnyen belátható: *Az 5.12. definícióban az első feltételt elhagyhatjuk.*

5.13. Tétel. *Egy G csoport valamely H komplexusára az alábbi feltételek ekvivalensek:*

(I) *H a G-nek részcsoportja.*

(II) $HH \subseteq H$ *és* $H^{-1} \subseteq H$. (II′) $HH = H$ *és* $H^{-1} = H$.

(III) $H^{-1}H \subseteq H$. (III′) $H^{-1}H = H$.

Bizonyítás. Az 5.12. definíció (2) és (3) pontja biztosítja, hogy az (I) feltételből következik a (II) feltétel. Ha (II) igaz, akkor az 5.11. tétel felhasználásával kapjuk, hogy $H^{-1}H \subseteq HH \subseteq H$, vagyis teljesül (III). Tegyük most fel, hogy (III) igaz. Mivel H nem üres, ezért létezik egy $a \in H$, így $1 = a^{-1}a \in H^{-1}H \subseteq H$ következik. Ha most tekintjük a H egy tetszőleges a elemét, akkor $1 \in H$ következtében $a^{-1} = a^{-1}1 \in H^{-1}H \subseteq H$. Legyenek végül a és b tetszőleges elemei H-nak. Ekkor, mint már láttuk, $a^{-1} \in H$, amiből azt kapjuk, hogy $ab = (a^{-1})^{-1}b \in H^{-1}H \subseteq H$. Így H-ra teljesül az 5.10. definíció mindhárom feltétele; tehát H-ra igaz (I). A (II′), illetve a (III′) feltételből nyilvánvalóan következik a (II), illetve a (III) feltétel; így csupán csak azt kell még belátni, hogy bármely H részcsoportra teljesül mind (II′), mind (III′). A $H^{-1} \subseteq H$ feltételből azonnal kapjuk, hogy $H = (H^{-1})^{-1} \subseteq (H)^{-1}$; ami biztosítja, hogy $H^{-1} = H$. Ezt felhasználva, a (III′) feltétel is $HH = H$ alakba írható át. A (II) feltétel szerint $HH \subseteq H$, és $1 \in H$ miatt $H = 1H \subseteq HH$; ami biztosítja a kívánt feltétel teljesülését. ■

A következőkben megadjuk, hogy miképpen állítható elő egy csoport valamely K komplexusa által generált részcsoport.

5.14. Tétel. *A G csoport egy K komplexusa által generált részcsoport:*

$$\langle K \rangle = \left\{ \bigcup (\{1\} \cup K \cup K^{-1})^n \mid n = 1, 2, \ldots \right\};$$

azaz a generátum elemei az egységelemen kívül azok a szorzatok, amelyeknek minden tényezője vagy K-beli, vagy egy K-beli elem inverze.

Bizonyítás. Mivel bármely részcsoport tartalmazza az egységelemet, továbbá minden elemével együtt annak inverzét is, ezért $\{1\} \cup K \cup K^{-1} \subseteq \langle K \rangle$. Tekintettel arra, hogy egy részcsoport a szorzásra is zárt, ezért a bal oldal minden hatványa (a komplexusok szorzásra vonatkozó félcsoportjában) része $\langle K \rangle$-nak. Azt kell tehát még bizonyítani, hogy a tételbeli formula jobb oldalán álló halmaz részcsoport. A csoport egységeleme e halmazban nyilván benne van. A komplexusok félcsoportjára vonatkozó $L^n L^k = L^{n+k}$ összefüggés alapján a szorzásra való zártság is teljesül. Végül az 5.11. tétel (IV)-ben szereplő második összefüggés és $(\{1\} \cup K \cup K^{-1})^{-1} = \{1\} \cup K \cup K^{-1}$ biztosítják, hogy $\langle K \rangle$-ban minden elemmel együtt annak inverze is fellép. ■

Igen fontos speciális esetet mond ki az

5.15. Következmény. *Ha az A_i komplexusok a G csoportnak részcsoportjai, akkor az egyesítésük által generált részcsoport:*

$$\left\{ \left(\bigcup A_i \right)^n \mid n = 1, 2, \ldots \right\}.$$

Bizonyítás. $1 \in \bigcup A_i$ és $\left(\bigcup A_i\right)^{-1} = \bigcup (A_i)^{-1} = \bigcup A_i$ alapján az állítás az 5.14. tétel közvetlen folyománya. ■

Felhívjuk a figyelmet arra, hogy az n kitevő nem hagyható el. Egy-egy részcsoporton belül ugyan nincs szükség a többtényezős szorzatra, hiszen minden részcsoport zárt a szorzásra; a különböző csoportokból vett elemek szorzatának a hosszát azonban – általában – nem lehet korlátozni.

Az általános definíciónak megfelelően *ciklikusnak nevezünk egy (rész-)csoportot, ha egyetlen elemmel generálható.*

5.16. Következmény. *Az a elem generálta részcsoport elemei az a^n alakú elemek (n tetszőleges egész szám).*

Ciklikus csoport bármely részcsoportja is ciklikus.

Bizonyítás. Az 5.14. tételből azonnal adódik az első állítás. Legyen $H \leq \langle a \rangle$ és tekintsük az egész számoknak az $A = \{m \mid a^m \in H\}$ halmazát. H-nak a szorzásra és az inverzképzésre való zártsága következtében A zárt az összeadásra és a kivonásra. Az egész számokra vonatkozó maradékos osztás tulajdonságai alapján A elemei egyetlen $k \geq 0$ szám többszöröseiből állnak, így $H = \langle a^k \rangle$. (A részletes bizonyítás hasonló az 5.25. tétel bizonyításához.) ■

Mivel egy csoport minden egyes részcsoportja tartalmazza a csoport egységelemét, ezért egy csoport tetszőleges részcsoportjainak a metszete soha nem lehet üres. Ebből azonnal következik:

5.17. Tétel. *Egy csoport részcsoportjai bármely rendszerének a közös része részcsoport.* ■

Minden csoportnak van két részcsoportja; nevezetesen az egyedül az egységelemből álló csoport, valamint az egész csoport. Ezeket *triviális részcsoportoknak* nevezzük. Ha a csoportnak legalább két eleme van, akkor a két triviális részcsoportja különböző. Az egyelemű csoportot *triviális csoportnak* nevezzük. A csoportnak önmagától különböző részcsoportjait *valódi részcsoportoknak* nevezzük.

5.4. Mellékosztályok; elem és csoport rendje

Az 5.13. tétel (III) feltétele szerint, ha a és b elemei a G csoport egy H részcsoportjának, akkor $a^{-1}b$ is H-ban van. Fordítva ez nem igaz, $a^{-1}b$ máskor is eleme lehet H-nak. De az a kapcsolat, amelyet $a^{-1}b \in H$ fejez ki, igen alapvető.

5.18. Tétel. *Legyen $H \subseteq G$ rögzített, de tetszőleges részcsoport. Definiáljuk a G elemeire a $\lambda = \lambda(H)$ relációt az*

$$(a, b) \in \lambda \quad \text{akkor és csak akkor, ha} \quad a^{-1}b \in H$$

összefüggéssel. Ez a reláció minden H esetén ekvivalenciareláció.

Bizonyítás. $a^{-1}a = 1 \in H$ miatt a reláció reflexív. Ha $a^{-1}b \in H$, akkor $b^{-1}a = (a^{-1}b)^{-1} \in H^{-1} = H$ alapján a reláció szimmetrikus. Végül $a^{-1}b, b^{-1}c \in H$ esetén $a^{-1}c = (a^{-1}b)(b^{-1}c) \in HH = H$ teljesül; ami a tranzitivitást bizonyítja. ■

Könnyen belátható, hogy a G csoport tetszőleges H részhalmaza esetén a fenti λ reláció csak akkor ekvivalenciareláció, ha $H \leq G$.

5.19. Tétel. *Legyen $H \leq G$. A $\lambda(H)$ ekvivalenciarelációnak megfelelő osztályozás elemei az aH alakú komplexusok ($a \in G$); amelyeket H szerinti bal oldali mellékosztályoknak nevezünk.*

Bizonyítás. $(a, x) \in \lambda(H)$ azt jelenti, hogy $a^{-1}x \in H$, ami az $x \in aH$ feltétellel ekvivalens. ■

Az előző két tételhez hasonlóan látható be az alábbi is:

5.20. Tétel. *Legyen $H \leq G$, és legyen $(a, b) \in \mu(H)$ pontosan akkor, ha $ab^{-1} \in H$. Ez a $\mu(H)$ bármely H részcsoportra ekvivalenciareláció; és a hozzá tartozó osztályozásnál az osztályok a Ha alakú, úgynevezett jobb oldali mellékosztályok.* ■

A mellékosztályok természetesebb bevezetése szerint ezek az aH, illetve Ha alakú halmazok. A számolások közben viszont hasznos az itt szereplő forma.

Adott $H \leq G$ esetén a bal oldali és jobb oldali mellékosztályok általában különböznek. Valami kapcsolat azonban mégis van közöttük:

5.21. Tétel. *Legyen $H \leq G$. Ekkor bijekció létesíthető a H bal oldali és jobb oldali mellékosztályai között. Speciálisan, ha egyikükből véges sok van, akkor a másikból is pontosan ugyanannyi van. Ezt a számot (a H bal oldali, ill. jobb oldali mellékosztályainak számát) a H részcsoport G-beli indexének nevezzük, és $[G : H]$-val jelöljük. (A $(G : H)$ jelölés is használatos.)*

Bizonyítás. A $\varphi(a) = a^{-1}$ leképezés $\varphi(\varphi(a)) = a$ következtében bijektív – még a G csoport komplexusainak a halmazán is. A $\varphi(G) = G$ és a $\varphi(H) = H$ összefüggések felhasználásával az 5.11. tétel alapján kapjuk, hogy a kívánt bijekció aH-nak Ha^{-1}-et felelteti meg. A bijekció létezése biztosítja a véges esetre vonatkozó állítást is. ■

5.22. Definíció. Egy G csoport $|G|$ rendjén tartóhalmaza elemszámát értjük. □

Megjegyezzük, hogy végtelen csoportoknál mi általában nem adjuk meg a fenti számosságot, csupán azt mondjuk, hogy G *végtelen csoport*. Amennyiben nem ez a helyzet, akkor a csoportot *végesnek* nevezzük. Végtelen csoportok bizonyos vizsgálatánál meg szokták adni a számosságot. Így beszélhetünk *megszámlálható csoportról* vagy *kontinuum számosságú csoportról* stb.

5.23. Tétel (LAGRANGE). *Ha H a véges G csoport részcsoportja, akkor $|G| = |H| \cdot [G : H]$. Speciálisan: H rendje osztója a G rendjének.*

Bizonyítás. Az 5.11. tétel szerint a H szerinti mellékosztályok mindegyikének az elemszáma $|H|$. Mivel e mellékosztályok diszjunktak, ezért egyesítési halmazuk elemszáma

$|H| \cdot [G : H]$. Tekintettel arra, hogy G minden eleme benne van valamelyik mellékosztályban, ezért ez a szám megegyezik $|G|$-vel. A tétel második állítása azonnal következik abból, hogy $[G : H]$ egész. ■

5.24. Definíció. Legyen a a G csoport tetszőleges eleme. Ha van olyan d pozitív egész szám, amelyre $a^d = 1$, akkor a legkisebb ilyen számot az a rendjének nevezzük. Ha ilyen szám nincs, akkor azt mondjuk, hogy az a elem végtelen rendű. Az a elem rendjét $o(a)$ jelöli. □

5.25. Tétel. *Legyen a a G csoport tetszőleges eleme, és tegyük fel, hogy az n és k olyan egész számok, amelyekre $a^n = a^k$ teljesül. Végtelen rendű elem esetén ez pontosan akkor áll fenn, ha $n = k$; míg véges rendű elemre pontosan akkor, ha $n - k$ osztható az a elem rendjével.*

Bizonyítás. Nem megy az általánosság rovására, ha feltesszük, hogy $n \geq k$. Az elem hatványaira vonatkozó összefüggések alapján $a^n = a^k$ pontosan akkor teljesül, ha $a^{n-k} = 1$. Végtelen rendű elem esetén ez pontosan akkor áll fenn, ha $n-k = 0$, azaz, ha $n = k$. Legyen most az a elem véges rendű, és rendje legyen d. A maradékos osztás szerint léteznek olyan q és r egész számok, hogy $n - qk = qd + r$, ahol r nemnegatív és d-nél kisebb. Ebből:

$$1 = a^{n-k} = a^{qd+r} = (a^d)^q \cdot a^r = 1^q \cdot a^r = a^r$$

következik. Mivel $r < d$, és d a legkisebb olyan pozitív egész, amelyre $a^d = 1$ igaz, ezért r nem lehet pozitív, vagyis $r = 0$. Így d valóban osztja $(n - k)$-t. Fordítva, ha $n - k = dq$ (q egész szám), akkor $a^{n-k} = (a^d)^q = 1$. ■

5.26. Tétel. *Egy csoport bármely elemének a rendje megegyezik az általa generált (ciklikus) részcsoport rendjével.*

Bizonyítás. Végtelen rendű elemre az állítás nyilvánvaló. Legyen a G-beli a elem rendje d. Ekkor az $1, a, \ldots, a^{d-1}$ elemek mind hozzátartoznak az a generálta $\langle a \rangle$ részcsoporthoz, és a 5.25. tétel szerint mind különbözőek. Ugyancsak a 5.25. tételből következik, hogy bármely n egész számhoz létezik a d-nél kisebb olyan nemnegatív r egész szám, amelyre $a^n = a^r$. Így $\langle a \rangle = \{1, a, \ldots, a^{d-1}\}$. ■

5.27. Következmény. *Ha a eleme az n-edrendű G csoportnak, akkor $a^n = 1$.*

Bizonyítás. Legyen $o(a) = d$. Ekkor az 5.26. tétel szerint $|\langle a \rangle| = d$, és Lagrange tétele alapján d osztója n-nek. Ebből viszont a 5.25. tétel szerint következik az állítás. ■

Ez a tétel az úgynevezett Euler-féle kongruenciatétel általánosítása. Tekintsük ugyanis a modulo m vett redukált maradékosztályok multiplikatív félcsoportját. Ezek száma – mint ismeretes – $\varphi(m)$ (ahol φ az Euler-függvény). Mivel minden redukált maradékosztály – definíció szerint – relatív prím a modulushoz, ezért e félcsoportban érvényes az egyszerűsítési szabály; az 5.6. tétel szerint tehát csoport. Így az 5.27. tételből éppen az $a^{\varphi(m)} \equiv 1(m)$ Euler-féle kongruenciatétel következik.

5.28. Definíció. Egy G csoport valamely R részhalmazát a H részcsoport szerinti bal oldali (jobb oldali) reprezentánsrendszernek nevezzük, ha minden, H szerinti bal oldali (jobb oldali) mellékosztályból pontosan egy elemet tartalmaz. Ha R mind bal, mind jobb oldali reprezentánsrendszer, akkor kétoldali reprezentánsrendszernek hívjuk. □

Majd látni fogjuk, hogy egy tetszőleges bal oldali reprezentánsrendszer általában nem jobb oldali.

5.29. Tétel. *Tetszőleges véges G csoport bármely H részcsoportjához létezik kétoldali reprezentánsrendszer.*

Bizonyítás. Az állítást D. W. HALL egy gráfelméleti tételére vezetjük vissza. Egy V alaphalmazú $\varrho \in V \times V$ (irányítatlan) gráfot *párosnak* nevezünk, ha alaphalmazát két diszjunkt, A és B részre bonthatjuk úgy, hogy két csúcspont *csak* akkor van összekötve, ha nem esnek ugyanabba a részbe (persze ez nem jelenti azt, hogy valóban össze is vannak kötve). A páros gráfot az (A, B, ϱ) szimbólummal jelöljük. Az A tetszőleges C részhalmazához hozzárendeljük a

$$C^+ = \{b \in B \mid \exists c \in C, (c, b) \in \varrho\}$$

részhalmazt. (C^+ tehát éppen azoknak a pontoknak a halmaza, amelyek legalább egy C-beli ponttal össze vannak kötve.) Azt mondjuk, hogy egy véges páros gráf kielégíti a Hall-feltételt, ha A minden C részhalmazára $|C^+| \geq |C|$ teljesül. Hall tétele szerint, ha az (A, B, ϱ) véges páros gráf kielégíti a Hall-feltételt, akkor létezik olyan $\varphi : A \to B$ injekció, amelyre tetszőleges $a \in A$ esetén $(a, \varphi(a)) \in \varrho$ teljesül. [A bizonyítás A elemszámára vonatkozó teljes indukcióval történik. E bizonyítás gondolatmenete a következő: Ha az A minden C valódi részhalmazára $|C^+| > |C|$ teljesül, akkor bármely $(a, b) \in \varrho$ párral elkezdhetjük az injekciót; a fennmaradó $(A \setminus \{a\}, B \setminus \{b\}, \varrho')$ gráfra alkalmazható az indukciós feltétel, ahol ϱ' a ϱ-ból az összes $\{(a, b') \mid b' \in B\}$ és az összes $\{(a', b) \mid a' \in A\}$ alakú élek elhagyásával adódik. Ha viszont van az A-nak olyan C valódi része, amelyre $D = C^+$ esetén $|D| = |C|$, akkor a feltétel külön-külön alkalmazható a $(C, D, \varrho \cap (C \times D))$ és az $(A \setminus C, B \setminus D, \varrho \cap ((A \setminus C) \times (B \setminus D)))$ gráfokra. Ez utóbbi gráf esetében a feltétel teljesülése úgy bizonyítható, hogy a C-t tartalmazó A-beli részhalmazokat vesszük figyelembe.]

Legyenek most az A halmaz elemei a H szerinti bal oldali mellékosztályok, a B halmazéi pedig a H szerinti jobb oldali mellékosztályok. Egy bal oldali és egy jobb oldali mellékosztály pontosan akkor legyen éllel összekötve, ha van közös elemük. Tekintsünk bármely k darab bal oldali mellékosztályt. Ezek elemeinek a száma összesen $k \cdot |H|$, mivel diszjunktak és elemszámuk megegyezik $|H|$-val. Mivel k-nál kevesebb jobb oldali mellékosztálynak – az előzőhöz hasonlóan – $k \cdot |H|$-nál kevesebb eleme van, ezért legalább k darab olyan jobb oldali mellékosztály van, amely a fenti elemek valamelyikét tartalmazza, azaz a megadott k bal oldali mellékosztály közül valamelyikkel van közös eleme. Így a megadott páros gráf kielégíti a Hall-féle feltételt. Létezik tehát olyan injekció, hogy minden bal oldali mellékosztálynak van közös eleme a neki megfeleltetett jobb oldali mellékosztállyal. Ez az injekció az 5.21. tétel következtében csak bijekció lehet. Vegyünk ki minden bal oldali mellékosztályból egy-egy olyan elemet, amely a neki megfeleltetett jobb oldali mellékosztályban is benne van. Az így kapott elemek mindegyike más és más bal oldali mellékosztályban és ugyancsak más és más jobb oldali mellékosztályban van, amiből következik, hogy ez a halmaz kétoldali reprezentánsrendszer. ■

5.5. Invariáns részcsoportok

Tetszőleges kommutatív csoport esetében teljesül, hogy bármilyen részcsoportja bal oldali mellékosztályai pontosan ugyanazok, mint a jobb oldali mellékosztályai. Ez a tulajdonság általában is igen fontos.

5.30. Definíció. A G csoport egy N részcsoportját invariáns vagy normális részcsoportnak, vagy normálosztónak nevezzük, ha minden N szerinti bal oldali mellékosztály jobb oldali is és viszont. Ezt a kapcsolatot $N \lhd G$ ($G \rhd N$) jelöli. □

Minden csoportnak normálosztója önmaga és az egységelemből álló részcsoport. Ezek *triviális normálosztók*. Minden más normálosztót *nemtriviálisnak vagy valódinak* nevezünk.

Az invariáns részcsoportokat nagyon sokféle módon szokták definiálni. Ezért megadunk néhány további definíciót, és megmutatjuk, hogy az eredetivel ekvivalensek. A leggyakrabban használtak és talán a legfontosabbak az tételbeli (1.1), (2.1) és (3.1) feltételek.

5.31. Tétel. *A G csoport egy N részcsoportja akkor és csak akkor invariáns, ha az alábbi ekvivalens feltételek bármelyike teljesül rá: Az N szerinti*

(1.1) *minden bal oldali mellékosztály jobb oldali is;*

(1.2) *minden bal oldali mellékosztály egy N szerinti jobb oldaliban van;*

(1.3) *minden jobb oldali mellékosztály bal oldali is;*

(1.4) *minden jobb oldali mellékosztály egy N szerinti bal oldaliban van.*

A G csoport bármely a elemére:

(2.1) $aN = Na$; (2.2) $aN \subseteq Na$;

(2.3) $Na = aN$; (2.4) $Na \subseteq aN$.

(3.1) $N = a^{-1}Na$; (3.2) $N \subseteq a^{-1}Na$;

(3.3) $N = aNa^{-1}$; (3.4) $N \subseteq aNa^{-1}$

teljesül.

Bizonyítás. Mindenekelőtt az első négy feltételt is átírjuk. Ezek szerint a csoport minden a eleméhez létezik olyan G-beli c elem, amire

(1.1) $aN = Nc$; (1.2) $aN \subseteq Nc$;

(1.3) $Na = cN$; (1.4) $Na \subseteq cN$

teljesül. Mivel két, ugyanazon oldali mellékosztálynak csak úgy lehet közös eleme, ha megegyeznek, ezért az (1.i) feltételből következik a (2.i) feltétel ($i = 1, 2, 3, 4$). Fordítva ez triviálisan igaz, mert a $b = a$ választás megfelelő. A (2.i) és (3.i) feltételek ekvivalenciája azonnal következik a komplexusszorzás elemi tulajdonságaiból. Az a elem helyébe a^{-1}-et téve, azonnal adódik a (3.1) és (3.3), illetve a (3.2) és (3.4) feltételek ekvivalenciája. Mivel (3.1)-ből azonnal következik a (3.2), ezért a fenti feltételek ekvivalenciájához már csak azt kell kimutatni, hogy (3.2)-ből is következik (3.1). Mivel (3.2)-ből következik a (3.4) összefüggés, ezért következik az $a^{-1}Na \subseteq a^{-1}(aNa^{-1}) = N$ összefüggés is, ami az eredeti (3.2)-vel együtt (3.1)-et adja. Ha tehát a felsorolt összefüggések valamelyike fennáll, akkor mindegyik teljesül.

Mármost (1.1) és (1.3) együttesen pontosan azt fejezi ki, hogy N invariáns részcsoport. ■

5.32. Tétel. *Egy G csoport valamely részcsoportja akkor és csak akkor invariáns, ha bármely két bal oldali (jobb oldali) mellékosztály komplexusszorzata is bal oldali (jobb oldali) mellékosztály; illetve, ha benne van egy bal oldali (jobb oldali) mellékosztályban.*

Bizonyítás. Az invariáns részcsoport definíciójának szimmetriája alapján elegendő a bal oldali mellékosztályokra vonatkozó állítást bizonyítani. Mivel az első tulajdonságból nyilvánvalóan következik a második, ezért elég azt kimutatni, hogy ha két mellékosztály szorzata mindig benne van egy harmadikban, akkor a részcsoport invariáns, míg ez utóbbi esetben bármely két mellékosztály szorzata is mellékosztály. Tegyük fel, hogy az N részcsoportra bármely G-beli a és b elem esetén létezik olyan $c \in G$, amelyre $aNbN \subseteq cN$. Mivel az ab szorzat eleme a bal oldalnak, ezért az 5.19. tétel alapján $cN = abN$ adódik. Ebből

$$NbN = a^{-1}(aNbN) \subseteq a^{-1}(abN) = bN,$$

továbbá

$$Nb = Nb1 \subseteq NbN \subseteq bN$$

következik, ami éppen az 5.31. tétel (2.4) feltételét adja. Fordítva, ha N invariáns részcsoport G-ben, akkor a (2.1) feltétel alapján minden G-beli b elemre teljesül a $bN = Nb$ összefüggés. Ebből – az 5.13. tétel (II′) feltételét felhasználva – tetszőleges G-beli a elem esetén

$$aNbN = a(bN)N = ab(NN) = abN$$

következik; és így bármely két bal oldali mellékosztály komplexusszorzata is bal oldali mellékosztály. ■

Jegyezzük meg, hogy a definíció szimmetriája alapján invariáns részcsoportok esetében a mellékosztályoknak a „bal oldali”, illetve „jobb oldali” jelzője elhagyható. Ezért a továbbiakban invariáns részcsoportok esetén általában mellékosztályról fogunk beszélni.

Az alábbiakban néhány, az invariáns részcsoportok jelentőségét megvilágító tételt bizonyítunk be.

5.33. Tétel. *Egy G csoport valamely N invariáns részcsoportja szerinti mellékosztályok a csoport egy kompatibilis osztályozását adják; és G minden kompatibilis osztályozásában az osztályok G egy alkalmas normálosztójának a mellékosztályai.*

Bizonyítás. A szorzásra való kompatibilitáshoz az kell, hogy $aN = bN$ és $cN = dN$ esetén ac és bd ugyanabban a mellékosztályban legyenek. Ez teljesül, hiszen

$$acN = (aN)(cN) = (bN)(dN) = bdN.$$

Az invertálással való kompatibilitás azt jelenti, hogy $aN = bN$ esetén $a^{-1}N = b^{-1}N$ is igaz; ami

$$a^{-1}N = (Na)^{-1} = (aN)^{-1} = (bN)^{-1} = (Nb)^{-1} = b^{-1}N$$

következménye. Az egységelem képzésével mint művelettel való kompatibilitás triviális.

Tekintsük most a G csoportnak egy kompatibilis osztályozását, és legyen N az 1-gyel egy osztályban levő elemek halmaza. Ha $a, b \in N$, akkor a kompatibilitás alapján ab ugyanabba az osztályba esik, mint $1 \cdot 1 = 1$, és a^{-1} ugyanabba, mint $1^{-1} = 1$. Így N részcsoport. Ha $x \in N$ és $a \in G$, akkor $a^{-1}xa$ és $a^{-1}1a = 1$ egy osztályba esnek, azaz

$a^{-1}Na \subseteq N$, vagyis $N \subseteq aNa^{-1}$. Az 5.31. tétel (3.4) pontja szerint tehát N invariáns részcsoport. A kompatibilitás alapján, ha a és b egy osztályban vannak, akkor $a^{-1}b$ egy osztályban van az $a^{-1}a = 1$ elemmel; s ez utóbbi esetben b és $a1 = a$ egy osztályban vannak. Az 5.19. tétel szerint tehát az osztályozás során éppen az N szerinti mellékosztályok lépnek fel. ■

5.34. Tétel. *A G csoport egy N részcsoportja akkor és csak akkor normálosztó, ha bármely K komplexus esetén $KN = NK$. Ha N normálosztó és H tetszőleges részcsoport, akkor az általuk generált $\langle N, H\rangle$ részcsoport megegyezik az NH komplexusszorzattal.*

Normálosztók – mint részcsoportok – generálta részcsoport normálosztó.

Bizonyítás. $KN = \left\{\bigcup aN \mid a \in K\right\}$, illetve $NK = \left\{\bigcup Na \mid a \in K\right\}$ alapján az első állítás nyilvánvaló. Ha N és H tetszőleges részcsoportok, akkor $NH \subseteq \langle N, H\rangle$ (és hasonlóan $HN \subseteq \langle N, H\rangle$) teljesül, mert a generátum mindkét részcsoportot tartalmazza, és szorzásra zárt. Azt mutatjuk ki, hogy ha N normálosztó, akkor a generátum benne van NH-ban (és HN-ben is). Mivel $NH \supseteq N1 = N$ és $NH \supseteq 1H = H$, ezért elég azt bizonyítani, hogy NH részcsoport. $1 = 1 \cdot 1 \in NH$ miatt NH nem üres. A tétel első állítását figyelembe véve az és 5.13. tételt felhasználva:

$$(NH)(NH) = N(HN)H = N(NH)H = (NN)(HH) = NH;$$

$$\text{és} \quad (NH)^{-1} = H^{-1}N^{-1} = HN = NH$$

adódik, vagyis NH részcsoport.

Ha N és M normálosztók, akkor az előző állítás szerint NM az általuk generált részcsoport. Mármost erre tetszőleges $g \in G$ esetén $gNM = NgM = NMg$ adódik; így generátumuk normálosztó. Ebből teljes indukcióval azonnal következik az állítás véges sok normálosztó esetére. Ha $\{N_i \mid i \in I\}$ normálosztók végtelen rendszere, akkor ezek generátumának tetszőleges a eleme az 5.15. következmény szerint benne van egy $\{N_i \mid i \in \in J \subseteq I\}$ rendszer $\widetilde{N}$ generátumában. A véges sok normálosztóra bizonyítottak szerint tetszőleges $g \in G$ mellett $g^{-1}ag \in \widetilde{N}$, ami része az eredeti generátumnak; az 5.31. tétel szerint tehát ez a generátum valóban normálosztó. ■

5.35. Tétel. *2 indexű részcsoport normálosztó.*

Bizonyítás. Legyen $H < G$ és $[G : H] = 2$. Ez azt jelenti, hogy H-n kívül még egyetlen bal oldali és egyetlen jobb oldali mellékosztály van: aH és Hb $(a, b \notin H)$. Mivel aH diszjunkt a H bal oldali mellékosztálytól, ezért diszjunkt a H jobb oldali mellékosztálytól is, tehát benne van a másik jobb oldali mellékosztályban, Hb-ben. Így az 5.31. tétel (1.2) pontja szerint H normálosztó. ■

Feladatok

Tekintettel arra, hogy a csoportszorzás a másik két műveletet már egyértelműen meghatározza, így csak ezt a műveletet adjuk meg.

1. Bizonyítsuk be, hogy a komplex számok csoportot alkotnak az összeadásra nézve. Ennek részcsoportjai például a valós számok, a racionális számok, az egész számok. Ciklikus részcsoportjait úgy kaphatjuk, hogy vesszük egy tetszőleges szám egész számú többszöröseit. Egy ciklikus részcsoportjának általában végtelen sok eleme van; kivéve az egyedül 0-ból álló részcsoportot, amely egyelemű.

2. Bizonyítsuk be, hogy egy tetszőleges vektortér vektorai csoportot alkotnak az összeadásra nézve. Ennek részcsoportjai (például) az alterek. Ha a vektortér elemei négyzetes mátrixok, akkor részcsoportot alkotnak (például) a szimmetrikus vagy az antiszimmetrikus mátrixok.

3. Bizonyítsuk be, hogy a nemnulla komplex számok csoportot alkotnak a szorzásra nézve. Ennek fontosabb részcsoportjai: a nemnulla valós számok, a pozitív valós számok, a nemnulla racionális számok, az 1 abszolút értékű komplex számok, az összes egységgyökök, rögzített p prímszám mellett a p^k-adik egységgyökök (ahol k tetszőleges, nemnegatív egész szám), rögzített n mellett az n-edik egységgyökök. Itt egy ciklikus részcsoport elemei egy rögzített elem egész kitevőjű hatványaiból állnak. Ha a rögzített elem nem egységgyök, akkor a kapott ciklikus csoportnak végtelen sok eleme van. Ha a rögzített elem primitív n-edik egységgyök, akkor a kapott ciklikus csoportnak pontosan n eleme van.

4. Bizonyítsuk be, hogy egy H halmaznak egy $\langle G;\cdot\rangle$ csoportra való leképezései csoportot alkotnak a következő művelettel:

Ha f és g egy-egy leképezés, akkor tetszőleges H-beli a-ra legyen $(f\cdot g):a\to f(a)\cdot g(a)$.

Speciális esetben legyen H a valós számok egy intervalluma és G a valós számok additív csoportja. Ekkor a kapott csoport az adott intervallumon értelmezett valós függvények additív csoportja. Ennek néhány fontos részcsoportja: a (valamilyen értelemben) integrálható függvények, a folytonos függvények, a deriválható függvények, a polinomfüggvények.

Egy másik speciális esetet kapunk, ha H-nak a pozitív egész számok halmazát választjuk (G az előbbi). Ekkor a valós számsorozatok additív csoportját kapjuk. Itt néhány fontos részcsoport: a korlátos sorozatok, a konvergens sorozatok, azok a sorozatok, amelyekben az elemek négyzetösszege konvergens, a stacionárius (valahonnét kezdve csupa azonos elemből álló) sorozatok, a 0-hoz tartó sorozatok.

5. Bizonyítsuk be, hogy egy H halmaz önmagára való bijekciói csoportot alkotnak a függvénykompozícióra.

[Igen fontos speciális esetet kapunk, ha a H halmaznak valamilyen „szerkezete” (struktúrája) van, és a H halmazon vizsgált $\mathcal{S}$ struktúrát megtartó bijekciókat tekintünk. Ilyen esetekben az $\mathcal{S}$ struktúra automorfizmusairól beszélünk. Például a H halmazon értelmezett reláció esetén automorfizmusok azok a bijekciók, amelyek relációban álló elemeket (és csak ilyeneket!) relációban álló elemekbe visznek. Ha a H halmaz egy $\mathcal{S}$ algebrai struktúra tartóhalmaza, akkor automorfizmusok azok a bijekciók, amelyek a szóban forgó $\mathcal{S}$ algebrai struktúrának izomorfizmusai. Ha a H halmaz a geometriai sík vagy tér, akkor attól függően, hogy az $\mathcal{S}$ struktúrát a hasonlóság, az egybevágóság, vagy ezenfelül a forgásirány stb. adja meg, az automorfizmusok a hasonlósági transzformációk, az egybevágósági transzformációk, az egybevágósági irányítástartó transzformációk, az eltolások, adott pont körüli forgatások, egy adott alakzatot (részhalmazt) önmagába vivő egybevágósági transzformációk stb. Ha a H halmaz a valós számok egy zárt intervalluma, akkor ilyen csoport például a monoton bijektív függvények, a monoton növő bijektív függvények, a monoton növő bijektív deriválható függvények összessége, azoknak a monoton növő függvényeknek a halmaza, amelyek valahonnét kezdve

minden számnak önmagát feleltetik meg. Ilyen függvénycsoportot alkotnak például a nem 0 valós számok halmazán értelmezett $x, 1/x, -x, -1/x$ függvények is.]

6. Legyen $\mathcal{G} = \{G_\lambda \mid \lambda \in \Lambda\}$ a G csoport végesen (azaz véges sok elemmel) generált részcsoportjainak olyan halmaza, hogy bármely két $\mathcal{G}$-beli részcsoport benne van egy $\mathcal{G}$-beli részcsoportban. Bizonyítsuk be, hogy az összes $\mathcal{G}$-beli részcsoport egyesítése is részcsoport. Mi a feltétele annak, hogy az egyesítés is végesen generált legyen?

Mutassuk meg, hogy G részcsoportjai $\mathcal{G}$ halmazának egyesítése akkor is lehet részcsoport, ha e részcsoportok közül egyetlen párt sem tartalmaz $\mathcal{G}$-beli részcsoport.

7. Rögzített n esetén tekintsük az n sorú négyzetes reguláris felső háromszög mátrixokat (ezek olyanok, hogy a diagonális alatt csak 0 szerepel). Bizonyítsuk be, hogy ezek a mátrixszorzásra nézve csoportot alkotnak. Keressük ennek részcsoportjait, normálosztóit és faktorcsoportjainak (l.: a következő pont) teljes reprezentánsrendszerét.

8. Mutassunk (minél többféle) példát olyan csoportokra, amelyek előállnak ciklikus csoportok növő sorozatának egyesítéseként.

9. Legyen $J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Írjuk le a J generálta multiplikatív csoportot. Legyen I a kétszer kettes identitásmátrix. Írjuk le a $\begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$, $\begin{bmatrix} J & 0 \\ 0 & -J \end{bmatrix}$ generálta multiplikatív csoportot.

10. Tekintsük azokat az n sorú négyzetes mátrixokat, amelyekben minden sornak és minden oszlopnak egyetlen eleme +1 és az összes többi elem 0. Bizonyítsuk be, hogy ezek a mátrixok csoportot alkotnak a mátrixszorzásra nézve, amelynek normálosztóját alkotják az 1 determinánsúak. Mi változik, ha +1 helyett -1 is megengedett?

11. A szabályos n-szög izometriái (távolságtartó önmagára való bijekciói) a függvényszorzásra nézve egy D_n csoportot, az úgynevezett diédercsoportot alkotják. Határozzuk meg ennek rendjét, részcsoportjait, normálosztóit. Bizonyítsuk be, hogy D_n generálható két másodrendű elemével. Definiáljuk D_∞-t.

12. Tekintsük azokat a felső háromszög mátrixokat, amelyekben a főátlóban minden eleme 1. Csoport-e ez, ha

(1) a mátrixok mérete véges,

(2) a mátrixok mérete végtelen,

(3) a mátrixok mérete végtelen, de a diagonálison kívül csak véges sok elem nem 0.

13. Megadhatók-e egy rögzített G csoporton olyan további műveletek, hogy pontosan a normálosztók, illetve pontosan a kommutatív részcsoportok legyenek részalgebrák? Megadhatók-e G-n olyan további műveletek, hogy pontosan a bal odali, illetve pontosan a jobb oldali mellékosztályok legyenek részalgebrák?

14. Legyen D egy rögzített négyzetmentes egész szám, és tekintsük azokat az $a + b\sqrt{D}$ alakú számokat, amelyekre $|a^2 - Db^2| = 1$ $(a, b \in \mathbb{Z})$. (A testbővítések tárgyalásánál látni fogjuk, hogy ez a felírás egyértelmű.) E számok G halmazán tekintsük a szorzást mint műveletet. Bizonyítsuk be, hogy G csoport. Bizonyítsuk be, hogy az $a^2 - Db^2 = 1$ feltételnek eleget tevő számok H halmaza G-nek részcsoportja. Alkalmas pozitív D megadásával mutassunk példát arra, hogy H megegyezik, illetve különbözik G-től. Mutassuk meg, hogy G-nek mindig eleme +1 és -1. Mutassuk meg, hogy $D < -1$ esetén G-nek nincs több eleme. Bizonyítsuk be, hogy $D > 1$ esetén, ha van G-nek (+1)-től és (-1)-től különböző eleme, akkor van végtelen rendű eleme is. (Egyébként a $D > 1$ esetben mindig

van G-ben ilyen elem.) Bizonyítsuk be, hogy a $D > 1$ esetben van olyan $\alpha \in G$, hogy G minden eleme (egyértelműen) $\pm\alpha^n$ alakba írható, ahol $n \in \mathbb{Z}$.

15. Tekintsük az öt szabályos test bármelyikének izometriáit. Mutassuk meg, hogy ezek a függvényszorzásra nézve csoportot alkotnak. Bizonyítsuk be, hogy e csoport elemszáma a tetraéder esetében 24, a kocka és az oktaéder esetében 48, a dodekaéder és az ikozaéder esetében 120. Mutassuk meg, hogy e csoportok egyike sem kommutatív; és azok az izometriák, amelyek térbeli mozgatással megvalósíthatók, e csoportnak valódi normálosztóját alkotják.

5.6. Faktorcsoport, homomorfizmus-, izomorfizmustételek

Az 5.33. tétel alapján bármely G csoport esetében kölcsönösen egyértelmű megfeleltetés létesíthető a csoport kongruenciarelációi és a csoport normálosztói között. Ez a lehetőség a kongruenciarelációk igen kényelmes megadásához vezet, mert a megfelelő osztályozás során elegendő egyetlen osztályt – nevezetesen a szóban forgó normálosztót – megadni. A kongruenciát tulajdonképpen bármelyik mellékosztály megadná, de a megadás módját is egyértelművé tesszük azzal, hogy mindig az egységelemet tartalmazó mellékosztályt választjuk ki. Ennek alapján – csoportok esetében – a homomorfizmussal kapcsolatos fogalmakat lehetséges (és célszerű) kissé módosítani. Valójában ezek a fogalmak először a csoportelméletben alakultak ki. Szó szerinti általánosításuk tetszőleges algebrai struktúrákra éppen azért nem volt lehetséges, mert kompatibilis osztályozás esetén egyetlen osztály nem mindig határozza meg a többit. Például egy balzérus félcsoport bármely osztályozása kompatibilis – ami mutatja, hogy még félcsoportok esetére sem érvényes az általánosítás.

Mindenekelőtt az 5.6. tétel egy átfogalmazását mondjuk ki:

5.36. Tétel. *Ha φ a G_1 csoportot a G_2 csoportba képező félcsoport-homomorfizmus, akkor φ csoporthomomorfizmus és* Im φ *részcsoportja G_2-nek.* ■

5.37. Definíció. Legyen $N \lhd G$, és Θ az N meghatározta kongruenciareláció. G-nek Θ szerinti faktoralgebráját a G csoport N szerinti faktorcsoportjának nevezzük, s ezt G/N-nel jelöljük. Legyen $\varphi : G \to \widetilde{G}$ tetszőleges csoporthomomorfizmus, és N G-nek az a normálosztója, amelyet a φ-hez tartozó kompatibilis osztályozás meghatároz. Ekkor N-et a φ magjának nevezzük, és Ker φ-vel jelöljük. □

Ezt a definíciót az 5.31. tétel alapján adhattuk meg.

A Ker φ jelölést már használtuk a φ által meghatározott osztályozásra. Tekintettel arra, hogy N egyértelműen megadja ezt az osztályozást, ezért nem okoz zavart ez a jelölés. (Egyébként, amíg csak csoportokat és „csoportszerű” algebrai struktúrákat vizsgáltak, addig csak ez a jelölés létezett.)

A 2.23. tételt csoportokra átfogalmazva a következőt kapjuk:

5.38. Tétel. *Ha $\varphi : G \to \widetilde{G}$ tetszőleges csoporthomomorfizmus, akkor*

$$G/(\text{Ker } \varphi) \cong \text{Im } \varphi.$$

Ezt az izomorfizmust az $\widetilde{\varphi} : aN \to \varphi(a)$ bijekció hozza létre ($N =$ Ker φ). ■

E tétel – az úgynevezett *homomorfizmustétel* – segítségével bizonyíthatók az Emmy Noethertől származó, úgynevezett *izomorfizmustételek*, amelyek a csoportelméletben alapvető szerepet játszanak.

5.39. Tétel (első izomorfizmustétel). *Ha $H \leq G$ és $N \lhd G$, akkor $N \lhd HN$, valamint $(H \cap N) \lhd H$ és*

$$HN/N \cong H/(H \cap N).$$

Bizonyítás. Az 5.34. tétel szerint HN részcsoport, és az 5.31. tétel (2.1) pontja alapján N normálosztója HN-nek is. Tekintsük a $\varphi : h \to hN$ megfeleltetést, ahol h végigfut H elemein. Ez a megfeleltetés egyértelmű, hiszen minden H-beli elemhez az őt tartalmazó N szerinti mellékosztályt rendeltük hozzá. Így φ H-nak a G/N-be való leképezése. $(hN)(kN) = hkN$ alapján φ félcsoport-homomorfizmus; az 5.36. tétel szerint tehát csoporthomomorfizmus. Mivel $HN = \left\{\bigcup hN \mid h \in H\right\}$, ezért Im $\varphi = HN/N$. Másrészt, $h \in$ Ker φ pontosan akkor teljesül, ha h képe az egységelem, azaz, ha $hN = N$. Ez azt jelenti, hogy h ugyanabba a mellékosztályba tartozik, mint az 1, tehát $h \in N$. A $h \in H$ feltételt figyelembe véve, Ker $\varphi = H \cap N$ adódik; így tehát $H \cap N \lhd H$, s a homomorfizmustétel biztosítja a kívánt izomorfizmust. ■

5.40. Tétel (második izomorfizmustétel). *Ha $N, M \lhd G$ és $N \subseteq M$, akkor $M/N \lhd$ $\lhd G/N$ és*

$$(G/N)/(M/N) \cong G/M.$$

Bizonyítás. A $\varphi : aN \to aM$ megfeleltetés egyértelmű, mert minden N szerinti mellékosztálynak az őt tartalmazó M szerinti mellékosztály felel meg. Az $abN = (aN)(bN)$ és $(aM)(bM) = abM$ összefüggések miatt φ félcsoport-homomorfizmus; az 5.36. tétel szerint tehát csoporthomomorfizmus. Mivel a a G-nek tetszőleges eleme lehet, ezért Im $\varphi =$ $= G/M$. Ha $aN \in$ Ker φ, akkor aM a kép egységeleme, azaz $aM = M$, ami akkor és csak akkor teljesül, ha $a \in M$. Ez a feltétel $N \subseteq M$ miatt azzal ekvivalens, hogy $aN \subseteq M$. Ezért Ker φ elemei éppen M-nek N szerinti mellékosztályai, amelyek (definíció szerint) az M/N elemei. ■

A második izomorfizmustétel lényegében az algebrákra általánosan vonatkozó 2.24. tétel csoportelméleti speciális esete. Az első izomorfizmustételt viszont csak igen speciális algebraosztályokra lehet általánosítani.

5.41. Definíció. A G csoport egy N normálosztóját (H részcsoportját) maximálisnak nevezzük, ha ez a G-től különböző normálosztók (részcsoportok) tartalmazásra nézve részbenrendezett halmazában maximális elem. A legalább kételemű G csoportot egyszerűnek nevezzük, ha 1 maximális normálosztója G-nek (azaz, ha G-nek nincs valódi normálosztója). □

Az egyszerű csoportok és a maximális normálosztók igen szoros kapcsolatban állnak egymással. Ennek a kapcsolatnak a leírásához az alábbi tételt használjuk fel, amely megadja – speciális esetként – a kívánt kapcsolatot.

5.42. Tétel. *Legyen $\varphi : G \to \widetilde{G}$ szürjektív homomorfizmus és $N =$ Ker φ. Ekkor φ olyan bijekciót létesít G-nek az N-et tartalmazó részcsoportjai és $\widetilde{G}$ összes részcsoportjai között, amelynél pontosan a normálosztók képe normálosztó. φ-nél a közös rész (generátum) képe a képek közös része (generátuma).* ■

Bizonyítás. Az 5.38. tétel szerint $\widetilde{\varphi} : aN \mapsto \varphi(a)$ bijekció.

Természetesen a G tetszőleges H komplexusa esetén $\widetilde{\varphi} : H \mapsto \varphi(H)$ e bijekciónak kiterjesztése G/N részhalmazaira, amit ugyancsak $\widetilde{\varphi}$-vel jelölhetünk.

Ha H részcsoport, akkor $\varphi(H)$ – mint H homomorf képe – szintén részcsoport $\widetilde{G}$-ben. Fordítva, ha $a, b \in \varphi^{-1}(\widetilde{H})$ a $\widetilde{G}$ valamely $\widetilde{H}$ részcsoportjára, akkor $\varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b) \in \widetilde{H}$ miatt $a^{-1}b \in \varphi^{-1}(\widetilde{H})$, és így $\widetilde{\varphi}$ a részcsoportok között is bijekciót létesít. Legyen $N \leq H$, $\varphi(H) = \widetilde{H}$, $\varphi(a) = a'$. Ekkor $\widetilde{\varphi}$ az aH mellékosztályt $a'\widetilde{H}$-be képezi le, mégpedig $N \leq H$ miatt bijektíven ($a \in G$). Így $\widetilde{\varphi}$ bijekciót létesít a H, illetve a $\widetilde{H}$ bal oldali mellékosztályai között; és teljesen hasonlóan a jobb oldali mellékosztályok között is. A normálosztót definiáló feltétel tehát egyszerre teljesül H-ra és $\widetilde{H}$-re; ami bizonyítja a normálosztókra vonatkozó állításunkat. A tétel utolsó állítása nyilvánvaló. ■

5.43. Következmény. *N a G csoportban akkor és csak akkor maximális normálosztó, ha G/N egyszerű.*

Bizonyítás. Az 5.42. tételbeli bijekció N-nek a G/N egységelemét, G-nek pedig G/N-et felelteti meg. Minden más, az N-et tartalmazó G-beli normálosztónak tehát G/N egy valódi normálosztója felel meg és viszont. N tehát akkor és csak akkor nem maximális normálosztója G-nek, ha $1 \cdot N$ nem maximális G/N-ben. ■

5.44 Tétel. *Kommutatív csoport pontosan akkor egyszerű, ha prímrendű.*

Bizonyítás. Mivel kommutatív csoportban minden részcsoport eleve invariáns, ezért egy kommutatív csoport pontosan akkor egyszerű, ha nincs valódi részcsoportja. Legyen $a \neq 1$ a G csoport tetszőleges eleme. Mivel $\langle a \rangle$ nem lehet valódi részcsoport, ezért $G = \langle a \rangle$. Az a elem nem lehet végtelen rendű, hiszen ha az volna, akkor pl. a^2 a G-nek valódi részcsoportját generálná. Legyen p az a rendjének egy prímosztója. Ekkor a rendje egyetlen n természetes szám esetén sem oszthatja $(pn - 1)$-et, és így az 5.25. tétel szerint $a \notin \langle a^p \rangle$. Ha tehát G egyszerű, akkor $\langle a^p \rangle \neq G$ miatt csak $a^p = 1$ lehet, vagyis G prímrendű (ciklikus) csoport. Fordítva, prímrendű csoportnak – a Lagrange-tétel következtében – nem lehet valódi részcsoportja; prímrendű csoport tehát egyszerű. ■

5.7. Csoportok direkt szorzata

A 2.25. definíció alapján bármilyen struktúrafajta esetében beszélhetünk direkt szorzatról. Tekintsük csoportoknak egy tetszőleges $\mathcal{G} = \{\mathfrak{G}_i \mid i \in I\}$ rendszerét, ahol I tetszőleges indexhalmaz és G_i a $\mathfrak{G}_i$ csoport tartóhalmaza. Feltehető, hogy mindegyik csoportban az egymás mellé írás jelöli a csoportszorzást, 1 (esetleg 1_i) az egységelemet és $^{-1}$ az inverzképzést.

Ekkor a $\mathfrak{G} = \prod \mathfrak{G}_i$ *direkt szorzat* tartóhalmaza a G_i halmazok $G = \prod G_i$ direkt (Descartes-) szorzata. E halmaz $\mathbf{a} = (\ldots, a_i, \ldots)$ és $\mathbf{b} = (\ldots, b_i, \ldots)$ elemének a szorzatát $\mathbf{ab} = (\ldots, a_i b_i, \ldots)$, az $\mathbf{a}$ elem inverzét $\mathbf{a}^{-1} = (\ldots, a_i^{-1}, \ldots)$, míg az egységelemet

$\mathbf{1} = (\ldots, 1_i, \ldots)$ definiálja. Ha az indexhalmaz véges, $I = \{1, 2, \ldots, r\}$, akkor a direkt szorzatra a $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2 \times \ldots \times \mathfrak{G}_r$ jelölés is használatos. Mint a 2.26 tételben, itt is használhatjuk az $a_i = \mathbf{a}(i)$ jelölést. A 2.27. tételnek megfelelően a $\pi : \mathbf{a} \mapsto \mathbf{a}(i)$ megfeleltetés a direkt szorzatnak az i-edik komponensre való vetítése. Természetesen – mint általában – itt is feltehetjük, hogy a szereplő csoportoknak legalább két elemük van. A továbbiakban ismét ugyanazt a betűt használjuk egy csoportnak és tartóhalmazának a jelölésére.

Noha a direkt szorzatot továbbra is a komponensekből előállított vektorokként kezeljük, mégis célszerű e helyütt egy elvi definíciót megadni. Ez tulajdonképpen a direkt szorzatnak egy jellemző tulajdonsága, amely bizonyos értelemben egyszerűbbé teszi a számolást. Igaz, ez a tulajdonság nem nagyon szemléletes; de mégis hasznos.

5.45. Tétel. *Legyen G a $\{G_i \mid i \in I\}$ csoportok direkt szorzata a $\pi_i : G \to G_i$ projekciókkal. Ekkor ez univerzális rendszer, ami azt jelenti, hogy bármely adott H csoport és $\tau_i : H \to G_i$ homomorfizmusok esetén létezik olyan egyértelműen megadott $\varphi : H \to G$ homomorfizmus, amelyre minden egyes*

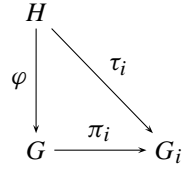


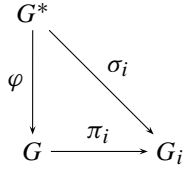
diagram kommutatív, azaz $\tau_i = \pi_i\varphi$ ($\iota_i : G_i \to G_i$ az identitás).

Fordítva, ha $\{\sigma_i : G^* \to G_i \mid i \in I\}$ univerzális rendszer, akkor G^* izomorf a direkt szorzattal, abban az erősebb értelemben, hogy létezik olyan $\eta : G^* \to G$ izomorfizmus, amelyre tetszőleges $i \in I$ esetén $\sigma_i = \pi_i\eta$ (és $\pi_i = \sigma_i\eta^{-1}$).

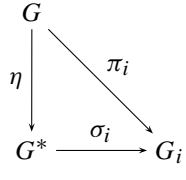
Ha a direkt szorzat univerzalitását is ki akarjuk fejezni, akkor a $G = \prod\{G_i \mid i \in I\}$ jelölés mellett a $G = \prod\{G_i \mid \pi_i : G \to G_i, i \in I\}$ jelölést is használni fogjuk.

Bizonyítás. A $\tau_i = \pi_i\varphi$ feltétel alapján tetszőleges $h \in H$ esetén $\varphi(h)$-nak az i-edik komponense csak $\tau_i(h)$ lehet; azaz az ilyen φ egyértelműen meghatározott. Azt kell belátni, hogy ez valóban homomorfizmus; ami viszont tüstént következik abból, hogy a direkt szorzatban a műveleteket komponensenként végezzük.

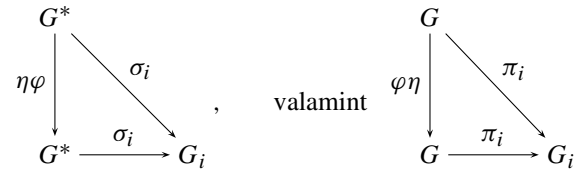
Legyen most a $\{\pi_i : G \to G_i \mid i \in I\}$ direkt szorzaton kívül $\{\sigma_i : G^* \to G_i \mid i \in I\}$ is univerzális rendszer. Ekkor feltétel szerint létezik megfelelő φ és η homomorfizmus úgy, hogy a



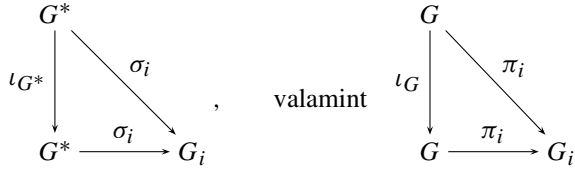
, valamint



diagramok mindegyike kommutatív. A kommutativitás jelentését figyelembe véve a



diagramok kommutativitása adódik. Emellett triviálisan kommutatívak a



diagramok is. Az univerzalitás miatt $\eta\varphi = \iota_{G^*}$ és $\varphi\eta = \iota_G$, azaz $\varphi = \eta^{-1}$. Tehát η izomorfizmus és fennállnak a kívánt szorzatösszefüggések is. ■

Az 5.45. tétel lényegében azt mondja ki, hogy a $\{G_i \mid i \in I\}$ csoportok direkt szorzata a „legkisebb" olyan csoport, amelyik a G_i csoportokra „függetlenül" leképezhető.

Az a tény, hogy minden csoportnak van egyelemű részcsoportja, lehetőséget ad arra, hogy a G_i csoportokat másképpen is kapcsolatba hozhassuk direkt szorzatukkal.

5.46. Tétel. *Legyen* $G = \prod\{G_i \mid i \in I\}$, $G^{(j)} = \prod\{G_i \mid i \in I, i \neq j\}$, *továbbá* $\pi^{(j)} : G \to G^{(j)}$ *a* j*-edik komponens elhagyásával létrejövő homomorfizmus. Legyen* $A_j = \mathrm{Ker}\,(\pi^{(j)})$, $B = \langle A_i \mid i \in I\rangle$ *és* $B_j = \langle A_i \mid i \in I, i \neq j \in I\rangle$. *Ekkor a következők teljesülnek:*

(1) $G_i \cong A_i \lhd G$.

(2) $B \lhd G$, $B_j \lhd G$.

(3) $A_i \cap B_i$ *az* A_i *egységeleme.*

(4) $A_i \leq B_j$, *ha* $i \neq j$.

(5) $B = G$ *pontosan akkor, ha* I *véges.*

Bizonyítás. A tételt először véges I indexhalmazra bizonyítjuk. A $\pi^{(j)}$ homomorfizmus magja azokból a vektorokból áll, amelyekben az j-edik komponensen kívül mindenütt az egységelem áll, azaz a mag $A_j \lhd G$. A π_j homomorfizmus képe G_j és magja azokból a vektorokból áll, amelyekben a j-edik helyen 1 áll. Ez azt jelenti, hogy π_j-nek az A_j-re való megszorítása bijekció, tehát izomorfizmus; így (1) teljesül.

Az 5.34. tétel utolsó állítása szerint normálosztók generátuma normálosztó, ami bizonyítja (2)-t.

(3)-at és (4)-et egyszerre bizonyítjuk. Legyen $J \subseteq I$ és jelölje A_J azoknak az A_i normálosztóknak a generátumát, amelyekre $i \in J$ teljesül. Speciálisan $A_\emptyset = \{1\}$, $A_i = A_{\{i\}}$, $B_j = A_{I\setminus j}$ és $A_I = B$. Így elegendő azt megmutatni, hogy tetszőleges $J, K \subseteq I$

esetén $A_{J\cap K} = A_J \cap A_K$. A_i azokból a vektorokból áll, amelyekben az i-edik helyen G_i tetszőleges eleme áll, míg a többi helyen az egységelem. Mivel a direkt szorzatban a műveleteket komponensenként végezzük és I véges, ezért A_J elemei azok a vektorok, amelyekben az i-edik komponens bármi, ha $i \in J$ és 1, ha $i \notin J$. Ebből viszont azonnal következik, hogy tetszőleges $J, K \subseteq I$ esetén $A_{J\cap K} = A_J \cap A_K$. Ezzel (5)-öt is igazoltuk véges I esetében.

Ha I végtelen, akkor (1) és (2) bizonyítása változatlan. A továbbiak bizonyításához vegyük figyelembe, hogy végtelen sok normálosztó generátumában minden elem olyan szorzatként áll elő, amelyben csak véges sok tényező szerepelhet. Ennek megfelelően az A_J elemei olyan vektorok, amelyekben az $i \in J$ esetben is csak véges sok i-re szerepelhet 1-től különböző elem. A továbbiak bizonyítása a véges I esetéhez hasonlóan történhet. ■

5.47. Tétel. *Legyenek $\{A_i \mid i \in I\}$ a G-nek részcsoportjai és jelölje B_i az $\langle A_j \mid j \in I, j \neq i\rangle$ részcsoportot. Ha teljesülnek az 5.46. tételben megfogalmazott feltételek, amelyek szerint $A_i \lhd G$, $A_i \cap B_i = \{1\}$, továbbá $\langle A_j \mid j \in I\rangle = G$, akkor teljesülnek az alábbiak:*

(1) *Ha $a_i \in A_i$, $a_j \in A_j$, és $i \neq j$, akkor $a_i a_j = a_j a_i$.*

(2) *G minden eleme felírható véges sok, különböző A_i-ből vett elem szorzataként.*

(3) *A fenti felírás a tényezők sorrendjétől és egységelem-tényezőktől eltekintve egyértelmű.*

Bizonyítás. Mivel $A_j \lhd G$, ezért $a_i a_j a_i^{-1} a_j^{-1} = (a_i a_j a_i^{-1}) a_j^{-1} \in A_j A_j^{-1} = A_j$. Hasonlóképpen $a_i a_j a_i^{-1} a_j^{-1} = a_i (a_j a_i^{-1} a_j^{-1}) \in A_i A_i^{-1} = A_i$, mert $A_j \lhd G$. Az $A_i \cap A_j \leq A_i \cap$ $\cap B_i = \{1\}$ feltétel miatt $a_i a_j a_i^{-1} a_j^{-1} = 1$, azaz $a_i a_j = a_j a_i$.

Véges I esetén az 5.34. tétel alapján G az adott normálosztók bármilyen sorrendben vett komplexusszorzata, ami biztosítja a (2) alatti előállítást. Végtelen I esetében még annyit kell ehhez hozzátenni, hogy a generátum minden eleme benne van egy véges sok normálosztó által generált részben.

Tegyük most fel, hogy a G-beli g elemnek adott két megfelelő felírása. Mivel mindkét felírásban csak véges sok elem szerepel, ezért feltehető, hogy ezen elemek mindegyike például az $A_1, A_2, \ldots, A_r$ normálosztókhoz tartozik:

$$g = a_1 \cdot a_2 \cdot \ldots \cdot a_r = b_1 \cdot b_2 \cdot \ldots \cdot b_r, \qquad a_i, b_i \in A_i.$$

A már bizonyított (1) tulajdonság szerint

$$b_i^{-1} a_i = c_1 \cdot \ldots \cdot c_{i-1} \cdot c_{i+1} \cdot \ldots \cdot c_r,$$

ahol $c_j \in A_j$, $1 \leq j \leq r$, $j \neq i$. Az $A_i \cap \langle A_1, \ldots, A_{i-1}, A_{i+1}, \ldots, A_r\rangle \leq A_i \cap B_i = \{1\}$ feltétel miatt $b_i = a_i$, mint állítottuk. ■

5.48. Tétel. *Tegyük fel, hogy a G csoport $\{A_i \mid i \in I\}$ részcsoportjaira teljesül az* 5.47. *tétel* (1), (2), (3) *feltétele, és legyen $G^* = \prod A_i$ a $\pi_i : G \to A_i$ projekciókkal. Jelölje továbbá $\pi^{(i)} : G^* \to \prod\{A_j \mid j \in I, j \neq i\}$ azt a homomorfizmust, amelyet az i-edik komponens elhagyásával nyerünk. Ekkor létezik olyan egyértelmű $\varphi : G \to G^*$ injekció, amelynél $\varphi(A_i) = \operatorname{Ker}(\pi^{(i)})$.*

Ha I véges, akkor φ izomorfizmus.

Bizonyítás. A (2) tulajdonság szerint minden $g \in G$ elem felírható $g = a_{i_1} \cdot \ldots \cdot a_{i_r}$ alakban, ahol $a_{i_t} \in A_{i_t}$ $(1 \leq t \leq r)$. Az elemek felírásának egyértelműsége alapján a $\tau_{i_t} : g \mapsto a_{i_t}$ megfeleltetés függvény, amely (1) következtében homomorfizmus. A direkt szorzat „absztrakt" definíciója (5.45. tétel) szerint létezik tehát olyan egyértelmű $\varphi : G \to$ $\to G^*$ homomorfizmus, amelyre tetszőleges i esetén $\pi_i \varphi = \tau_i$. Ha $g \in \text{Ker } \varphi$, akkor $\tau_i(g) = \pi_i(1) = 1$ miatt $g \in A_i$ teljesül minden i-re, (3) szerint tehát $g = 1$, vagyis φ injektív. Definíció szerint τ_i a G csoportot az A_i-re képezi és a $\pi^{(i)}$ magja – ugyancsak a definíció szerint – szintén A_i. Így valóban $\varphi(A_i) = \text{Ker } (\pi^{(i)})$. Ha I véges, akkor (3) miatt φ szürjektív; tehát valóban izomorfizmus. ■

Megjegyzések. 1. Véges sok csoport direkt szorzatát az 5.45., 5.46., 5.47. és 5.48. tételek bármelyikében található feltételcsoportok bármelyikével definiálhatjuk. (Az 5.46. tételből elég azokat feltenni, amelyeket az 5.47. tétel bizonyításában felhasználtunk. A többiekre a bizonyítás megfogalmazásához, illetve a megfelelő részcsoportok azonosításához volt szükség.) Az 5.45. tétel bármely algebrai struktúrafajta esetében definiálja a direkt szorzatot. Az 5.46. és 5.47. tételek esetében a direkt szorzat csoporton belüli jellemzése szerepel, ezért ilyenkor *belső direkt szorzatról* beszélünk; ekkor az eredeti fogalom esetében a *külső direkt szorzat* elnevezés szerepel. Maga a direkt szorzat elnevezés is csoportelméleti eredetű. Ha ugyanis a G csoport az $A_1, \ldots, A_r$ részcsoportjainak a direkt szorzata, akkor G – mint láttuk – e részcsoportok $A_1 \cdot \ldots \cdot A_r$ komplexusszorzatával egyenlő.

2. Az 5.48. tétel mutat rá arra, hogy végtelen sok csoport esetében a belső direkt szorzat nem tartalmazza a direkt szorzat minden elemét, hanem csak azokat, amelyekben véges sok helyen van 1-től különböző elem. Ilyen esetben azt is szokták mondani, hogy *majdnem minden* komponense 1. Megkülönböztetésül ezt a részt *diszkrét direkt szorzatnak nevezik*; ilyenkor a direkt szorzatra a *teljes (komplett) direkt szorzat* elnevezés használatos.

3. Az 5.46. tételben felsorolt „többlet" megmutatja, hogy *a direkt szorzat mint csoportok közti „művelet" kommutatív és asszociatív* (természetesen csak izomorfizmus erejéig). Az 5.47. tétel arra mutat rá, hogy a direkt szorzatra érvényes a *finomítási tulajdonság*, azaz, ha G az A_i csoportok direkt szorzata és ezek – megfelelően – az $A_{i,j}$ csoportok direkt szorzata (rögzített i-vel), akkor G előáll az összes $A_{i,j}$ csoport direkt szorzataként.

4. Kommutatív csoportok esetében a szorzásjel helyett összeadásjelet használunk, ennek megfelelően véges indexhalmaz esetében használatos a *direkt összeg* elnevezés és a $G = A_1 + \cdots + A_r$ (esetenként a $G = A_1 \oplus \cdots \oplus A_r$) jelölés. Végtelen indexhalmaz esetében a diszkrét direkt szorzatot nevezik direkt összegnek, ennek jelölésére használatos a $\sum\{A_i \mid i \in I\}$ jelölés. □

5.8. Véges Abel-csoportok

Abel-csoportoknak a kommutatív csoportokat nevezik (N. H. Abel norvég matematikusról). Ezeknek a szerkezete természetesen sokkal egyszerűbben leírható, mint a tetszőleges csoportoké. Például a véges Abel-csoportokról teljesen áttekinthető leírást adhatunk a direkt szorzat felhasználásával. Abel-csoportok esetében igen sokszor a (kétváltozós) műveletet nem szorzással, hanem összeadással jelölik. Mi is ezt a jelölésmódot követjük. Természetesen, ekkor nem kitevők szerepelnek, hanem „együttható"k; azaz a^n helyett az na jelölést fogjuk használni (n tetszőleges egész szám lehet). Avégett, hogy a csoportelemeket ne tévesszük össze a számegyüttható kkal, az Abel-csoportok elemeit vastag betűkkel fogjuk jelölni (mint a vektorok esetében).

5.49. Definíció. Tetszőleges n természetes szám és A Abel-csoport esetén nA jelöli az $\{n\mathbf{a} \mid \mathbf{a} \in A\}$ halmazt. Ha valamely n-re $nA = \{\mathbf{o}\}$ ($\mathbf{o}$ a csoport nulleleme), akkor a legkisebb ilyen n-et az A csoport exponensének nevezzük. Ha A exponense egy p prímszám hatványa, akkor A-t p-csoportnak nevezzük. □

Megjegyezzük, hogy az exponens és a p-csoport fogalma a nemkommutatív esetben is hasonlóan értelmezhető. Világos, hogy véges csoportnak mindig van exponense.

A p-csoport általában olyan csoportot jelent, amelyben bármely elem rendje a rögzített p prímszám egy hatványa.

Az Abel-csoportok az $n : \mathbf{a} \to n\mathbf{a}$ megfeleltetéssel ($\mathbf{a} \in A$, $n \in \mathbb{Z}$) $\mathbb{Z}$-modulussá válnak. Tekintettel arra, hogy az egész számok euklideszi gyűrűt alkotnak, ezért a véges Abel-csoportok lényegében egyértelműen felírhatók prímhatványrendű ciklikus csoportok direkt összegeként (I. kötet, 8.12. tétel 5. következmény). E tételre most egy másik bizonyítást adunk, amely szinte változtatás nélkül átvihető euklideszi gyűrűk feletti végesen generált torziómodulusokra. Az itt közölt bizonyítás nagyon egyszerűen adja a felbontás létét; csak az egyértelműség bizonyítása jelent gondot. A bizonyítás a következőn alapszik:

5.50. Tétel. *Legyen G (legalább kételemű) véges Abel-csoport és $\mathbf{a} \in G$ maximális prímhatványrendű elem. Legyen $A = \langle \mathbf{a} \rangle$ és jelölje $[\mathbf{b}] \in G/A$ azt a mellékosztályt, amelyik $\mathbf{b}$-t tartalmazza. Ekkor van olyan $\mathbf{b}' \in [\mathbf{b}]$, amelyre $o(\mathbf{b}') = o([\mathbf{b}])$.*

Bizonyítás. Mindenekelőtt megjegyezzük, hogy a végesség miatt minden elem véges rendű. Ha $o(\mathbf{b}) = n \cdot k$, akkor $o(n\mathbf{b}) = k$, így a csoportban van prímrendű elem; s a végesség miatt van olyan $\mathbf{a}$ elem, amelynek a rendje maximális kitevőjű prímhatvány. Ha $k\mathbf{b} = \mathbf{o}$, akkor $\mathbf{o} \in k[\mathbf{b}]$ miatt csak $k[\mathbf{b}] = A$ lehet, vagyis $o([\mathbf{b}]) \leq o(\mathbf{b})$ (sőt mi több, $o([\mathbf{b}])$ osztója $o(\mathbf{b})$-nek). A tétel állításának igazolására tehát olyan $\mathbf{b}' \in [\mathbf{b}]$ elemet kell találni, amelyre $o([\mathbf{b}]) \geq o(\mathbf{b}')$, azaz $o([\mathbf{b}])\mathbf{b}' = \mathbf{o}$. Legyen $o(\mathbf{a}) = p^n$ (p prímszám) és $o([\mathbf{b}]) = p^r k$, ahol $(p^r, k) = 1$. Ez azt jelenti, hogy $p^r k[\mathbf{b}] = A$, vagyis $p^r k\mathbf{b} = p^s t\mathbf{a}$, alkalmas p-hez relatív prím t egész számmal. Feltételünk szerint $p^n\mathbf{a} = \mathbf{o}$, de $p^{n-1}\mathbf{a} \neq \mathbf{o}$, és ezért $(p, t) = 1$ következtében $p^n(t\mathbf{a}) = \mathbf{o}$, de $p^{n-1}(t\mathbf{a}) \neq \mathbf{o}$. n maximalitása következtében $n - s + r \geq 0$, és így $p^{n-s+r}(k\mathbf{b}) = \mathbf{o}$, de $p^{n-s+r-1}(k\mathbf{b}) \neq \mathbf{o}$. n maximalitása alapján tehát $n - s + r \leq n$, vagyis $s \geq r$. Mivel $(k, p) = 1$, ezért $(k, p^n) = 1$ is igaz; léteznek tehát olyan x, y egész számok, amelyekre $xk + yp^n = 1$. Ebből azt kapjuk, hogy

$$p^r k\mathbf{b} = p^s t\mathbf{a} = p^s txk\mathbf{a} + p^s typ^n\mathbf{a} = p^s txk\mathbf{a} = p^r k(p^{s-r}tx\mathbf{a}).$$

Mármost a $\mathbf{b}' = \mathbf{b} - p^{s-r}tx\mathbf{a}$ elem ugyancsak eleme a $[\mathbf{b}]$ mellékosztálynak; és a fentiek szerint $p^r k\mathbf{b}' = \mathbf{o}$, vagyis $o(\mathbf{b}') \leq p^r k = o([\mathbf{b}])$. ■

A véges Abel-csoportok alaptételének a kimondásához szükségünk van az alábbiakra:

5.51. Definíció. Egy G Abel-csoport $\{\mathbf{a}_i \mid i \in I\}$ elemrendszerét függetlennek nevezzük, ha $\mathbf{a}_i \neq \mathbf{o}$ és ha bármely véges $\sum c_i\mathbf{a}_i = \mathbf{o}$, akkor minden egyes $c_i\mathbf{a}_i = \mathbf{o}$.

Egy G Abel-csoport $\{\mathbf{a}_i \mid i \in I\}$ elemrendszere bázis, ha független generátorrendszer. □

Megemlítjük azt a könnyen belátható tényt, hogy egy G Abel-csoport $\{\mathbf{a}_i \mid i \in I\}$ elemrendszere pontosan akkor bázis, ha G minden eleme egyértelműen felírható véges

$\sum c_i \mathbf{a}_i$ összegként, ahol az egyértelműség azt jelenti, hogy $\sum c_i \mathbf{a}_i = \sum d_i \mathbf{a}_i$ esetén minden egyes i indexre $c_i \mathbf{a}_i = d_i \mathbf{a}_i$ teljesül.

Figyeljük meg, hogy a definícióban nem tettük fel a csoport végességét. Bázisról tehát végtelen Abel-csoportok esetében is lehet beszélni. Sőt, az sem lényeges, hogy a bázis elemszáma véges legyen. Ennek ellenére van olyan Abel-csoport, amelynek nincs bázisa. Bizonyos tulajdonságú Abel-csoportokról könnyen belátható, hogy nem létezik bázisuk:

A G Abel-csoportot *oszthatónak* nevezzük, ha minden n természetes számra teljesül az $nG = G$ összefüggés. Ez azt jelenti, hogy bármely $\mathbf{a} \in G$ és bármely n természetes szám esetén található olyan $\mathbf{b} \in G$, amelyre $n\mathbf{b} = \mathbf{a}$. *Osztható csoport homomorf képe is osztható*, hiszen a kép bármely $\mathbf{a}'$ eleméhez és tetszőleges n természetes számhoz tekintsük azt a $\mathbf{b}$ elemet, amelyre $\mathbf{a} = n\mathbf{b}$ képe az $\mathbf{a}'$ elem (ilyen $\mathbf{a}$ a szürjektivitás miatt, és ilyen $\mathbf{b}$ éppen az oszthatóság alapján létezik). Ennek a $\mathbf{b}$ elemnek a $\mathbf{b}'$ képére a homomorfizmus alaptulajdonsága következtében $n\mathbf{b}' = \mathbf{a}'$ teljesül. Tegyük most fel, hogy egy G osztható csoport ciklikus: $G = \langle \mathbf{a} \rangle$. Az oszthatóság alapján van olyan $\mathbf{b} \in G$, amelyre $\mathbf{a} = 2\mathbf{b}$. A ciklikusság miatt $\mathbf{b} = n\mathbf{a}$, alkalmas n egész számmal, amiből $(2n-1)\mathbf{a} = \mathbf{o}$ következik; ami azt jelenti, hogy $\mathbf{a}$ véges rendű. Legyen $k\mathbf{a} = \mathbf{o}$, és válasszuk G-nek egy olyan $\mathbf{c}$ elemét, amelyre $k\mathbf{c} = \mathbf{a}$. Mivel $\mathbf{c} = n\mathbf{a}$ alkalmas n egész számmal, ezért $\mathbf{a} = k\mathbf{c} = kn\mathbf{a} = n(k\mathbf{a}) = \mathbf{o}$, azaz *egy osztható csoport csak akkor ciklikus, ha egyelemű.*

Ebből máris következik, hogy nemtriviális osztható csoportnak nincs bázisa. Ennél többet bizonyítunk. Egy bázis ugyanis nyilvánvalóan minimális generátorrendszer, azaz olyan generátorrendszer, amelyből bármely elemet elhagyva, már nem kapunk generátorrendszert. Azt fogjuk belátni, hogy ha egy osztható csoport bármely generátorrendszeréből elhagyunk egy elemet, ismét generátorrendszert kapunk. Legyen ugyanis $\mathbf{a}$ a G osztható csoport egy generátorrendszerének eleme, és legyen H a generátorrendszer többi eleme generálta csoport. G/H osztható, és ciklikus, mert $\mathbf{a}$-nak a képe generálja. Így egyelemű, azaz $H = G$, tehát az $\mathbf{a}$ elemet elhagyva ismét generátorrendszert nyertünk.

Egyetlen kérdést kell még tisztázni, nevezetesen azt, hogy létezik-e osztható csoport. Erre a válasz igenlő: például a racionális számok additív csoportja nyilvánvalóan osztható.

5.52. Tétel. *Minden legalább kételemű véges Abel-csoportnak létezik prímhatványrendű elemekből álló bázisa.*

Bizonyítás. A tételt a G véges Abel-csoport rendjében fellépő prímszámok számára vonatkozó teljes indukcióval bizonyítjuk. Ha ez a szám 1, akkor G prímrendű, tehát ciklikus. Ezért G bármely generátoreleme bázis és eleve prímrendű.

Tegyük most fel, hogy az állítás igaz minden olyan véges Abel-csoportra, amelynek rendjében n-nél kevesebb (nem feltétlenül különböző) prímtényező szerepel és legyen a G véges Abel-csoport rendjében fellépő prímtényezők száma n. Az 5.50. tétel szerint G-ben van olyan $\mathbf{a}_1$ prímhatványrendű elem, hogy az általa generált A csoport szerinti faktor minden eleme tartalmaz ezzel az elemmel megegyező rendű G-beli elemet.

Lagrange tételéből következik, hogy $|G| = |G/A| \cdot |A|$. Így G/A rendjében kevesebb prímtényező lép fel, mint G rendjében; ezért G/A-ra igaz a tétel állítása. Legyen e csoportnak egy prímhatványrendű elemekből álló bázisa $[\mathbf{a}_2], \ldots, [\mathbf{a}_k]$. Az 5.50. tétel alapján feltehető, hogy az $\mathbf{a}_2, \ldots, \mathbf{a}_k$ elemeket eleve úgy választottuk, hogy $o(\mathbf{a}_i) = o([\mathbf{a}_i])$ legyen

$(2 \le i \le k)$. Legyen $\mathbf{g} \in G$ tetszőleges. Ekkor $[\mathbf{g}]$ felírható $\sum_{i=2}^{k} c_i[\mathbf{a}_i]$ alakban, amiből $\mathbf{g} - \sum_{i=2}^{k} c_i\mathbf{a}_i \in A$, azaz $\mathbf{g} - \sum_{i=2}^{k} c_i\mathbf{a}_i = c_1\mathbf{a}_1$ következik; és így $\mathbf{g} = \sum_{i=1}^{k} c_i\mathbf{a}_i$. Eszerint az $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k$ elemek G-nek generátorrendszerét alkotják. Ezen elemek egyike sem $\mathbf{o}$. Tegyük most fel, hogy $\sum_{i=1}^{k} c_i\mathbf{a}_i = \mathbf{o}$. Az A szerinti faktorcsoportra térve ebből $\sum_{i=2}^{k} c_i[\mathbf{a}_i] = [\mathbf{o}]$ következik. Mivel ezek a mellékosztályok bázist alkotnak, ezért azt kapjuk, hogy minden egyes $2 \le i \le k$ esetében $c_i[\mathbf{a}_i] = [\mathbf{o}]$. Az $\mathbf{a}_i$-k választása szerint tehát $c_i\mathbf{a}_i = \mathbf{o}$ minden $2 \le i \le k$ esetén. Ezeket a kiindulási $\sum_{i=1}^{k} c_i\mathbf{a}_i = \mathbf{o}$ egyenletbe behelyettesítve $c_1\mathbf{a}_1 = \mathbf{o}$ adódik; tehát ezek az elemek valóban bázist alkotnak. A teljes indukciós feltételből és a $\mathbf{a}_i$-k választásából következik, hogy e bázis elemeinek a rendje prímhatvány. ■

Be fogjuk bizonyítani, hogy az 5.52. tételben szereplő bázis lényegében egyértelmű, ami azt jelenti, hogy a báziselemek száma és azok rendjeinek a rendszere nem függ a bázistól (hasonlatosan egy vektortér bázisához). Ehhez előkészületül szükségünk van néhány önmagában is érdekes eredményre:

5.53. Tétel. *nG bármely G Abel-csoportban minden n-re részcsoport. Legyen a G exponense $n = km$ alakú, ahol $(m, k) = 1$. Ekkor:*

(1) *kG exponense m, mG exponense k;*

(2) *$G = kG \oplus mG$;*

(3) *ha $H \le G$ és H exponense osztója m-nek, akkor $H \le kG$.*

Ha A, illetve B a G-nek k, illetve m exponensű részcsoportja, ahol $(k, m) = 1$ és $G = A + B$, akkor G exponense km és $A = mG$, $B = kG$.

Bizonyítás. $n\mathbf{a} - n\mathbf{b} = n(\mathbf{a} - \mathbf{b})$ bizonyítja az első állítást. A G csoport tetszőleges $\mathbf{a}$ elemére $m(k\mathbf{a}) = k(m\mathbf{a}) = \mathbf{o}$ teljesül, amiből következik, hogy kG-nek az m_1 exponense osztója m-nek, és mG-nek a k_1 exponense osztója k-nak.

A $(k, m) = 1$ feltételből következik, hogy léteznek olyan u és v egész számok, amelyekre $ku + mv = 1$ teljesül. Ennek következménye az

$$\mathbf{a} = (ku + mv)\mathbf{a} = u(k\mathbf{a}) + v(m\mathbf{a}) \qquad (\mathbf{a} \in G)$$

felírás. Ebből $k\mathbf{a} \in kG$ és $m\mathbf{a} \in mG$ miatt következik, hogy $G \le \langle kG, mG \rangle$. Ha $\mathbf{a} \in kG \cap mG$, azaz $\mathbf{a} = k\mathbf{b} = m\mathbf{c}$, akkor $m\mathbf{a} = mk\mathbf{b} = \mathbf{o}$ és $k\mathbf{a} = km\mathbf{c} = \mathbf{o}$; amiből az $\mathbf{a}$ fenti felírása szerint $\mathbf{a} = \mathbf{o}$ következik. Mivel kG és mG részcsoportok és Abel-csoportban minden részcsoport normálosztó, ezért igaz (2).

Legyen most $\mathbf{a} = \mathbf{b} + \mathbf{c}$, ahol $\mathbf{b} \in kG$ és $\mathbf{c} \in mG$. A $k_1m_1\mathbf{a} = k_1(m_1\mathbf{b}) + m_1(k_1\mathbf{c}) = \mathbf{o} + \mathbf{o} = \mathbf{o}$ egyenlőség következtében G exponense osztója k_1m_1-nek. Mivel G exponense $n = km$, ezért km osztója k_1m_1-nek. Láttuk viszont, hogy k_1 a k-nak és m_1 az m-nek osztója. Ezekből, a szereplő egész számok pozitivitása következtében azonnal következik a $k_1 = k$ és az $m_1 = m$ egyenlőség; vagyis az (1) alatti állítás.

Legyen most a $H \leq G$ részcsoport m_1 exponense osztója m-nek, és írjuk fel a H egy elemét $\mathbf{a} = \mathbf{b} + \mathbf{c}$ alakban, ahol $\mathbf{b} \in kG$ és $\mathbf{c} \in mG$. Ekkor $\mathbf{o} = m\mathbf{a} = m\mathbf{b} + m\mathbf{c} = \mathbf{o} + m\mathbf{c}$ következtében $m\mathbf{c} = \mathbf{o}$, azaz a $ku + nv = 1$ egyenlőséget felhasználva $\mathbf{c} = u(k\mathbf{c}) + v(m\mathbf{c}) = \mathbf{o}$, és ebből $H \leq kG$ adódik.

Az utolsó állítás bizonyításához írjuk fel a G csoport egy elemét $\mathbf{g} = \mathbf{a} + \mathbf{b}$ alakban ($\mathbf{a} \in A$, $\mathbf{b} \in B$). Ebből azt kapjuk, hogy $k\mathbf{g} = k\mathbf{a} + k\mathbf{b} = \mathbf{o} + k\mathbf{b} \in B$, amiből $kG \leq B$, és hasonlóan $mG \leq A$ következik. Az A tetszőleges elemét $\mathbf{a} = u(k\mathbf{a}) + v(m\mathbf{a})$ alakba írva, $k\mathbf{a} = \mathbf{o}$ miatt azt kapjuk, hogy $\mathbf{a} \in kG$ következik. Így $A = mG$ és $B = kG$. A G csoport n exponensére $nA = nB = \{\mathbf{o}\}$ miatt m és k mindegyike osztója n-nek. Másrészt – újból felhasználva, hogy G bármely eleme $\mathbf{g} = \mathbf{a} + \mathbf{b}$ alakban írható ($\mathbf{a} \in A$, $\mathbf{b} \in B$) azt kapjuk, hogy $km\mathbf{g} = m(k\mathbf{a}) + k(m\mathbf{b}) = \mathbf{o}$. Így $n = km$, felhasználva, hogy k és m relatív prímek. ■

5.54. Tétel. *Bármely véges Abel-csoport egyértelműen felbontható különböző prímszámokhoz tartozó (véges kommutatív) p-csoportok direkt összegére. Ezeket a csoport p-komponenseinek nevezzük.*

Bizonyítás. Az 5.53. tétel ismételt alkalmazásával, a direkt szorzat finomítási tulajdonsága alapján minden véges Abel-csoport felbontható olyan részcsoportjainak a direkt összegére, amelyek exponensét nem lehet relatív prím tényezőkre bontani. Mivel e tulajdonsága csak a prímhatványoknak van meg, ezért a felbonthatóság teljesül. Legyen egy ilyen felbontás:

$$G = G_1 + \cdots + G_r,$$

ahol G_i exponense a p_i prímszám $s(i)$-edik hatványa és a p_i prímszámok különbözőek. Az 5.53. tétel (1) állításából az is következik, hogy G exponense $n = p_1^{s(1)} \cdot \ldots \cdot p_r^{s(r)}$. Tegyük most fel, hogy G-nek létezik egy másik felbontása:

$$G = H_1 + \cdots + H_t,$$

ahol az egyes komponensek prímhatvány-exponensűek, különböző prímszámokkal. Mivel bármelyik H_i exponense osztója G exponensének, ezért osztója valamelyik $p_j^{s(j)}$-nek. Az 5.53. tétel (3) pontja szerint tehát feltehető, hogy – az indexek megfelelő átszámozása után – $H_i \leq G_i$. Mivel a második felbontásban is direkt összeg áll, ezért alkalmazhatjuk az 5.53. tétel utolsó állítását, amiből $H_i = G_i$ következik. ■

Érdemes megjegyezni, hogy az 5.54. tétel bizonyítása során nem használtuk ki a G végességét, csupán azt, hogy az exponense véges. Így ez azt az erősebb tételt is bizonyítja, hogy bármely véges exponensű Abel-csoportnak létezik a fenti típusú egyértelmű felbontása. A bizonyítás csekély módosításával még erősebb eredményt kaphatunk.

Torziócsoportnak neveznek egy olyan csoportot, amelyben minden elem véges rendű. Az is igaz, hogy Abel-féle torziócsoport felbontható p-csoportok direkt összegére. Ez a direkt összeg azonban nem azonos a direkt szorzattal, mert itt kizárólag olyan vektorok szerepelhetnek, amelyekben csak véges sok komponens különbözik **o**-tól. E felbontásban a komponensekről még azt sem tudjuk, hogy véges exponensűek, csupán annyit, hogy p-csoportok.

Tekintettel arra, hogy a p-komponensek egyértelműek, ezért a bázis „egyértelműségének” a bizonyításához elég megmutatni, hogy ez Abel-féle véges p-csoportokra teljesül:

5.55. Tétel. *Legyen G véges Abel-féle p-csoport (p rögzített prímszám) és $\mathbf{a}_1, \ldots, \mathbf{a}_n$ a G-nek egy bázisa, amelyben $o(\mathbf{a}_1) \geq \ldots \geq o(\mathbf{a}_n)$. Ekkor a G csoport bármely bázisának ugyancsak n eleme van; s ha a $\mathbf{b}_1, \ldots, \mathbf{b}_n$ bázisra $o(\mathbf{b}_1) \geq \ldots \geq o(\mathbf{b}_n)$ teljesül, akkor minden szóba jövő i-re igaz az $o(\mathbf{b}_i) = o(\mathbf{a}_i)$ egyenlőség.*

Bizonyítás. Azt fogjuk megmutatni, hogy tetszőleges bázis esetén azoknak a bázis-elemeknek a száma, amelyeknek a rendje ugyanaz a p^i prímhatvány, nem függ a bázistól. Ezt először az $i = 1$ esetben bizonyítjuk.

Legyen a rögzített $\mathbf{a}_1, \ldots, \mathbf{a}_n$ bázis első k elemének a rendje legalább p^2, s a többi $n - k$ elemé p. Tetszőleges m természetes szám esetén jelölje $G[m] = \{\mathbf{a} \in G \mid m\mathbf{a} = \mathbf{o}\}$ a csoport azon elemeinek a halmazát, amelyeknek az m-szerese a nullelem. Világos, hogy ezek G-nek részcsoportját alkotják. Ha $\mathbf{a} \in G[p]$, akkor $p\mathbf{a} = \mathbf{o}$ miatt ez a részcsoport vektortér a modulo p vett maradékok $\mathbb{Q}_p$ teste felett. Ha $\sum_i c_i\mathbf{a}_i \in G[p]$, akkor $\sum_i pc_i\mathbf{a}_i = \mathbf{o}$. Mivel a szereplő elemek bázist alkotnak, ezért ebből az egyenlőségből $pc_i\mathbf{a}_i = \mathbf{o}$ következik. Ha $o(\mathbf{a}_i) = p^{n(i)}$, akkor a most kapott egyenlőség alapján pc_i osztható $p^{n(i)}$-vel, azaz $c_i = p^{n(i)-1}d_i$ alakú. Legyen $\mathbf{b}_i = p^{n(i)-1}\mathbf{a}_i$. Világos, hogy $\mathbf{b}_i \in G[p]$, és e csoport minden eleme előáll a $\mathbf{b}_1, \ldots, \mathbf{b}_n$ elemek lineáris kombinációjaként; így ezek az elemek generátorrendszert alkotnak. Ha $\sum_i u_i\mathbf{b}_i = \mathbf{o}$, azaz $\sum_i u_i p^{n(i)}\mathbf{a}_i = \mathbf{o}$, akkor ebből minden i-re $u_i p^{n(i)-1}\mathbf{a}_i = \mathbf{o}$ következik, mert a $\mathbf{a}_1, \ldots, \mathbf{a}_n$ elemek bázist alkotnak. Így $p^{n(i)}$ osztója $u_i p^{n(i)-1}$-nek, vagyis u_i osztható p-vel, azaz u_i a p elemű test nulleleme, tehát $\mathbf{b}_1, \ldots, \mathbf{b}_n$ a $G[p]$ $\mathbb{Q}_p$-vektortér bázisa. Eszerint G báziselemeinek a száma a $G[p]$ vektortér dimenziója, ami nem függ a kiindulásul felvett bázistól.

Tekintsük most a $pG \cap G[p]$ részcsoportot, amely altere a $G[p]$ vektortérnek. Ebben az altérben benne vannak a $\mathbf{b}_1, \ldots, \mathbf{b}_k$ elemek, hiszen $\mathbf{b}_i = p^{n(i)-1}\mathbf{a}_i$, s ha $i \leq k$, akkor $n(i) - 1 \geq 1$. Mint láttuk, ezek az elemek lineárisan függetlenek. Legyen $\mathbf{g} \in pG \cap G[p]$. Ez azt jelenti, hogy $\mathbf{g} = \sum_i pv_i\mathbf{a}_i$ alakú. Mivel $i > k$ esetén $p\mathbf{a}_i = \mathbf{o}$, ezért $\mathbf{g} = \sum_{i=1}^{k} pv_i\mathbf{a}_i$. A $\mathbf{g} \in G[p]$ feltételből $p\mathbf{g} = \sum_{i=1}^{k} p^2v_i\mathbf{a}_i = \mathbf{o}$, s az $\mathbf{a}_i$ elemek bázisvoltából $p^2v_i\mathbf{a}_i = \mathbf{o}$ következik. Így $p^{n(i)}$ osztója p^2v_i-nek, ezért $p^{n(i)-2}$ osztója v_i-nek, azaz $v_i = p^{n(i)-2}w_i$. Ebből $\mathbf{g} = \sum_{i=1}^{k} p^{n(i)-1}w_i\mathbf{a}_i = \sum_{i=1}^{k} w_i\mathbf{b}_i$ következik, tehát $\mathbf{b}_1, \ldots, \mathbf{b}_k$ bázis. Eszerint k a bázistól függetlenül megadható mint a $pG \cap G[p]$ altér dimenziója; azaz $n-k$, a p-edrendű báziselemek száma nem függ a bázistól.

Tekintsük ezután a pontosan p^j-edrendű báziselemeket. Legyen az $\mathbf{a}_1, \ldots, \mathbf{a}_k$ bázis-elemek rendje nagyobb, mint p^j, az $\mathbf{a}_{k+1}, \ldots, \mathbf{a}_\ell$ báziselemek rendje pontosan p^j, míg a többieké kisebb, mint p^j. Legyen továbbá $A = G[p^{j-1}]$ és $H = G/A$. E faktorcsoport-nak generátorrendszerét alkotják a $[\mathbf{a}_1], \ldots, [\mathbf{a}_n]$ mellékosztályok. Tekintettel arra, hogy

$i > \ell$ esetén $p^{j-1}\mathbf{a}_i = \mathbf{o}$, ezért már az $[\mathbf{a}_1], \ldots, [\mathbf{a}_\ell]$ mellékosztályok is generátorrendszert alkotnak. Legyen $\sum_{i=1}^{\ell} c_i[\mathbf{a}_i] = [\mathbf{o}]$, azaz $\sum_{i=1}^{\ell} c_i\mathbf{a}_i \in A$, vagyis $\sum_{i=1}^{\ell} p^{j-1}c_i\mathbf{a}_i = \mathbf{o}$. A bázis függetlenségi tulajdonsága alapján ebből minden $i \leq \ell$ esetén $p^{j-1}c_i\mathbf{a}_i = \mathbf{o}$ adódik, és így $p^{n(i)}$ osztója $p^{j-1}c_i$-nek, tehát $p^{n(i)-j+1}$ osztója c_i-nek: $c_i = p^{n(i)-j+1}d_i$. Ezért $p^{j-1}c_i\mathbf{a}_i = p^{n(i)}\mathbf{a}_i = \mathbf{o}$, vagyis $c_i\mathbf{a}_i \in A$, azaz $[c_i\mathbf{a}_i] = [\mathbf{o}]$; bizonyítva az $[\mathbf{a}_1], \ldots, [\mathbf{a}_\ell]$ mellékosztályok függetlenségét. Tekintettel arra, hogy ebben a bázisban pontosan az $[\mathbf{a}_{k+1}], \ldots, [\mathbf{a}_\ell]$ elemek rendje p, ezért a tárgyalt speciális esetre vonatkozó eredmény alapján $\ell - k$ egyértelmű. ■

5.56. Következmény. *Egy véges Abel-csoport rendjében és exponensében ugyanazok a prímtényezők szerepelnek. Ha a G Abel-csoport exponense k, akkor a csoportnak van k-adrendű eleme. n-edrendű G Abel-csoportban pontosan akkor van p-edrendű elem, ha p osztója n-nek. G pontosan akkor ciklikus, ha n minden p prímosztójára $|G[p]| = p$.*

Bizonyítás. Tekintsük a G Abel-csoportnak az 5.54. tételben szereplő komponensekre való $G = G_1 + \cdots + G_r$ felbontását, ahol G_i exponense a G exponensében fellépő maximális p_i-hatvány. Az 5.53. tétel szerint G exponense a G_i-k exponenseinek a szorzata. Tekintettel arra, hogy $|G| = |G_1| \cdot \ldots \cdot |G_r|$, ezért az első állítást elég Abel-féle p-csoportokra bizonyítani. Legyen a H véges (kommutatív) p-csoport egy bázisa $\mathbf{a}_1, \ldots, \mathbf{a}_n$, ahol $o(\mathbf{a}_i) = p^{s(i)}$ és $s(1) \geq \ldots \geq s(n)$. Ekkor H exponense $p^{s(1)}$, míg rendje $p^{s(1)+\ldots+s(n)}$. Ha az eredeti $G = G_1 + \cdots + G_r$ felbontásban G_i exponense $p_i^{s_i}$, akkor tehát van olyan $\mathbf{a}^{(i)}$ eleme, amelynek rendje ugyancsak $p_i^{s_i}$. Mint láttuk, G exponense $k = p_1^{s_1} \cdot \ldots \cdot p_r^{s_r}$. E prímhatványok relatív prímek, amiből könnyen következik, hogy $\mathbf{a}^{(1)} + \cdots + \mathbf{a}^{(r)}$ rendje pontosan k. A további állítások ebből már könnyen adódnak; a bizonyítás végigvitelét az olvasóra bízzuk. ■

A véges Abel-csoportok alaptétele kiterjeszthető végesen generáltakra (mint ahogy az I. kötetben is láttuk). Itt a felbontásban végtelen ciklikus csoportok is fellépnek. A kommutativitás következtében a véges rendű elemek egy részcsoportot alkotnak, amelynek *torzió-részcsoport* a neve. Ha a G csoport végesen generált, akkor a $T(G)$ torzió részcsoport direkt összeadandó. A szerinte vett faktor *torziómentes* – azaz $\mathbf{o}$ az egyetlen véges rendű eleme. Ezt a $G/T(G)$ csoportot egyértelműen felbonthatjuk véges sok végtelen ciklikus csoport direkt összegére. $T(G)$ viszont végesen generált torziócsoport (tehát véges), ezért egyértelműen felbontható véges sok prímhatványrendű ciklikus csoport direkt összegére. Ha viszont a G csoport nem végesen generált, akkor $T(G)$ nem feltétlenül direkt összeadandó G-ben. Bizonyítható, hogy ha $p_1 < p_2 < \ldots < p_n < \ldots$ prímszámok, C_i p_i-edrendű (ciklikus) csoport és $G = \prod_{i=1}^{\infty}$ direkt szorzat, akkor $T(G)$ nem direkt összeadandó G-ben.

Mint a direkt szorzatnál már utaltunk rá, Abel-csoportok esetében a véges direkt szorzat megegyezik a direkt összeggel. A direkt összegnek is van egy „elvi" jellemzése, ami nagyon hasonlít a direkt szorzatéhoz. Ezt a következőképpen fogalmazhatjuk meg: *a direkt összeg a „legkisebb" olyan csoport, amely a tagokat függetlenül tartalmazza.* Ha tehát adottak a $\mu_i : A_i \to G$ injektív leképezések (ahol $G = \sum A_i$ a direkt összeg), akkor minden

$\nu_i : A_i \to H$ leképezésrendszerhez létezik olyan egyértelműen meghatározott $\varphi : G \to H$ homomorfizmus, amelyre $\varphi\mu_i = \nu_i$ teljesül bármely i esetében. Mivel ez a homomorfizmusrendszer mintegy duálisa az eredetinek, ezért *ko-szorzatnak* nevezik. Ennek jelölése $\coprod A_i$. Érdemes tudni, hogy míg a szorzat csoportok és Abel-csoportok esetében megegyezik, a ko-szorzat nem.

Feladatok

1. Az 5.45. tételben szereplő $\{\sigma_i : G^* \to G_i \mid i \in I\}$ univerzális rendszer esetében nem kívántuk meg, hogy a σ_i homomorfizmusok szürjektívek legyenek, noha ez a direkt szorzat esetében teljesül. Bizonyítsuk be, hogy a szürjektivitás következik a feltételekből.

2. Legyen $\varphi : G \to H$ homomorfizmus. Bizonyítsuk be, hogy $G \cong H \times K$ direkt szorzattal, ha van olyan $\psi : H \to G$ homomorfizmus, amelyre $\varphi\psi$ az identitás és $\text{Im } \psi \cap \text{Ker } \varphi = \{\mathbf{o}\}$. Mutassuk meg, hogy e két feltétel egyike sem hagyható el.

3. Legyen $\eta : G \to G$ idempotens endomorfizmus (azaz $\eta^2 = \eta$). Mutassuk meg, hogy $G \cong \text{Im } \eta \times \text{Ker } \eta$.

4. Bizonyítsuk be, hogy osztható Abel-csoportok direkt összege is és direkt szorzata is osztható Abel-csoport.

5. Bizonyítsuk be, hogy az egységgyökök multiplikatív csoportja osztható.

6. Bizonyítsuk be, hogy minden p prímszámhoz létezik osztható p-csoport.

7. Bizonyítsuk be, hogy minden Abel-csoportban az osztható részcsoportok generátuma is osztható.

8. Legyen a Q osztható csoport részcsoportja a G csoportnak. Bizonyítsuk be, hogy direkt összeadandó G-ben.

9. Legyen G kételemű csoport. Mint tudjuk, ekkor az Abel-csoportok körében ko-szorzatuk: $G + G$ egy négyelemű csoport. Bizonyítsuk be, hogy e ko-szorzatnak a csoportok körében végtelen sok eleme van.

10. Legyen G Abel-csoport, $H \leq G$. Bizonyítsuk be, hogy tetszőleges n természetes számra $H_n = \{\mathbf{x} \in G \mid n\mathbf{x} \in H\}$ részcsoport. Bizonyítsuk be, hogy $\bigcup_n H_n$ is részcsoport. Mi a feltétele annak, hogy $H_n = H$?

5.9. Speciális részcsoportok és normálosztók

Az eddigiekben már találkoztunk különféle struktúrák endomorfizmusaival, illetve automorfizmusaival. Vektorterek esetén ezek a lineáris transzformációk, illetve a reguláris lineáris transzformációk. Ezek a homomorfizmusok csoportoknál is fontos szerepet játszanak.

5.57. Tétel. *Egy G csoport összes endomorfizmusai a függvényszorzásra nézve egy $E(G)$ monoidot, automorfizmusai pedig ennek egy $A(G)$ részcsoportját alkotják. Azok a φ_a leképezések, amelyek a G csoport tetszőleges x elemét az axa^{-1} elemre képezik le, az $A(G)$-nek egy $B(G)$ normálosztóját alkotják; ennek elemeit belső automorfizmusoknak nevezzük. Az $a \to \varphi_a$ leképezés G-nek $B(G)$-re való szürjektív homomorfizmusa, amelynek C magját G centrumának nevezzük. C azokból az elemekből áll, amelyek G minden elemével felcserélhetők.*

A csoport centruma annyira fontos fogalom, hogy érdemes külön kimondani:

5.57/A. Definíció. Egy G csoport összes elemével felcserélhető elemeinek halmazát a csoport centrumának nevezzük. □

Bizonyítás. Tekintettel arra, hogy homomorfizmusok szorzata is homomorfizmus és az identitás is művelettartó, ezért $E(G)$ monoid. Mivel bijekciók szorzata és tetszőleges bijekció inverze is bijekció, ezért G tartóhalmazának összes, önmagára való bijekciója a függvényszorzásra nézve egy S_G csoportot alkot (egységeleme az identikus leképezés). Világos, hogy $A(G)$ az $E(G) \cap S_G$ részfélcsoportja. Azt kell még megmutatni, hogy $A(G)$-beli elem inverze is művelettartó. Mint az 5.36. tételben láttuk, elég a szorzattartást bizonyítani:

$$\varphi^{-1}(ab) = \varphi^{-1}(\varphi\varphi^{-1}(a)\varphi\varphi^{-1}(b)) = \varphi^{-1}(\varphi(\varphi^{-1}(a)\varphi^{-1}(b))) = \varphi^{-1}(a)\varphi^{-1}(b).$$

A belső automorfizmusokról először is azt kell kimutatni, hogy G-nek automorfizmusai. Itt is elég a szorzattartás bizonyítása, ami $a(xy)a^{-1} = axa^{-1}aya^{-1} = (axa^{-1})(aya^{-1})$ alapján igaz. Azt, hogy $B(G)$ csoport, bebizonyítjuk, ha megmutatjuk, hogy az $a \mapsto \varphi_a$ megfeleltetés homomorfizmus. Itt is csak a szorzattartást kell bizonyítani:

$$\varphi_{ab}(x) = (ab)x(ab)^{-1} = a(bxb^{-1})a^{-1} = \varphi_a(\varphi_b(x)).$$

Legyen most $\psi \in A(G)$ és tekintsük $B(G)$ tetszőleges φ_a elemét. Ekkor

$$\psi\varphi_a\psi^{-1}(x) = \psi(a\psi^{-1}(x)a^{-1}) = \psi(a)x(\psi(a)^{-1}) = \varphi_{\psi(a)}(x).$$

Így $\psi B(G)\psi^{-1} \leq B(G)$ tetszőleges $\psi \in A(G)$ esetén, tehát $B(G) \lhd A(G)$.

$g \in C$ azt jelenti, hogy φ_g az identikus automorfizmus, azaz tetszőleges $x \in G$ esetén $gxg^{-1} = x$, vagyis $gx = xg$; ami pontosan azt jelenti, hogy g minden G-beli x elemmel felcserélhető. ■

5.58. Definíció. A G csoport egy K komplexusának konjugáltjain a $\varphi_a(K)$ komplexusokat értjük. Ha K-nak egyetlen konjugáltja önmaga, akkor azt mondjuk, hogy K (a belső automorfizmusokra) invariáns. □

5.59. Tétel. *Az a reláció, amelyben minden komplexus a konjugáltjaival áll relációban, ekvivalenciareláció. Az a elemet tartalmazó $K(a)$ ekvivalenciaosztály (úgynevezett konjugált elemosztály) akkor és csak akkor egyelemű, ha a eleme a centrumnak. Egy részcsoport minden konjugáltja is részcsoport és a részcsoport akkor és csak akkor invariáns komplexus, ha normálosztó. Egy részcsoport összes konjugáltjainak metszete (illetve az általuk generált részcsoport) az adott részcsoportban levő legnagyobb (illetve az adott részcsoportot tartalmazó legkisebb) normálosztó. Invariáns részhalmazok közös része is invariáns; normálosztók közös része normálosztó.*

Bizonyítás. Mivel $B(G)$ részcsoport, ezért az identitás belső automorfizmus (egyébként φ_1-gyel egyenlő), és így a definiált reláció reflexív. $B(G)$-nek a szorzásra, illetve az invertálásra való zártságából pedig azonnal következik a reláció tranzitivitása és szimmetrikussága. $K(a)$ definíció szerint akkor és csak akkor egyelemű, ha bármely G-beli x-re $xax^{-1} = a$, azaz $xa = ax$, ami a centrum előbbi jellemzése szerint azt jelenti, hogy a eleme G centrumának. A részcsoportokra vonatkozó állítás azonnal következik abból, hogy tetszőleges homomorfizmus esetén egy részcsoport képe ismét részcsoport. $\varphi_a(K) = K$ azt jelenti, hogy $aK = Ka$, amiből azonnal következik, hogy a részcsoportok közül pontosan a normálosztók az invariáns komplexusok. Legyen most $H \leq G$, és az $N, M \lhd G$ csoportokra teljesüljön, hogy $N \leq H \leq M$. Ekkor tetszőleges $a \in G$ esetén

$$N = aNa^{-1} \leq aHa^{-1} \leq aMa^{-1} = M.$$

Ha tehát $\widetilde{N} = \bigcap\{aHa^{-1} \mid a \in G\}$ és $\widetilde{M} = \langle aHa^{-1} \mid a \in G\rangle$, akkor nyilván $N \leq \widetilde{N}$ és $\widetilde{M} \leq M$. Azt kell még belátni, hogy $\widetilde{N}$ és $\widetilde{M}$ mindegyike normálosztó. A konstrukció folytán mindkettő eleve részcsoport. Legyen $\mathcal{A}$ az aHa^{-1} részcsoportok halmaza. Mivel ezek a részcsoportok egymás konjugáltjai, ezért tetszőleges belső automorfizmus csupán permutálja e részcsoportokat. Eszerint belső automorfizmusnál $\mathcal{A}$ nem változik meg. Ekkor viszont közös részük és generátumuk sem változik; tehát $\widetilde{N}$ is és $\widetilde{M}$ is invariáns.

Ha a eleme egy K invariáns részhalmaznak, akkor definíció szerint K tartalmazza a minden konjugáltját, azaz $K(a) \subseteq K$. Így, ha $\{K_i \mid i \in I\}$ invariáns részhalmazok rendszere és $a \in \bigcap\{K_i \mid i \in I\}$, akkor $K(a) \subseteq \bigcap\{K_i \mid i \in I\}$, ezért $\bigcap\{K_i \mid i \in I\}$ is invariáns. Ebből azonnal adódik, hogy normálosztók közös része is normálosztó. ■

A G csoport normálosztóin, azaz a $B(G)$-invariáns részcsoportjain kívül fontos szerepet játszanak az $A(G)$- és $E(G)$-invariáns részcsoportok is.

5.60. Definíció. A G csoport egy H részcsoportját karakterisztikus (teljesen karakterisztikus) részcsoportnak nevezzük, ha H-t a G minden automorfizmusa (endomorfizmusa) H-ba viszi.

A részcsoport definíciójából azonnal világos, hogy egy G csoport valamely H részcsoportjának bármely K részcsoportja az eredeti csoportnak is részcsoportja. A normálosztókra vonatkozó megfelelő állítás általában nem igaz, mert K nem feltétlenül invariáns G *összes* belső automorfizmusára. Ezt figyelembe véve adódik:

5.61. Tétel. *Ha $N \lhd G$ és H karakterisztikus részcsoportja N-nek, akkor $H \lhd G$.*

Bizonyítás. $H \leq G$ igaz, ezért csak azt kell belátni, hogy bármely $a \in G$ esetén $\varphi_a(H) \subseteq H$. Mivel $N \lhd G$, ezért φ_a az N-nek automorfizmusa. Tekintettel arra, hogy H

karakterisztikus részcsoportja N-nek, ezért a φ-nek N-re való megszorítása H-t önmagába viszi. ■

5.62. Definíció. Legyen $a, b \in G$. Az $[a;b] = aba^{-1}b^{-1}$ elemet az a és b kommutátorának nevezzük. Ha A és B a G-nek részcsoportjai, akkor ezek $[A;B]$ kölcsönös kommutátorcsoportján az $\{[a;b] \mid a \in A, b \in B\}$ halmaz generálta részcsoportot értjük. A $\widetilde{G} = [G;G]$ részcsoportot a G kommutátor-részcsoportjának nevezzük. □

Az alábbiakban a kommutátorok néhány elemi tulajdonságát bizonyítjuk be.

5.63. Tétel. *A G csoport kommutátorainak a halmaza az inverzképzésre zárt teljesen karakterisztikus komplexus.* $[a;b] = 1$ *akkor és csak akkor teljesül, ha a és b felcserélhetők. Ha* $A, B \lhd G$, $a \in A$, $b \in B$, *akkor* $[a;b] \in A \cap B$.

$[uv;b] = \varphi_u([v;b]) \cdot [u;b]$; *ha u és b felcserélhetők, akkor* $[v;b]$ *eleme az uv generálta normálosztónak.*

Bizonyítás. Legyen $\psi \in E(G)$. A művelettartás alapján

$$\psi([a;b]) = \psi(aba^{-1}b^{-1}) = \psi(a)\psi(b)\psi(a)^{-1}\psi(b)^{-1} = [\psi(a);\psi(b)].$$

Emellett $[a;b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b;a]$; ami bizonyítja az első állítást. A második állítás azonnal adódik a nyilvánvaló $ab = [a;b] \cdot ba$ összefüggésből. Mivel B normálosztó, ezért $aba^{-1} \in B$, így $[a;b] \in BB^{-1} = B$. Hasonlóan adódik, hogy $[a,b] = [b,a]^{-1} \in A$.

A következő állítás számolással látható be:

$$[uv;b] = uvbv^{-1}u^{-1}b^{-1} = u(vbv^{-1}b^{-1})u^{-1}(ubu^{-1}b^{-1}) = \varphi_u([v;b]) \cdot [u;b].$$

Ha u és b felcserélhetők, akkor $[u;b] = 1$ miatt $[v;b]$ az $[uv;b]$ konjugáltja; ami benne van az uv-t tartalmazó bármely normálosztóban. ■

Megjegyezzük, hogy a tétel utolsó állítását csak a szimmetrikus csoport normálláncának a vizsgálatánál fogjuk használni.

5.64. Tétel. *A G csoport G' kommutátor-részcsoportja (teljesen) karakterisztikus. G/N akkor és csak akkor kommutatív, ha $G' \leq N$.*

Bizonyítás. Az 5.63. tétel szerint a kommutátorok halmaza teljesen karakterisztikus és zárt az inverzképzésre. Mivel szorzat endomorf képe az endomorf képek szorzata, ezért a kommutátorok generálta részcsoport is teljesen karakterisztikus. Legyen most $\varphi : G \to H$ tetszőleges homomorfizmus. φ akkor és csak akkor képezi le G'-t a H egységelemére, ha G' egy generátorrendszerét – például a kommutátorok halmazát – a H egységelemére képezi. $\varphi([a;b]) = [\varphi(a);\varphi(b)]$ miatt ez pontosan akkor teljesül, ha bármely $a, b \in G$ esetén $\varphi(a)\varphi(b) = \varphi(b)\varphi(a)$, azaz ha Im φ kommutatív. ■

Megjegyezzük, hogy a kommutátorok szorzata általában nem kommutátor.

5.65. Tétel. *Bármely csoportban a centrum karakterisztikus részcsoport.*

Bizonyítás. Azt kell megmutatni, hogy a csoport bármely φ automorfizmusa minden c centrumelemet ugyancsak centrumelembe visz, azaz, hogy $\varphi(c)$ a csoport minden x elemével felcserélhető. Mivel φ-nek létezik inverze, ezért $x = \varphi(\varphi^{-1}(x))$, amiből

$$\varphi(c)x = \varphi(c)\varphi(\varphi^{-1}(x)) = \varphi(c\varphi^{-1}(x)) = \varphi(\varphi^{-1}(x)c) = x\varphi(c)$$

következik. ■

A kommutátorcsoporttal ellentétben, a centrum általában nem teljesen karakterisztikus, mert nem minden endomorfizmus képez le minden centrumelemet centrumelembe.

5.66. Tétel. *Ha egy csoportnak a centrum szerinti faktorcsoportja ciklikus, akkor a csoport kommutatív – és így a faktorcsoport csak egyelemű lehet.*

Bizonyítás. Legyen C a G csoport centruma, és legyen aC a faktorcsoport generátoreleme. Ekkor a faktorcsoport elemei az a^iC alakú mellékosztályok (i egész szám). Így a csoport minden eleme felírható (nem feltétlenül egyértelműen) a^ic alakban (i egész szám és c centrumelem). Legyen a^jd a csoport egy másik eleme (j egész szám és d centrumelem). Mivel egy elem hatványai egymással, a centrumelemek pedig minden csoportelemmel felcserélhetők, ezért:

$$(a^ic)(a^jd) = a^i(ca^j)d = (a^ia^j)(cd) = (a^ja^i)(dc) = (a^jd)(a^ic),$$

ami éppen azt jelenti, hogy a csoport kommutatív. Így a centruma önmaga, tehát a centrum szerinti faktor egyelemű. ■

5.67. Következmény. *Tetszőleges G csoport automorfizmuscsoportja csak akkor lehet páratlan rendű ciklikus, ha egyelemű; speciálisan az automorfizmuscsoport rendje nem lehet páratlan prímszám.*

Bizonyítás. Tegyük fel, hogy a G csoportnak az $A(G)$ automorfizmuscsoportja páratlan rendű ciklikus csoport. Az 5.17. tétel szerint ekkor $B(G)$ is ciklikus. Mivel $B(G)$ izomorf a centrum szerinti faktorcsoporttal, ezért a 5.66. tétel alapján egyelemű, vagyis G kommutatív. Elég tehát azt kimutatni, hogy kommutatív csoport automorfizmuscsoportja csak akkor lehet páratlan rendű, ha az automorfizmuscsoport egyelemű. Ehhez viszont Lagrange tétele alapján elég annak a megmutatása, hogy ha egy kommutatív csoportnak van nem triviális automorfizmusa, akkor van másodrendű is.

Kommutatív csoportok esetében a $\varphi(a) = a^{-1}$ megfeleltetés automorfizmus, amelynek a négyzete az identitás. Ha φ nem az identitás, akkor tehát egy másodrendű automorfizmus, így készen vagyunk. Azt az esetet kell még megnézni, amikor G minden eleme megegyezik az inverzével, azaz $a \in G$ esetén $a^2 = 1$. Ha G-nek legfeljebb két eleme van, akkor egyetlen automorfizmusa az identitás. Egyébként G legalább kétdimenziós vektortér a kételemű $\mathbb{Q}_2$ test felett. Ekkor az a megfeleltetés, amely az első két báziselemet felcseréli, a többit változatlanul hagyja, kiterjeszthető egy reguláris lineáris transzformációvá (azaz G egy automorfizmusává), amelynek a négyzete önmaga – tehát másodrendű.

A speciális állítás azonnal adódik abból, hogy prímrendű csoport ciklikus. ■

Megjegyezzük, hogy a tétel bizonyításában nem kellene feltétlenül a vektorterekre hivatkozni; a fenti bizonyítás átírható csoportelméleti bizonyításra; de a Teichmüller–Tukey-lemmát fel kell használni. (Persze erre a vektortereknél is szükség van.)

Egy csoport részcsoportjai általában nem invariánsak. Lehet azonban találni olyan részcsoportokat, amelyekben egy-egy kiválasztott részcsoport „még éppen” invariáns. Ezt a fogalmat tetszőleges komplexusra lehet – és célszerű – vizsgálni.

5.68. Definíció. Legyen K a G csoport tetszőleges komplexusa. K normalizátorán az

$$N(K) = \{a \in G \mid aK = Ka\}$$

halmazt értjük. K centralizátorának nevezzük a

$$C(K) = \left\{\bigcap N(a) \mid a \in K\right\}$$

halmazt, azaz a K minden egyes elemével felcserélhető elemek halmazát. □

5.69. Tétel. *Egy G csoport bármely K komplexusára $N(K)$ és $C(K)$ a G-nek részcsoportja. Ha $K \subseteq N(K)$, illetve $K \subseteq C(K)$, akkor $N(K)$, illetve $C(K)$ a maximális olyan részcsoport, amelyben K invariáns részhalmaz, illetve amelynek a centruma tartalmazza K-t.*

Ha K egyelemű vagy K részcsoport, akkor teljesül a $K \subseteq N(K)$ feltétel.

Bizonyítás. Ha $aK = Ka$ és $bK = Kb$, akkor $(ab)K = a(bK) = a(Kb) = (aK)b = (Ka)b = K(ab)$ alapján $N(K)$ zárt a szorzásra. $a^{-1}K = a^{-1}(Ka)a^{-1} = a^{-1}(aK)a^{-1} = Ka^{-1}$ miatt $N(K)$ az inverzképzésre is zárt; és a triviális $1K = K1$ összefüggés következtében $N(K)$ csoport. $C(K)$ tehát csoportok közös része és ezért ugyancsak csoport. Ha K egy H részcsoportnak invariáns részhalmaza, akkor bármely H-beli a-ra $aKa^{-1} \subseteq K$ és $a^{-1} \in H$ miatt $a^{-1}Ka \subseteq K$; és így $aK = Ka$, tehát $H \subseteq N(K)$. Ahhoz, hogy K invariáns részhalmaz legyen az $N(K)$-ban, természetesen szükséges a $K \subseteq N(K)$ feltétel. A $K \subseteq C(K)$ feltételből következik, hogy K-nak bármelyik két eleme felcserélhető egymással. Ha K benne van egy H részcsoport centrumában, akkor H minden eleme benne van $C(K)$-ban.

A $K \subseteq N(K)$ azt jelenti, hogy minden $a \in K$ esetén $aK = Ka$. Ez pedig akkor is igaz, ha K egyelemű és akkor is, ha részcsoport. ■

5.70. Tétel. *Ha G véges csoport, $a \in G$, akkor $|K(a)| = (G : N(a))$, ahol $K(a)$ az a konjugáltjaiból álló komplexus és $N(a)$ az a normalizátora.* (Megjegyezzük, hogy a tétel általánosabban is igaz.)

Bizonyítás. A G csoport elemei között egy G-beli a-tól függő relációt vezetünk be: $x \sim y$ akkor és csak akkor, ha $xax^{-1} = yay^{-1}$. Ez a reláció nyilvánvalóan reflexív, szimmetrikus és tranzitív. A definíció alapján az is világos, hogy a relációnak megfelelő osztályozásban az osztályok száma megegyezik $K(a)$ elemszámával. Az $xax^{-1} = yay^{-1}$ feltétel nyilvánvalóan ekvivalens az $y^{-1}xa = ay^{-1}x$ feltétellel. Ez utóbbi viszont – definíció szerint – pontosan akkor teljesül, ha $y^{-1}x \in N(a)$. Az 5.18. és az 5.19. tételek alapján a kapott osztályozás osztályai éppen az $N(a)$ szerinti bal oldali mellékosztályok, amelyeknek a száma – ugyancsak definíció szerint – $(G : N(a))$. ■

Az automorfizmusok felhasználásával lehetőség nyílik egy hasznos és fontos csoportkonstrukció megadására. Az első izomorfizmustételnél láttuk, hogy $N \lhd G$ és $H \leq G$

esetében $\langle N, H\rangle = NH$. Ha H is normálosztó és $N \cap H = \{1\}$, akkor a $G = NH$ speciális esetben $G = N \times H$ (direkt szorzat). Ekkor, mint láttuk, N felcserélhető H minden elemével. Ha viszont H nem normálosztó, akkor $h \in H$ esetén h csak az N komplexussal cserélhető fel, elemeivel nem. Ezért az $x \mapsto hxh^{-1}$ megfeleltetés az N elemeinek egy automorfizmusát adja, amelyik általában nem identikus.

5.71. Definíció. Ha $N \lhd G$, $H \leq G$, $G = HN$ és $N \cap H = \{1\}$, akkor azt mondjuk, hogy G az N-nek és a H-nak szemidirekt (féldirekt) szorzata. Erre a $G = N \rtimes H$ jelölést használjuk.

Ha $H \leq G$ és létezik olyan $N \lhd G$, amire G az N és a H féldirekt szorzata, akkor N-et a H normál komplementumának nevezik. □

Megjegyzések. 1. Felhívjuk a figyelmet arra, hogy az elnevezés nem szimmetrikus, elöl a normálosztó szerepel, a részcsoport a második. Ezt a jelölés is mutatja: $\rtimes$ a $>$ és az $\lhd$ jelekből van előállítva ($> \lhd$); bal oldalra mutat a normálosztójel, jobb oldalra a részcsoportjel.

2. A fenti jelölés még hiányos, mert nincs megadva, miképpen „hatnak” H elemei az N normálosztón. □

A féldirekt szorzat fenti definíciója „belső” definíciónak tekinthető. Mivel konstrukcióról van szó, ezért meg kell adni, hogy adott csoportokból miképpen állíthatunk elő féldirekt szorzatot.

5.72. Tétel. *Legyenek adva az A és a B csoportok és legyen $\varphi : B \to A(A)$ tetszőleges homomorfizmus ($A(A)$ jelöli az A automorfizmuscsoportját).*

Tekintsük az adott csoportok tartóhalmazának $A \times B$ direkt szorzatát. E szorzaton definiálja a szorzást $(a, b) \times (c, d) = (a\varphi_b(c), bd)$, ahol φ_b a b elemnek φ-nél vett képe. Legyen N az $(a, 1)$ alakú és H az $(1, b)$ alakú elemek halmaza.

Ekkor G a fenti műveletekre nézve csoport, $N \lhd G$, $H \leq G$, $G = N \rtimes H$, $A \cong N$, $B \cong H$, φ_b az $(1, b)$ elemmel való konjugálás, és A, B, φ egyértelműen meghatározzák G-t.

Bizonyítás. A szorzás definíciója szerint az

$$[(a, b)(c, d)](e, f), \qquad \text{illetve az} \qquad (a, b)[(c, d)(e, f)]$$

szorzatra

$$(a\varphi_b(c)\varphi_{bd}(e), bdf), \qquad \text{illetve} \qquad (a\varphi_b(c\varphi_d(e)), bdf)$$

adódik. Mivel φ homomorfizmus, ezért $\varphi_{bd} = \varphi_b\varphi_d$. Mivel φ_b az A-nak izomorfizmusa, ezért $\varphi_b(c\varphi_d(e)) = \varphi_b(c)\varphi_b(\varphi_d(e))$. Így mindkét szorzat $(a\varphi_b(c)\varphi_b(\varphi_d(e)), bdf)$; G tehát félcsoport. Triviálisan látható, hogy $(1, 1)$ a G-nek egységeleme és (a, b) (jobb oldali) inverze $(\varphi_b^{-1}(a^{-1}), b^{-1})$. G tehát csoport.

Mivel φ homomorfizmus és $A(A)$-ba képez, ezért N is és H is részcsoport. $(a, 1)(1, b) = (a, b)$ miatt $G = NH$ és $N \cap H = \{1\}$, hiszen $(a, 1) = (1, b)$ csak úgy lehet, hogy $a = 1$ és $b = 1$. Az N elemeivel való konjugálás N-et önmagába viszi. $G = NH$ alapján az $(1, b)(a, 1)(1, b)^{-1} = (\varphi_b(a), 1)$ összefüggésből következik, hogy N normálosztó. Ezzel azt is beláttuk, hogy $G = N \rtimes H$. A legutóbbi összefüggés azt is megmutatja, hogy N-nek az $(1, b)$ elemmel való konjugálása ugyanaz, mint a b elemhez tartozó automorfizmusa.

G (izomorfizmustól eltekintett) egyértelműsége abból következik, hogy a G-beli elemeket és műveleteket A, B és φ egyértelműen meghatározzák. ■

Az 5.72. tétellel leírt esetben is használni fogjuk a féldirekt szorzat elnevezést és a $\rtimes$ jelölést is. Amennyiben nem csak azt akarjuk kifejezni, hogy a G csoport féldirekt szorzat, akkor a $\varphi : B \to A(A)$ homomorfizmus megadására is szükség van. Ekkor az $A \rtimes_\varphi B$ jelölést használjuk.

Feladatok

1. Legyen $H \leq G$. Bizonyítsuk be, hogy van olyan $\widetilde{H} \leq G$, hogy H bal oldali mellékosztályainak a halmaza megegyezik $\widetilde{H}$ jobb oldali mellékosztályainak a halmazával.

2. Igaz-e az, hogy egy Abel-csoport minden részcsoportja karakterisztikus? Igaz-e az, hogy minden karakterisztikus részcsoportja teljesen karakterisztikus?

3. Legyen $H \leq G$. Igaz-e, hogy H karakterisztikus részcsoportja $N(H)$-nak? Igaz-e az, hogy $N(N(H)) = N(H)$?

4. Mutassuk meg, hogy (teljesen) karakterisztikus részcsoportok generálta részcsoport szintén (teljesen) karakterisztikus.

5. Legyen Z végtelen ciklikus csoport. Határozzuk meg $A(Z)$-t és $E(Z)$-t.

6. Legyen Z végtelen ciklikus csoport és G tetszőleges csoport. Mi lehet a $Z \rtimes G$?

7. Legyen Q a racionális számok additív csoportja. Határozzuk meg $A(Q)$-t és $E(Q)$-t.

8. Legyen Q a racionális számok additív csoportja és G véges csoport. Határozzuk meg $Q \rtimes G$-t.

9. Legyen Q a racionális számok additív csoportja. Határozzuk meg $Q \rtimes Q$-t.

10. Bizonyítsuk be, hogy az n-edrendű ciklikus csoport automorfizmuscsoportja izomorf a modulo n vett redukált maradékosztályok multiplikatív csoportjával. Mivel izomorf e csoport endomorfizmusmonoidja?

11. Bizonyítsuk be, hogy egy csoport automorfizmuscsoportja nem lehet a végtelen ciklikus csoport.

12. Bizonyítsuk be, hogy egy G csoport a és b elemei pontosan akkor konjugáltak, ha van olyan $x, y \in G$, amire $a = xy$ és $b = yx$.

13. Mely csoport(ok) automorfizmuscsoportja egyelemű?

5.10. Sylow-részcsoportok

Míg a véges Abel-csoportok alaptétele e csoportoknak egy, szinte teljes leírását adja, a véges nemkommutatív csoportok szerkezete igen bonyolult. Nagyon komoly segédeszközökre volt például ahhoz szükség, hogy Feit és Thompson bebizonyítsák Burnside-nak azt a sejtését, hogy minden páratlan rendű csoport feloldható. (A feloldhatóság definícióját a 6. pontban adjuk meg.)

A véges csoportok szerkezetének vizsgálatánál általában azt szokták megnézni, hogy bizonyos speciális típusú részcsoportjaikról mit lehet mondani. Ezek közül a legfontosabbak a csoportnak azok a részcsoportjai, amelyek p-csoportok. Vizsgálatainkat egy egyszerű, de meglepő tétellel kezdjük.

5.73. Tétel. *Ha a G csoport rendje osztható a p^k prímhatvánnyal, akkor vagy van a csoportnak olyan valódi részcsoportja, amelynek a rendje osztható p^k-val, vagy a csoport centrumában van p-edrendű elem.*

Bizonyítás. Legyen $|G| = n$, és a csoport C centrumának a rendje m. Az 5.59. tétel szerint G felbomlik diszjunkt konjugált elemosztályok egyesítésére, amelyek közül pontosan azok egyeleműek, amelyekben ez az elem a centrumban van. Legyenek $a_1, \ldots, a_r$ a G-nek olyan centrumon kívüli elemei, amelyek egymásnak nem konjugáltjai, legyenek az ehhez tartozó konjugált elemosztályok $K(a_1), \ldots, K(a_r)$, és legyen ezeknek a rendje, sorra $k_1, \ldots, k_r$. Ekkor a következő úgynevezett *osztályegyenletet* kapjuk:

$$n = m + k_1 + \cdots k_r.$$

Az 5.70. tétel szerint minden i-hez van a G-nek olyan H_i részcsoportja, amelyre $(G : H_i) = k_i$. ($H_i \neq G$, mert a_i nem eleme a centrumnak.) Ha ezek között a k_i számok között valamelyik nem osztható p-vel, akkor a Lagrange-tételből adódó $|G| = k_i \cdot |H_i|$ összefüggés alapján H_i rendje osztható p^k-val; és így az első lehetőség áll fenn. Ha viszont p minden egyes k^i-nek osztója, akkor a felírt egyenlőségből $p \mid n$ alapján $p \mid m$ következik. Mivel a centrum kommutatív, ezért alkalmazhatjuk az 5.56. következményt, aminek alapján van a centrumnak p-edrendű eleme. ■

5.74. Következmény. *Legyen $|G| = n$.*

(1) *Ha $p \mid n$, akkor G-ben van p-edrendű elem (Cauchy tétele).*

(2) *Ha G p-csoport, akkor n p-nek hatványa.*

(3) *Minden nemtriviális p-csoportnak van nemtriviális centruma.*

(4) *Minden nemtriviális p-csoportban van p indexű normálosztó.*

(5) *Minden p^2-rendű csoport kommutatív.*

Bizonyítás. Az (1) állítás p-edrendű csoportra triviálisan igaz. Tegyük fel, hogy igaz az állítás minden olyan csoportra, amelynek rendje kisebb, mint n. Az 5.73. tétel szerint tehát vagy van a csoportnak olyan részcsoportja, amely tartalmaz p-edrendű elemet, vagy a csoport centrumában van ilyen elem. Ebből azonnal következik (2) is, ugyanis p-csoportban egyetlen elem rendje sem lehet p-től különböző prímszám, tehát G rendje nem lehet osztható p-től különböző prímszámmal. Így egy (véges) p-csoport rendje p^k alakú.

Ha G rendje p^k, akkor egyetlen G-től különböző részcsoport rendje sem lehet p^k-val osztható, így a 5.73. tételben szereplő minden egyes k_i osztható p-vel, tehát a centrum rendje is osztható p-vel. Tekintettel arra, hogy a centrumnak van eleme (nevezetesen az egységelem), ezért a centrumnak legalább p eleme van, tehát nem triviális. (Abból, hogy m a p-nek hatványa, ez még nem következik, mert $1 = p^0$ is lehet.)

Ezek szerint $|G| = p^k$. A (4) állítást k-ra vonatkozó teljes indukcióval bizonyítjuk. $k = 1$ esetben az állítás triviálisan igaz. Ha G Abel csoport, akkor az 5.52. tétel szerint van p-hatványrendű ciklikus faktora, amelynek van p-edrendű faktora; ami a második izomorfizmustétel szerint G-nek is p-edrendű faktora; s ennek magja p indexű. Ha G nem kommutatív, akkor C centruma különbözik tőle, s a $\widetilde{G} = G/C$ faktorcsoport nem egyelemű, tehát rendje p^m alakú, ahol $1 < m < k$. A teljes indukciós feltétel szerint tehát $\widetilde{G}$-ben létezik olyan $\widetilde{H}$ normálosztó, amelynek indexe p. Legyen $\varphi : G \to \widetilde{G}$ a természetes homomorfizmus és legyen H a $\widetilde{H}$ teljes inverz képe. Ekkor az 5.42. tétel szerint $H \lhd G$ és a második izomorfizmustétel alapján $[G : H] = (\widetilde{G} : \widetilde{H}) = p$. A (3) állítás szerint G-nek van nemtriviális centruma. Így egy p^2-rendű csoport centrum szerinti faktorcsoportja vagy egyelemű vagy p elemű. Tekintettel arra, hogy p elemű csoport ciklikus és a centrum szerinti faktorcsoport nem lehet valódi ciklikus, ezért a csoport megegyezik a centrumával, vagyis kommutatív. ■

5.75. Tétel. *Tetszőleges, véges G csoportra érvényesek az alábbiak:*

(1) *Ha p^k osztója a csoport rendjének, akkor a csoportnak van p^k-rendű részcsoportja.*

(2) *Ha p osztója G rendjének, akkor G-nek vannak p-Sylow részcsoportjai, azaz olyan p-csoportjai, amelyeknek indexe nem osztható p-vel. (Sylow I. tétele)*

(3) *G p-Sylow részcsoportjainak a száma kongruens 1-gyel modulo p. (Sylow II. tétele)*

(4) *G-ben a rögzített p-hez tartozó p-Sylow részcsoportok egymás konjugáltjai. (Sylow III. tétele)*

(5) *G minden olyan részcsoportja, amely p-csoport, benne van G egy p-Sylow részcsoportjában.*

A Sylow-részcsoport is igen fontos fogalom, ezt is célszerű külön kimondani:

5.75/A. Definíció. Tetszőleges p prímszám esetén a G csoport egy P részcsoportját a G egy p-Sylow részcsoportjának nevezzük, ha P p-csoport, és indexe nem osztható p-vel. (Ez utóbbi azt jelenti, hogy maximális lehetséges p-hatvány.)

Bizonyítás. Először a (2) állítást bizonyítjuk, a G csoport rendjére vonatkozó teljes indukcióval. Ha ez a rend p-nél kisebb, akkor $\{1\}$ a G-nek p-Sylow részcsoportja. Legyen $|G| \geq p$, és tegyük fel, hogy az állítás igaz minden olyan csoportra, amelynek a rendje kisebb, mint $|G|$. Ha G-nek van olyan valódi részcsoportja, amelynek az indexe nem osztható p-vel, akkor ennek a részcsoportnak az indukciós feltevés értelmében létezik p-Sylow részcsoportja, amely – az indexre kirótt megkötés miatt – G-nek is p-Sylow részcsoportja. Ha ilyen részcsoportja nincs G-nek, akkor az 5.73. tétel szerint G centrumában van p-edrendű elem. Az ezen elem generálta H részcsoport csak centrumelemekből áll, így normálosztó, és H rendje p. Ha $|G| = p^k n$, ahol $p \nmid n$, akkor $|G/H| = p^{k-1} n$, és

e faktorcsoportnak a feltevés szerint van p-Sylow részcsoportja, amelynek a rendje p^{k-1}. E részcsoport K teljes inverz képére a $H \leq K$ és $|K/H| = p^{k-1}$ feltételek alapján $|K| = p^k$ következik, ami azt jelenti, hogy K a G-nek egy p-Sylow részcsoportja.

Mivel egy p-Sylow részcsoport rendje a maximális olyan p-hatvány, amely osztója a csoport rendjének, ezért az (1) állítást elegendő p-csoportokra bizonyítani. Sőt, elég csak azt kimutatni, hogy minden véges p-csoportnak van p indexű részcsoportja, mert ennek többszöri alkalmazásával kaphatjuk, hogy bármilyen p-hatványrendű részcsoport létezik. Ilyen részcsoport az 5.74. következmény (4) állítása szerint létezik.

A további állítások bizonyítása előtt négy lemmát bizonyítunk be.

1. Lemma. *Ha G-nek a P p-Sylow részcsoportja G-ben normálosztó, akkor minden $Q \leq G$ p-csoport része P-nek.*

Az első izomorfizmustétel szerint $PQ/P \cong Q/(P \cap Q)$, amiből $|PQ| = |P| \cdot |Q/(P \cap Q)|$ következik. Mivel p-hatványrendű csoport faktorcsoportja is p-hatványrendű, ezért a jobb oldalon két p-hatvány szorzata áll. Így PQ is egy G-beli p-csoport. Mivel P egy p-Sylow részcsoport, ezért PQ rendje nem lehet P rendjénél nagyobb, amiből $Q = P \cap Q$ következik; ez bizonyítja a lemma állítását.

2. Lemma. *Ha P a G-nek p-Sylow részcsoportja, és Q egy G-beli p-csoport, akkor $N(P) \cap Q = P \cap Q$. ($N(P)$ a P normalizátora).*

Az nyilvánvaló, hogy $P \cap Q$ része a $Q_1 = N(P) \cap Q$ részcsoportnak. Mivel $P \lhd N(P)$ és Q_1 – mint a Q p-csoport része – p-csoport $N(P)$-ben, ezért az 1. lemma szerint $Q_1 \leq P$. Ezt a triviális $Q_1 \leq Q$ tartalmazással összevetve adódik a lemma állítása.

3. Lemma. *Legyen $Q \leq G$ p-csoport. Ekkor a P G-beli p-Sylow részcsoport Q-beli elemekkel vett különböző konjugáltjainak a száma $(Q : Q \cap P)$.*

Az 5.70. tétel bizonyításához hasonlóan látható be, hogy a G csoport x és y elemeivel való konjugálás akkor és csak akkor adja egy H részcsoportnak ugyanazt a konjugáltját, ha ugyanabban az $N(H)$ szerinti mellékosztályban vannak. Esetünkben a P konjugáltjait vizsgáljuk. Mivel csak Q elemeivel konjugálunk, ezért az $y^{-1}x \in N(P)$ feltétel mellett $y^{-1}x \in Q$ is teljesül. Így a különböző konjugáltak száma megegyezik $N(P) \cap Q$-nak a Q-beli indexével. Ez pedig a 2. lemma szerint éppen $(Q : P \cap Q)$.

4. Lemma. *Legyen $\mathcal{P} = \{P_1, \ldots, P_s\}$ a G p-Sylow részcsoportjainak olyan halmaza, amely minden benne levő részcsoporttal együtt annak összes konjugáltját tartalmazza. Tegyük fel továbbá, hogy a Q G-beli p-csoport $\mathcal{P}$ elemei közül pontosan t-nek része. Ekkor $s \equiv t \pmod{p}$.*

Osztályozzuk $\mathcal{P}$ elemeit aszerint, hogy Q elemeivel konjugálva egymásba vihetők-e. A 3. lemma szerint a P_i-t tartalmazó osztály elemszáma $(Q : Q \cap P_i)$. Ez a szám mindig p-nek hatványa, és pontosan akkor 1, ha $Q \cap P_i = Q$, azaz $Q \leq P_i$. Elhagyva tehát $\mathcal{P}$ elemeiből azt a t darabot, amelyek Q-t tartalmazzák, a fennmaradók olyan osztályokba sorolhatók, amelyek elemszáma mindig osztható p-vel. Így p osztója $(s-t)$-nek, ami éppen a bizonyítandó összefüggést adja.

Az 5.75. tétel bizonyításának a folytatásához tekintsünk most egy, a 4. lemmában leírt rendszert. Ha Q-nak a $\mathcal{P}$ valamelyik elemét választjuk, akkor a 4. lemma szerint $s \equiv 1 \pmod{p}$, hiszen a kiválasztott p-Sylow részcsoportot egyedül önmaga tartalmazza. Ha mármost két, a feltételnek eleget tevő, $\mathcal{P}_1$ és $\mathcal{P}_2$ rendszer volna, megfelelően s_1 és s_2 elemmel, akkor $1 \equiv (s_1 + s_2) \equiv 1 + 1 \pmod{p}$ lenne, hiszen a két rendszer egyesítése is eleget tesz a kirótt feltételnek. Mivel a kapott kongruencia soha sem állhat fenn, ezért igaz (4), és így automatikusan (3) is.

Vegyük most G p-Sylow részcsoportjainak halmazát. Ezek közül a Q p-csoportot tartalmazók t számára $t \equiv s \equiv 1 \pmod{p}$ teljesül, ami igazolja az 5. állítást is. ■

5.11. Néhány speciális csoport

A Sylow-tételek lehetőséget adnak adott elemszámú csoportok meghatározására. Ha e tételek segítségével meghatároztuk, milyen lehet egy csoport szerkezete, akkor valamilyen módszerrel meg kell konstruálni a szóba jövő csoportokat (ha léteznek). Jelenleg egy ilyen konstrukciós módszer van a kezünkben: a szemidirekt szorzat (ez persze magában foglalja a direkt szorzatot is). A későbbiekben más csoport-előállítási módszereket is fogunk tárgyalni. Az alábbiakban megmutatjuk, miképpen használhatók a Sylow-tételek. Ezek segítségével tárgyaljuk a húsznál kevesebb elemű csoportokat. A leírásban természetesen csak izomorfizmustól eltekintve soroljuk fel őket.

Lagrange tétele alapján tudjuk, hogy prímrendű (és egyelemű) csoport mindig ciklikus, tehát egyértelmű. Az 5.74. következmény szerint p^2-rendű csoport kommutatív. A véges Abel-csoportok alaptételéből következik, hogy p^2-rendű csoport kétféle lehet, ciklikus vagy két p-rendű csoport direkt szorzata. Így a következőket tudjuk:

Egy olyan csoport van, amelynek a rendje $1, 2, 3, 5, 7, 11, 13, 17, 19 \ldots$.

Két olyan csoport van, amelynek a rendje $4, 9, \ldots$.

A legkisebb természetes szám, amelyik kimaradt, a 6. A hatelemű csoportok leírása helyett rögtön a $2p$ elemszámú csoportokat vizsgáljuk meg, ahol p tetszőleges páratlan prímszám. Legyen G egy ilyen csoport, és legyen P a G-nek p-Sylow részcsoportja. $(G : P) = 2$ miatt $P \lhd G$. Mivel $|P| = p$ prímszám, ezért azt is tudjuk, hogy P ciklikus, $P = \langle a \rangle$. Cauchy tétele szerint G-nek van egy másodrendű b eleme. $2 \nmid p$ miatt $b \notin P$. Mivel P normálosztó, ezért $bPb^{-1} = P$, vagyis alkalmas k egész számra $bab^{-1} = a^k$ $(0 \leq k < p)$. Így

$$a = (b^2)a(b^{-1})^2 = b(bab^{-1})b^{-1} = ba^k b^{-1} = b(ab^{-1})^k = a^{k^2}.$$

Az elem rendjének a definíciójából $p \mid (k^2 - 1)$ következik, ami csak a $k = 1$ vagy a $k = p - 1$ esetben lehet. Tekintettel arra, hogy $P \lhd G$ és a $\langle b \rangle = B$ részcsoportra $PB = G$ és $P \cap B = \{1\}$, ezért $G = P \rtimes B$. A féldirekt szorzathoz meg kell adni a $\varphi : B \to A(P)$ homomorfizmust. Mint a fenti számolás mutatja, $A(P)$-ben két másodrendű automorfizmus lehet, $a \mapsto a$ és $a \mapsto a^{p-1}$. $(a^{p-1})^{p-1} = a$ miatt ezek valóban másodrendű automorfizmusok, tehát valóban létezik két ilyen csoport. Az első automorfizmus esetében kommutatív csoportot kapunk, a második automorfizmusnál nem.

Két olyan csoport van tehát, amelynek a rendje 6, 10, 14 . . ., ezek egyike kommutatív, másikuk nem.

Ezen a ponton érdemes megnézni az összes szóba jövő $G = N \rtimes B$ csoportot, ahol $N = \langle a \rangle$, $B = \langle b \rangle$ és $|B| = 2$. Legyen $|N| = n$. Az $n = 1$ eset érdektelen, az $n = 2$ esetben G két másodrendű csoport direkt szorzata. Ha $n > 2$, akkor mindig van két automorfizmus: $a \mapsto a$ és $a \mapsto a^{-1}$. Az első esetben az $N \times B$ direkt szorzathoz jutunk. A második esetben a D_n úgynevezett diédercsoportot kapjuk. $D_n = \langle a, b \rangle$, ahol $a^n = b^2 = 1$ és $bab^{-1} = a^{n-1}$; és ezek az egyenlőségek egyértelműen meghatározzák e csoportot. A legutóbbi egyenlőség átírható az egyszerűbb $aba = b$ vagy ($b^2 = 1$ miatt) $abab = 1$ alakba. Ez a felírás azt sugallja, hogy érdemes a helyett a $c = ab$ elemet nézni. Ekkor ugyanis $c^2 = 1$ (c másodrendű) és $a = cb$. Természetesen $D_n = \langle b, c \rangle$, ahol $b^2 = c^2 = 1$ és $o(cb) = n$. Könnyen látható, hogy D_n izomorf a szabályos n-szög egybevágósági transzformációinak a csoportjával. Az a elem megfelel a teljes szög n-edrészével való forgatásnak és b egy tükrözésnek. Ha csak a $b^2 = c^2 = 1$ feltételt tekintjük, akkor a kapott csoport az egész számok rendezett halmazának az egybevágósági transzformációit adja.

A legkisebb rendű csoport, amelyiket még nem vizsgáltunk, a 8-adrendű. Általában a p^3-rendű csoportokról a következőket tudjuk. Ha a csoport kommutatív, akkor három lehetőség van a véges Abel-csoportok alaptétele szerint. Vagy ciklikus a csoport, vagy egy p-edrendű és egy p^2-rendű ciklikus csoportnak a direkt szorzata, vagy három p-edrendűnek a direkt szorzata. Ha a csoport nem kommutatív, akkor centrumának az indexe nem lehet p, így centruma p-edrendű. A centrum szerinti faktorcsoport nem ciklikus, és így csak két p-edrendű csoport direkt szorzata lehet. Kicsit bonyolultabb számítással kimutatható, hogy páratlan prímszám esetén aszerint lehet két esetet megkülönböztetni, hogy van-e a csoportban p^2-rendű elem vagy sem.

A 8 elemű csoportról először is kimutatjuk, hogy – ha nem kommutatív – van negyedrendű eleme. Általában igaz ugyanis az, hogy *ha egy csoport minden eleme másodrendű, akkor a csoport kommutatív.* Valóban, ha $a^2 = b^2 = (ab)^2 = 1$, akkor

$$ba = 1ba1 = aababb = a(ab)^2b = a1b = ab.$$

Így a kérdéses csoportban van egy negyedrendű a elem. Ha $b \notin \langle a \rangle$, akkor $\langle a, b \rangle$ rendje nagyobb, mint négy, tehát ez az egész csoport. Mivel a centrum szerinti faktorcsoport nem lehet ciklikus, ezért $\langle a \rangle$ képe ebben a faktorcsoportban nem lehet az egész csoport. Ez azt jelenti, hogy $\langle a \rangle$-ban van 1-től különböző centrumelem, ami csak a^2 lehet, mert a centrumnak nem lehet négy eleme. Mivel a csoport nem kommutatív, ezért generátorelemeik nem felcserélhetőek. Így az $[a; b] = aba^{-1}b^{-1}$ nem az egységelem. A centrum szerinti faktor azonban kommutatív, így a fenti kommutátor benne van a centrumban, azaz $aba^{-1}b^{-1} = a^2$. Ebből azonnal adódik a $ba = a^3b$ összefüggés. Ha $b^2 = 1$, akkor a kapott csoport nyilván D_4 lesz. A másik lehetséges eset az, hogy $b^2 = a^2$ amikor az úgynevezett kvaterniócsoportot nyerjük. Ezt a következőképpen szokták megadni: A Q kvaterniócsoport elemei $\{i, j, k, -i, -j, -k, 1, -1\}$. A csoport centrumában van a -1, amely másodrendű, és $-i = (-1)i$, $-j = (-1)j$, $-k = (-1)k$. Továbbá teljesülnek az $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, valamint a $ji = -k$, $kj = -i$, $ik = -j$ összefüggések. A kvaterniócsoportot nem lehet („valódi") féldirekt szorzat alakjában megadni, mert -1 eleme bármely legalább kételemű részcsoportnak.

Legyen most G 12-edrendű csoport, H egy 2-Sylow, K egy 3-Sylow részcsoportja G-nek. A 2-Sylow részcsoportok száma (páratlan) osztója 3-nak, azaz vagy 1, vagy 3. A 3-Sylowoké 4-nek olyan osztója, amely 3-mal osztva 1-et ad maradékul, tehát vagy 1, vagy 4. Tekintettel arra, hogy $\langle H, K\rangle$ rendje 3-mal is és 4-gyel is osztható, ezért ez a generátum pontosan G. Mivel 3 és 4 relatív prímek, ezért $H \cap K = \{1\}$. Ez azt jelenti, hogy akár H, akár K normálosztója G-nek, G mindenképpen ezek szemidirekt szorzata. Jegyezzük meg, hogy K háromelemű, ezért ciklikus. H négyelemű, tehát vagy ciklikus, vagy két másodrendű ciklikus csoport direkt szorzata. Nézzük először azt az esetet, amikor $H \lhd G$. Tegyük fel, hogy H ciklikus. Ekkor automorfizmuscsoportja kételemű. Egy háromelemű csoportnak egy kételemű csoportba való homomorfizmusa minden elemet az egységbe visz; így a konjugálás triviális, a csoport kommutatív, egy három- és egy négyelemű csoportnak a direkt szorzata: egy 12 elemű ciklikus csoport. A második eset legyen az, amikor H két másodrendű csoport szorzata. Ennek három másodrendű eleme van. Ezeket ciklikusan felcserélve két harmadrendű automorfizmust kapunk. Ha K generátorelemét az identikus automorfizmusra képezzük le, akkor ismét kommutatív csoportot nyerünk. Könnyen látható, hogy ez egy másodrendű és egy hatodrendű ciklikus csoport szorzata. Ez nem izomorf a korábban kapott kommutatív csoporttal. Ha a H másodrendű elemei a, b, c és K generátorelemének az $a \mapsto b \mapsto c \mapsto a$ automorfizmust feleltetjük meg, akkor egy újabb féldirekt szorzatot kapunk. Ez a csoport könnyen leírható permutációk segítségével (l.: 1. kötet I. rész 2.3); a leírás részletesen fog szerepelni a permutációcsoportokról szóló fejezetben. A fenti automorfizmus inverzére képezve a kapott csoport az előbbivel izomorf lesz. Nézzük most azt az esetet, ha K nem normálosztó, ekkor négy konjugáltja van. Tekintettel arra, hogy két különböző harmadrendű csoportnak csak 1 lehet közös eleme, ezért K konjugáltjaiban $4 \times 2 = 8$ egységtől különböző elem van, a fennmaradó négy elem mindegyike benne van egy 2-Sylowban. Mivel egy 2-Sylownak négy eleme van, ezért G-ben egyetlen 2-Sylow van, ami normálosztó. Azokat az eseteket kell tehát még megvizsgálni, amikor K normálosztó, tehát $G = K \rtimes H$. Ha φ a H-t az $A(K)$ egységelemére képezi, akkor direkt szorzatot nyerünk; ezeket az eseteket már láttuk. Mivel H négyelemű és $A(K)$ kételemű, ezért van olyan $a \in H$, amit φ az identikus automorfizmusra képez. Az általa generált A részcsoportra tehát az $L = K \rtimes A$ féldirekt szorzat ciklikus hatelemű csoport. Így $(G : L) = 2$, tehát $L \lhd G$. Most ismét két lehetőséget kell megvizsgálni. Ha H két kételemű csoport direkt szorzata és $K \rtimes H$ nem direkt, akkor van olyan $b \in H$, ami nincs benn K centralizátorában. A B generálta B csoportra tehát létezik a nemtriviális $L \rtimes B$ féldirekt szorzat; ami éppen a D_6-ot adja. Az ötödik esetben H ciklikus. Legyen a a K-nak és b a H-nak a generátoreleme. Most is igaz az, hogy $\langle a, b^2\rangle$ ciklikus hatelemű csoport. Viszont $bab^{-1} \neq a$ miatt csak $bab^{-1} = a^2$ lehet. Ez egy jóldefiniált nemkommutatív féldirekt szorzat. Ebben a csoportban van negyedrendű elem, míg az előző nemkommutatív 12 elemű csoportokban nem volt; ez tehát egy újabb 12 elemű csoport; így a 12 elemű csoportok száma öt.

A következő eset a 15 elemű csoportok vizsgálata. Általában, ha p és q különböző páratlan rendű prímszámok, akkor a p-Sylow részcsoportok száma q-nak olyan osztója, amely p-vel osztva 1-et ad maradékul. (Hasonló igaz a q-Sylowra is.) Egy p-Sylow részcsoport tehát csak akkor lehet nem normálosztó, ha $q \equiv 1 \pmod{p}$. Ez biztosan nem teljesül, ha $q < p$; az egyik Sylow-csoport tehát mindig normálosztó. $5 \not\equiv 1 \pmod 3$ következtében 15 elemű csoportban mindkét Sylow normálosztó: 15 elemű csoport tehát mindig ciklikus.

A 16 elemű csoportok meghatározása sok számolást igényelne. Ezek között öt kommutatív van, a nemkommutatívak közül öt 4-exponensű és négy 8-exponensű, ez összesen 14 nem izomorf csoport.

A 18 elemű csoportnál az N 3-Sylow részcsoport 2 indexű, tehát normálosztó. Ezen kívül a Cauchy-tétel alapján kell lennie egy c másodrendű elemnek. Ekkor $G = N \rtimes C$, ahol c a C generátoreleme. Ha N az a generálta ciklikus csoport, akkor N-nek két automorfizmusa van. Ha $cac^{-1} = a$, akkor G ciklikus, ha $cac^{-1} = a^{-1}$, akkor $G = D_9$. Ha N két harmadrendű csoport direkt szorzata (az a és b generátorokkal), akkor a c-vel való konjugálás lehet az identikus automorfizmus, vagy leképezhet minden elemet az inverzére, vagy lehet, hogy $cac^{-1} \notin \langle a \rangle$. Ez öt különböző csoport.

Ezzel a 20-nál kevesebb elemű csoportokat megvizsgáltuk.

Feladatok

1. Határozzuk meg az összes $N \rtimes B$ csoportot, ahol N ciklikus és B kételemű.

2. A G csoport *ferde automorfizmusán* a tartóhalmaz egy olyan ψ bijekcióját értjük, amelyre $\psi(ab) = \psi(b)\psi(a)$. Mutassuk meg, hogy ezek az automorfizmusokkal együtt az összes bijekció csoportjának egy $F(G)$ részcsoportját alkotják. Bizonyítsuk be, hogy $A(G), B(G) \lhd F(G)$. Melyek azok a G csoportok, amelyekre $F(G) = A(G)$, illetve $F(G) = B(G)$?

3. Írjuk le az összes 20 elemű csoportot.

4. Mutassuk meg, hogy létezik 21 elemű nemkommutatív csoport.

5. Írjuk le az összes $4p$ rendű csoportot, ahol p páratlan prímszám.

6. Legyenek $p > q > r$ páratlan rendű prímek. Bizonyítsuk be, hogy minden olyan G csoportban, amelynek a rendje r^3 vagy q^2r, vagy qr^2, vagy pqr léteznek olyan egymástól különböző H és K valódi részcsportok, amelyekre $\{1\} \lhd K \lhd H \lhd G$.

7. Határozzuk meg az összes olyan nem izomorf csoportot, amelynek a rendje $2pq$, ahol p és q nem feltétlen különböző páratlan prímszámok.

8. Legyen $M_3(p)$ azoknak a háromszor hármas felső háromszög mátrixoknak a halmaza, amelyeknek elemei a p elemű testből valók, és főátlójuk minden eleme 1. Bizonyítsuk be, hogy ezek a mátrixok a mátrixszorzásra nézve egy G csoportot alkotnak. Mennyi a G rendje? Mennyi a G elemeinek a rendje páratlan p-re és mennyi a $p = 2$ esetben? Határozzuk meg G centrumát és (izomorfizmus erejéig) a centrum szerinti faktorcsoportot. Határozzuk meg G kommutátorcsoportját.

9. Legyen $M_n(p)$ azoknak az $(n \times n)$-es felső háromszög mátrixoknak a halmaza, amelyeknek elemei a p elemű testből valók, és főátlójuk minden eleme 1. A mátrixszorzásra nézve ezek is csoportot alkotnak. Milyen esetben lesz e csoportnak az exponense p?

5.12. Szabad csoportok

Láttuk, hogy a Sylow-tételek módot adnak annak a meghatározására, hogy bizonyos feltételeknek eleget tevő (például adott elemszámú) csoportoknak milyen lehet a szerkezetük. A féldirekt szorzat lehetőséget adott ilyen csoportok előállítására. A csoportok egy másik megadási módját kaphatjuk akkor, ha megadjuk generátorrendszerüket. Ez persze nem elég, mert még azt is tudni kell, hogy milyen kapcsolatok állnak fenn a generátorrendszer elemei között. Arra nincs lehetőség, hogy az összes kapcsolatot felírjuk (mert ezek száma végtelen), de annyi kapcsolatot kell felírni, amennyiből az összes többi következik. Természetesen, ebből még nem következik az, hogy ilyen tulajdonságú csoport valóban létezik. A létezést általában úgy lehet ellenőrizni, hogy a csoportot ismert, jól leírható csoportok részcsoportjaként állítjuk elő. A későbbiekben két ilyen, viszonylag jól leírható csoportot adunk majd meg, a permutációk csoportját és a reguláris mátrixok csoportját.

A generátorokkal és a relációkkal való megadáshoz mindenekelőtt olyan csoportokra van szükségünk, ahol a generátorelemek között semmiféle reláció nem teljesül, csak azok, amelyek a csoportaxiómákból következnek. Ezeket a csoportokat szabad csoportoknak; pontosabban az adott generátorokkal szabadon generált csoportoknak nevezzük. A szabad csoportokat „fogalmilag” ugyanúgy definiáljuk, mint a szabad félcsoportokat.

5.76. Definíció. A $G_X = \langle X; \{\cdot, {}^{-1}, 1\}\rangle$ csoportot az X generálta szabad csoportnak nevezzük, ha tetszőleges $G = \langle G; \{\cdot, {}^{-1}, 1\}\rangle$ csoport esetén minden $\varphi : X \to G$ függvénynek létezik olyan egyértelmű $\psi : G_X \to G$ kiterjesztése, amely homomorfizmus.

Az X elemeit a G_X csoport szabad generátorainak, e csoportokat pedig szabad csoportoknak nevezzük. □

5.77. Tétel. *Minden X halmazra létezik általa generált szabad csoport. Minden csoport egy alkalmas szabad csoport homomorf képe.*

Bizonyítás. Az X halmaz minden x eleméhez tekintsünk egy új, x'-vel jelölt elemet. Ezek halmazát jelöljük X'-vel, és X' minden x' elemére legyen $(x')' = x$. Ezzel az $X \cup \cup X'$ halmazon egy olyan függvényt értelmeztünk, amely rendelkezik a szabad félcsoportok utáni 4.5. pontban (Faktorfélcsoportok invertálással) megkívánt tulajdonsággal.

Azt fogjuk bebizonyítani, hogy az $M_{X\cup X'}$ szabad monoid rövidíthetetlen szavai a 4.28. tételben definiált szorzással a G_X szabad csoportot alkotják. A 4.28. tétel szerint, ez a félcsoport izomorf az $M_{X\cup X'}/\Theta_G$ faktorfélcsoporttal, amelyben a 4.27. tétel szerint minden elemnek létezik inverze. Így valóban csoportot kaptunk. E csoportnak mint monoidnak $X \cup \cup X'$ generátorrendszere. Tekintettel arra, hogy a rövidítés definíciója alapján tetszőleges $x \in X$ elem inverze éppen az X'-beli megfelelő x' elem, ezért e csoportot (mint csoportot) az X elemei generálják. Jelöljük ezt a csoportot G_X-szel. Azt már láttuk, hogy X generálja G_X-et, amiből következik, hogy bármely $\varphi : X \to G$ függvényt legfeljebb egyféleképpen terjeszthetünk ki G_X homomorfizmusává. A kiterjeszthetőség bizonyításához a $\psi : X \to G$ függvényt először is terjesszük ki X'-re a $\psi(x') = (\psi(x))^{-1}$ definícióval. Ez a leképezés – mint láttuk – kiterjeszthető az $M_{X\cup X'}$ szabad monoid homomorfizmusává. Mivel $\psi(x')$ és $\psi(x)$ képe egymásnak inverzei, ezért egy tetszőleges szó képe megegyezik bármely

rövidítésének a képével. Így minden rövidített alaknak egyértelmű képe van; ami a kívánt leképezés homomorfizmus kiterjesztését adja.

A tétel második állításának a bizonyításához elegendő tekinteni a G csoport egy tetszőleges $\{\ldots, g_i, \ldots\}$ generátorrendszerét, és minden egyes generátorelemhez hozzárendelni egy új x_i elemet. Ezen elemek X halmaza generálta szabad csoportnak homomorf képe lesz az eredeti csoport, ha kiindulásul a $\varphi : x_i \mapsto g_i$ függvényt tekintjük (a képek ugyanis generálják a csoportot). Természetesen azt is be kell látni, hogy minden csoportnak van generátorrendszere, de a csoport összes eleme nyilván generátorrendszer. ■

Tekintsünk most egy G csoportot, és ennek egy $\{\ldots, g_i, \ldots\}$ generátorrendszerét. Mint láttuk, ekkor létezik olyan G_X szabad csoport az $X = \{\ldots, x_i, \ldots\}$ szabad generátorrendszerrel és $\psi : G_X \to G$ homomorfizmussal, amelyre $\psi(x_i) = g_i$ teljesül tetszőleges i index esetén. Ha a G csoport fenti generátorrendszerére valamilyen „reláció" teljesül, az azt jelenti, hogy a generátorelemek egy-egy hatványszorzata megegyezik. Tekintettel arra, hogy csoportban minden elemnek van inverze, ez azt jelenti, hogy e generátorelemek valamilyen hatványszorzata a G egységeleme. Ha most az X elemeinek a megfelelő hatványszorzatát – azaz egy G_X-beli w szót veszünk, akkor azt kapjuk, hogy $\psi(w)$ a G-nek egységeleme. Eszerint *a G csoport generátorelemeire vonatkozó relációin a* Ker ψ *elemeit értjük.* Mint már megjegyeztük, az összes relációt nem lehet megadni, hiszen (szinte mindig) végtelen sok reláció van. Erre azonban nincs is szükség; elég annyit megadni, amennyiből már az összes többi „következik". Tekintettel arra, hogy Ker $\psi \lhd G_X$, ezért elég egy olyan D részhalmazt megadni, amely által generált normálosztó Ker ψ-vel egyenlő.

5.78. Definíció. Az X halmaz elemeivel mint generátorelemekkel és az X generálta szabad csoport egy D részhalmazának elemeivel mint definiáló relációkkal megadott

$$G = \langle \ldots, x, \ldots \mid \ldots, w = 1, \ldots \rangle \qquad (x \in X, w \in D)$$

csoporton a G/N faktorcsoportot értjük, ahol N a D generálta normálosztó. □

Természetesen D egyáltalán nem egyértelmű. Ebből következik, hogy igen nehéz eldönteni definiáló relációkkal megadott csoportok izomorfizmusát. Ezen túlmenően az is gondot okoz, hogy a megadott relációkból milyen további relációk következnek; az is előfordulhat, hogy a kapott csoport egyelemű. D elemei helyett sokszor célszerűbb $u = v$ relációkat felírni, ami természetesen azt jelenti, hogy $uv^{-1} = 1$.

A definiáló relációkkal megadott csoportok konstruálásakor sokszor jól használható az az észrevétel, hogy ha a G és $\widetilde{G}$ csoportoknak ugyanaz a generátorrendszerük, és G minden definiáló relációja fellép $\widetilde{G}$ definiáló relációi között, akkor $\widetilde{G}$ a G-nek faktorcsoportja (Dyck tétele). Ez abból következik, hogy ha a megfelelő definiáló részhalmazokra $D \subseteq D'$, akkor a megfelelő normálosztókra $N \leq \widetilde{N}$; így a második izomorfizmustételből $\widetilde{G} = G_X/\widetilde{N} = (G_X/N)/(\widetilde{N}/N) = G/(\widetilde{N}/N)$ következik.

A szabad csoportokhoz hasonlóan definiálhatjuk a *szabad kommutatív csoportokat.*

5.79. Definíció. A_X az X halmaz generálta szabad Abel-csoport, ha tetszőleges A Abel-csoport esetén minden $\varphi : X \to A$ leképezésnek létezik egyértelmű homomorfizmus kiterjesztése A_X-re.

Feladatok

1. Bizonyítsuk be, hogy $D_n = \langle a, b \mid a^n = b^2 = baba = 1 \rangle$.

2. Bizonyítsuk be, hogy $D_n = \langle a, b \mid a^2 = b^2 = (ba)^n = 1 \rangle$.

3. Legyen $D_\infty = \langle a, b \mid a^2 = b^2 = 1 \rangle$. Bizonyítsuk be, hogy minden egyes D_n homomorf képe D_∞-nek.

4. Legyenek a és b a G csoport elemei. Bizonyítsuk be, hogy ha $a^2 = 1$ és $b^2a = ab^3$, akkor $b^5 = 1$.

5. Legyenek a és b a G csoport elemei. Bizonyítsuk be, hogy ha $b^2a = ab^3$, és $a^2b = ba^3$, akkor $a = b = 1$.

6. Bizonyítsuk be, hogy az egy elemmel generált szabad csoport megegyezik az egy elemmel generált szabad Abel-csoporttal.

7. Bizonyítsuk be, hogy az X halmaz generálta szabad csoport megegyezik az összes X-beli x elem által (külön-kükön) generált szabad csoport ko-szorzatával.

8. Bizonyítsuk be, hogy az X halmaz generálta szabad Abel-csoport megegyezik az összes X-beli x elem generálta szabad Abel-csoportok ko-szorzatával, ami nem más, mint e ciklikus csoportok direkt összege.

9. Bizonyítsuk be, hogy $A_X = \langle X \mid xy = yx \rangle$, ahol x, y végigfutnak az X halmazon.

10. Bizonyítsuk be, hogy a legalább két elemmel generált szabad csoport centruma egyelemű.

11. Legyen $G_{x,y}$ szabad csoport és $A_{x,y}$ szabad Abel-csoport; továbbá $\psi : G_{x,y} \to A_{x,y}$ az $x \mapsto x$, $y \mapsto y$ leképezés homomorfizmus kiterjesztése. Bizonyítsuk be, hogy Ker ψ mint *normálosztó* egy elemmel generálható.

12. Írjuk fel (gondolatban) a $G_{x,y}$ szabad csoport elemeit x és y hatványainak szorzataként. A kitevőkre vonatkozó milyen feltétel mellett lesz egy ilyen szorzat a kommutátorcsoport eleme?

13. Legyen $G_{x,y}$ szabad csoport. Bizonyítsuk be, hogy $G_{x,y}$ nem lehet két ciklikus csoport direkt összege.

6. Feloldhatóság

A csoport fogalma a magasabbfokú egyenletek gyökjelekkel való megoldhatóságánál merült fel. Minden magasabbfokú egyenlethez hozzárendelhető egy csoport; és az egyenlet megoldhatóságának az a feltétele, hogy a csoportban létezzék részcsoportjainak bizonyos feltételnek eleget tevő lánca. Az ilyen csoportokat nevezik feloldható csoportoknak. Az egyenlethez hozzárendelt csoport elemei az egyenlet gyökeinek bizonyos permutációiból állnak. Ezért alapvető a permutációk részletesebb vizsgálata.

6.1. Normállánc

Mint említettük, egy csoport valamely normálosztójának tetszőleges normálosztója az egész csoportban nem feltétlenül lesz normálosztó. Ennek ellenére, a normálosztók képzésével lépésenként előállítható részcsoportok (az úgynevezett szubnormális részcsoportok) igen fontos szerepet játszanak a csoportok vizsgálatában. Előkészületül néhány definícióra van szükségünk.

6.1. Definíció. Valamely G csoport részcsoportjainak egy

$$\mathcal{N}: \qquad G = G_0 \geq G_1 \geq \ldots \geq G_i \geq \ldots \geq G_r = \{1\}$$

rendszerét a G egy r hosszúságú normálláncának nevezzük, ha minden i-re $(0 \leq i < r)$ $G_{i+1} \lhd G_i$ teljesül. A G_i-k az $\mathcal{N}$ elemei, a G_i/G_{i+1} faktorcsoportok pedig $\mathcal{N}$ faktorai. $\mathcal{N}$ valódi normállánc, ha egyetlen G_i eleme sem egyenlő G_{i+1}-gyel. A

$$\mathcal{K}: \qquad G = H_0 \geq H_1 \geq \ldots \geq H_i \geq \ldots \geq H_s = \{1\}$$

normállánc az $\mathcal{N}$ valódi normállánc finomítása, ha $\mathcal{N}$ minden eleme $\mathcal{K}$-nak is eleme. $\mathcal{K}$ valódi finomítás, ha valódi normállánc, és van olyan eleme, amely nem eleme $\mathcal{N}$-nek. $\mathcal{K}$ kompozíciólánc, ha valódi normállánc, és nincs valódi finomítása. A G csoport $\mathcal{N}$ és $\mathcal{K}$ normálláncát izomorfaknak ($\mathcal{N} \cong \mathcal{K}$) nevezzük, ha van olyan bijekció, amely $\mathcal{N}$ faktorainak a $\mathcal{K}$ faktorait felelteti meg, és az egymásnak megfeleltetett faktorok izomorfak. □

6.2. Tétel. *Egy normállánc akkor és csak akkor valódi, ha elemei mind különbözőek, illetve ha faktorai között nincs egyelemű. Egy normállánc akkor és csak akkor kompozíciólánc, ha minden G_i eleme maximális normálosztója G_{i-1}-nek, illetve, ha faktorai nem triviális egyszerű csoportok. Normálláncok izomorfizmusa ekvivalencia, amelynél valódi normállánc csak valódi normállánccal, kompozíciólánc csak kompozíciólánccal lehet ekvivalens. Egy normállánc egy finomításának bármely faktora az eredeti normállánc valamely faktora egy részcsoportjának a homomorf képe.*

Bizonyítás. A valódi normálláncokra vonatkozó állítás triviális. Legyen $\mathcal{N}$ a G csoport egy valódi normállánca, és tekintsük ennek egy olyan finomítását, amelyik ugyancsak valódi normállánc. Mivel az $\mathcal{N}$ tetszőleges G_i eleme ennek a finomításnak is eleme, ezért ezek mindegyikéhez létezik a finomításban egy olyan, tőle különböző H_i amely G_i-ben normálosztó, és amelyik a G_{i+1}-et tartalmazza (nevezetesen a finomításban a G_i után következő első olyan, amelyik G_i-től különbözik). Így minden szóba jövő i-re $G_i \rhd H_i \geq G_{i+1}$ és $H_i \neq G_i$. A finomítás pontosan akkor valódi, ha legalább egy szóba jövő i-re $H_i \neq = G_{i+1}$, ami éppen azt jelenti, hogy legalább egy i-re G_{i+1} nem maximális normálosztója G_i-nek. Az 5.43. következmény szerint ez azzal ekvivalens, hogy legalább egy faktor nem egyszerű. Normálláncok izomorfizmusa triviálisan ekvivalenciareláció. Az izomorfizmusra vonatkozó másik két állítás pedig abból következik, hogy mindkét fogalom megfogalmazható a faktorok segítségével.

Az utolsó állítás bizonyításához tekintsük a finomítás két egymás után következő elemét: $C \rhd D$. Tekintettel arra, hogy közöttük a finomításban sincs elem, ezért az eredeti normálláncban is minden elem vagy tartalmazza C-t, vagy benne van D-ben. Ha A az eredeti normálláncban a legkisebb, C-t tartalmazó, és B a legnagyobb, D-ben levő elem, akkor az eredeti normálláncban ezek egymás után következnek, azaz $A \rhd B$. Az A és B választása

folytán $A \geq C \geq D \geq B$, továbbá $B \lhd A$ miatt $B \lhd C$ is teljesül. A második izomorfizmustétel szerint tehát $C/D \cong (C/B)/(D/B)$, azaz C/D a C/B-nek homomorf képe. C/B viszont az eredeti normállánc egy faktorának – nevezetesen A/B-nek – a részcsoportja. ■

A továbbiakhoz szükségünk lesz a csoport normálosztóinak egy jellegzetes tulajdonságára, amit *modularitási tulajdonságnak* nevezünk. Ehhez azonban ismét újabb fogalmakat kell bevezetnünk.

6.3. Definíció. Legyen $A \leq B$ a G csoport két részcsoportja. Jelölje $[A, B]$ az $A \leq \leq X \leq B$ részcsoportok hálóját, ahol a generátum a legkisebb felső korlát és a közös rész a legnagyobb alsó korlát művelete. Legyen $[A, B]$ és $[C, D]$ két intervallum. Azt mondjuk, hogy a részcsoportokra definiált $\varphi : [A, B] \to [C, D]$ leképezés izomorfizmus, ha művelettartó bijekció az első intervallum részcsoportjairól a másodikéira. □

6.4. Tétel. *Legyen $N \lhd G$, $H \leq G$ és $G = NH$. Tekintsük G részcsoportjaira a $\varphi : X \mapsto X \cap H$ és $\psi : Y \mapsto NY$ leképezéseket. φ-nek az $[N, G]$ intervallumra való α megszorítása izomorf módon képez le $[N \cap H, H]$-ra; ennek β inverze a ψ-nek az $[N \cap H, H]$-ra való megszorítása. α és β mindegyike a megfelelő intervallum normálosztóit a másik intervallum normálosztóira képezi (azaz, ha $N \leq N_1 \lhd G$, illetve $N \cap H \leq N_2 \lhd H$, akkor $N \cap H \leq \alpha(N_1) \lhd H$, illetve $N \leq \beta(N_2) \lhd G$); és mindegyikük normálláncot normálláncba visz.*

Bizonyítás. Ha $N \leq X \leq G$, akkor $N \cap H \leq X \cap H \leq H$; ha $N \cap H \leq Y \leq H$, akkor $N = N(N \cap H) \leq NY \leq G$. Így valóban $\varphi : [N, NH] \to [N \cap H, H]$, illetve $\psi : [N \cap H, H] \to [N, NH]$.

$N \leq X$ és $X \cap H \leq X$ miatt $N(X \cap H) \leq X$. Az $X \leq NH$ egyenlőtlenségből következik, hogy tetszőleges X-beli x elem $x = nh$ alakú, ahol $n \in N$ és $h \in H$. Mivel $N \leq X$, ezért $n \in X$, vagyis $h = n^{-1}x \in X$. Eleve teljesül $h \in H$, tehát $h \in X \cap \cap H$. Végeredményben $x \in N(X \cap H)$, és így $X \leq N(X \cap H)$; amiből $X = N(X \cap H)$ következik.

$Y \leq H$ és $Y \leq NY$ miatt $Y \leq NY \cap H$. Ha $h \in NY \cap H$, akkor $h = ny$ alakú, ahol $h \in H$, $n \in N$ és $y \in Y$. Az $Y \leq H$ feltétel következtében $y \in H$, vagyis $n = hy^{-1} \in H$. Mivel $n \in N$, ezért $n \in H \cap N \leq Y$, vagyis $h = ny \in Y$. Így $NY \cap H \leq Y$; végeredményben $NY \cap H = Y$.

Ez azt jelenti, hogy $\alpha\beta$ és $\beta\alpha$ mindegyike identitás, vagyis α és β egymás inverzei, következésképpen bijekciók is.

$\varphi(X_1 \cap X_2) = (X_1 \cap X_2) \cap H = (X_1 \cap H) \cap (X_2 \cap H)$, vagyis φ metszetet tart.

$N(\langle Y_1, Y_2 \rangle) = \langle N, Y_1, Y_2 \rangle = \langle \langle N, Y_1 \rangle, \langle N, Y_2 \rangle \rangle$ miatt ψ generátumot tart. Mivel e két függvény egymásnak inverze, ezért mindegyik tartja a metszetet is és a generátumot is. Ezért mindkét leképezés (háló-)izomorfizmus.

Tekintsük most a normálosztókra vonatkozó állítást:

Ha $N \lhd X \lhd G$, akkor az első izomorfizmustétel szerint $X \cap H \lhd H$. Legyen most $N \cap H \leq Y \lhd H$, és tekintsük NY-t. Mivel $N \leq NY$, ezért $nNY = NYn$, ha $n \in N$. Amennyiben $Y \lhd H$, akkor $hY = Yh$, ha $h \in H$, és $N \lhd G$ miatt $hN = Nh$ minden $h \in H$ mellett. E két összefüggésből $hNY = NYh$ adódik a H-beli h elemekre. Így minden $n \in N$ és minden $h \in H$ elemre $nhNY = NYnh$. Mivel $G = NH$, ezért NY normálosztó G-ben.

Az utolsó állításhoz elég azt belátni, hogy ha $G \geq X \geq X_1 \geq N$ és $H \geq Y \geq Y_1 \geq N \cap H$ a fenti izomorfizmusnál egymásnak megfeleltetett csoportláncok, akkor az $X_1 \lhd X$ és $Y_1 \lhd Y$ feltételek ekvivalensek.

Mivel $X = NY$ és $N \cap H = Y \cap H$, ezért α-nak az $[X, N]$-re való megszorítása az $[Y, N \cap H]$-ra való izomorfizmus. A már belátottak szerint (G helyébe X-et téve) az adódik, hogy $X_1 \lhd X$ esetén $X_1 \cap Y \lhd Y$ és $Y_1 \lhd Y$ esetén $NY_1 \lhd X$, ami pontosan a kívánt állítást adja. ■

A bizonyítás jól követhető az alábbi ábrán:

$$\begin{array}{ccccccc} G & \geq & X & \rhd & X_1 & \geq & N \\ \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\ H & \geq & Y & \rhd & Y_1 & \geq & N \cap H \end{array} \quad , \quad \text{ahol} \quad \begin{array}{cc} X & NY \\ \alpha\downarrow & \beta\downarrow \\ X \cap H & Y \end{array}$$

6.5. Tétel (Jordan–Hölder)**.** *Véges, nemtriviális csoportnak van kompozíciólánca, minden valódi normállánca kompozíciólánccá finomítható és bármely két kompozíciólánca izomorf.*

Bizonyítás. Mivel $G \rhd \{1\}$ valódi normállánc, ezért az első állítás következik a másodikból:

Tekintsük a G valódi normálláncainak azokat a finomításait, amelyek ugyancsak valódi normálláncok. Mivel G-nek csak véges sok részcsoportja van, ezért e finomítások között van olyan, amelynek a hossza maximális. Ennek bármely finomítása természetesen az eredetinek is finomítása, és így, ha valódi normállánc, akkor nem lehet több eleme, mint a maximális hosszúságú finomításának. Ez pedig éppen azt jelenti, hogy a maximális hosszúságú finomítás kompozíciólánc. (Természetesen egy adott normállánc maximális hosszúságú finomítása általában nem egyértelmű.)

A bizonyítás további részében nem használjuk fel a csoport végességét, csak annyit, hogy a csoportnak létezik kompozíciólánca. A következőket fogjuk bizonyítani:

Ha egy nemtriviális csoportnak létezik kompozíciólánca, akkor minden normállánc az eredeti kompozíciólánccal azonos hosszúságú kompozíciólánccá finomítható és a csoport bármely két kompozíciólánca izomorf.

Tekintsünk tehát egy G csoportot, amelynek a feltevés szerint létezik kompozíciólánca; e kompozíciólláncok valamelyikének (például a legrövidebbnek) a hossza legyen n. Az állítást n-re vonatkozó teljes indukcióval bizonyítjuk.

Az $n = 1$ esetben a csoportnak van kételemű kompozíciólánca. Mivel G és $\{1\}$ mindig eleme a kompozíciólláncnak, ezért több eleme nem is lehet. Így az egyetlen kompozíciófaktor izomorf G-vel. A 6.2. tétel szerint tehát G egyszerű. Ezért egyetlen, G-től különböző normálosztója $\{1\}$, és egyetlen normállánca, mely egyben kompozíciólánc is: $G \rhd \{1\}$. Ez pedig azt bizonyítja, hogy G-re a fenti állítás igaz.

Tegyük most fel, hogy az állítás igaz minden olyan csoportra, amelyben van n-nél rövidebb kompozíciólánc, és legyen

$$\mathcal{N}: \qquad G = G_0 > G_1 > \ldots > G_n = \{1\}$$

a G csoport egy kompozíciólánca. Tekintsük G-nek egy tetszőleges

$$\mathcal{K}: \qquad G = H_0 > H_1 > \ldots > H_k = \{1\}$$

valódi normálláncát. Mivel $\mathcal{N}$ kompozíciólánc, ezért G_1 maximális normálosztója G-nek és G_1-ben létezik $n-1$ hosszúságú kompozíciólánc. Ez utóbbi következtében G_1-re alkalmazható az indukciós feltétel. Ha $H_1 \leq G_1$, akkor az indukciós feltétel szerint $\mathcal{K}$-nak H_1-gyel kezdődő részlánca finomítható G_1 egy $n-1$ hosszúságú kompozícióláncává, amelyhez G-t hozzávéve egy n hosszúságú finomítást nyerünk.

Egyébként G_1 maximalitásából következik, hogy $G = G_1 H_1$.

Mivel G_1-ben igaz az állítás, ezért a $G_1 \rhd G_1 \cap H_1 \rhd \{1\}$ normállánc egy $G_1 = Y_1 > > Y_2 > \ldots > Y_n$ ($n-1$ hosszúságú) kompozíciólánccá finomítható, amelyben valamely r indexre $Y_r = G_1 \cap H_1$:

$$G_1 = Y_1 > \ldots > Y_r = G_1 \cap H_1 > Y_{r+1} > \ldots > Y_n = \{1\}.$$

Alkalmazzuk most a modularitási tulajdonságot a már belátott $H_1 \lhd G$ és $G_1 \leq G$ feltételek mellett. Ekkor a $G = G_1 H_1 > X_1 > \ldots > X_r = H_1$ normállánchoz jutunk, amelyben az izomorfizmus miatt minden X_{i+1} maximális X_i-ben. Tekintettel arra, hogy $G_1 \lhd G$ is igaz, ezért $G_1 \cap H_1 \lhd H_1$; mégpedig maximális, hiszen G_1 is maximális normálosztó G-ben. Így

$$H_1 > G_1 \cap H_1 > Y_{r+1} > \ldots > Y_n = \{1\}$$

a H_1-nek egy $n-r-1$ hosszúságú kompozíciólánca. A $G \neq H_1$ feltétel miatt $r > 1$, tehát e kompozíciólánc hossza kisebb, mint n. Az indukciós feltevés szerint a $H_1 > H_2 > \ldots > > H_k = \{1\}$ normállánc egy $H_1 > X_{r+1} > \ldots > X_n = \{1\}$ kompozícióláncca finomítható, így

$$G = X_0 > X_1 > \ldots > X_n = \{1\}$$

$\mathcal{K}$-nak kompozícióláncca való finomítása.

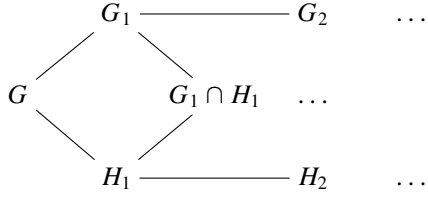
A kompozícióláncok izomorfizmusát is a lánc hosszára vonatkozó teljes indukcióval bizonyítjuk. Azt már tudjuk, hogy ha a csoportnak van kompozíciólánca, akkor bármely két kompozícióláncnak megegyezik a hossza. Ha ez a hossz $n = 1$, akkor az izomorfizmus triviálisan igaz. Tegyük most fel, hogy minden olyan csoportban izomorfak a kompozícióláncok, amelyben ezek hossza kisebb, mint n, és legyen

$$\mathcal{N}: \qquad G = G_0 > G_1 > \ldots > G_n = \{1\},$$

valamint

$$\mathcal{K}: \qquad G = H_0 > H_1 > \ldots > H_n = \{1\}$$

a G csoport két kompozíciólánca. A $G_1 = H_1$ esetben a teljes indukciós feltétel alapján teljesül az izomorfizmus. Egyébként G_1 és H_1 maximalitása alapján $G = G_1 H_1$, és így $G_1 \cap H_1$ valódi normálosztója G_1-nek is és H_1-nek is. Ez a helyzet az alábbi módon képzelhető el:



A rajzon még további két normállánc látható:

$$G > G_1 > G_1 \cap H_1 > \{1\}, \quad \text{valamint} \quad G > H_1 > G_1 \cap H_1 > \{1\}.$$

A teljes indukciós feltétel alapján G_1 bármely normállánca kompozíciólánccá finomítható. Mivel H_1 maximális normálosztó G-ben, ezért $G_1 \cap H_1$ is maximális normálosztó G_1-ben. Az előbb felírt első normállánc tehát egy

$$\mathcal{N}' : G = G_0 > G_1 > G_1 \cap H_1 > K_3 > \ldots > K_n = \{1\}$$

kompozíciólánccá finomítható. Ennek megfelelően

$$\mathcal{K}' : G = H_0 > H_1 > G_1 \cap H_1 > K_3 > \ldots > K_n = \{1\}$$

ugyancsak kompozíciólánc. Tekintettel arra, hogy G_1 bármely két kompozíciólánca izomorf és $\mathcal{N}$, valamint $\mathcal{N}'$ első kompozíciófaktorai megegyeznek, ezért $\mathcal{N} \cong \mathcal{N}'$. Hasonlóan adódik az is, hogy $\mathcal{K} \cong \mathcal{K}'$. Az $\mathcal{N}'$ és a $\mathcal{K}'$ kompozíciófaktorai a harmadiktól kezdve megegyeznek. Az $\mathcal{N}'$ és a $\mathcal{K}'$ első két kompozíciófaktorára az első izomorfizmustétel alapján $G/G_1 \cong H_1/(G_1 \cap H_1)$, illetve $G/H_1 \cong G_1/(G_1 \cap H_1)$ teljesül. Ezért $\mathcal{N}' \cong \mathcal{K}'$; és a tranzitivitás alapján $\mathcal{N} \cong \mathcal{K}$. ■

6.2. Feloldhatóság

Mint említettük, csoportok feloldhatósága az egyenletnek gyökjelekkel való megoldásakor játszik alapvető szerepet.

6.6. Definíció. Egy G véges csoportot feloldhatónak nevezünk, ha kompozícióláncainak faktorai prímrendűek. □

A Jordan–Hölder-tétel szerint a feloldhatóság nem függ attól, hogy melyik kompozícióláncot vesszük, tehát valóban a szóban forgó csoport tulajdonsága.

6.7. Tétel. *Egy véges G csoportra az alábbi tulajdonságok ekvivalensek:*

(1) *G feloldható.*

(2) *G valamely normálláncának faktorai prímrendűek.*

(3) *G valamely normálláncának faktorai ciklikusak.*

(4) *G valamely normálláncának faktorai kommutatívak.*

Bizonyítás. Ha G feloldható, akkor bármely kompozíciólánca eleget tesz a (2) feltételnek. Ha G-nek van olyan normállánca, amely eleget tesz a (2) (illetve (3)) feltételnek, akkor ez a normállánc eleve eleget tesz a (3) (illetve (4)) feltételnek; hiszen minden prímrendű csoport ciklikus, és minden ciklikus csoport kommutatív. Tegyük most fel, hogy G-nek van egy olyan normállánca, amelyre teljesül a (4) feltétel. E normálláncot a Jordan–Hölder-tétel szerint kompozíciólánccá finomíthatjuk, amelynek faktorai a 6.2. tétel utolsó állítása alapján kommutatívak, hiszen kommutatív csoport részcsoportja is és faktorcsoportja is kommutatív. Az 5.44. tétel szerint pedig e kompozíciólánc faktorai prímrendűek; tehát a csoport feloldható. ■

Kommutatív csoportok része és faktora is kommutatív, és a 6.7. tétel azt mutatja meg, hogy miképpen „építhetők fel" a feloldható csoportok a kommutatívakból. A feloldható csoportokból hasonló módon tovább lehet lépni. A következő tétel azt mondja ki, hogy e továbblépéssel már nem kapunk újabb típusú csoportot.

6.8. Tétel. *Feloldható csoport minden részcsoportja és faktorcsoportja is feloldható. $N \lhd G$ esetén, ha N, valamint G/N feloldhatók, akkor G is az.*

Bizonyítás. Először a részcsoportokra vonatkozó állítást bizonyítjuk, a megadott G csoport kompozícióláncának hosszára vonatkozó teljes indukcióval. Ha ez 1, akkor a csoport prímrendű, és így minden részcsoportja triviálisan feloldható. Legyen

$$G = G_0 > G_1 > \ldots > G_n = \{1\}$$

a csoport egy kompozíciólánca. Az indukciós feltevés miatt a $G_1 \cap H$ csoport feloldható, van tehát egy kívánt tulajdonságú kompozíciólánca. Azt fogjuk megmutatni, hogy ez a kompozíciólánc kiegészíthető H kompozíciólláncává; és egyetlen új kompozíciófaktor lép be: $H/(G_1 \cap H)$, amelyik prímrendű vagy egyelemű. Az állítás nyilvánvaló $H \leq G_1$ esetén. Egyébként G_1 maximalitása miatt $HG_1 = G$, és az első izomorfizmustételből $H/(G_1 \cap H) \cong G/G_1$. Ezzel H feloldhatóságát igazoltuk.

Ha $N \lhd G$, akkor a $G \rhd N$ normállánc kompozíciólánccá finomítható:

$$G = G_0 > G_1 > \ldots > G_k = N > \ldots .$$

Mivel $N \lhd G$, ezért $N \lhd G_i$ $(i = 1, \ldots, k)$; és a második izomorfizmustétel szerint $(G_i/N)/(G_{i+1}/N) \cong G_i/G_{i+1}$. A G_i/N faktorok tehát a G/N egy olyan normálláncát alkotják, amelynek faktorai prímrendűek, ami azt jelenti, hogy G/N is feloldható.

Tegyük most fel, hogy $N \lhd G$, és mind N, mind G/N feloldható. Most kompozíciólánccá finomítjuk a $G \rhd N$ normálláncot:

$$G = G_0 > G_1 > \ldots > G_s = N > G_{s+1} > \ldots > G_r = \{1\}.$$

Az előzőhöz hasonlóan most azt kapjuk, hogy $(G_i/N)/(G_{i+1}/N)$ egyszerű, ha $i < s$, amiből G/N feloldhatósága alapján következik, hogy G_i/G_{i+1} prímrendű $(i < s)$. Ha $i \geq s$, akkor a G_i/G_{i+1} faktor N feloldhatósága következtében prímrendű, és így a fent konstruált normállánc faktorai prímrendűek – tehát G feloldható. ■

A feloldhatóságot a kommutátorok segítségével is megfogalmazhatjuk.

6.9. Definíció. A G véges csoport kommutátorláncának nevezzük a

$$G = K_0 \geq K_1 \geq K_2 \geq \ldots$$

sorozatot, ahol $K_{i+1} = [K_i; K_i]$. A G csoport kommutátorlánca záródik, ha van olyan r természetes szám, amelyre $K_r = \{1\}$. □

6.10. Tétel. *A kommutátorlánc normállánc, amely pontosan akkor záródik, ha G feloldható.*

Bizonyítás. Az első állítás azonnal következik abból, hogy bármely csoport kommutátor-részcsoportja a csoportnak normálosztója. Ha a kommutátorlánc záródik, akkor a kommutátorlánc olyan normállánc, amelynek faktorai az 5.64. tétel szerint kommutatívak; a 6.7. tétel szerint tehát a csoport feloldható. Ha a csoport feloldható, akkor bármely maximális normálosztója szerinti faktor kommutatív. Ugyancsak az 5.64. tétel alapján azt kapjuk, hogy G kommutátor-részcsoportja G-nek valódi része, amely a 6.8. tétel szerint ugyancsak feloldható. Ezt az eredményt ismételten alkalmazva: ha $K_i \neq \{1\}$, akkor $K_{i+1} \neq K_i$; amiből következik, hogy a kommutátorlánc záródik. ■

6.11. Következmény. *Feloldható csoportnak van kommutatív normálosztója.*

Bizonyítás. Ha a G csoport feloldható, akkor kommutátorlánca záródik. Legyen tehát $K_r = \{1\}$; és feltehető, hogy $K_{r-1} \neq \{1\}$. Az 5.64. tételből az is következik, hogy K_{r-1} kommutatív. Állításunk bizonyításához azt fogjuk megmutatni, hogy K_{r-1} normálosztója G-nek. Ennél többet is bizonyítunk, nevezetesen azt, hogy minden K_i normálosztója G-nek. A bizonyítás i-re vonatkozó teljes indukcióval történik. $i = 0$ esetén az állítás triviális. Tegyük fel, hogy $K_i \lhd G$. Az 5.64. tétel szerint K_{i+1} karakterisztikus részcsoportja K_i-nek, az 5.61. tétel szerint tehát K_{i+1} is normálosztója G-nek. ■

6.12. Következmény. *Feloldható csoportnak van olyan normállánca, amelynek elemei a csoport normálosztói (és a faktorok kommutatívak).* ■

Megjegyezzük, hogy végtelen csoportok esetén is értelmezhető a feloldhatóság. Itt az elfogadott definíció az, hogy létezik olyan normállánc, amelynek faktorai kommutatívak. A normállánc definíciója viszont ugyanaz, mint a véges esetben; megengedve a végtelen sok elemből álló normálláncot is (ilyenkor természetesen gondot okozhat a „következő” részcsoport definiálása).

Feladatok

1. Tekintsük egy G véges vagy végtelen Abel-csoport normálláncát. Két lehetőséget veszünk figyelembe: A) Minden normállláncra igaz a minimumfeltétel; B) Minden normállláncra igaz a maximumfeltétel. Bizonyítsuk be, hogy ha A) és B) mindegyike teljesül, akkor G véges. Egyébként van olyan G csoport, amelyben A) igaz, de B) nem, illetve B) igaz, de A) nem, és olyan eset is van, amikor egyik sem igaz.

2. Mutassunk példát olyan feloldható csoportra, amelynek a centruma triviális.

3. Bizonyítsuk be, hogy minden p-csoport feloldható.

4. Bizonyítsuk be, hogy ha egy csoport elemszáma legfeljebb három prímszám szorzata, akkor a csoport feloldható.

5. Bizonyítsuk be SCHREIER tételét, amely szerint, ha egy G csoportnak van két normállánca, akkor ezeknek van olyan finomításuk, amelyek izomorfak.

6. Mi a szükséges feltétele annak, hogy két (véges) csoportnak lehessenek izomorf kompozícióláncai? Mutassuk meg, hogy ez a feltétel elégséges is, ha mindkét csoport feloldható.

7. Legyen a G csoport rendje $p_1 \cdot p_2 \cdot \ldots \cdot p_r$, ahol e tényezők nem feltétlenül különböző prímszámok. Nevezzük a G csoportot „nagyon feloldhatónak”, ha a fenti szorzat tényezőit bármely $q_1, \ldots, q_r$ sorrendbe írva a csoportnak létezik olyan kompozíciólánca, amelyben az i-edik kompozíciófaktor rendje q_i.

Mutassuk meg, hogy minden (véges) Abel-csoport és minden (véges) p-csoport nagyon feloldható. Mutassuk meg, hogy van olyan feloldható csoport, amely nem nagyon feloldható.

8. Mutassuk meg, hogy nagyon feloldható csoportok direkt szorzata is nagyon feloldható.

9. Mutassuk meg, hogy egy véges csoport akkor és csak akkor nagyon feloldható, ha p-csoportok direkt szorzata.

10. Egy G véges csoportot *nilpotensnek* neveznek, ha vagy $|G| = 1$, vagy van nemtriviális centruma, és az e szerinti faktorcsoport nilpotens. Bizonyítsuk be, hogy minden nagyon feloldható csoport nilpotens (fordítva is igaz), és minden nilpotens csoport feloldható.

11. Legyen Z a (véges) G csoport centruma. Bizonyítsuk be, hogy ha G egy M maximális részcsoportja nem tartalmazza Z-t, akkor M normálosztó. Bizonyítsuk be, hogy nilpotens csoportokra ez akkor is igaz, ha $Z \leq M$.

12. Bizonyítsuk be, hogy nilpotens csoport minden Sylow-részcsoportja normálosztó; következésképpen a csoport Sylow-részcsoportjainak direkt szorzata.

13. Legyen G (véges) nilpotens csoport. Bizonyítsuk be, hogy $H < G$ esetén $H < N(H)$, és ha H nem normálosztó G-ben, akkor $N(H) < N(N(H))$.

6.3. Permutációcsoportok

A csoportelméleti – és ezzel együtt az absztrakt algebrai – kutatások megindulása lényegében a permutációcsoportok vizsgálatára vezethető vissza. Eredetileg egy egyenlet gyökei „helyettesítéseinek” (szubsztitúcióinak) a csoportját vizsgálták, de ehelyett igen hamar rátértek a gyökök permutálásainak a csoportjára, mert ez sokkal jobban kezelhető volt.

6.13. Tétel. *Egy H halmaz permutálásai – azaz önmagára való bijektív leképezései – a függvénykompozícióra mint szorzásra nézve csoportot alkotnak. Ezt a csoportot S_H jelöli.*

Bizonyítás. A szorzásra való zártság abból következik, hogy bijekciók szorzata is bijekció. A H halmaz $\iota = \iota_H$ identikus leképezése nyilvánvalóan bijekció, amely az S_H egységeleme. Ha ugyanis σ az S_H tetszőleges eleme, akkor bármely $a \in H$ esetén

$$\sigma\iota(a) = \sigma(\iota(a)) = \sigma(a) \qquad \text{és} \qquad \iota\sigma(a) = \iota(\sigma(a)) = \sigma(a)$$

teljesül, vagyis $\sigma\iota = \iota\sigma = \sigma$. Legyen most σ az S_H tetszőleges eleme. Definiáljuk a σ^{-1} leképezést a $\sigma^{-1}(\sigma(a)) = a$ összefüggéssel. Mivel σ szürjektív, ezért a leképezést H minden elemére definiáltuk; és σ injektivitása miatt egyértelműen. Tekintettel arra, hogy a választása tetszőleges, ezért σ^{-1} szürjektív. $\sigma^{-1}(\sigma(a)) = \sigma^{-1}(\sigma(b))$ esetén $a = b$, amiből $\sigma(a) = \sigma(b)$, és így végül is σ^{-1} injektivitása következik. A definiált leképezés tehát bijekció, amelyre nyilvánvalóan fennáll a $\sigma^{-1}\sigma = \iota$ összefüggés. Az 5.2. tétel (IV) pontja alapján tehát S_H csoport. ■

6.14. Definíció. Az S_H egy G részcsoportját tranzitívnak nevezzük, ha bármely $a, b \in H$ elemekhez létezik olyan $\sigma \in G$, amelyre $\sigma(a) = b$. A H egy K részhalmazának G-beli stabilizátorán a G elemeinek azt a G^K részhalmazát értjük, amely a K minden elemét önmagára képező permutálásokból áll. Az $\{1, \ldots, n\}$ halmaz permutációcsoportját S_n-nel jelöljük, és n-edfokú szimmetrikus csoportnak nevezzük, ennek részcsoportjait pedig n-edfokú permutációcsoportoknak. □

6.15. Tétel. *Legyen G az S_H egy részcsoportja. Ekkor*

(1) *G^K a H minden K részhalmazára részcsoport.*

(2) $\left\{\bigcap G^{\{a\}} \;\middle|\; a \in H\right\} = \{\iota\}$.

(3) *Ha G tranzitív, akkor a $G^{\{a\}}$ részcsoportok egymás konjugáltjai.*

(4) *Ha G n-edfokú tranzitív, akkor $(G : G^{\{i\}}) = n$ $(i = 1, \dots, n)$.*

(5) *S_n rendje $n!$.*

Bizonyítás. Világos, hogy az identitás eleme G^K-nak; a szorzásra és az inverzképzésre való zártság pedig nyilvánvaló. Ugyancsak nyilvánvaló a (2) állítás, hiszen csak az identitás képez minden elemet önmagára.

(3) bizonyításához válasszunk egy olyan G-beli σ-t, amelyre $\sigma(a) = b$. Ha $\tau \in G^{\{a\}}$, akkor $\sigma\tau\sigma^{-1}(b) = \sigma\tau(a) = \sigma(a) = b$ miatt $\sigma G^{\{a\}}\sigma^{-1} \leq G^{\{b\}}$. Hasonlóképpen adódik, hogy $\sigma^{-1}G^{\{b\}}\sigma \leq G^{\{a\}}$, ami bizonyítja állításunkat.

(3) alapján (4)-ben elegendő az $i = 1$ esetet nézni. $\sigma^{-1}\tau \in G^{\{i\}}$ pontosan akkor teljesül, ha $\sigma^{-1}\tau(1) = 1$, azaz $\tau(1) = \sigma(1)$. A $G^{\{1\}}$ egy-egy bal oldali mellékosztálya tehát pontosan azokból a G-beli elemekből áll, amelyek az 1-et ugyanabba az elembe viszik. A tranzitivitás alapján tehát a mellékosztályok száma n, mint állítottuk.

Az (5) állítás $n = 1$ esetén triviális. S_n nyilván tranzitív, mert két elem felcserélése permutálás (a többi elem fixen marad). Így S_n-re alkalmazható a (4) alatti eredmény. $(S_n)^{\{n\}} = S_{n-1}$ miatt, a Lagrange-tételt figyelembe véve $|S_n| = n \cdot |S_{n-1}|$ adódik; és egy nyilvánvaló indukcióval kapjuk a kívánt összefüggést. ■

6.16. Tétel. *Legyen $G \leq S_H$, és legyen $\sim_G \subseteq H \times H$ az a reláció, amelynél $a \sim_G b$ pontosan akkor, ha van olyan $\sigma \in G$, amelynél $\sigma(a) = b$. Ez a reláció ekvivalenciareláció. A megfelelő osztályozásban az $a \in H$ elemet tartalmazó $P_G(a)$ osztályt a G egy pályájának nevezzük. A G elemei megszoríthatók a $K = P_G(a)$ halmazra; $G^K \lhd G$ és a létrehozott permutálások csoportja izomorf a G/G^K faktorcsoporttal. E permutálások az S_K-nak egy tranzitív részcsoportját alkotják. G pontosan akkor tranzitív részcsoportja S_H-nak, ha G-nek egyetlen pályája van.*

Bizonyítás. $\iota \in G$ miatt a reláció reflexív. G-nek a szorzásra való zártsága biztosítja a reláció tranzitivitását, míg az inverzképzésre való zártság a szimmetriát. Ha $b \in K = P_G(a)$, akkor van olyan $\tau \in G$, amire $b = \tau(a)$. Ha mármost $\sigma \in G$, akkor G szorzásra való zártsága alapján $\sigma(b) = \sigma(\tau(a)) \in K$; tehát G megszorítható K-ra. Ha $\tau \in G^K$, akkor bármely $\sigma, \varrho \in G$ esetén $\tau(\varrho\sigma(a)) = \varrho\sigma(a)$, azaz $\varrho^{-1}\tau\varrho(\sigma(a)) = \sigma(a)$, vagyis $\varrho^{-1}\tau\varrho \in G^K$, tehát G^K normálosztó. Több permutálás is hathat ugyanúgy K-n. α és β pontosan akkor ilyenek, ha $\alpha^{-1}\beta$ az identikus permutálást hozza létre K-n, azaz, ha $\alpha^{-1}\beta \in G^K$. Eszerint a G/G^K-ban levő bármely mellékosztály minden eleme ugyanúgy hat K-n. Tekintettel arra, hogy bármely $b \in P_G(a)$ esetén van olyan $\sigma \in G$, amire $b = \sigma(a)$, ezért G a K-n tranzitív. Az utolsó állítás ebből triviálisan következik. ■

6.17. Definíció. Tetszőleges $\sigma \in G$ esetén $K = P_\sigma(a) = P_{\langle\sigma\rangle}(a)$, amit σ pályájának hívunk. Ha K egyelemű, akkor a pálya triviális, egyébként valódi. Ha σ-nak egyetlen valódi pályája van, akkor σ-t ciklusnak vagy ciklikus permutálásnak nevezzük. A valódi pályák T_σ egyesítése a σ tartóhalmaza. □

Érdemes megfigyelni a következőket: A σ egy pályája a $\ldots, \sigma^{-1}(a), a, \sigma(a), \ldots$ elemekből áll. Ha $\sigma^k(a) = a$, akkor e pálya elemei: $\{a, \sigma(a), \ldots, \sigma^{k-1}(a)\}$. Ez az eset például akkor, ha σ rendje k.

A továbbiakban – ha mást nem mondunk – csak véges halmazok permutálásaival fogunk foglalkozni. Tetszőleges H és K, valamint $\varphi : H \to K$ bijekció esetén S_H és S_K természetes módon izomorfak: a $\sigma \in S_H$ permutálásnak megfeleltetve a $\varphi\sigma\varphi^{-1}$ permutálást. Mivel egy n elemű halmaz bijektíven leképezhető az $\{1, \ldots, n\}$ elemek halmazára, ezért a továbbiakban az S_n vizsgálatára szorítkozhatunk. A továbbiakban rögzített n mellett vizsgáljuk az S_n-t.

6.18. Tétel. *A $\sigma, \tau \in S_H$ permutálásokat idegeneknek vagy diszjunktaknak nevezzük, ha tartóhalmazaik idegenek. Idegen permutálások felcserélhetők; ha σ és τ felcserélhetők, akkor σ bármely pályája vagy benne van τ tartóhalmazában, vagy idegen tőle.*

Legyenek $\sigma_1, \ldots, \sigma_r$ páronként idegen permutálások, és legyen σ a szorzatuk. Ekkor T_σ a $T_{\sigma_1}, \ldots, T_{\sigma_r}$ tartóhalmazok diszjunkt egyesítése, és σ-t T_{σ_i}-re megszorítva a σ_i permutálást kapjuk.

Bizonyítás. Világos, hogy $T_\sigma = \{i \mid \sigma(i) \neq i\}$. A σ és τ permutálások tehát pontosan akkor idegenek, ha bármely $1 \leq i \leq n$ egész számra $\sigma(i)$ és $\tau(i)$ közül legalább az egyik megegyezik i-vel (esetleg mindkettő is).

Ha i egyik permutálás tartóhalmazában sincs benne, akkor $\sigma\tau(i) = \tau\sigma(i) = i$. Ha $i \in T_\sigma$, akkor σ injektivitása miatt $\sigma\sigma(i) \neq \sigma(i)$, tehát $\sigma(i) \in T_\sigma$ is teljesül. A két permutálás idegensége alapján tehát $\tau\sigma(i) = \sigma(i) = \sigma\tau(i)$. A T_τ elemeire ugyanígy látható be, hogy rajtuk $\sigma\tau$ és $\tau\sigma$ ugyanúgy hat; és a felvett két permutálás idegensége alapján más elem nincs. Így $\sigma\tau = \tau\sigma$. Tegyük fel most, hogy $\sigma\tau = \tau\sigma$, és legyen $i \notin T_\tau$. Ekkor $\tau\sigma(i) = \sigma\tau(i) = \sigma(i)$ miatt $\sigma(i) \notin T_\tau$, és így $\sigma^k(i)$ sohasem eleme T_τ-nak. A pálya definíciója szerint (6.16. tétel) tehát, ha σ egy pályájának valamelyik eleme nincs benne τ tartóhalmazában, akkor a szóban forgó pálya egyetlen eleme sincs benne.

Legyenek $\sigma_1, \ldots, \sigma_r$ páronként idegen permutálások, és legyen σ a szorzatuk. Tekintettel arra, hogy e permutálások idegenek, ezért tartóhalmazaik T egyesítése diszjunkt egyesítés. Ha $i \notin T$, akkor i-t a fenti permutálások mindegyike, s így szorzatuk is önmagába viszi, tehát $T_\sigma \subseteq T$. Legyen most i a tényezők valamelyikének a tartóhalmazában. Mivel e permutálások felcserélhetők, ezért feltehetjük, hogy $i \in T_{\sigma_1}$. Mivel a többi permutálás i-t fixen hagyja, ezért $\sigma(i) = \sigma_1(i) \neq i$. Ebből egyrészt az adódik, hogy $T_\sigma \subseteq T$, vagyis T a σ tartóhalmaza; másrészt azt is kapjuk, hogy σ-t T_{σ_i}-re megszorítva a σ_i permutálást kapjuk. ■

6.19. Tétel. *Minden permutálás egyértelműen felbontható idegen ciklusok szorzatára, amelyeket a permutálás idegen ciklustényezőinek nevezünk.*

Bizonyítás. Legyenek $T_1, \ldots, T_r$ a σ pályái. Definiáljuk a σ_i leképezéseket úgy, hogy $\sigma_i(j) = \sigma(j)$, ha $j \in T_i$, és minden más j-re legyen $\sigma_i(j) = j$. Mindenekelőtt bebizonyítjuk, hogy a fenti leképezések permutálások. A bijektivitás nyilvánvaló a T_i-n kívüli elemekre. Ha $j, k \in T_i$, akkor $\sigma_i(j) = \sigma_i(k)$ esetén σ_i definíciójából és σ injektivitásából $j = k$ következik, tehát σ_i injektív. Ha $k \in T_i$, akkor válasszuk azt – a σ szürjektivitása miatt létező – j elemet, amelyre $\sigma(j) = k$. A pálya definíciója szerint $j \in T_i$, amiből σ_i definíciója alapján $\sigma_i(j) = k$ következik. Így a fenti leképezések valóban permutálások. Definíciójukból következik, hogy mindegyikük ciklus, és páronként idegenek. Legyen $\sigma' = \sigma_1 \cdot \ldots \cdot \sigma_r$. Ha $\sigma(j) = j$, akkor minden i-re $\sigma_i(j) = j$, amiből $\sigma'(j) = j = \sigma(j)$ következik. Tegyük most fel, hogy $j \in T_i$, valamelyik i-re. Mivel σ ciklusténye zői idegenek, a 6.18. tétel szerint felcserélhetők, ezért feltehető, hogy $i = 1$. Ugyancsak a ciklusténye zők idegenségét felhasználva, bármely $j \in T_1$ elemre $\sigma'(j) = \sigma_i(j) = \sigma(j)$ adódik, azaz $\sigma' = \sigma$. Ezzel a felbontás létezését igazoltuk.

Az egyértelműség azonnal következik a 6.18. tétel utolsó állításából. ■

6.20. Tétel. *Ha a σ ciklus tartóhalmazának k eleme van, akkor ezek – amelyeket σ elemeinek is nevezünk – úgy írhatók $i_1, i_2, \ldots, i_k$ sorrendbe, hogy σ minden egyes elemet a következőre, i_k-t pedig i_1-re képezi. A felírást a tartóhalmaz bármely elemével kezdhetjük. σ-ra a $\sigma = (i_1, i_2, \ldots, i_k)$ (ha nem okoz gondot, akkor a $\sigma = (i_1 i_2 \ldots i_k)$) jelölést használjuk, és a k számot σ hosszának nevezzük. Egy ciklus rendje megegyezik a hosszával, és egy tetszőleges permutálás rendje megegyezik idegen ciklusténye zői hosszának legkisebb közös többszörösével. A σ ciklus inverze $\sigma^{-1} = (i_k, \ldots, i_2, i_1)$.*

Bizonyítás. Induljunk ki a tartóhalmaz tetszőleges i_1 eleméből; és ha i_j-t már meghatároztuk, akkor legyen $i_{j+1} = \sigma(i_j)$. Mivel véges sok elemet permutálunk, lesz egy első olyan lépés, amikor már előzőleg felsorolt elemet kapunk. Az injektivitás miatt ez az elem csak az i_1 lehet. Ekkor σ a felsorolt elemek bármelyikét egy, már ugyancsak felsorolt elembe viszi, amiből következik, hogy a felsorolt elemek σ egy pályájának elemei. Mivel σ ciklus, ezért a tartóhalmaz minden elemét felírtuk. Ha $r \leq k - 1$, akkor $\sigma^r(i_1) = i_{r+1} \neq$ $= i_1$, míg $\sigma^k(i_1) = i_1$. Mivel kiindulásul a tartóhalmaz bármely elemét választhattuk, ezért σ rendje valóban k.

A permutálás rendjére vonatkozó állítást az idegen ciklusténye zők számára vonatkozó teljes indukcióval bizonyítjuk. Az előbb belátott eredmény következtében ehhez elég azt bizonyítani, hogy idegen permutálások szorzatának rendje megegyezik rendjeik legkisebb közös többszörösével. Legyen σ rendje k, τ rendje m, és legyen $n = [k, m]$. Az idegen permutálások felcserélhetősége alapján $(\sigma\tau)^n = \sigma^n\tau^n = \iota\iota = \iota$. Tegyük most fel, hogy $(\sigma\tau)^t = \iota$. A felcserélhetőséget és a tartóhalmazok diszjunktságát felhasználva azt kapjuk, hogy T_σ bármely i elemére $\sigma^t(i) = \sigma^t\tau^t(i) = (\sigma\tau)^t(i) = i$. Mivel T_σ-n kívüli elemeket már σ is önmagába visz, ezért $\sigma^t = \iota$, azaz $k \mid t$. Hasonlóan adódik, hogy $m \mid t$, amiből $n \mid t$ következik. Az utolsó állítás nyilvánvaló. ■

Az előző tétel alapján a következő módon képzelhetjük el egy permutálás hatását. T_σ az a rész, amelyiken a permutálás ténylegesen hat. Ezen belül egy-egy $P_\sigma(a)$ pálya elemeit egy-egy kör kerületére írjuk fel. E részeken a permutálás (egymástól függetlenül) egyidejűleg egy-egy lépéssel forgat. Ha a permutálást csak egy-egy pályán belül figyeljük, akkor itt

éppen a megfelelő idegen ciklusténye zőt kapjuk. Ha a permutálást többször egymás után alkalmazzuk, akkor előfordul, hogy valamelyik pályán identikus leképezést kapunk. Az első olyan lépésszám, amelyiknél ez minden egyes pályán egyszerre történik meg, éppen a permutáció rendjét adja. A 6.19. tételből azonnal adódik:

6.21. Következmény. *A ciklusok generálják S_n-t.* ■

Megjegyezzük, hogy a kapott eredmény igen gyenge, mert az S_n-beli $n!$ számú elemből mintegy $e \cdot (n-1)!$ számú elem ciklus ($e = 2{,}718\ldots$). Sokkal jobb eredményt szolgáltat majd az alábbi triviális felbontási tétel:

6.22. Tétel. *Ha $1 < i < k$, akkor*

$$(1, 2, \ldots, i-1, i, i+1, \ldots, k) = (1, 2, \ldots, i-1, i)(i, i+1, \ldots, k).$$

Minden permutálás felbontható 2 hosszúságú ciklusok – úgynevezett transzpozíciók – szorzatára. (Ezek általában nem felcserélhető tényezők, és a felbontás nem egyértelmű!)

A transzpozíciók generálják S_n-t.

Bizonyítás. Nyilván elegendő bizonyítani, hogy a fenti szorzatfelbontás valóban igaz. A szorzat $\sigma = \tau\varrho$ alakú, és a $\sigma(j) = \tau\varrho(j)$ összefüggés minden olyan j-re világos, amely

1. nem szerepel a felírt számok között,
2. $i \le j < k$ (ekkor $\varrho(j) = \sigma(j)$ és τ a $\varrho(j)$-t fixen hagyja),
3. $j < i$ (ekkor $\varrho(j) = j$ és $\sigma(j) = \tau(j)$).

Az egyetlen kimaradt eset az, amikor $j = k$. Ekkor $\sigma(k) = 1$, és $\tau\varrho(k) = \tau(i) = 1$. ■

Mivel S_n transzpozícióinak a száma $\binom{n}{2}$, ezért a kapott generátorrendszer lényegesen kevesebb elemű, mint a 6.21. következményben levő.

A fent megadott mindkét generátorrendszer igen fontos, de még az utóbbi elemszáma is igen nagy (az S_n rendje $n!$): a kapott generátorrendszer elemszáma – durván – a rend logaritmusának a négyzete. Az elemszám tetszőleges csoport esetében is csökkenthető, és olyan generátorrendszert konstruálhatunk, amelyiknek az elemszáma nagyságrendben a csoport rendjének logaritmusa. Ha ugyanis egy elemrendszerhez mindig egy olyan újabb elemet veszünk, amelyik nincs benn az előzőek generálta részcsoportban, akkor az újabb generátum elemszáma – Lagrange tétele alapján – legalább kétszer akkora, mint az előzőé (az is világos, hogy ez csak igen speciális esetben állhat fenn minden lépésben). Ezt az eljárást figyelembe véve, a fenti generátorrendszerből is ki tudunk venni $n-1$ darabot úgy, hogy ez még mindig generátorrendszer maradjon. Az $(i, j) = (i, i+1)(i+1, j)(i, i+1)$ könnyen ellenőrizhető összefüggés alapján minden transzpozíció visszavezethető $(i, i+1)$ alakúak szorzatára. Az S_n szerkezetének a „bonyolultságát” mutatja, hogy a generátorrendszer elemszáma tovább csökkenthető; például az $(1, 2)$ és $(1, 2, \ldots, n)$ ciklusok is generálják S_n-t! Ezt a következőképpen láthatjuk be. Triviális számolással adódik, hogy

$$(1, 2, \ldots, n)(1, 2)(n, \ldots, 2, 1) = (2, 3).$$

Mivel $(n, \ldots, 2, 1) = (1, 2, \ldots, n)^{-1}$ és egy ciklust bármely elemével kezdhetünk, ezért $(2, 3)$ benne van a kérdéses generátumban, és ugyanígy belátható, hogy minden $(i, i+1)$ is benne van.

6.23. Definíció. Azt mondjuk, hogy 1-nél nagyobb egész számok egy $(k_1, \ldots, k_r)$ rendszere a σ permutálás típusa, ha σ idegen ciklusténye zőinek a hossza – valamilyen sorrendben – éppen $k_1, \ldots, k_r$. □

Világos, hogy egy permutálás típusa pontosan azt adja meg, hogy a permutálás miképpen hat az alaphalmazon. A 6.23. definícióban adott típus azt jelenti, hogy az alaphalmaznak léteznek $k_1, \ldots, k_r$ elemű diszjunkt részhalmazai, amelyeknek az elemeit σ különkülön ciklikusan permutálja. Megmutatjuk, hogy az azonos típusú permutálások sokkal szorosabb kapcsolatban állnak egymással.

6.24. Tétel. *Két permutálás típusa akkor és csak akkor egyenlő, ha ezek konjugáltak.*

Bizonyítás. Először azt mutatjuk meg, hogy a σ permutálás minden konjugáltja vele megegyező típusú. Nyilvánvaló, hogy a permutálás típusa nem függ attól, hogy az egyes T_i halmazokban éppen melyik számok fordulnak elő. Írjuk ezért minden egyes szóba jövő j szám helyébe a $\varrho(j)$ számot, ahol ϱ az S_n tetszőleges eleme. Ezáltal egy olyan τ permutálást kapunk, amelyik σ-val egyenlő típusú, és a $\varrho(j)$-t a $\varrho(\sigma(j))$-be viszi. Így minden j-re teljesül a $\tau\varrho(j) = \varrho\sigma(j)$ összefüggés, amiből $\tau\varrho = \varrho\sigma$, azaz $\tau = \varrho\sigma\varrho^{-1}$ következik. Mivel ϱ tetszőleges volt, ezért azt kaptuk, hogy σ bármely konjugáltjának ugyanaz a típusa, mint σ-nak.

Tekintsük most az egyenlő típusú τ és ϱ permutálásokat. Legyenek e permutációk pályái (a triviálisakat is belevéve!): $P_1, \ldots, P_s$, illetve $Q_1, \ldots, Q_s$, úgy felsorolva, hogy $|P_i| = |Q_i|$ $(1 \le i \le s)$. Válasszunk ki minden egyes P_i-ből egy v_i és minden egyes Q_i-ből egy u_i elemet. Definiáljuk a ϱ leképezést a $\varrho(\sigma^k(u_i)) = \tau^k(v_i)$ összefüggéssel $(1 \le i \le s$, $k \ge 0$ egész szám). Mindenekelőtt be kell látni, hogy ϱ valóban leképezés. Ez azonnal következik abból, hogy $\sigma^k(u_i) = \sigma^m(u_i)$ esetén $\tau^k(v_i) = \tau^m(v_i)$ is fennáll, mert a két permutáció azonos típusú és a pályákat megfelelően rendeztük sorba. Mivel teljesen analóg módon a $\tau^k(v_i) = \tau^m(v_i)$ feltételből is következik a $\sigma^k(u_i) = \sigma^m(u_i)$ egyenlőség, ezért ϱ injektív. Figyelembe véve végül azt, hogy minden 1 és n közötti egész szám felírható – alkalmas k és i választásával – $\sigma^k(u_i)$, illetve $\tau^k(v_i)$ alakban, azt kapjuk, hogy ϱ az egész $\{1, \ldots, n\}$ halmazt képezi önmagába, mégpedig injektíven. Így ϱ e halmaz permutációja. Tetszőleges $j = \sigma^k(u_i)$ esetén:

$$\varrho\sigma(j) = \varrho\sigma^{k+1}(u_i) = \tau^{k+1}(v_i) = \tau(\tau^k(v_j)) = \tau(\varrho\sigma^k(u_i)) = \tau\varrho(j),$$

amiből $\varrho\sigma = \tau\varrho$, illetve $\tau = \varrho\sigma\varrho^{-1}$ következik. ■

Az S_n tetszőleges σ elemét alkalmazhatjuk bármely n-határozatlanú polinomra a

$$\sigma : f(x_1, x_2, \ldots, x_n) \mapsto f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

definíció alapján. Igen fontos az az eset, amikor a

$$V_n = V_n(x_1, x_2, \ldots, x_n) = \begin{vmatrix} 1 & x_1 & \ldots & (x_1)^{n-1} \\ 1 & x_2 & \ldots & (x_2)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \ldots & (x_n)^{n-1} \end{vmatrix}$$

Vandermonde-determinánssal megadott, úgynevezett *alternáló polinomból* indulunk ki.

6.25. Tétel. *Az S_n bármely σ eleme a V_n polinomot vagy önmagába, vagy negatívjába viszi. Azok a permutálások, amelyek V_n-et önmagába képezik, az S_n egy A_n normálosztóját alkotják, amelynek indexe $n \geq 2$ esetén 2. Ezt a normálosztót n-edfokú alternáló csoportnak nevezzük. Egy permutálás akkor és csak akkor képezi V_n-et önmagára, ha transzpozíciókra való felbontásában a transzpozíciók száma páros. A transzpozíciók számának párossága a felbontástól független. Az A_n elemeit páros permutációknak nevezzük, a többi permutációt páratlannak.*

Bizonyítás. A határozatlanok permutálásával a V_n Vandermonde-determináns sorai permutálódnak, és így vagy nem változik meg, vagy előjelet vált. Az identitás V_n-et fixen hagyja, s ha két permutálás önmagába viszi, akkor nyilván a szorzatuk is. Mivel S_n véges, ebből már következik, hogy A_n részcsoport. Legyen $\tau \in S_n$ tetszőleges transzpozíció (ilyen elem pontosan $n \geq 2$ esetén létezik). Ekkor a determinánsok alaptulajdonságai szerint $\tau(V_n) = -V_n$. Így tetszőleges σ permutálásra $\tau\sigma(V_n) = -\sigma(V_n)$, amiből azonnal következik, hogy $\tau\sigma$ akkor és csak akkor eleme A_n-nek, ha $\sigma \notin A_n$, és akkor és csak akkor nem eleme A_n-nek, ha $\sigma \in A_n$. Tehát $n \geq 2$ esetén $(S_n : A_n) = 2$, amiből az 5.35. tétel szerint következik, hogy $A_n \lhd S_n$. Ha egy σ permutálást k darab transzpozíció szorzatára tudunk bontani, akkor $\sigma(V_n) = (-1)^k V_n$. Minthogy $\sigma(V_n)$ a felbontástól független, ezért k párossága sem függ a felbontástól. ■

Érdemes megjegyezni a következőket. A 6.22. tételbeli felbontás alapján egy k hosszúságú ciklust $k - 1$ transzpozíció szorzatára bonthatunk fel. Ez például teljes indukcióval látható be, az $i = k - 1$ választással. Így egy ciklus rendje akkor és csak akkor páros, ha hossza páratlan.

A szimmetrikus és alternáló polinomokkal már találkoztunk az első kötetben az I. rész 4.4. pontjában. Ott lényegében bizonyítást nyert, hogy egy permutálás az összes szimmetrikus polinomot fixen hagyja és a páros permutálások pontosan az alternáló polinomokat. Ezért nevezik e csoportokat szimmetrikus, illetve alternáló csoportoknak.

6.4 Csoport-előállítás permutációcsoportokkal

A továbbiakban is elsősorban véges permutációcsoportokra gondolunk; ahol ezt nem tesszük, S_n helyett S_H-t írunk. Mint már említettük, a permutációcsoportok vizsgálata volt a csoportelmélet kiindulópontja. Az „absztrakt” csoportelméletnek nagy haszna az, hogy nem kell magunkkal vinni a permutálások sokszor „esetlen” felírását. A most következő tétel azt mutatja meg, hogy az „absztrakt” csoportelmélet a csoportok belső szerkezetét illetően nem tud a permutációcsoportoktól különböző csoportot előállítani.

6.26. Tétel (Cayley-féle reprezentációs tétel). *Legyen G a $\mathfrak{G}$ csoport tartóhalmaza. Ekkor $\mathfrak{G}$ izomorf S_G egy részcsoportjával. Speciálisan minden n-edrendű csoport izomorf egy n-edfokú permutációcsoporttal.*

Bizonyítás. ($\mathfrak{G}$ helyett ismét a G alaphalmazt tekintjük.) A G csoport tetszőleges a eleméhez hozzárendelünk egy G-n értelmezett egyváltozós λ_a függvényt, amelyet a-val való balszorzásnak nevezünk:

$$\lambda_a(x) = ax \text{ (minden } G\text{-beli } x \text{ elemre).}$$

Mindenekelőtt kimutatjuk, hogy $\lambda_a \in S_G$. A szorzás egyértelműsége következtében λ_a egyértelműen meghatározott, s tekintettel arra, hogy az $ax = b$ egyenlet bármely csoportban egyértelműen megoldható, valóban S_H egy elemét kaptuk. Azt fogjuk bebizonyítani, hogy a $\Lambda : a \mapsto \lambda_a$ megfeleltetés izomorfizmus. A megfeleltetés nyilvánvalóan egyértelmű a balszorzások halmazára. $\Lambda : G \to S_G$ homomorfizmus, mert a $\Lambda(ab) = \lambda_{ab}$ leképezésre $\lambda_{ab}(x) = (ab)(x) = a(b(x)) = \lambda_a(\lambda_b(x))$ alapján $\Lambda(ab) = \Lambda(a)\Lambda(b)$ teljesül. $\mathrm{Im}(\Lambda)$ elemei – mint láttuk – a balszorzások (ezzel egyúttal azt is bizonyítottuk, hogy a balszorzások S_G egy részcsoportját alkotják). Ha $a \in \mathrm{Ker}\ (\Lambda)$, akkor λ_a az identitás, és így $1 = \lambda_a(1) = a1 = a$, a leképezés tehát a kívánt izomorfizmus. ■

Az eddigiekben megismerkedtünk csoportok konstruálásának néhány lehetőségével. Ezek közt egy olyan volt, amelynél valamilyen feltételnek eleget tevő csoportot kerestünk: nevezetesen egy csoport megadása definiáló relációkkal. Ez azonban nem biztosítja egy olyan csoport létezését, amely pontosan a kívánt tulajdonságokkal rendelkezik. Ilyen leírás lehet már ismert „számokkal jellemezhető" csoport részeként való megadás. Két fontos ilyen eset van: a permutációcsoportok és a reguláris mátrixok csoportja. Ez utóbbival később, a gyűrűk részletesebb tárgyalása után foglalkozunk majd. Az előbbire a Cayley-tétel ad lehetőséget. Ez a tétel viszont igen nagy fokú permutációcsoport részeként ábrázol. Gondoljuk meg, az S_n csoport Cayley-féle reprezentálásához $S_{n!}$-ra van szükség! A továbbiakban azt fogjuk megnézni, mennyire csökkenthető le a felhasznált permutációcsoport mérete.

6.27. Tétel. *A G csoport akkor és csak akkor ágyazható be S_k-ba tranzitív részcsoportként, ha van olyan $H \leq G$, amelyre $(G : H) = k$, és H konjugáltjainak a metszete egyedül az egységelemből áll.*

Bizonyítás. Legyen $H \leq G$ és legyen K a H bal oldali mellékosztályainak a halmaza. A Cayley-tételhez hasonlóan $\lambda_a : xH \mapsto axH$ a K-n értelmezett permutálás. Az is világos, hogy $\Lambda : a \mapsto \lambda_a$ homomorfizmus. Ahhoz, hogy ez beágyazás legyen, az szükséges, hogy magja egyedül az egységelemből álljon. Az $a \in \mathrm{Ker}\,\Lambda$ tartalmazás pontosan akkor igaz, ha minden $x \in G$ esetén $axH = xH$ teljesül. Ezzel az $x^{-1}ax \in H$, illetve $a \in xHx^{-1}$ feltétel ekvivalens. Ezáltal létrehoztunk egy $\Lambda : G \to S_k$ beágyazást. Ha xH és yH adott bal oldali mellékosztályok, akkor az $a = yx^{-1}$ elemre $\lambda_a : xH \mapsto yH$; a beágyazásnál kapott részcsoport tehát tranzitív.

Megfordítva, tegyük fel, hogy G ábrázolható a kívánt módon S_K-ban, ahol K tetszőleges halmaz. Legyen $u \in K$ tetszőleges elem, és legyen H a G-nek az u elemhez tartozó stabilizátora. Mivel G tranzitív, alkalmazhatjuk a 6.15. tételt, amely szerint a $G^{\{u\}}$ stabilitási részcsoport kielégíti a feltételeket. ■

Ha H végtelen, de indexe $(G : H) = k$ véges, akkor a fenti Λ homomorfizmus képe véges, amiből azonnal következik, hogy egy csoport bármely véges indexű részcsoportja tartalmaz véges indexű normálosztót.

Egy hatelemű kommutatív csoportra a fenti eredmények csak S_6-ban való ábrázolást tesznek lehetővé. Pedig a generátorelemnek megfeleltetve az (12)(345) permutálást, az S_5-ben való reprezentáláshoz jutunk. Persze, ez nem tranzitív részcsoport. Érdemes tehát általában megnézni a lehetőségeket. Ez annál inkább fontos, mert amennyiben a feltételek bizonyos k-ra nem teljesülnek, akkor tudjuk, hogy erre az S_k-ban való ábrázolás lehetetlen.

6.28. Tétel. *A G csoport akkor és csak akkor ágyazható be S_k-ba, ha vannak olyan $H_1, \dots, H_r$ részcsoportjai, amelyekre $(G : H_i) = k_i$ és $k = k_1 + \cdots + k_r$, továbbá a fenti részcsoportok és konjugáltjaik metszete egyedül az egységelemből áll.*

Bizonyítás. Legyen K az összes H_i-k bal oldali mellékosztályainak a halmaza. Mint az előzőekben, minden $a \in G$ elemnek megfeleltetjük az $xH_i \mapsto axH_i$ leképezést (minden $1 \leq i \leq r$ mellett). A megfeleltetés itt is homomorfizmus, amelynek a magja az összes H_i és konjugáltjainak a metszete; tehát e megfeleltetés injektív.

A megfordítás bizonyításához tekintsük a $G \leq S_k$ csoport $T_1, \dots, T_r$ pályáit. Legyen ezeknek mérete rendre $k_1, \dots, k_r$. Mivel e pályák idegenek, ezért $k_1 + \cdots + k_r = k$. Minden egyes T_i-ben választunk egy u_i elemet, és legyen H_i a G-nek ehhez tartozó stabilitási részcsoportja. A 6.27. tételből következik, hogy H_i indexe k_i; és a megfeleltetés magja az összes H_i-nek és konjugáltjaiknak a metszete. $G \leq S_k$ alapján e mag egyedül az egységelemből áll. ■

Feladatok

1. Határozzuk meg S_n p-Sylow részcsoportjait ($p \in \{2, 3\}$, $n < 5$).

2. Adjuk meg D_n reprezentációját S_k-ban, ahol k lehetőleg „kicsi”. Mely elemeknek felelhetnek meg páratlan permutálások?

3. Mutassuk meg, hogy minden csoport reprezentálható csak páros permutációkkal.

4. Bizonyítsuk be, hogy a Q kvaterniócsoport csak akkor ágyazható be S_n-be, ha $n \geq 8$.

5. Legyen S_∞^* az egész számok azon permutálásainak összessége, amelyeknek a tartóhalmaza véges, és S_∞ az összeseké (permutálás=bijekció). Bizonyítsuk be, hogy $S_\infty^* \lhd S_\infty$.

6. Bizonyítsuk be, hogy S_∞^* nem generálható véges sok elemével.

7. Adjunk meg olyan n elemű csoportokat, amelyek nem generálhatók $\log_2 n$-nél kevesebb elemmel.

8. Bizonyítsuk be, hogy van olyan $\sigma, \tau \in S_\infty$, hogy az általuk generált csoport tartalmazza S_∞^*-t.

9. A szabályos testekhez adjunk meg minél kisebb n-et (persze mindegyikhez mást lehet), amelyre S_n tartalmazza ezek egybevágósági transzformációinak a csoportját. A minimális n esetén mely transzformációknak felel meg páros permutálás?

10. Legyen L_n a modulo n vett maradékosztályok M halmazán az $x \mapsto ax + b$ alakban adott azon leképezéseinek az összessége, amelyekre $(a, n) = 1$. Bizonyítsuk be, hogy ez csoport, továbbá feloldható; és reprezentáljuk S_M-ben. Határozzuk meg az $(S_n : L_n)$ indexet.

11. A G csoport a elemének feleltessük meg a $\mu_a : x \mapsto xa$ permutációt. Milyen tulajdonságai vannak e megfeleltetésnek?

12. Bizonyítsuk be, hogy minden G csoporthoz van olyan unáris algebra, amelynek automorfizmuscsoportja izomorf G-vel.

13. Legyen $n = 3k + r$, ahol $k \geq 0$ és $r \in \{2, 3, 4\}$. Bizonyítsuk be, hogy S_n maximális méretű kommutatív részcsoportjának az elemszáma $3^k \cdot r$.

14. Bizonyítsuk be, hogy S_p-ben a p-Sylowok száma $(p-2)!$.

15. Bizonyítsuk be, hogy $n > 2$ esetén S_n centruma triviális.

6.5. A szimmetrikus csoport kompozícióláncai

Mint említettük, mind a permutációcsoportoknak, mind a feloldhatóságnak a fogalma az egyenletek gyökeinek a vizsgálata során merültek fel. Ezek összekapcsolása végett a továbbiakban az S_n kompozícióláncait vizsgáljuk. Mint látni fogjuk, S_n általában nem feloldható; éppen ezért bizonyos speciális esetekben majd azt is megnézzük, hogy S_n-nek mely részcsoportjai lehetnek feloldhatók.

6.29. Tétel. *Ha $n \geq 3$, akkor A_n-t generálják a hármas ciklusok. Legyen N az A_n-nek vagy az S_n-nek egy normálosztója. Ha N tartalmaz transzpozíciót, akkor $N = S_n$, ha N tartalmaz hármas ciklust, akkor vagy $N = A_n$, vagy $N = S_n$.*

Bizonyítás. A 6.28. tétel alapján azt kell bizonyítani, hogy bármely permutálás, amely páros sok transzpozíció szorzata, felírható hármas ciklusok szorzataként. Ehhez természetesen elég annak a megmutatása, hogy két transzpozíció szorzatát elő tudjuk így állítani. Ha a két transzpozíció megegyezik, akkor szorzatuk az identitás, tehát nincs mit bizonyítani. Ha a két transzpozíciónak egyetlen közös eleme van, akkor a kérdéses szorzat (12)(23) alakú, ami éppen (123). (Ez egyébként a 6.22. tétel speciális eseteként is adódik.) Ha a két transzpozíciónak egyetlen közös eleme sincs, akkor az alábbi triviális számolással kaphatjuk a kívánt előállítást:

$$(12)(34) = (12)(23)(23)(34) = (123)(234),$$

figyelembe véve az előző esetet.

Legyen most $N \lhd S_n$. Ha N-ben van egy k hosszúságú ciklus, akkor a 6.24. tétel szerint minden k hosszúságú ciklus benne van. Ebből a $k = 2$ esetben a 6.22. tétel alapján kapjuk, hogy $N = S_n$, illetve a $k = 3$ esetben a most belátottak szerint azt kapjuk, hogy $A_n \subseteq N$. Ez utóbbi esetben $(S_n : A_n) = 2$ miatt vagy $N = A_n$, vagy $N = S_n$ lehetséges.

Ha $N \lhd A_n$, akkor N csak páros permutációkat tartalmaz, tehát transzpozíciókat nem. Így az az eset áll elő, hogy N-ben van hármas ciklus. A hármas ciklusok konjugáltak S_n-ben, de A_n-ben már nem feltétlenül. Például az

$$(123)^2 = (132) = (12)(123)(12)$$

felírás alapján egy hármas ciklusból a négyzetét páratlan permutálással konjugálva kapjuk. Legyen $\sigma = (123) \in N$, és tekintsünk egy tetszőleges $\varrho = (ijk)$ hármas ciklust. Ekkor van olyan $\mu \in S_n$, amelyre $\varrho = \mu^{-1}\sigma\mu$. Ha μ páros, akkor $\varrho \in N$. Ha μ páratlan, akkor az (ij) transzpozícióra $\tau = \mu(ij)$ páros, és így $(jik) = \tau^{-1}\sigma\tau \in N$. Ebből pedig $(ijk) = (jik)^2 \in N$ következik; tehát $N = A_n$. ■

6.30. Tétel. *Ha N az A_n-nek vagy az S_n-nek legalább kételemű normálosztója, akkor N tartalmaz vagy egy transzpozíciót, vagy egy hármas ciklust, vagy két idegen transzpozíció szorzatát. Ha $n \neq 4$, akkor az első két eset valamelyikének kell teljesülnie.*

Bizonyítás. A bizonyítás a következő meggondoláson alapszik. A keresett permutálások olyanok, hogy a tartóhalmazuk „nagyon kicsi". Az N egy tetszőleges σ permutálásában tehát „le kell vágni" a tartóhalmaz nagy részét. Ez úgy történhet, hogy a permutálást felírjuk $\sigma = \tau\varrho$ alakban a 6.22. tétel felhasználásával, úgy, hogy τ-nak viszonylag kicsi legyen a tartóhalmaza. Az 5.63. tétel szerint tetszőleges μ-vel – amelyet célszerű A_n-belinek választani, hogy mindkét esetre használható legyen – a $[\sigma;\mu]$ kommutátor N-ben van. Ha mármost μ idegen ϱ-hoz, akkor a 6.18. tétel első állítása szerint felcserélhetők, amiből ugyancsak az 5.63. tétel felhasználásával azt kapjuk, hogy $[\tau;\mu] \in N$. Amennyiben μ-t úgy választjuk, hogy τ valamelyik ciklusa ne legyen benne μ tartóhalmazában, de ne is legyen idegen hozzá, akkor a 6.18. tétel második állítása miatt τ és μ nem lehetnek felcserélhetők; a kapott kommutátor tehát nem az identikus permutálás. Mivel a kapott kommutátor tartóhalmaza nyilvánvalóan benne van a $T_\tau \cup T_\mu$ halmazban, ezért elég kicsi – azaz jól kezelhető permutálást kapunk.

A bizonyítás során σ ciklusfelbontásától függően néhány esetet kell megkülönböztetnünk.

1. Ha σ-ban szerepel egy legalább négy hosszúságú ciklus, például $\sigma = (1234\ldots)\ldots$ …, akkor a felbontásnál lehet $\tau = (1234)$, és feltehető, hogy ϱ-ban 2, 3, 4 nem fordul elő. (Idegen ciklusténye zőkben a felsorolt négy szám nem szerepelhet, s ha alkalmazzuk a 6.22. tételt, akkor ϱ-ban a felsorolt négy szám közül legfeljebb még egy léphet fel.)

2. Ha σ-ban nincs legalább 4 hosszúságú ciklus, de van hármas ciklus, és szerepel más is, például $\sigma = (123)(45\ldots)\ldots$, akkor a felbontásban legyen $\tau = (123)(45)$, és feltehető, hogy ϱ-ban 1, 2, 3, 4 nem fordulnak elő.

3. Ha σ-ban egyetlen hármas ciklus van, akkor az állítás máris igaz.

4. Ha σ-ban hármas ciklus sincs, de legalább három transzpozíció van, például $\sigma = (12)(34)(56)\ldots$, akkor legyen $\tau = (12)(34)$, és ϱ-ban 1, 2, 3, 4 egyike sem fordul elő.

5. Ha σ-ban legfeljebb két transzpozíció lép fel, akkor az állítás ugyancsak igaz.

(A τ és ϱ megadásában csak annyi önkényesség volt, hogy a permutálandó objektumokat általunk választott számjeggyel jelöltük, ami nyilván megtehető.)

Válasszuk most a $\mu = (234)$ permutálást, ami minden esetben megtehető, mert ez a három számjegy szerepel a τ tartóhalmazában, és így σ-ében is. Világos, hogy μ-re teljesülnek az előzetes meggondolásban kirótt feltételek. Így mindegyik esetben kaptunk egy olyan N-beli, nemidentikus permutálást, amelyiknek a tartóhalmaza a 2. esetben legfeljebb ötelemű, minden egyéb esetben legfeljebb négyelemű.

A kapott σ_1 permutálásra a következő lehetőségeink vannak: Ha tartóhalmaza ötelemű, és σ_1 5 hosszúságú ciklus, akkor ismét alkalmazhatjuk az 1. esetet, és olyan permutálást kapunk, amelynek tartóhalmaza legfeljebb négyelemű. Ha a tartóhalmaz ötelemű, és σ_1 egy hármas és egy kettes ciklus szorzata, akkor négyzete hármas ciklus és ekkor készen vagyunk. Ha σ_1 tartóhalmaza négyelemű és σ_1 egy négyes ciklus, akkor négyzete két idegen transzpozíció szorzata, s ez nyilván eleme N-nek. Így négyelemű tartóhalmaz esetében is találtunk alkalmas, N-beli permutálást. Ha a tartóhalmaz legfeljebb háromelemű, akkor a permutálás triviálisan eleget tesz a követelményeknek.

Azt kell még bebizonyítani, hogy $n \neq 4$ esetén, ha $\sigma = (12)(34)$ és eleme N-nek, akkor tudunk konstruálni N-ben egy transzpozíciót vagy egy hármas ciklust. $n < 4$ esetén N-ben ilyen elem nincs – tehát az állítás igaz. Ha $n > 4$, akkor a már szereplő négy számon kívül *létezik egy újabb*, például az 5. A $\tau = (12)$, $\varrho = (34)$ és $\mu = (125)$ választással az

előzetesen leírt eljárás segítségével olyan, N-beli permutálást állíthatunk elő, amelynek a tartóhalmaza legfeljebb háromelemű és nem triviális. ■

6.31. Tétel. *Ha $n > 2$ és $n \neq 4$, akkor S_n egyetlen kompozíciólánca*

$$S_n \rhd A_n \rhd \{\iota\}.$$

$n \geq 5$ esetén A_n egyszerű és nem feloldható. S_4-nek három kompozíciólánca van:

$$S_4 \rhd A_4 \rhd V_4 \rhd H_i \rhd \{\iota\} \qquad (i = 2, 3, 4),$$

ahol H_i-nek az identitáson kívül egyetlen σ_i eleme van:

$$\sigma_2 = (12)(34), \quad \sigma_3 = (13)(24), \quad \sigma_4 = (14)(23),$$

és V_4 (az úgynevezett Klein-féle négyescsoport) elemei $\iota, \sigma_2, \sigma_3, \sigma_4$.

Bizonyítás. A 6.29. és a 6.30. tételek alapján, ha $n > 2$ és $n \neq 4$, akkor S_n egyetlen valódi normálosztója A_n, és A_n-nek nincs valódi normálosztója. Ebből következik, hogy a felírt lánc valóban az egyetlen kompozíciólánc. Mivel A_n egyszerű, ezért, ha nem prímrendű, nem is lehet feloldható. Ugyanígy nem feloldható S_n sem az $n \geq 5$ esetben. Azt kell még belátni, hogy $n = 4$ esetén pontosan a felírt kompozíciólláncok léteznek. A 6.30. tétel szerint, ha akár S_4-nek, akár A_4-nek van újabb normálosztója, ez csak V_4 egy részcsoportja lehet. A 6.29. tétel szerint S_4-nek nem is lehet más újabb normálosztója, csak V_4, ami normális részhalmaz. Mivel V_4 bármely elemének négyzete az identitás, és $\sigma_2, \sigma_3, \sigma_4$ közül bármelyik kettőnek a szorzata a harmadik, ezért V_4 normálosztó S_4-ben, és így A_4-ben is. Egyszerű számolással belátható, hogy a H_i csoportok egyike sem normálosztó A_4-ben, ami igazolja, hogy ezek az S_4 összes kompozícióláncai. ■

A továbbiakban egy tetszőleges, de rögzített $p > 3$ prímszám mellett vizsgáljuk az S_p-t. Kényelmi szempontokból ezt most a $P = \{0, 1, \ldots, p-1\}$ halmaz permutálásaiként fogjuk tekinteni. Ezt a halmazt egyúttal a modulo p vett maradékosztályok testjének tekintjük.

6.32. Tétel. (1) *Az S_p-nek a $\sigma(i) \equiv ai + b \pmod{p}$ összefüggéssel megadott elemei ($a, b \in P$, $a \not\equiv 0 \pmod{p}$) egy $L_p < S_p$ részcsoportot alkotnak (úgynevezett lineáris csoport).*

(2) *S_p egy tranzitív részcsoportja akkor és csak akkor feloldható, ha L_p-ben van.*

(3) *Ha S_p valamely tranzitív feloldható részcsoportjának egy eleme P-nek két elemét fixen hagyja, akkor ez az identikus permutálás.*

(Mint már láthattuk a feladatok között, L_p mint részcsoport nem egyértelmű, attól függ, hogy a tartóhalmaz elemeihez hogyan rendeljük hozzá a modulo p vett maradékosztályokat!)

Bizonyítás. (1) Ha $ai + b \equiv aj + b \pmod{p}$, akkor $p \nmid a$ miatt $i \equiv j \pmod{p}$. Így a felsorolt leképezések injektívek; tehát P végessége miatt permutálások. Ha $\varrho(i) \equiv ci + d \pmod{p}$, akkor $\sigma\varrho(i) = aci + (ad + b) \pmod{p}$; a végesség miatt tehát L_p csoport (az identitás nyilván eleme).

(2) Tekintsük most az S_p egy G tranzitív részcsoportját. Mindenekelőtt kimutatjuk, hogy G-nek bármely nemtriviális normálosztója is tranzitív. Legyen $N \lhd G$ nemtriviális, és tekintsük az N-nek a $P_1, \ldots, P_r$ pályáit. Válasszunk ki közülük két tetszőlegeset, legyenek

ezek P_1 és P_2. Tekintsünk egy olyan $\sigma \in G$ elemet, amely egy $a \in P_1$ elemet egy P_2-beli b elembe visz. Legyen $u \in P_1$ tetszőleges. Mivel P_1 az N egy pályája, ezért van olyan $\tau \in N$, amelyre $u = \tau(a)$. Mivel N normálosztó, ezért $\sigma\tau\sigma^{-1} \in N$ is igaz, és így $\sigma(u) = \sigma\tau(a) = \sigma\tau\sigma^{-1}(b) \in P_2$, hiszen P_2 is egy pálya. Eszerint $\sigma(P_1) \subseteq P_2$, amiből $\sigma(P_1) = P_2$, hiszen $\sigma^{-1} \in G$ is igaz. A G tranzitivitása miatt tehát ezeknek a pályáknak az elemszáma megegyezik. Mivel p prímszám, ezért vagy minden egyes pálya egyelemű, vagy csak egyetlen pálya van. Az első esetben N egyedül az identitásból állna, de mivel N nem triviális, ezért N tranzitív.

Tegyük most fel, hogy N az S_p-nek egy tranzitív kommutatív részcsoportja. Azt fogjuk megmutatni, hogy ekkor N ciklikus, és generátora egy p hosszúságú τ ciklus, amelyet a $\tau(i) \equiv i+1 \pmod{p}$ összefüggéssel definiálhatunk. Mivel N kommutatív, ezért P bármely elemének N-beli stabilizátora normálosztója N-nek. A 6.15. tétel (2) és (3) pontja alapján e stabilizátorok egyedül az identitásból állnak. Legyen most $\tau \in N$, $\tau \neq \iota$ és legyen τ típusa $(k_1, \ldots, k_r)$, ahol feltehető, hogy $k_1 \leq \ldots \leq k_r$. Ekkor τ-nak a k_1-edik hatványa az első ciklus elemeit fixen hagyja, így eleme ezek stabilizátorának, tehát az identitás. Ez csak úgy lehet, hogy a fellépő ciklusténye zők mindegyikének ugyanaz a hossza. Mivel τ nem az identitás, ezért tartóhalmaza P; és így csak a $k_1 = p$ lehetséges, mert p prímszám. Nem megy az általánosság rovására, ha feltesszük, hogy $\tau = (0, 1, \ldots, p-1)$. Legyen most $\varrho \in N$, és legyen $\varrho(0) = i$. Ekkor $\tau^{-i}\varrho(0) = 0$ alapján $\varrho = \tau^i$, hiszen 0 stabilizátora csak az identitást tartalmazza. Végül megjegyezzük, hogy az itt felírt τ valóban definiálható a kívánt összefüggéssel.

Legyen most G az S_p-nek egy feloldható tranzitív részcsoportja. A 6.11. következmény szerint G-nek van egy N kommutatív normálosztója. Ez, mint láttuk, tranzitív, s mint tranzitív kommutatív csoport, $N = \langle\tau\rangle$, ahol $\tau(i) \equiv i + 1 \pmod{p}$. Mivel $N \lhd G$, ezért G tetszőleges σ eleméhez van olyan $a \in P$, hogy $\sigma\tau\sigma^{-1} = \tau^a$. Tekintettel arra, hogy az identitás csak önmagának lehet konjugáltja, ezért $a \neq 0$. Mármost a P tetszőleges j elemére:

$$\sigma(j+1) \equiv \sigma\tau(j) \equiv \tau^a\sigma(j) \equiv a + \sigma(j) \pmod{p}.$$

Ha $\sigma(0) = b$, akkor a fenti összefüggésből azonnal adódik – j szerinti teljes indukcióval –, hogy $\sigma(i) \equiv ai + b \pmod{p}$, amit bizonyítani akartunk. Számolással könnyen belátható, hogy a fenti τ generálta részcsoport az L_p-nek normálosztója. E normálosztó izomorf a mod p vett maradékosztályok additív csoportjával, a szerinte vett faktorcsoport pedig a redukált maradékosztályok multiplikatív csoportjával. Mivel ezek kommutatívak, így L_p – következésképpen L_p minden részcsoportja is – feloldható.

(3) Tekintsük most G egy tetszőleges σ elemét, amely P-nek i és j elemeit fixen hagyja. Ez azt jelenti, hogy az $(a-1)x \equiv -b \pmod{p}$ kongruenciának két, inkongruens megoldása van, ami csak az $a - 1 = -b = 0$ esetben lehet; és így σ valóban az identitás. ■

Feladatok

1. Bizonyítsuk be, hogy $S_n^{\{i\}}$ minden $1 \leq i \leq n$ esetén maximális részcsoport, és n-nél kisebb indexű részcsoport egyedül A_n.

2. Bizonyítsuk be, hogy $S_H^{\{a\}}$ maximális részcsoport minden $a \in H$ esetében.

3. Bizonyítsuk be, hogy egyszerű részcsoportok növő láncának uniója egyszerű; S_∞^* páros permutációi egy A_∞^* egyszerű részcsoportot alkotnak.

4. Határozzuk meg S_4-nek azokat az endomorfizmusait, amelyek nem automorfizmusok.

5. Bizonyítsuk be, hogy egy S_n-beli konjugált elemosztály vagy része A_n-nek, vagy idegen tőle. Mutassuk meg, hogy az A_n-be eső konjugált elemosztályok vagy A_n-ben is konjugáltak, vagy két A_n-beli konjugált elemosztályból állnak. Mi a feltétele a „szétválásnak"?

6. Az S_∞^*-beli konjugált elemosztály vagy része A_∞^*-nak, vagy idegen tőle. Mutassuk meg, hogy az A_∞^*-ba esők itt is egyetlen konjugált elemosztályt alkotnak.

7. Bizonyítsuk be, hogy páratlan p prímszám esetén a $4p^n$ és $5p^n$ rendű csoportok feloldhatók.

8. Bizonyítsuk be, hogy egy nem feloldható csoportnak legalább 60 eleme van.

9. Mutassuk meg, hogy $n > 2$ esetén A_n-nek van külső automorfizmusa.

10. Bizonyítsuk be, hogy $\{1\} \lhd A_\infty^* \lhd S_\infty^* \lhd S_\infty$ egy kompozíciólánc.

11. Legyen H (akármilyen nagy számosságú) végtelen halmaz és jelölje S_H^* azoknak a permutálásoknak a halmazát, amelyek tartóhalmaza véges. Mutassuk meg, hogy ez csoport. Legyen A_H^* az S_H^* azon elemeinek a halmaza, amelyek tartóhalmazukon páros permutációt hoznak létre. Mutassuk meg, hogy A_H^* mindig egyszerű csoport, $A_H^* \lhd S_H^*$ és $(S_H^* : A_H^*) = 2$.

12. Legyen H számossága $\mathfrak{a}$ és legyen $\mathfrak{b}$ egy olyan végtelen számosság, amelyre $\mathfrak{b} \leq \mathfrak{a}$. Tekintsük S_H azon elemeit, amelyek tartóhalmazának számossága legfeljebb $\mathfrak{b}$, illetve kisebb, mint $\mathfrak{b}$. Bizonyítsuk be, hogy ezek egy $S_{H,\mathfrak{b}}$, illetve egy $S_{H,\mathfrak{b}}^*$ normálosztóját alkotják S_H-nak.

13. Nevezzük az A halmaz egy B részhalmazát *kovégesnek*, ha komplementere véges. Nevezzünk egy $\varphi : A \to A$ leképezést *kvázipermutálásnak*, ha A egy kovéges részhalmazát bijektíven képezi le A egy kovéges részhalmazára (nem feltétlen ugyanarra). Jellemezzük a kvázipermutálásukat magjukkal és képükkel; bizonyítsuk be, hogy a kvázipermutálások egy $\mathcal{Q}(A)$ félcsoportot alkotnak.

Tekintsünk két kvázipermutálást ekvivalensnek, ha egy kovéges halmazon megegyeznek. Bizonyítsuk be, hogy ez egy Θ kongruenciareláció, és $\mathcal{P}(A) = \mathcal{Q}(A)/\Theta$ csoport. „Keressük" e csoport részcsoportjait, normálosztóit.

14. Bizonyítsuk be, hogy S_n bármely kommutatív faktorának legfeljebb két eleme van.

6.6. Az S_n automorfizmuscsoportja

Mint láttuk, S_n centruma egyedül az egységelemből áll, ha $n > 2$. Ez azt jelenti, hogy automorfizmuscsoportja „tartalmazza" S_n-t. A következőkben azt mutatjuk meg. hogy egyetlen kivételtől eltekintve más automorfizmus nem is létezik. Előkészületül megmutatjuk az alábbit:

6.33. Tétel. *Legyen $H \leq S_n$, $n \neq 4$, $H \neq A_n$. Ekkor $(S_n : H) \geq n$.*

Bizonyítás. Legyen $k = (S_n : H)$. Mivel esetünkben S_n-nek egyetlen valódi normálosztója A_n, ezért – feltételünk alapján – H összes konjugáltjának a metszete az egységelemből áll. Ez – a 6.27. tétel alapján – azt jelenti, hogy S_n beágyazható S_k-ba, vagyis $k \geq n$. ■

6.34. Tétel. *$n \neq 6$ esetén S_n minden automorfizmusa belső.*

Bizonyítás. Legyen φ az S_n egy tetszőleges automorfizmusa. Mivel egy automorfizmus megtartja az elemek rendjét, ezért φ minden transzpozíciót idegen transzpozíciók szorzatába visz.

Az alternáló csoport az S_n egyetlen 2 indexű részcsoportja. Ezért φ ezt önmagába viszi. Így páratlan permutálás képe ismét páratlan permutálás. Ez azt jelenti, hogy φ minden transzpozíciót páratlan sok idegen transzpozíció szorzatába visz.

$\varphi(a^{-1}ba) = \varphi(a)^{-1}\varphi(b)\varphi(a)$ alapján egy automorfizmus minden konjugált elemosztályt egy konjugált elemosztályba visz. Tekintettel arra, hogy egy automorfizmus inverze is automorfizmus, ezért a leképezés egy teljes konjugált elemosztályra történik.

Mint tudjuk, két permutálás pontosan akkor konjugált, ha egyező típusúak. Ez azt jelenti, hogy a φ-hez létezik olyan páratlan k természetes szám, amelyre a transzpozíciók képei pontosan azok a permutálások, amelyek k darab idegen transzpozíció szorzatából állnak. Ez persze csak úgy lehet, ha $2k \leq n$. Az $n < 6$ esetben ezeknek a feltételeknek csak $k = 1$ tesz eleget. Az $n = 6$ esetben $k = 1$ mellett $k = 3$ is szóba jön. A továbbiakban feltesszük, hogy $n > 6$.

S_n-ben pontosan $\binom{n}{2}$ transzpozíció van. k darab idegen transzpozíció kiválasztási lehetőségeinek a száma $\binom{n}{2} \cdot \ldots \cdot \binom{n-2k+2}{2}$. E transzpozíciók felcserélhetősége alapján a transzpozíciók bármely sorrendje ugyanazt a permutálást adja; ezért a szóban forgó konjugált elemosztály számát úgy kapjuk, hogy a most kapott szorzatot $k!$-sal elosztjuk. A feltételezett egyenlőséget átalakítva a

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

egyenlőséghez jutunk. Úgy fogjuk kimutatni ennek a lehetetlenségét, hogy bebizonyítjuk: a jobb oldal mindig nagyobb a bal oldalnál.

A bal oldal nem függ az n-től. Tekintsük a jobb oldalnak n-ben vett minimumát. Ezt akkor kapjuk, ha n helyébe a legkisebb szóba jövő értéket, $2k$-t tesszük. Ekkor a jobb oldal $(2k-2)!$, így elég kimutatni, hogy a $k \neq 1$ esetben $k! \cdot 2^{k-1} < (2k-2)!$ lehetetlen (egy esetet, ahol egyenlőtlenség helyett egyenlőség áll, majd külön meg kell nézni). Ennek kimutatására elég belátni annyit, hogy

$$2^{k-1} < (2k-2) \cdot \ldots \cdot (k+1).$$

Ezt k-ra vonatkozó teljes indukcióval bizonyítjuk. A legkisebb szóba jövő érték $k = 3$. Ekkor mindkét oldalon 4 áll. Mivel $n \neq 6$, ezért ez az „egyenlőség" úgy jött létre, hogy az eredeti feltételezett egyenlőség jobb oldalát csökkentettük. Ezért az eredeti egyenlőtlenség ekkor is igaz. Tegyük most fel, hogy

$$2^{k-1} \leq (2k-2) \cdot \ldots \cdot (k+1)$$

igaz. Ekkor a nyilvánvaló $k+1 < k(2k-1)$ egyenlőtlenség alapján:

$$2^k = 2 \cdot 2^{k-1} \leq 2 \cdot (2k-2) \cdot \ldots \cdot (k+1) < 2k \cdot \ldots \cdot (k+2),$$

mint állítottuk.

Ezek szerint $n \neq 6$ esetén a φ automorfizmus minden transzpozíciót transzpozícióba visz. Nézzünk tehát egy olyan φ automorfizmust, amely rendelkezik ezzel a tulajdonsággal (most $n = 6$ is lehet). Mivel $n < 3$ esetén S_n-nek egyáltalán nincs is nemtriviális automorfizmusa, ezért feltehető, hogy $n > 2$.

Ha két transzpozíciónak van közös eleme, akkor szorzatuk harmadrendű, ha nincs, akkor másodrendű. Mivel egy automorfizmus az elem rendjét megtartja, ezért nem idegen transzpozíciók szorzata sem idegen.

Mint tudjuk, az $(1, 2)(1, 3)(1, 4)$ szorzat egy negyedrendű permutálás. E három transzpozíció képe φ-nél olyan három transzpozíció, amelyeknek páronként van közös eleme. Az (a, b), (b, c), (c, a) transzpozíciók együttesen legfeljebb három elemet mozgatnak, ezért szorzatuk nem lehet negyedrendű. Eszerint, ha három különböző transzpozíciónak van egy közös eleme, akkor ugyanez igaz egy automorfizmusnál kapott képeikre is. Eszerint az $(1, 2), \ldots, (1, n)$ transzpozíciók képei közül bármely háromnak van közös eleme. Teljes indukcióval bebizonyítjuk, hogy ekkor ezek közül bármely $k > 3$ transzpozíciónak is van. Feltétel szerint az első $(k-1)$-nek a képe $(a, b_1), (a, b_2), \ldots, (a, b_{k-1})$ Ekkor az első kettőnek és a k-adik transzpozíció (c, d) képének is van közös eleme. Mivel $b_1 \neq b_2$, ezért ez a közös elem csak a lehet; vagyis az állítás k darab transzpozíció esetében is igaz. Ezek szerint létezik az $\{1, \ldots, n\}$ halmaznak olyan π permutálása, amelyre

$$\varphi((1, i)) = (\pi(1), \pi(i)) = \pi(1, i)\pi^{-1}.$$

Mivel az $(1, i)$ permutálások generálják S_n-t, ezért φ ugyanaz, mint a π-vel való konjugálás. ■

6.35. Tétel. *Ha S_n minden automorfizmusa belső – azaz $n \neq 6$ –, akkor minden n indexű részcsoportja egy stabilitási részcsoport.*

Bizonyítás. Legyen H az S_n egy n indexű részcsoportja. A H részcsoport mellékosztályain való Λ ábrázolásnál a $g \in S_n$ elemnek a $\lambda_g : xH \mapsto gxH$ automorfizmust feleltetjük meg. Amennyiben $h \in H$, akkor λ_h a H mellékosztálynak stabilitási részcsoportja. Így Λ egy olyan automorfizmus, amelynél H képe egy stabilitási részcsoport. Mivel ez a Λ automorfizmus belső és egy belső automorfizmus inverze minden stabilitási részcsoportot stabilitási részcsoportba visz, ezért H valóban egy stabilitási részcsoport. ■

Megjegyzés. A fenti tétel megfordítása is igaz. Tegyük fel, hogy S_n minden n indexű részcsoportja stabilitási részcsoport, és legyen φ az S_n egy tetszőleges automorfizmusa. Az i elemhez tartozó $S_n^{\{i\}}$ stabilitási részcsoport φ-nél vett képe is n indexű, ezért ez is egy stabilitási részcsoport: $S_n^{\{j_i\}}$ (a fixen hagyott elem természetesen az i-től függ). Mivel φ automorfizmus, ezért különböző stabilitási részcsoportok képe is különböző. Ez azt jelenti, hogy $\sigma : i \to j_i$ egy permutálás. Erre természetesen tetszőleges i mellett teljesül a $\sigma(S_n^{\{i\}}) = S_n^{\{j_i\}} = \varphi(S_n^{\{i\}})$ összefüggés. Más szóval a $\sigma^{-1}\varphi$ automorfizmus minden stabilitási részcsoportot fixen hagy. Ekkor viszont fixen hagyja az ezekből képezett metszeteket is. Tekintsük rögzített u, v mellett a többi elemhez tartozó $n-2$ stabilitási részcsoport közös részét. Ez azokból áll, amelyek u és v kivételével minden elemet fixen hagynak. Ilyen permutálás kettő van, az identitáson kívül az (u, v) permutálás. Így $\sigma^{-1}\varphi$ ezt, és hasonlóan minden transzpozíciót fixen hagy. Mivel ezek generálják S_n-t, ezért $\sigma^{-1}\varphi$ az identitás, tehát $\varphi = \sigma$. □

6.36. Tétel. *Ha $(G : H) = n > 1$, és H konjugáltjainak a metszete az egységcsoport, akkor a H szerinti mellékosztályokon való ábrázolásnál G képe nem stabilitási részcsoport.*

Valójában ez az eredmény szerepel már a 6.27. tételben, de célszerű itt újból megfogalmazni.

Bizonyítás. Legyenek $a_1H, \ldots, a_nH$ a mellékosztályok. Ekkor tetszőleges $g \in G$ elemnek a $\sigma_g : a_iH \to ga_iH$ permutálás felel meg. A kiszemelt a_iH objektumot azok a σ_g permutálások hagyják fixen, amelyekre $ga_iH = a_iH$, azaz $g \in a_iHa_i^{-1}$. Tekintettel arra, hogy $(G : H) = n > 1$, mindig van olyan $g \in G$, amelyik nincs benne H egy adott konjugáltjában, azaz G képe valóban nem stabilitási részcsoport. ■

6.37. Tétel. *S_6-nak van külső automorfizmusa; és van olyan 6 indexű részcsoportja, amelyik nem stabilitási részcsoport.*

Bizonyítás. Tekintsük az S_5-beli L_5 lineáris csoportot. Ennek rendje $4 \cdot 5 = 20$, és ezért indexe $\frac{120}{20} = 6$. Mivel S_5 egyetlen valódi normálosztója A_5, ezért L_5 konjugáltjainak a metszete egyedül az egységelemet tartalmazza. Az előző tétel szerint tehát az L_5 szerinti mellékosztályokon való ábrázolás S_5-öt nem stabilitási részcsoportként ágyazza ba S_6-ba. Így S_6-ban az S_5 ezen képe nem stabilitási részcsoport. Mint láttuk, ebből következik, hogy S_6-nak van külső automorfizmusa. ■

6.38. Tétel. *$Aut(S_6)$-ban S_6 indexe 2.*

Bizonyítás. Legyenek φ és ψ az S_6 két külső automorfizmusa. Mint láttuk, ekkor ezek mindegyike a transzpozíciókból álló konjugált osztályt a diszjunkt transzpozícióhármasokból álló konjugált osztályba viszi. Így $\varphi^{-1}\psi$ a transzpozíciókból álló konjugáltosztályt önmagába viszi; s ezért – mint láttuk – egy belső automorfizmus. Mivel létezik külső automorfizmus, ezért az index 2. ■

6.7. Lineáris transzformációk csoportja

Mint említettük, kétféle jól „látható” csoport van: a permutálások és a reguláris mátrixok csoportja. Az előbbiekkel való ábrázolást tárgyaltuk, az utóbbiakról a későbbiekben lesz szó. Egyelőre csak a mátrixok segítségével előállítható egyszerű csoportokról szólunk.

6.39. Definíció. Legyen $\mathbb{K}$ egy test és $\mathcal{V}$ a $\mathbb{K}$ feletti n-dimenziós vektortér ($n > 1$). *Általános lineáris csoportnak* (**g**eneral **l**inear group) nevezzük e vektortér invertálható lineáris transzformációinak $GL(\mathcal{V})$ csoportját. E csoport egy rögzített bázis segítségével azonosítható a $\mathbb{K}$ feletti $n \times n$-es invertálható mátrixok csoportjával (e csoportok izomorfak). Ez utóbbi csoportot $GL(n, \mathbb{K})$ jelöli. Ha a $\mathbb{K}$ test elemszáma a q prímhatvány, akkor e csoportra a $GL(n, q)$ jelölés használatos. □

(Majd látni fogjuk, hogy véges test elemszáma mindig egy prímhatvány, és minden q prímhatványhoz izomorfiától eltekintve egyetlen q elemű test létezik.)

Célunk e csoport normálosztóinak a meghatározása. Mindenekelőtt tekintsük azt a δ megfeleltetést, amely minden mátrixnak a determinánsát felelteti meg (tehát $\delta(M) = \det(M)$, ha M négyzetes mátrix). Ez szorzattartó; tehát homomorfizmus. Ker (δ)-ra az $SL(\mathcal{V}) = SL(n, \mathbb{K}) = SL(n, q)$ jelölés (**s**pecial **l**inear group) használatos, a csoport neve *speciális lineáris csoport*. Ennek elemei tehát az 1-determinánsú $n \times n$-es mátrixok.

Legyen **P** a $\mathcal{V}$ egydimenziós altereinek a halmaza. Mivel egy invertálható lineáris transzformáció minden egydimenziós alteret egy egydimenziós altérbe visz, ezért $GL(\mathcal{V})$ elemei **P** permutálásainak tekinthetők. Ez nem egy „hű" ábrázolás, mert különböző elemek is adhatják ugyanazt a permutálást. Feleltessük meg minden egyes lineáris transzformációnak a **P**-n indukált permutálást. A megfeleltetésnél kapott permutációcsoportot $PGL(\mathcal{V})$ jelöli (*projektív lineáris csoport*). E homomorfizmus magja azokból a transzformációkból áll, amelyek minden egydimenziós alteret önmagába visznek; azaz azokból, amelyeknek minden vektor sajátvektoruk. Mint tudjuk, ezek pontosan a skalármátrixok. Ha Z jelöli ezeknek a csoportját, akkor tehát $PGL(\mathcal{V}) \simeq GL(\mathcal{V})/Z$.

Legyen $Z_1 = SL(\mathcal{V}) \cap Z$. Az első izomorfizmustétel szerint, Z_1 normálosztója $SL(\mathcal{V})$-nek, a szerinte vett faktorcsoport: $PSL(\mathcal{V}) \simeq SL(\mathcal{V})/Z_1$. Z_1 egyébként azokból a skalármátrixokból áll, amelyekben a fellépő c skalárra $c^n = 1$.

Célunk annak a megmutatása, hogy két triviális esettől eltekintve Z_1 maximális normálosztó $SL(\mathcal{V})$-ben. Ez azzal ekvivalens, hogy $PSL(\mathcal{V})$ egyszerű. Az elv itt is hasonló ahhoz, amit az alternáló csoportnál követtünk. Nevezetesen meg fogunk adni 1 determinánsú transzformációkat, amelyek néhány speciális transzformációnak konjugáltjai, és együttesen generálják $SL(\mathcal{V})$-t.

6.40. Tétel. *$SL(\mathcal{V})$ kétszeresen tranzitív* **P***-n.*

Bizonyítás. Azt kell belátnunk, hogy tetszőleges $\langle \mathbf{v}_1 \rangle \neq \langle \mathbf{v}_2 \rangle$ és $\langle \mathbf{w}_1 \rangle \neq \langle \mathbf{w}_2 \rangle$ alterekhez van olyan csoportelem, amely az első kettőt megfelelően a második kettőbe viszi.

Független elemek kiegészíthetők bázissá, így létezik $\mathcal{V}$-ben egy $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ és egy $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n$ bázis. Tetszőleges c skalárra van olyan α_c transzformáció, amelyet $\alpha_c(\mathbf{v}_1) = c\mathbf{w}_1$, $\alpha_c(\mathbf{v}_i) = \mathbf{w}_i$ $(i = 2, \ldots, n)$ definiál. A $c = \delta(\alpha_1)^{-1}$ választással $\delta(\alpha_c) = 1$; és így α_c az $SL(\mathcal{V})$ eleme. ■

6.41. Tétel. *Legyen H a* **M** *halmazon kétszeresen tranzitív G csoport egy stabilitási részcsoportja. Ekkor H maximális részcsoport.*

Bizonyítás. Mivel H egy stabilitási részcsoport, legyen ez az $m \in \mathbf{M}$ elemet fixen hagyók csoportja. Legyen $\varphi \in G \setminus H$, és γ a G tetszőleges eleme. Ha $\gamma(m) = m$, akkor $\gamma \in H$. Egyébként $m_1 = \varphi(m)$ és $m_2 = \gamma(m)$ mindegyike különbözik m-től. A kétszeres tranzitivitás miatt van olyan G-beli α, amire $\alpha(m) = m$, $\alpha(m_1) = m_2$. Az első feltétel szerint $\alpha \in H$. A második feltételből azt kapjuk, hogy

$$\varphi^{-1}\alpha^{-1}\gamma(m) = \varphi^{-1}\alpha^{-1}(m_2) = \varphi^{-1}(m_1) = m,$$

azaz $\varphi^{-1}\alpha^{-1}\gamma = \beta \in H$. Eszerint $\gamma = \alpha\varphi\beta \in H\varphi H$, azaz $G = H \cup H\varphi H$, vagyis bármely $\varphi \notin H$ esetén $\langle \varphi, H \rangle = G$, bizonyítva H maximalitását. ■

Válasszuk most G-nek $SL(\mathcal{V})$-t és H-nak az $\mathbf{e}_1$ bázisvektort rögzítő lineáris transzformációk $G_{\mathbf{e}_1}$ stabilitási részcsoportját. Mátrixalakban:

$$H = \left\{ \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2} & \dots & a_{nn} \end{pmatrix} \;\middle|\; a_{11} \cdot \det \begin{pmatrix} a_{22} & \dots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{n2} & \dots & a_{nn} \end{pmatrix} = 1 \right\}.$$

Jegyezzük meg, hogy a részcsoport szerinti mellékosztályokon való permutációs ábrázolás alapján fennáll a következő összefüggés: $\bigcap \{\gamma H \gamma^{-1} \mid \gamma \in G\} = Z_1$.

Ezeket a mátrixokat $\begin{pmatrix} a & \mathbf{a}^T \\ \mathbf{o} & A \end{pmatrix}$ alakba írhatjuk, ahol A egy $\mathbb{K}$ feletti $(n-1)\times(n-1)$-es mátrix, $\mathbf{o}$ az $(n-1)$-dimenziós tér nullvektora, $\mathbf{a}$ pedig e tér egy vektora.

6.42. Tétel. *Az* $\begin{pmatrix} 1 & \mathbf{a}^T \\ \mathbf{o} & I \end{pmatrix}$ *alakú mátrixok* H*-nak egy* T *kommutatív normálosztóját alkotják.*

Bizonyítás. A H elemeinek a szorzatát kiszámítva

$$\begin{pmatrix} a & \mathbf{a}^T \\ \mathbf{o} & A \end{pmatrix} \cdot \begin{pmatrix} b & \mathbf{b}^T \\ \mathbf{o} & B \end{pmatrix} = \begin{pmatrix} ab & a\mathbf{b}^T + \mathbf{a}^T B \\ \mathbf{o} & AB \end{pmatrix}$$

adódik, ami azt mutatja, hogy az $\begin{pmatrix} a & \mathbf{a}^T \\ \mathbf{o} & A \end{pmatrix} \to A$ megfeleltetés csoporthomomorfizmus, mert $a \cdot \det(A) = 1$ miatt $\det(A) \neq 0$. Ennek magja éppen T, így T valóban normálosztó. Az $a = b = 1$ és $A = B = I$ esetben a fenti formula éppen e normálosztó kommutativitását szolgáltatja. ■

Azokat a T-beli mátrixokat, amelyekben $\mathbf{a}^T$ minden eleme – az utolsót kivéve – 0 („házi használatra") *speciális mátrixoknak* fogjuk nevezni. Röviden emlékeztetünk az első kötet II. részében a 4.6. definícióra és az utána következő részekre: Elemi bázistranszformáció, amikor egy bázis valamelyik eleméhez egy tőle különböző elemnek a skalárszorosát hozzáadjuk, ha egy bázisvektort nem-0 skalárral szorzunk, illetve ha két bázisvektort felcserélünk. Ezeknek a mátrixát elemi mátrixoknak fogjuk nevezni. A megfelelő bázisban létrehozott elemi mátrixátalakítások azt jelentik, hogy a mátrix soraival vagy oszlopaival hasonló eljárást végzünk.

6.43. Tétel. $n > 2$ *esetén az* 1 *determinánsú elemi mátrixok egymás konjugáltjai.* $n = 2$ *esetén az* 1 *determinánsú elemi transzformációk mindegyike egy-egy speciális mátrix konjugáltja* $SL(\mathcal{V})$*-ben. Az* 1 *determinánsú elemi transzformációk generálják* $SL(\mathcal{V})$*-t.*

Bizonyítás. Az, hogy $SL(\mathcal{V})$ minden eleme elemi mátrixok szorzataként állítható elő, úgy látható be, mint az, hogy ilyen transzformációval minden mátrix az egységmátrixba vihető. Tekintettel arra, hogy egy oszlopnak skalárral való szorzását nem egy 1 determinánsú mátrixszal való szorzás hozza létre, ezért a kapott mátrix csak diagonális lesz. Viszont azt tudjuk, hogy a diagonális elemeinek a szorzata 1. Az alábbi átalakítássorozatot

1 determinánsú speciális mátrixokkal jobbról való szorzás hozza létre:

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \to \begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix} \to \begin{pmatrix} 0 & 1 \\ -ab & b \end{pmatrix} \to \begin{pmatrix} 0 & 1 \\ -ab & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 1 \\ -ab & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ -ab & ab \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & ab \end{pmatrix}.$$

Az eljárást folytatva végül olyan diagonális mátrixot kapunk, amelyben a diagonális elemei az utolsóig 1-esek, s az utolsó elem éppen a determináns. Mivel ez is 1, ezért az eredeti mátrix inverze 1 determinánsú elemi transzformációk szorzata, s ezért maga az eredeti mátrix is ilyen.

Legyen β egy tetszőleges 1 determinánsú elemi mátrix. Ehhez egy olyan T-beli α speciális mátrixot keresünk, amelynek β a konjugáltja. Mivel mindketten 1 determinánsú elemi mátrixok, ezért létezik olyan $\mathbf{u}_1, \ldots, \mathbf{u}_n$ és $\mathbf{v}_1, \ldots, \mathbf{v}_n$ bázis, amelyekre:

$$\beta(\mathbf{v}_i) = \mathbf{v}_i, \qquad \alpha(\mathbf{u}_i) = \mathbf{u}_i, \qquad \text{ha} \qquad i < n;$$

továbbá

$$\beta(\mathbf{v}_n) = \mathbf{v}_n + b \cdot \mathbf{v}_1, \qquad \alpha(\mathbf{u}_n) = \mathbf{u}_n + a \cdot \mathbf{u}_1, \qquad \text{ahol} \quad a, b \in \mathbb{K}.$$

β adott, és $\alpha \in T$ kell, hogy legyen. Ez azt jelenti, hogy mindkét bázis adott, de $a \in \mathbb{K}$ szabadon választható.

Tekintsük azt a φ reguláris lineáris transzformációt, amelyre $\varphi(\mathbf{v}_i) = \mathbf{u}_i$ $(i = 1, \ldots, n)$. Legyen d a φ determinánsa. Ha $n > 2$, legyen ψ a következőképpen definiálva: $\psi(\mathbf{v}_2) = d^{-1} \cdot \varphi(\mathbf{v}_2)$, és $\psi(\mathbf{v}_i) = \varphi(\mathbf{v}_i)$, ha $i \neq 2$. Világos, hogy ψ 1 determinánsú és az $a = b$ választással β az α-nak ψ-vel való konjugáltja. Ez az eljárás azt is szolgáltatja, hogy a speciális mátrixok is egymás konjugáltjai $SL(\mathcal{V})$-ben.

$n = 2$ esetén ψ-t a következőképpen definiáljuk: $\psi(\mathbf{v}_1) = d^{-1} \cdot \varphi(\mathbf{v}_1)$, és $\psi(\mathbf{v}_2) = \varphi(\mathbf{v}_2)$. Világos, hogy ψ most is 1 determinánsú. A $\beta_1 = \psi\beta\psi^{-1}$ leképezésre:

$$\beta_1(\mathbf{u}_1) = \psi\beta\psi^{-1}(\mathbf{u}_1) = \psi\beta(d \cdot \mathbf{v}_1) = \psi(d \cdot \mathbf{v}_1) = \mathbf{u}_1,$$

$$\beta_1(\mathbf{u}_2) = \psi\beta\psi^{-1}(\mathbf{u}_2) = \psi\beta(\mathbf{v}_2) = \psi(\mathbf{v}_2 + b \cdot \mathbf{v}_1) = \mathbf{u}_2 + \frac{b}{d} \cdot \mathbf{u}_1.$$

Az $a = \dfrac{b}{d}$ választással $\alpha \in T$, és β az α konjugáltja. ■

6.44. Tétel. *Ha $n > 2$, vagy $n = 2$ és $|\mathbb{K}| > 3$, akkor $SL(n, \mathbb{K})$ megegyezik kommutátor-részcsoportjával.*

Bizonyítás. Mivel a kommutátor-részcsoport normálosztó, ezért a 6.44. tétel alapján elég azt bizonyítani, hogy minden speciális mátrix előáll kommutátorként; sőt az $n > 2$ esetben ezt elegendő egyetlen speciális mátrixra megmutatni. Legyen D egy tetszőleges $(n-1) \times (n-1)$-es reguláris mátrix, és legyen $d = \det(D)$.

Ekkor a $\begin{pmatrix} d & \mathbf{o}^T \\ \mathbf{o} & D^{-1} \end{pmatrix}$ és a $\begin{pmatrix} 1 & \mathbf{u}^T \\ \mathbf{o} & I \end{pmatrix}$ mátrixok mindegyike $SL(\mathcal{V})$-beli és kommutátoruk:

$$\left[\begin{pmatrix} d & \mathbf{o}^T \\ \mathbf{o} & D^{-1} \end{pmatrix}, \begin{pmatrix} 1 & \mathbf{u}^T \\ \mathbf{o} & I \end{pmatrix}\right] = \begin{pmatrix} d & \mathbf{o}^T \\ \mathbf{o} & D^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & \mathbf{u}^T \\ \mathbf{o} & I \end{pmatrix} \cdot \begin{pmatrix} d^{-1} & \mathbf{o}^T \\ \mathbf{o} & D \end{pmatrix} \cdot \begin{pmatrix} 1 & -\mathbf{u}^T \\ \mathbf{o} & I \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & d\mathbf{u}^T D - \mathbf{u}^T \\ \mathbf{o} & I \end{pmatrix}.$$

Az $n > 2$ esetben legyen $\mathbf{u}$ az a vektor, amelynek az utolsó két koordinátája 1 s a többi 0; D pedig az a diagonális mátrix, amelynek fődiagonálisában minden elem 1, az utolsó előtti sor utolsó eleme is 1, és a többi elem 0. Ekkor D determinánsa $d = 1$, ezért $d\mathbf{u}^T D - \mathbf{u}^T = \mathbf{u}^T(D - I)$. E vektornak viszont az utolsó eleme 1, a többi 0, így kommutátorként egy speciális mátrixot kaptunk.

Az $n = 2$ esetben D is és $\mathbf{u}^T$ is egyelemű. Avégett, hogy $(d^2 - 1)u$ alakban $\mathbb{K}$ bármely nem-0 elemét megkaphassuk (azaz bármely speciális mátrix előálljon kommutátorként), arra van szükség, hogy a $d \neq 0$ feltétel mellett $d^2 - 1 \neq 0$ is teljesüljön. Ha $\mathbb{K}$-nak legalább négy eleme van, akkor létezik ilyen d; egyébként ez lehetetlen. ■

6.45. Tétel. *Ha $n > 2$, vagy $n = 2$ és $|\mathbb{K}| > 3$, akkor $PSL(n, \mathbb{K})$ egyszerű.*

Bizonyítás (Iwasawa)**.** Azt kell megmutatnuk, hogy ha $N \lhd G = SL(n, \mathbb{K})$ és $Z_1 \subseteq N \subseteq G$, akkor vagy $N = Z_1$, vagy $N = G$.

Tegyük fel először, hogy $N \subseteq H = G_{\mathbf{e}_1}$. Ekkor tetszőleges $\gamma \in G$ esetén $N = \gamma N \gamma^{-1} \subseteq \gamma H \gamma^{-1}$ miatt $N \subseteq \bigcap\{\gamma H \gamma^{-1} \mid \gamma \in G\} = Z_1$, azaz $N = Z_1$.

Nézzük most azt az esetet, amikor $N \not\subseteq H$. Ekkor $NH \supset H$; H maximalitása (vö. 6.41. tétel) alapján tehát $NH = G$. $T \lhd H$ miatt $NT \lhd NH = G$ is igaz. Ebből viszont $T \subseteq NT$ következtében $NT = G$ adódik, hiszen a 6.43. tétel alapján G az egyetlen T-t tartalmazó normálosztó. Az első izomorfizmustétel szerint

$$G/N = NT/N \simeq T/(T \cap N),$$

ami – mint a kommutatív T csoport egy faktorcsoportja – maga is kommutatív. Ebből viszont az következik, hogy N tartalmazza G kommutátor-részcsoportját; tehát a 6.43. tétel következtében $N = G$. ■

Természetesen azonnal felmerül a kérdés, hogy ezek a csoportok különbözőek-e és különböznek-e az alternáló csoportoktól. (A ciklikus egyszerű csoportoktól biztosan különböznek, mert nem kommutatívak.) A legkézenfekvőbb az elemszámok összehasonlításával kísérelni meg a kérdés eldöntését. Könnyen kiszámítható, hogy

$$|PSL(n, q)| = \frac{(q^n - 1) \cdot (q^n - q) \cdot \ldots \cdot (q^n - q^{n-1})}{(q - 1) \cdot \mathrm{lnko}(n, q - 1)}.$$

Tulajdonképpen ez egy háromparaméteres kifejezés; a vektortér méretén kívül a prímszámtól és annak a kitevőjétől is függ. Mi most ezt a kitevőt 1-nek, n-et pedig 2-nek választjuk. Ekkor q helyébe p-t írva, az elemszámra $(p^3 - p)/2$ adódik. Ez a szám különböző prímekre különböző, és csak akkor egyezhet meg a k-adfokú alternáló csoport elemszámával, ha $p^3 - p = k!$. Ekkor p biztosan osztója $k!$-nak, ami csak a $p \leq k$ esetén lehet. Ha $k > 5$, akkor $k! > k^3 \geq p^3 > p^3 - p$ teljesül. Eszerint csak néhány esetben lehet egyenlőség. Mindenesetre végtelen sok újabb egyszerű csoportot találtunk.

Néhány esetben lehet megegyezés. Így:

(1) $PSL(2, 4) \cong PSL(2, 5) \cong A_5$ (60 elem).

(2) $PSL(2, 7) \cong PSL(3, 2)$ (168 elem).

(3) $PSL(2, 9) \cong A_6$ (360 elem).

(4) $PSL(4,2) \cong A_8$ (20 160 elem – $PSL(3,4)$ elemszáma is ennyi, de az ezekkel nem izomorf).

A többi $PSL(n,q)$ esetében nemcsak az igaz, hogy egyéb izomorfizmus nincs, de az elemszámok között sem lehet megegyezés. Ez az eredmény Emil Artin egy 1955-ben publikált cikkében található.

Az alábbiakban további három olyan csoportsorozatot mutatunk meg, amelynek az elemei egyszerűek (valójában e sorozatok egyike még további háromra bomlik).

Evégett a $\mathcal{V}$ vektorteret három különböző „skalárszorzat"-tal látjuk el, azaz bizonyos $f : \mathcal{V} \times \mathcal{V} \to \mathbb{K}$ bilineáris függvényeket tekintünk. A kiindulásul vett csoport az ezt a függvényt megtartó lineáris transzformációk

$$G_f = \{\alpha \in GL(\mathcal{V}) \mid \forall(\mathbf{u}, \mathbf{v} \in \mathcal{V}),\ \ f(\alpha(\mathbf{u}), \alpha(\mathbf{v})) = f(\mathbf{u}, \mathbf{v})\}$$

csoportja.

Az itt definiált csoport akkor lesz megfelelő, ha f nemelfajuló (azaz egyedül a nullvektorra lesz minden más vektor f-ortogonális), és az alábbi feltételek valamelyike teljesül:

I. $f(\mathbf{v}, \mathbf{u}) = f(\mathbf{u}, \mathbf{v})$ (azaz f szimmetrikus),

II. $f(\mathbf{v}, \mathbf{u}) = -f(\mathbf{u}, \mathbf{v})$ (azaz f antiszimmetrikus),

III. $f(\mathbf{v}, \mathbf{u}) = \overline{f(\mathbf{u}, \mathbf{v})}$ (azaz f „Hermite-féle").

Mindenekelőtt néhány megjegyzést teszünk. Hermite-féle azt jelenti, hogy „$x \to \overline{x}$" a $\mathbb{K}$ testnek egy másodrendű automorfizmusa (mint a konjugálás). Ha $\mathbb{K}$ 2 karakterisztikájú, azaz minden $a \in \mathbb{K}$ esetén $a + a = 0$, akkor az I. esetben egy kvadratikus alakot kell tekinteni, míg a II. esetben azt követeljük meg, hogy $f(\mathbf{u}, \mathbf{u}) = 0$. Ez utóbbi persze minden más esetben ekvivalens az eredeti feltétellel.

A G_f csoport a $GL(\mathcal{V})$ csoporthoz hasonlóan „majdnem" egyszerű, éspedig – néhány kivételtől eltekintve – az mutatható meg, hogy a

$$G'_f \ / \ (G'_f \cap Z)$$

csoport egyszerű. (Itt Z a fent vizsgált csoport, és G' a G kommutátor-részcsoportját jelöli.)

Először a III. esetet nézzük, mert ez a legkönnyebb. A véges testek tárgyalásánál látni fogjuk, hogy pontosan akkor van másodrendű automorfizmusuk, ha elemszámuk négyzetszám; és ebben az esetben ez az automorfizmus egyértelmű. Amit kapunk, az tehát „nem függ" az automorfizmustól. Ebben az esetben a felírt bilineáris függvényhez mindig létezik ortonormált bázis, ami azt jelenti, hogy f báziscsere erejéig egyértelműen meghatározott. Ebben az esetben a G_f csoport neve *unitér csoport*, erre az $U(n, \mathbb{K})$ jelölés használatos. Az ebből származtatott egyszerű csoportot $PSU(n, \mathbb{K})$ jelöli. Ez a csoport $n \neq 3$ esetén egyszerű, kivéve a $|\mathbb{K}| = 4$ esetet, amelyik feloldható.

A II. esetben szintén lényegében egyértelmű az f. A most kapott csoport neve *szimplektikus csoport*. Itt az derül ki, hogy a dimenzió szükségképpen páros; ennek a csoportnak a jelölése: $Sp(2n, \mathbb{K})$. Az ebből származtatott egyszerű csoport jele: $PSp(2n, \mathbb{K})$. Itt $n \neq 2$; de a kételemű test esetén a kapott csoport $Sp(4,2) \cong S_6$.

A legbonyolultabb az I. eset. Gondoljuk meg, hogy például a valós test felett is a dimenziószámnál eggyel több lényegesen különböző eset van (a pozitív sajátértékek számától függően, mint azt a tehetetlenségi tétel mutatja – a 0 sajátértéket kizártuk!). Véges testek esetén ezeket *ortogonális csoportoknak* nevezik. Véges testek esetén két lényegesen különböző f definiálható; ha azonban a vektortér páratlan dimenziós, akkor ugyanazokat

a csoportokat nyerjük. Ennek megfelelően itt három csoportsorozatot definiálnak:

$$O^+(2n, q), \qquad O^-(2n, q), \qquad O(2n+1, q).$$

Az ezeknél kapott kommutátorcsoport szűkebb, mint $SO = O \cap SL$, ezt a kommutátorcsoportot Ω jelöli. Itt is faktorizálni kell a skalármátrixokkal, és a kapott csoport $n \geq 3$ esetén mindig egyszerű. Az így nyert három csoportsorozat:

$$P\Omega^+(2n, q), \qquad P\Omega^-(2n, q), \qquad P\Omega(2n+1, q).$$

Ezeket a már tárgyalt

$$PSL(n, q), \qquad PSU(n, q^2), \qquad PSp(2n, q)$$

sorozatokkal együtt úgy tartjuk számon, mint *klasszikus egyszerű csoportok*. E hat sorozaton felül van még az egyszerű alternáló csoportok sorozata; továbbá természetesen a prímrendű egyszerű csoportok.

A fentieken kívül a véges egyszerű csoportoknak még 10 végtelen sorozata ismert, az úgynevezett *kivételes Lie-típusú csoportok*.

Végezetül van még 26 olyan egyszerű csoport, amelyik e sorozatok egyikébe sem illik bele (és együtt sem alkotnak sorozatot). Ezeknek a neve *sporadikus* (szórványos) egyszerű csoportok.

Az úgynevezett **klasszifikációs tétel** szerint ezeken kívül (izomorfiától eltekintve) nincs más véges egyszerű csoport. Ennek a tételnek a bizonyítása többezer oldal terjedelmű.

Az első öt sporadikus csoportot még MATHIEU találta a XIX. században. Ezek „neve”: M_{11}, M_{12}, M_{22}, M_{23} és M_{24}. Itt az index azt mutatja, hogy hányadfokú permutációscsoportról van szó.

S_n n-tranzitív, és A_n $(n-2)$-tranzitív. A klasszifikációs tételből következik, hogy egyéb permutációs csoport legfeljebb 5-tranzitív lehet. Ilyenek M_{12} és M_{24}. Ezenkívül még M_{11} és M_{23} 4-tranzitívak. Teljes lista van a végtelen sok 3-tranzitív és 2-tranzitív permutációcsoportról. Az is belátható, hogy L_p mindig maximális részcsoportja S_p-nek.

A legnagyobb sporadikus csoport a FISCHER által felfedezett *monstrum*. Ennek

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 =$$

$$= 808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000 \sim$$

$$\sim 8.08 \cdot 10^{53}$$

eleme van. Ez a szám mintegy 200-szor akkora, mint a Föld tömege a protonéhoz viszonyítva.

Feladatok

1. Adott n-hez és q-hoz adjunk meg olyan minél kisebb k-t, amelyre $PSL(n, q)$ izomorf S_k egy részcsoportjával.

2. Igaz-e, hogy minden véges csoport beágyazható egy alkalmas véges test feletti (reguláris) felső háromszög mátrixok csoportjába?

3. Bizonyítsuk be, hogy minden véges csoport beágyazható $SL(n, q)$-ba alkalmas n esetén.

4. Egyszerű csoport-e $PSL(n, \mathbb{Q})$, ahol $\mathbb{Q}$ a racionális számtest?

5. Legyen $A \in SL(2, q)$, ahol q páratlan prímhatvány. Bizonyítsuk be, hogy:
(1) ha $Tr(A) = 0$, akkor A rendje 4,
(2) ha $Tr(A) = -1$ és $A \neq I$, akkor A rendje 3.
(3) ha $Tr(A) = -1$ és $A \neq -I$, akkor A rendje 6.

6. Bizonyítsuk be, hogy $|PSL(4, 2)| = |PSL(3, 4)|$, de e két csoport nem izomorf.

7. Tudjuk, hogy $Z \cap SL(n, \mathbb{K})$ általában maximális normálosztója $SL(n, \mathbb{K})$-nak ($\mathbb{K}$ véges test). Adjunk szükséges és elégséges feltételt arra, hogy Z maximális normálosztója legyen $GL(n, \mathbb{K})$-nak. Mutassuk meg, hogy Z végtelen sok esetben maximális normálosztó, és végtelen sok esetben nem az.

Vegyes csoportelméleti feladatok

1. Vezessük be egy G csoport elemeire a következő relációt: $\varrho(a, b)$ akkor és csak akkor igaz, ha $ab = ba$. Bizonyítsuk be, hogy az indukált Galois-kapcsolatban csak részcsoportok lehetnek zártak, és határozzuk meg a zárt részhalmazokat a $G = S_4$ esetben.

2. Bizonyítsuk be, hogy $\langle a, b \mid a^4 = b^3 = 1, a^{-1}ba = b^3 \rangle \cong L_5$. Adjuk meg L_p-t definiáló relációkkal.

3. Bizonyítsuk be, hogy $|D_6| = |A_4|$, de nem izomorfak.

4. Bizonyítsuk be, hogy két másodrendű elem generálta csoport az diédercsoport.

5. Tekintsük az $\langle a, b \mid a^{2^{n-1}} = 1, b^2 = a^i, b^{-1}ab = a^j \rangle$ csoportokat az alábbi esetekben:
(1) $i = 0$, $j = -1$;
(2) $i = 2^{n-2}$, $j = -1$;
(3) $i = 0$, $j = 1 + 2^{n-2}$;
(4) $i = 0$, $j = -1 + 2^{n-2}$.
Mivel izomorfak ezek, ha $0 < n < 4$? Mekkora a rendjük tetszőleges n esetében?

6. Adott p prímszámhoz és n természetes számhoz adjunk meg olyan direkt felbonthatatlan véges G csoportot, amelynek legalább p^n eleme van, és bármely elemének a rendje p vagy 1.

7. Van-e olyan direkt felbonthatatlan végtelen G csoport, amelyben bármely elem rendje p vagy 1?

8. Bizonyítsuk be, hogy S_n-ben egy legalább $n - 1$ hosszúságú ciklussal csak a hatványai felcserélhetők.

9. Adjunk egy számelméleti formulát az S_n-beli elemek maximális rendjére.

10. Bizonyítsuk be, hogy összetett n esetén van olyan tranzitív $G \leq S_n$, amelynek alkalmas N normálosztója nem tranzitív.

11. Bizonyítsuk be, hogy p^2q^k rendű csoport feloldható, ha $p < q$ prímek.

12. Mit generál S_n-ben az összes k hosszúságú ciklus ($k \leq n$)?

13. Legyen G p-csoport és $H < G$. Az alábbi állítások közül melyik igaz, melyik nem és miért:

(1) Ha H maximális, akkor normálosztó.

(2) Ha H normálosztó, akkor maximális.

14. Legyen a G csoport rendje három különböző prímszám szorzata azzal a feltétellel, hogy e prímszámok közül egyetlen pár szorzata sem kongruens 1-gyel modulo a harmadik. Bizonyítsuk be, hogy G-nek legalább hét különböző rendű részcsoportja van.

15. Bizonyítsuk be, hogy véges G Abel-csoport esetén végtelen sok olyan $n \in \mathbb{N}$ létezik, hogy bármely $g \in G$ elemre megoldható az $x^n = g$ egyenlet.

16. Bizonyítsuk be, hogy ha egy G csoport minden részcsoportja végesen generált, akkor minden valódi részcsoport benne van egy maximálisban.

17. Legyen $N \lhd G$, továbbá $|G|$ és $(G : N)$ végesek és relatív prímek. Bizonyítsuk be, hogy N karakterisztikus részcsoport G-ben és bármely $H \leq G$ esetében ha $|H|$ osztója $|N|$-nek, akkor $H \leq N$.

18. Bizonyítsuk be, hogy ha G-ben a 2-Sylow kételemű, akkor G-nek van 2 indexű normálosztója.

19. Legyen $G = Z_3 \rtimes_\varphi Z_4$, ahol $\varphi : Z_4 \to \mathrm{Aut}(Z_3)$ a Z_4 generátorelemét az $\mathrm{Aut}(Z_3)$ generátorelemébe viszi. Bizonyítsuk be, hogy G sem D_6-tal, sem A_4-gyel nem izomorf.

HARMADIK RÉSZ
GYŰRŰK

7. Kommutatív gyűrűk

A kommutatív gyűrűk fogalma a számgyűrűk és a polinomgyűrűk általánosításaként született meg. Itt az egyik alapvető kérdés az egyértelmű faktorizáció és annak általánosítása, amely a polinomgyűrűk esetében szorosan kapcsolódik az algebrai geometriához. Ehhez a kérdéskörhöz még vissza kell térni a modulusok tárgyalásánál. Ide tartozik a kommutatív testek elmélete is, amelyben egyik központi kérdés az egyenletek megoldhatósága.

A 7.1. és 7.2. pontok esetében általános gyűrűelméleti fogalmak szerepelnek. A 7.3. ponttól kezdve viszont csak kommutatív gyűrűkről lesz szó.

7.1. Gyűrűk definíciója és elemi tulajdonságai

Gyűrűkkel és a gyűrűkhöz kapcsolódó számos tulajdonsággal már az első kötetben is találkoztunk. A rendszeres tárgyalás végett mégis célszerű e fogalmak átismétlése. Egyelőre tetszőleges – tehát nem feltétlenül kommutatív – gyűrűkkel foglalkozunk.

7.1. Definíció. Egy $\mathfrak{R} = \langle R; \{+, \cdot\}\rangle$ algebrai struktúrát gyűrűnek nevezünk, ha $\langle R; \{+\}\rangle$ (additív) Abel-csoport, $\langle R; \{\cdot\}\rangle$ félcsoport, és a két műveletre teljesül a két disztributivitás – vagyis az R tetszőleges a, b, c elemeire fennáll

$$a(b + c) = ab + ac \qquad \text{és} \qquad (b + c)a = ba + ca$$

(ahol az egymás mellé írás a félcsoportműveletet jelöli). □

Általában – ha ez nem fog félreértést okozni – a gyűrűket is tartóhalmazukkal adjuk meg. Az $\langle R; \{+\}\rangle$ úgynevezett tartócsoportot R^+-szal, míg az $\langle R; \{\cdot\}\rangle$ félcsoportot $R^\times$-ral jelöljük. A két művelet neve rendre *gyűrűösszeadás*, illetve *gyűrűszorzás*.

Ha a gyűrűszorzás kommutatív, akkor *kommutatív gyűrűről* beszélünk.

Gyűrűkre már számos példát láttunk: Így az egész, racionális, valós és komplex számok, illetve ezeknek bármely az összeadásra, kivonásra és szorzásra zárt nemüres részhalmaza. De gyűrűt alkotnak a számgyűrű-együtthatós egy- vagy többváltozós polinomok; a valós függvények a függvényösszeadásra és -szorzásra, továbbá a folytonos, differenciálható, integrálható stb. függvények. A mátrixösszeadásra és mátrixszorzásra gyűrűt alkotnak

azok az azonos méretű négyzetes mátrixok, amelyek elemei egy adott számtestből vagy számgyűrűből valók (e gyűrűben a multiplikatív félcsoport nem kommutatív).

A legutóbbi példában láttuk, hogy a gyűrűszorzás nem feltétlenül kommutatív. Így a két disztributivitási feltétel egyikéből nem következik azonnal a másik is (ha a szorzás kommutatív, akkor természetesen elég az egyik disztributvitást feltenni). Ez azonban még nem zárja ki azt, hogy a két disztributivitás közül az egyik elhagyható volna. Megmutatjuk azonban egy példán, hogy nem így van, azaz létezik olyan algebrai struktúra, amelyben minden, a gyűrűkre vonatkozó feltétel teljesül – kivéve az egyik disztributivitást. Tekintsük pl. a valós együtthatós polinomokat az összeadás és a behelyettesítés műveletére. Világos, hogy itt a megfelelő műveletekre csoportot, illetve félcsoportot kapunk. A behelyettesítést $\circ$-rel jelölve ($f \circ g$ jelentése: „f-be helyettesítünk g-t") érvényes az $(f+g)\circ h = f\circ h + g\circ h$ összefüggés, tehát az egyik disztributivitás is fennáll. A másik azonban általában nem, pl.

$$x^2 \circ (x+1) = x^2 + 2x + 1, \quad \text{míg} \quad (x^2 \circ x) + (x^2 \circ 1) = x^2 + 1.$$

Éppen a fenti típusú példák mutatják, hogy az ilyen „*majdnem gyűrű*" algebrai struktúrák is fontos szerepet játszanak.

7.2. Definíció. Ha egy gyűrű egyetlen eleme tartócsoportjának nulleleme, akkor nullgyűrűről beszélünk. Ha egy gyűrűben bármely két elem szorzata a tartócsoport nulleleme, akkor a gyűrű neve zérógyűrű. □

Megjegyezzük, hogy egy nullgyűrű nyilván zérógyűrű.

7.3. Tétel. *Minden kommutatív csoport előáll egy alkalmas gyűrű tartócsoportjaként.*

Bizonyítás. Értelmezzük az adott kommutatív csoportban a szorzást úgy, hogy bármely két elem szorzata legyen a csoport nulleleme. Mivel minden, legalább kéttényezős szorzat ugyanaz az elem, ezért minden szorzat megegyezik, vagyis az asszociativitás igaz. A disztributivitás igazolásához is ezt használhatjuk fel, tekintetbe véve a csoport nullelemére fennálló $0 + 0 = 0$ összefüggést. ■

A disztributivitás egy igen fontos következménye:

7.4. Tétel. *Egy gyűrű multiplikatív félcsoportja zéruselemes félcsoport, amelynek zéruseleme az additív csoport nulleleme.*

Bizonyítás. Az additív csoportbeli kivonás egyértelműségét felhasználva az $a0 = a(0+0) = a0 + a0$ összefüggésből következik, hogy $a0 = 0$. A másik disztributivitásból hasonlóan adódik, hogy $0a = 0$. ■

7.5. Tétel. *Tetszőleges gyűrűben érvényesek az „előjelszabályok":* $(-a)b = a(-b) = -ab$ *és* $(-a)(-b) = ab$*; ahol* a, b *a gyűrű elemei.*

Bizonyítás. A 7.4. tétel alapján kapjuk, hogy $ab + (-a)b = (a + (-a))b = 0b = 0$, amiből az inverz egyértelműsége alapján következik, hogy $(-a)b = -ab$. Ugyanígy látható be $a0 = 0$ felhasználásával az $a(-b) = -ab$ összefüggés. E kettőből együtt adódik: $(-a)(-b) = -a(-b) = -(-(ab)) = ab$. ■

A félcsoportokra, illetve a csoportokra vonatkozó elemi eredményeket minden további nélkül felhasználhatjuk – megfelelően – a gyűrűkre is.

7.6. Definíció. Az additív csoport nullelemét a gyűrű nullelemének nevezzük, az additív csoportbeli inverzet additív inverznek vagy ellentettnek. Ha $R^\times$ egységelemes, akkor egységelemét R egységelemének nevezzük. □

Az összeadás kommutativitása és asszociativitása következtében, ha az R gyűrű elemeinek tetszőleges, véges A rendszerét tekintjük (tehát A-ban egy-egy elem többször is szerepelhet), akkor ezeknek az elemeknek az összege egyértelmű. Ezt az összeget $\sum A$ jelöli.

7.7. Tétel. *Legyenek A és B az R gyűrű tetszőleges véges részrendszerei. Ezeknek az $AB = \{ab|(a,b) \in A \times B\}$ összefüggéssel definiált szorzatára teljesül, hogy $\left(\sum A\right)\left(\sum B\right) = \sum AB$. (Általános disztributivitás.)*

Bizonyítás. A bizonyítást teljes indukcióval végezzük. Ha mind A, mind B egyelemű, nincs mit bizonyítani. Ha egyikük egyelemű, másikuk kételemű, akkor az állított egyenlőség megegyezik a disztributivitással. Legyen most $A = \{a\}$ és $B = \{b_1, \dots, b_r\}$, ahol $r > 2$. Ekkor a disztributivitást felhasználva, r szerinti teljes indukcióval kapjuk, hogy

$$a(b_1 + b_2 + \cdots + b_r) = a(b_1 + (b_2 + \cdots + b_r)) = ab_1 + a(b_2 + \cdots + b_r) = ab_1 + ab_2 + \cdots + ab_r.$$

Hasonlóképpen bizonyítható az egyenlőség, ha B egyelemű. Legyen most $A = \{a_1, \dots, a_s\}$ és $B = \{b_1, \dots, b_r\}$, ahol $s, r \geq 2$; legyen továbbá $a = a_1 + \cdots + a_s$. Most

$$\left(\sum A\right)\left(\sum B\right) = a\left(\sum B\right) = ab_1 + \cdots + ab_r =$$

$$= (a_1b_1 + \cdots + a_sb_1) + \cdots + (a_1b_r + \cdots + a_sb_r) = \sum AB,$$

mint állítottuk. ■

A csoportoknál (5.25. tétel), illetve az Abel-csoportoknál (5.50. tétel) látottak alapján adódik:

7.8. Tétel. *Legyen a az R gyűrű tetszőleges eleme és n egy egész szám. Definiáljuk az na elemet a következőképpen:*

$$na = 0, \quad \text{ha} \quad n = 0;$$

$$na = a, \quad \text{ha} \quad n = 1;$$

$$na = (n-1)a + a, \quad \text{ha} \quad n \geq 2;$$

$$na = -(-n)a, \quad \text{ha} \quad n \text{ negatív.}$$

Ekkor tetszőleges n, k egészekre és $a, b \in R$ elemekre

$$(n+k)a = na + ka,$$

$$n(a+b) = na + nb,$$

$$n(ka) = (nk)a, \quad \text{és}$$

$$n(ab) = (na)b = a(nb)$$

teljesülnek.

Bizonyítás. Az első három összefüggés már R^+-ban igaz; míg az utolsó kettő a 7.7. tétel speciális eseteként adódik, felhasználva az előjelszabályt is. ■

7.9. Definíció. Ha u és v az R gyűrű nemnulla elemei, amelyekre $uv = 0$ teljesül, akkor ezeket nullosztópárnak nevezzük; u bal oldali, v jobb oldali nullosztó. □

7.10. Tétel. *Az $R^\times$ félcsoport egy $a \neq 0$ elemével akkor és csak akkor lehet balról (jobbról) egyszerűsíteni, ha nem bal oldali (jobb oldali) nullosztó.*

Bizonyítás. Tegyük fel, hogy a nem bal oldali nullosztó, és legyen $ab = ac$. Ekkor $a(b - c) = ab - ac = 0$ miatt $b - c = 0$, amiből következik, hogy a-val balról lehet egyszerűsíteni. Ha viszont a-val lehet balról egyszerűsíteni és $ab = 0$, akkor $a0 = 0$ miatt $b = 0$ adódik, vagyis a nem bal oldali nullosztó. ■

7.11. Következmény. *Egy R gyűrűben ekvivalens az alábbi három feltétel:*

(1) *$R^\times$-ban érvényes a bal oldali egyszerűsítési szabály.*

(2) *$R^\times$-ban érvényes a jobb oldali egyszerűsítési szabály.*

(3) *R-ben nincsenek nullosztók.* ■

Érdemes megjegyezni az alábbiakat. A fenti következményből adódik, hogy a 7.3. tétel analogonja nem érvényes a multiplikatív félcsoportra. Ha ugyanis valamely gyűrű multiplikatív félcsoportjában érvényes a bal oldali egyszerűsítési szabály, akkor a jobb oldali egyszerűsítési szabálynak is teljesülnie kell. Nem ilyen például egy legalább kételemű jobbzérus félcsoport, ahol $ab = b$ következtében $ab = ac$ esetén $b = c$; míg, ha $b \neq c$, akkor például $bb = cb(= b)$, tehát a jobb oldali egyszerűsítési szabály nem érvényes.

Triviálisan nincsenek nullosztók a nullgyűrűben. Ezektől azonban célszerű eltekinteni:

7.12. Definíció. Az R legalább kételemű gyűrű nullosztómentes, ha nincsenek benne nullosztópárok. Kommutatív, nullosztómentes gyűrű neve: integritási tartomány. □

7.13. Tétel. *R akkor és csak akkor nullosztómentes, ha a nullelem elhagyásával kapott halmaz a szorzásra félcsoport. Ezt a félcsoportot R^*-gal jelöljük.*

Bizonyítás. Ha R^* félcsoport, akkor a nullától különböző elemek szorzata sem nulla, és így a gyűrűben nincsenek nullosztópárok. Továbbá R-nek legalább két eleme van, hiszen a nulla elhagyása után egy félcsoportot kaptunk, amely – definíció szerint – nem lehet üres. Tegyük most fel, hogy R nullosztómentes. Mivel R-nek legalább két eleme van, ezért R^* nem üres; s mivel R^*-beli elemek szorzata nem nulla, ezért félcsoport (az asszociativitást nem kell külön ellenőrizni, mert az eleve teljesül). ■

7.14. Definíció. Ha R^* csoport, akkor R-et testnek nevezzük. Ha emellett a szorzás kommutatív, akkor kommutatív testről beszélünk. □

Megjegyzések. 1. Általában a nullgyűrűt is nullosztómentesnek nevezik. Ez azért kényelmetlen, mert így az integritási tartomány, illetve a test definíciójában hozzá kell tenni, hogy a „multiplikatív rész" nem üres.

2. Ha egy vizsgálat során mindig kommutatív testek szerepelnek, akkor elhagyják a „kommutatív" jelzőt. Ilyenkor megkülönböztetésül test helyett a *ferdetest* elnevezés használatos. □

7.15. Tétel. *Véges nullosztómentes gyűrű test.*

Bizonyítás. Legyen R véges, nullosztómentes gyűrű. Ekkor R^* a 7.13. tétel szerint (véges) félcsoport, amelyben a 7.11. következmény alapján érvényes a kétoldali egyszerűsítési szabály. Az 5.8. tétel szerint tehát R^* csoport, így a 7.14. definíció szerint R test. ■

7.2. Részgyűrűk, ideálok

Ugyanúgy, mint tetszőleges algebrai struktúrák esetében, beszélhetünk egy R gyűrű részgyűrűiről. Tekintettel arra, hogy ez egyszersmind az R^+-nak részcsoportja, ezért létezik legkisebb részgyűrű – nevezetesen a 0 generálta részgyűrű. A $0 \cdot 0 = 0$ egyenlőség alapján ez egyedül a nullelemből áll. Mivel R maga is részgyűrű, ezért minden, legalább kételemű gyűrűnek van két részgyűrűje: $\langle 0; \{+, \cdot\}\rangle$ és R. Ezek *triviális részgyűrűk*, minden más részgyűrű neve *valódi részgyűrű*.

A gyűrűk vizsgálatában igen fontos speciális részgyűrűket definiálunk:

7.16. Definíció. Az R gyűrű valamely nemüres B (illetve J) részhalmazát balideálnak vagy bal oldali ideálnak (jobbideálnak vagy jobb oldali ideálnak) nevezzük, ha az R^+-nak részcsoportja, és tetszőleges $r \in R$ esetén $rB \subseteq B$ ($Jr \subseteq J$). Ha az R gyűrű I részhalmaza mind bal oldali, mind jobb oldali ideál, akkor I-t (kétoldali) ideálnak nevezzük. □

7.17. Tétel. *Egy gyűrű részgyűrűi, balideáljai, jobbideáljai és ideáljai a tartalmazásra nézve egy-egy algebrai hálót alkotnak, amelyekben a metszet ugyanaz, következésképpen legkisebb, illetve legnagyobb elemeik megegyeznek.*

Bizonyítás. A 3.31. tétel alapján elegendő a gyűrűn úgy értelmezni műveleteket, hogy éppen a részgyűrűk, balideálok, jobbideálok, illetve az ideálok legyenek a részalgebrák. Ebből azonnal következik a tétel utolsó állítása is, hiszen részalgebrák metszete a halmazelméleti metszet és az adott gyűrű a legnagyobb (részgyűrű, balideál, jobbideál, illetve ideál).

A részgyűrűk esete triviális, hiszen ezek pontosan az eredeti gyűrű részalgebrái. Az ideálok esete visszavezethető a fennmaradt két esetre, egyszerűen az összes olyan műveletet kell tekinteni, amelyek a két eset bármelyikében szerepeltek. A bal-, illetve jobbideálok esete szimmetrikus, de hasznos mindkét esetet megnézni.

Tekintsük az $\mathfrak{R} = \langle R; \{+, \cdot\}\rangle$ gyűrűt, és tartóhalmazán definiáljunk két algebrát a következőképpen:

$$_R R = \langle R; \{-, \ldots, \lambda_r, \ldots | r \in R\}\rangle,$$

$$R_R = \langle R; \{-, \ldots, \mu_r, \ldots | r \in R\}\rangle,$$

ahol λ_r és μ_r az R tetszőleges r eleméhez hozzárendelt unáris műveletek, amelyeket – megfelelően – $\lambda_r : x \mapsto rx$ és $\mu_r : x \mapsto xr$ definiálnak.

A szimmetria alapján elegendő azt megmutatni, hogy ${}_R R$ részalgebrái pontosan a balideálok. A B részhalmaz kivonásra való zártsága pontosan azt jelenti, hogy R^+-nak részcsoportja. A λ_r műveletre való zártság pedig azt, hogy $r \in R$ esetén $rB \subseteq B$, vagyis azt, hogy balideál. ■

Mivel a fenti tételben szereplő „részek" teljes hálót alkotnak, ezért beszélhetünk egy (vagy több) elem generálta részgyűrűről, balideálról, jobbideálról, illetve ideálról.

7.18. Definíció. Legyen H az R gyűrű tetszőleges részhalmaza. A H generálta részgyűrűt, balideált, jobbideált, illetve ideált – megfelelően – $\langle H \rangle$, $\langle H \rangle_b$, $\langle H \rangle_j$, illetve (H) fogja jelölni. Az egy elemmel generált ideál neve főideál. □

Megjegyezzük, hogy létezik bal oldali és jobb oldali főideál is, de itt nem fog szerepelni.

7.19. Tétel. *Legyen $a \in R$. Ekkor*

(1) $\langle \{a\} \rangle = \{n_1 a + \cdots + n_k a^k\}$,

(2) $\langle \{a\} \rangle_b = \{na + ra | r \in R\}$,

(3) $\langle \{a\} \rangle_j = \{na + as | s \in R\}$,

(4) $(\{a\}) = \{na + r_0 a + as_0 + r_1 a s_1 + \cdots + r_k a s_k | r_i, s_i \in R\}$,

ahol k természetes szám, $n, n_1, \ldots, n_k$ egész számok.

Ha H a diszjunkt H_i halmazok egyesítése, akkor a H generálta bal oldali, jobb oldali, illetve kétoldali ideálok elemei az egyes H_i-k generálta bal oldali, jobb oldali, illetve kétoldali ideálok elemeinek a véges összegeiként állnak elő.

Bizonyítás. Először az egy elemmel generált részekkel foglalkozunk. Nyilvánvaló, hogy a felsorolt elemek benne vannak a megfelelő generátumban. Az is világos, hogy megfelelő speciális választással az a elem is a megadott alakban írható. Azt kell még belátni, hogy a megadott elemek halmaza a megfelelő műveletekre zárt. A kivonásra való zártság mind a négy esetben nyilvánvaló. A gyűrűbeli elemmel való szorzásra vonatkozó zártság a disztributivitásnak, az asszociativitásnak és a 7.8. tétel utolsó egyenlőségpárjának a következménye.

A második rész bizonyításánál is világos, hogy a megfelelő összegek benne vannak a generátumban. Tetszőleges, szóban forgó összeg $a_1 + \cdots + a_t$ alakban írható, ahol a_i a H_i generátumának eleme. Tekintettel arra, hogy egy ilyen összegben valamelyik i indexre $a_i = 0$ is lehetséges, ezért két, tetszőleges összeget egyszerre nézve feltehetjük, hogy mindkettőben pontosan ugyanazok az indexek szerepelnek. Ha mármost $b_1 + \cdots + b_t$ egy másik összeg, akkor ezek különbsége is ilyen összegként írható, mert $a_i - b_i$ is benne van a H_i generátumában. Ha $r, s \in R$, akkor $ra_i, a_i s, ra_i s$ ugyancsak elemei a H_i generálta bal oldali, jobb oldali, illetve kétoldali ideálnak, amiből következik, hogy a megfelelő esetekben $r(a_1 + \cdots + a_t)$, $(a_1 + \cdots + a_t)s$ és $r(a_1 + \cdots + a_t)s$ is a kívánt alakban írhatók. Ha az egyes H_i halmazokat egyeleműeknek választjuk, akkor speciális esetként kapjuk, hogy miképpen állíthatók elő a bal oldali, jobb oldali és kétoldali ideálok elemei generátorelemeik segítségével. ■

Megjegyzések. 1. Ha H_1 és H_2 az R gyűrű részhalmazai, akkor $\langle H_1 \cup H_2 \rangle$ elemei általában **nem** állnak elő a $\langle H_1 \rangle$ elemeinek és a $\langle H_2 \rangle$ elemeinek véges összegeként.

2. Könnyen látható, hogy ha $a \in R$, akkor az Ra, illetve aR szorzat bal oldali, illetve jobb oldali ideál. Ez azonban nem egyezik meg az a generálta bal oldali, illetve jobb oldali ideállal, mert általában nem tartalmazza az a elemet. Ha viszont R egységelemes, akkor a fentiek alapján éppen a generátumot adják. □

7.20. Definíció. Jelölje $\varrho(ab)$ az R elemein az $ab = 0$ relációt. Ekkor a 3.11. definíció és a 3.12. tétel jelöléseit használva, tetszőleges $X \subseteq R$ részhalmaz esetén legyen

$$r(X) = \varrho(X) \quad \text{az} \quad X \quad \text{jobbannullátorainak a halmaza,}$$

$$\ell(X) = \varrho^{-1}(X) \quad \text{az} \quad X \quad \text{balannullátorainak a halmaza.} \qquad \square$$

7.21. Tétel. *Tetszőleges R gyűrű bármely X részhalmazára $r(X)$ jobbideál, $\ell(X)$ balideál; s ha X jobbideál (balideál), akkor $r(X)$ ($\ell(X)$) ideál.*

Bizonyítás. A szimmetria miatt elegendő a jobbannullátorokkal foglalkozni. A 3.12. tétel és a lezárás tulajdonságai alapján elegendő az első állítást egyelemű X halmazra bizonyítani, mert jobbideálok közös része is jobbideál.

Ha $xr = xs = 0$, akkor $x(r - s) = 0$ és $x(rt) = 0$ teljesül $(r, s, t \in R)$. Így $r(X)$ jobbideál. Legyen $Y = r(X)$, az R valamely jobbideáljára. Az R tetszőleges t elemére az asszociativitás miatt $X(tY) \subseteq XY$. Ezért $tY \subseteq r(X)$, tehát Y ideál. ■

A balideálmentes gyűrűk leírásához előkészületül bebizonyítunk egy önmagában is érdekes segédtételt.

7.22. Tétel. *Ha egy nullosztómentes R gyűrű valamely nemnulla a eleméhez található olyan e elem, amelyre $ae = a$ teljesül, akkor e az R egységeleme.*

Bizonyítás. Az R tetszőleges nemnulla b elemére kapjuk, hogy $aeb = ab$, s mivel R nullosztómentes, ezért a-val egyszerűsíthetünk: $eb = b$. Ez azt jelenti, hogy e bal oldali egységelem. Ugyanennek az okoskodásnak a duálisát végrehajtva kapjuk, hogy e egyszersmind jobb oldali egységelem is. ■

7.23. Tétel. *Egy R gyűrűnek akkor és csak akkor vannak csupán triviális balideáljai, ha R vagy prímszámelemű zérógyűrű, vagy test.*

Bizonyítás. Egy balideál az additív csoportnak részcsoportja is, így a Lagrange-tétel alapján prímszámelemű zérógyűrűnek nem lehet valódi balideálja. Mivel csoportokban az $ya = b$ egyenletek y-ban megoldhatók, ezért testben sem lehet balideál.

Tegyük most fel, hogy az R gyűrűben nincs nemtriviális balideál. A 7.21. tétel alapján $r(R)$ ideál; így a feltétel szerint vagy $r(R) = R$, vagy $r(R) = \{0\}$. Az első esetben R zérógyűrű. Ekkor világos, hogy R additív csoportjának minden részcsoportja ideál. Márpedig – mint az 5.44. tétel bizonyításánál láttuk – ha egy csoportnak nincs valódi részcsoportja, akkor a csoport prímrendű.

Tekintsük most az $r(R) = \{0\}$ esetet. Ekkor az R bármely, 0-tól különböző a elemére vizsgáljuk az $\ell(\{a\})$ halmazt. A 7.21. tétel szerint ez balideál. Ez a balideál nem lehet R, mert akkor $a \in r(R)$ volna. Így a feltételből $\ell(\{a\}) = 0$ következik; tehát R nullosztómentes. A nullosztómentességből az is következik, hogy Ra egy 0-tól különböző balideál, és így

$Ra = R$. Ez azt jelenti, hogy R-ben az $ya = b$ egyenletek megoldhatók. Speciálisan létezik olyan e, amelyre $ea = a$. A 7.22. tétel alapján tehát R egységelemes. Az 5.2. tétel szerint tehát R^* csoport, azaz R test. ■

Most gyűrűk homomorfizmusainak a vizsgálatára térünk rá. Mivel egy kompatibilis osztályozás bármely osztálya már az additív csoportot figyelembe véve is meghatározza a többi osztályt, ezért a homomorfizmus magját itt is úgy értelmezzük, mint a nullelemet tartalmazó kongruenciaosztályt.

7.24. Tétel. *Egy gyűrű tartóhalmazának valamely részhalmaza akkor és csak akkor magja egy alkalmas homomorfizmusnak, ha ideál.*

Bizonyítás. Legyen I az R gyűrű valamely Θ osztályozásában a nullelemet tartalmazó osztály. Azt kell bizonyítanunk, hogy ez az osztályozás pontosan akkor kompatibilis a gyűrűműveletekkel, ha ideál. Az R^+ műveleteivel való kompatibilitás feltétele – mint tudjuk – az, hogy I részcsoportja R^+-nak. A szorzással való kompatibilitás pontosan akkor teljesül, ha az $a \equiv b(\Theta)$ és $c \equiv d(\Theta)$ feltételekből $ac \equiv bd(\Theta)$ következik. Felhasználva, hogy az I szerinti mellékosztályok adják az osztályozást, a feltétel azt jelenti, hogy ha $a - b, c - d \in I$, akkor $ac - bd \in I$ is igaz. Az $a - b = x$ és $c - d = y$ jelöléssel a feltételt tovább alakíthatjuk:

„Ha $x, y \in I$, akkor tetszőleges $b, d \in R$ elemekkel $by + xd + xy \in I$."

Ez a feltétel nyilvánvalóan teljesül, ha I ideál; míg e feltétel teljesüléséből $x = 0$, illetve $y = 0$ választással azt kapjuk, hogy I jobbideál, illetve balideál. ■

Gyűrűk esetén a kompatibilis osztályozásnál fellépő osztályokat *maradékosztályoknak* nevezik. Ennek megfelelően a természetesen adódó *faktorgyűrű* elnevezés helyett a *maradékosztály-gyűrű* elnevezést is használják. Megemlítjük még, hogy a gyűrűkre is igaz a két Noether-féle izomorfizmustétel megfelelő analogonja. Ennek bizonyítását az olvasóra bízzuk; csupán azt kell kihasználni, hogy az eredeti bizonyításban a homomorfizmusok nemcsak az additív csoport, hanem egyszersmind a multiplikatív félcsoport homomorfizmusai is.

A gyűrűknél a normálosztó-jelöléssel analóg módon $I \lhd R$ jelöli azt, hogy *I az R-nek ideálja*. A faktorcsoport-jelöléshez hasonlóan $I \lhd R$ esetén *R/I jelöli R-nek I szerinti maradékosztály-gyűrűjét*.

7.25. Definíció. Az R gyűrű egy I ideálját maximálisnak nevezzük, ha az R-től különböző ideálok részbenrendezett halmazának egy maximális eleme. R egyszerű, ha $\{0\}$ maximális ideál. □

7.26. Tétel. *I az R-nek akkor és csak akkor maximális ideálja, ha R/I egyszerű. Minden test egyszerű gyűrű.*

Bizonyítás. Legyen $I \neq R$ tetszőleges ideál, és tekintsünk egy $J \neq I$ ideált, amely tartalmazza I-t. Ekkor a második izomorfizmustétel alapján $I \lhd J$ és $R/J \cong (R/I)/(J/I)$. Fordítva is igaz, hogy R/I minden nemnulla ideálja J/I alakú, ahol J – mint a tekintett ideál teljes inverz képe – egy, az I-t valódi módon tartalmazó ideál. Az izomorfizmus alapján a két maradékosztály-gyűrű csak egyszerre lehet egyelemű, azaz $R = J$ pontosan

akkor teljesül, ha $R/I = J/I$. Ez pedig éppen azt jelenti, hogy I maximalitása R-ben ekvivalens R/I egyszerűségével. Ebből azonnal következik a második állítás is, a 7.23. tétel figyelembevételével. ■

Ennek a fejezetnek a további részeiben csak kommutatív gyűrűkkel foglalkozunk.

7.3. Hányadosgyűrű, lokális gyűrűk

A következőkben annak a konstrukciónak az általánosítását tűzzük ki célul, amely az egész számokból a racionális számokat alkotja meg. Meglepő dolog, hogy a „törtek" bevezetésének a fő akadálya nem az, hogy egy gyűrűben esetleg nullosztók vannak, hanem az, hogy a szorzás nem kommutatív. Tekintettel arra, hogy most csak kommutatív gyűrűkkel foglalkozunk, ezért a konstrukciót egészen általánosan végezhetjük. Természetesen a nullosztóval való osztás a nullával való osztáshoz vezetne, ami a gyűrűk esetében sem lehetséges, hiszen $0x = a$ csak $a = 0$ esetén lehet, amikor viszont bármely x-re fennáll a $0x = 0$ összefüggés. Így eleve csak nem-nullosztókkal akarhatunk osztani.

7.27. Tétel. *Kommutatív gyűrűben a nem-nullosztók egy* 0*-t nem tartalmazó multiplikatív félcsoportot alkotnak. Egy kommutatív gyűrű nem-nullosztókból álló multiplikatív részfélcsoportjait osztórendszereknek fogjuk nevezni.*

Bizonyítás. Legyenek a és b nem-nullosztók az R gyűrűben, és tegyük fel, hogy az R valamely c elemére $(ab)c = 0$ teljesül. Mivel a nem-nullosztó, ezért az $a(bc) = (ab)c = 0$ feltételből $bc = 0$ következik, amiből viszont azt kapjuk, hogy $c = 0$, hiszen b sem nullosztó. ■

7.28. Definíció. Legyen M az R (kommutatív) gyűrű egy osztórendszere. Az S (kommutatív) gyűrűt az R gyűrű M szerinti hányadosgyűrűjének nevezzük, ha a következők teljesülnek:

(1) R az S-nek részgyűrűje.

(2) Bármely $m \in M$, $s \in S$ esetén az $mx = s$ egyenlet S-ben megoldható.

(3) Bármely $s \in S$, $s \neq 0$ elemhez létezik olyan $m \in M$, amelyre $ms \in R$, és $ms \neq 0$. □

A második feltétel azt mondja ki, hogy az M-beli elemekkel a bővebb gyűrűben már lehet osztani; míg a harmadik feltétel azt, hogy a bővebb gyűrűbe csupa olyan elemet vettünk be, amelyet az osztás elvégezhetősége érdekében be is kellett vennünk.

7.29. Tétel. *Ha S az R-nek M szerinti hányadosgyűrűje, akkor M az S-ben is osztórendszer.*

Bizonyítás. M nyilván félcsoport marad, csak azt kell belátni, hogy elemei S-ben sem nullosztók. Legyen $m \in M$ és $s \in S$, és $s \neq 0$. (3) szerint van olyan $m_1 \in M$, amelyre $m_1 s$ az R-nek 0-tól különböző eleme. Az M-re vonatkozó feltétel szerint tehát $m_1(ms) = m(m_1 s) \neq 0$, amiből $ms \neq 0$ következik. ■

7.30. Tétel. *Ha létezik az R-nek M szerinti hányadosgyűrűje, akkor ez – R-et fixen hagyó izomorfizmustól eltekintve – egyértelműen meghatározott.*

Bizonyítás. Az állításnál többet mutatunk ki, nevezetesen azt, hogy a hányadosgyűrű a legkisebb olyan gyűrű, amelyben az M elemeivel lehet osztani. Pontosabban:

Legyen $\varphi : R \to R'$ egy izomorfizmus, amely R-nek az M osztórendszerét az R' egy M' osztórendszerébe képezi le. Legyen továbbá S' olyan, az R'-t tartalmazó gyűrű, amelyben M' még mindig osztórendszer, továbbá bármely $s' \in S'$ és $m' \in M'$ esetén van olyan S'-beli x', amelyre $m'x' = s'$. Ekkor φ-nek pontosan egy homomorf kiterjesztése van S-re.

Mindenekelőtt megjegyezzük, hogy a szóban forgó x' egyértelmű. Ha ugyanis $m'x'' = s'$ is teljesül, akkor $m'(x' - x'') = 0$, amiből valóban $x' = x''$ következik, hiszen egy osztórendszerben nincsenek nullosztók.

Tegyük most fel, hogy egy $\psi : S \to S'$ homomorfizmusnak az R-re való megszorítása pontosan φ. (3) miatt tetszőleges S-beli s elemhez létezik olyan M-beli m, amire $ms = a \in R$ nem 0. Mivel ψ homomorfizmus és megszorítása φ, ezért $\varphi(a) = \psi(a) = \psi(s)\psi(m) = \psi(s)\varphi(m)$. Mivel $\varphi(M) \subseteq M'$, ezért $\varphi(a)$ és $\varphi(m)$ egyértelműen meghatározzák az $s' = \psi(s)$ elemet. Ez azt jelenti, hogy ez az egyetlen lehetőség a ψ definiálására.

Tekintettel arra, hogy az $s \in S$ elem nem határozza meg egyértelműen azt az $a \in R$ $(a \neq 0)$ és $m \in M$ elemet, amelyre $ms = a$, ezért be kell látni, hogy $\psi(s)$ nem függ az a és m speciális választásától. Ha $m_1 s = a_1$ és $m_2 s = a_2$, akkor a kommutativitás miatt $m_2 a_1 = m_2 m_1 s = m_1 a_2$ teljesül. Ez fordítva is igaz, ha $m_2 a_1 = m_1 a_2$, továbbá $m_1 s_1 = a_1$ és $m_2 s_2 = a_2$, akkor ebből $m_1 m_2 s_2 = m_2 m_1 s_1$, és így $s_1 = s_2$ következik. Ebből már könnyen belátható a $\psi(s)$ egyértelműsége. Azt kell még megmutatni, hogy az így definiált ψ művelettartó. Legyen $s, r \in S$ olyanok, hogy az R alkalmas a, b nemnulla elemeire és M-beli m, n elemekre $ms = a$ és $nr = b$. Ebből $mn(s + r) = na + mb$ és $mn(sr) = (ma)(nb)$ kapható, ami biztosítja a művelettartást. (Az $rs = 0$ esetben a művelettartás triviális.)

A tétel bizonyításához tegyük most fel, hogy $R' = R$, $M' = M$ és S' is hányadosgyűrű. Legyen φ' a φ inverze és ψ' a φ' kiterjesztése. Ekkor $\psi\psi'$ a $\varphi\varphi'$ és $\psi'\psi$ a $\varphi'\varphi$ egyértelmű kiterjesztése. Mivel e két utóbbi mindegyike az identitás és az identitásnak az identitás kiterjesztése, ezért a $\psi\psi'$ és a $\psi'\psi$ mindegyike megegyezik az identitással. Eszerint ψ és ψ' egymás inverzei, vagyis mindegyikük olyan izomorfizmus, amely R-t elemenként fixen hagyja. ■

A fenti tétel jogossá teszi, hogy az M szerinti hányadosgyűrűről beszéljünk, és azt mint csupán M (és R) függvényét jelöljük:

7.31. Definíció. Az R gyűrű M szerinti hányadosgyűrűjét $R//M$-mel jelöljük. □

7.32. Tétel. *Ha M az R gyűrű osztórendszere, akkor létezik $R//M$.*

Bizonyítás. A konstrukciót a 7.30. tétel bizonyítása alapján lehet elvégezni. Ez a tétel lényegében azt is kimondja, hogy az itt megadott konstrukció az egyetlen lehetséges. Itt csak a konstrukciót adjuk meg, anélkül, hogy a lépések „szükségességére” utalnánk.

Mindenekelőtt két műveletet értelmezünk az $R \times M$ halmazon:

$$(a, m) + (b, k) = (ak + bm, mk), \qquad (a, m) \cdot (b, k) = (ab, mk),$$

ahol $a, b \in R$ és $m, k \in M$. A definíció értelmes, mert M zárt a szorzásra. Könnyen látható, hogy mindkét művelet kommutatív és asszociatív. (Ennek belátását az olvasóra bízzuk. Azt is beláthatjuk, hogy a kivonás nem végezhető el, és hogy a disztributivitás nem teljesül.)

A fenti algebrában egy relációt vezetünk be:

$$(a, m) \sim (a', m') \qquad \text{pontosan akkor, ha} \qquad am' = a'm.$$

Kimutatjuk, hogy ez a reláció a fenti struktúrának kongruenciarelációja. A reláció reflexivitása és szimmetriája triviális. A tranzitivitás belátásához legyen még $(a', m') \sim (a'', m'')$. Ebből $am'm'' = a'mm'' = a''m'm$ következik, s mivel m' nem nullosztó, kapjuk, hogy $am'' = a''m$. Eszerint $(a, m) \sim (a'', m'')$, ami bizonyítja a tranzitivitást.

A tranzitivitás alapján elegendő a kongruenciareláció tulajdonságaihoz azt belátni, hogy ha a fenti műveletek bármelyik komponensét egy vele kongruenssel helyettesítjük, akkor az eredmény is kongruens lesz az eredeti eredménnyel. A műveletek kommutativitása alapján elegendő ezt például az első komponensekre belátni. Más szóval azt kell megmutatni, hogy ha $am' = a'm$, akkor $(ak + bm)m'k = (a'k + bm')mk$ és $abm'k = a'bmk$ is teljesülnek. Márpedig ezek nyilvánvalók.

Azt állítjuk, hogy a kapott faktoralgebra lesz a kívánt $R//M$ gyűrű. Annyit már bizonyosan tudunk, hogy ebben az algebrában értelmezve van két kommutatív és asszociatív művelet. Először kimutatjuk, hogy az egyik műveletre nézve az algebra csoport, majd azt, hogy a másik művelet erre nézve disztributív.

A $(0, m)$ alakú elemek nyilvánvalóan egy kongruenciaosztályt alkotnak, és $(0, m) + (a, k) = (am, km) \sim (a, k)$ miatt ez az osztály a faktoralgebra + műveletére nézve nullelem. Az $(a, m) + (-a, m) = (0, mm)$ összefüggés alapján a faktoralgebra a + műveletre nézve valóban csoport.

A disztributivitást bizonyítjuk:

$$((a, m) + (b, k)) \cdot (c, \ell) = (ak + bm, mk) \cdot (c, \ell) = (ack + bcm, mk\ell),$$

$$(a, m) \cdot (c, \ell) + (b, k) \cdot (c, \ell) = (ac, m\ell) + (bc, k\ell) = (ack\ell + bcm\ell, m\ell k\ell).$$

A kapott két elem pedig nyilván kongruens.

Most azt mutatjuk meg, hogy a kapott gyűrű tartalmazza R-et – pontosabban egy, az R-rel izomorf részgyűrűt.

Az (am, m) $(m \in M)$ elemek nyilván egy osztályban vannak. Az $(am, m) + (bm, m) \sim ((a + b)m, m)$ és $(am, m) \cdot (bm, m) \sim (abm, m)$ összefüggés alapján az $a \mapsto (am, m)$ megfeleltetés nyilvánvalóan izomorfizmus.

Az $(mm, m) \cdot (a, m) \sim (a, m)$ összefüggés biztosítja, hogy a 7.28. definícióban szereplő (2) és (3) feltételek is teljesülnek. ■

7.33. Következmény. *Minden (kommutatív) gyűrűnek van hányadosgyűrűje, azaz olyan legkisebb, őt tartalmazó gyűrű, amelyben minden nem-nullosztónak van (multiplikatív) inverze.*

Bizonyítás. A 7.32. tételben válasszuk M-nek a nem-nullosztók halmazát. ■

7.34. Következmény. *Minden integritási tartománynak van hányadosteste, azaz olyan legkisebb, őt tartalmazó test, amelyben minden nemnulla elemnek van inverze.*

Bizonyítás. A 7.33. következmény speciális esete. ■

A továbbiakban egy fontos speciális ideálfajtát vezetünk be.

7.35. Definíció. Az R gyűrű egy P ideálját prímideálnak nevezzük, ha $ab \in P$ esetén $a \in P$ vagy $b \in P$ teljesül. □

7.36. Tétel. *Egy R (kommutatív) gyűrű P ideáljára az alábbi feltételek ekvivalensek:*

(1) *P prímideál.*

(2) *R/P integritási tartomány.*

(3) *P-nek (az M) komplementerhalmaza a szorzásra zárt.*

Ha R egységelemes, akkor minden maximális ideál prím.

Bizonyítás. (3) az (1)-nek logikai átfogalmazása.

Legyen $[a]$, illetve $[b]$ az a-t, illetve a b-t tartalmazó R/P-beli osztály. A műveletartás alapján R/P nullosztómentessége úgy fogalmazható, hogy $[ab] = [0]$ esetén vagy $[a] = [0]$, vagy $[b] = [0]$. Ez viszont a homomorfizmus magjának a definíciója szerint pontosan azt jelenti, hogy P prímideál.

Legyen M maximális ideál. Mivel az egységelem képe is egységelem, ezért R/M nem zérógyűrű. A 7.26. tétel miatt tehát egyszerű. Így, a 7.23. tétel alapján csak test lehet, hiszen nem zérógyűrű. Ezért R/M integritási tartomány és (2) szerint M prímideál. ■

7.37. Definíció. Egy egységelemes R gyűrűt lokális gyűrűnek nevezünk, ha R-ben egyetlen maximális ideál van. □

7.38. Tétel. *Az R lokális gyűrű maximális ideálja egy P prímideál, amely minden R-től különböző ideált tartalmaz. Az R gyűrűben pontosan a P-n kívüli elemeknek van inverzük. Ha R-ben van olyan P ideál, hogy amennyiben egy $a \in R$ elemnek pontosan akkor van inverze, ha $a \notin P$, úgy R lokális gyűrű, amelyben P az egyetlen maximális ideál.*

Bizonyítás. A 7.36. tétel szerint P prímideál. Tekintettel arra, hogy R egységelemes, a Zorn-lemma alapján minden ideál benne van egy maximális ideálban, amely a lokális gyűrű definíciója szerint csak P lehet.

Ha $a \notin P$, akkor $a \in Ra$ miatt $Ra \not\subseteq P$, és így $Ra = R$, vagyis a P-n kívüli elemekkel lehet osztani ($xa = b$ mindig megoldható). Ha viszont az a elemnek létezik inverze, akkor $Ra = R$, tehát $a \notin P$. Legyen most Q az R-nek olyan ideálja, hogy a rajta kívüli elemeknek létezik inverze. A Q-n kívüli elemek tehát a szorzásra nézve csoportot alkotnak, amiből következik, hogy R egységelemes és Q prímideál. Ha egy ideál különbözik R-től, akkor nem tartalmazhat invertálható elemet, és így Q-nak része. ■

7.39. Tétel. *Ha P az R integritási tartomány egy prímideálja, akkor R-nek létezik olyan hányadosgyűrűje, amelyben a P generálta ideál prímideál és minden valódi ideált tartalmaz, tehát lokális gyűrű, amelyet P szerinti lokalizáltnak nevezünk.*

Bizonyítás. Legyen M a P komplementer halmaza. Mivel R nullosztómentes és P prímideál, ezért M osztórendszer. Így létezik az $R//M$ hányadosgyűrű. Kimutatjuk, hogy ez a kívánt tulajdonságú lokális gyűrű.

Nézzük meg először, hogy mely (a, m) elemeknek létezik inverze. Mivel (m, m) a hányadosgyűrű egységeleme, ezért ez az $(a, m) \cdot (b, k) \sim (m, m)$ feltételhez vezet, ami azzal ekvivalens, hogy $abm = mkm$, azaz $ab = mk$, mert m-mel egyszerűsíthetünk. Mivel M a szorzásra zárt, ezért $ab \in M$, és az ideáltulajdonság alapján $a \in M$. Fordítva, a (k, m) elemnek $(k, m \in M)$ nyilván van inverze, nevezetesen (m, k). Így pontosan azok az (a, m) elemek invertálhatók, amelyekre $a \in M$.

Ha $a \in P$, akkor a hányadosgyűrűben (am, m) a P-nek megfelelő részhalmaz eleme, s ezért $(m, mk) \cdot (am, m)$ benne van az általa generált ideálban. Az $(amm, mkm) \sim (a, k)$ összefüggés miatt a nem invertálható elemek benne vannak a szóban forgó generátumban. Az ideáltulajdonságból azonnal következik, hogy az (a, m) alakú elemek $(a \in P,\ m \in \in M)$ ideált alkotnak; s a 7.38. tétel alapján a gyűrű valóban a kívánt tulajdonságú lokális gyűrű. ■

Megjegyzés. A „lokális” elnevezés jelen esetben körülbelül azt fedi, hogy „helyhez kötött”. A racionális törtfüggvények (polinomok hányadosai) egy jól kezelhető testet alkotnak. Amennyiben viszont ezeket az (n-dimenziós) tér egy helyén vizsgáljuk, akkor azok a törtek, amelyekben a nevező 0-vá válik, nem értelmezhetők. Viszont azokkal a polinomokkal, amelyeknek az értéke e helyen nem 0, lehet osztani. Így keletkeznek lokális gyűrűk. A „hely” egyébként nem csak egy pont lehet, hanem bármely úgynevezett algebrai görbe vagy felület. □

Feladatok

1. A valós együtthatós polinomok + és $\circ$ műveletekkel definiált „majdnemgyűrűjében” határozzuk meg azokat a p elemeket, amelyekre bármely f és g polinom esetében igaz a $p \circ (f + g) = p \circ f + p \circ g$ összefüggés.

2. Bizonyítsuk be, hogy ha egy R gyűrűnek van valódi balideálja, akkor van valódi jobbideálja is; de ebből nem következik, hogy van valódi ideálja.

3. Határozzuk meg $\mathbb{Z}$ (az egészek gyűrűje) és az $\mathbb{Z}[x]$ polinomgyűrű maximális és prímideáljait.

4. Határozzuk meg $\mathbb{Z}$-ben, $\mathbb{Z}[x]$-ben és $\mathbb{Q}[x]$-ben ($\mathbb{Q}$ a racionális számtest) az „összes” lehetséges osztórendszert. Igaz-e, hogy ezek komplementere mindig prímideál?

5. Írjuk le $\mathbb{Z}$ összes lehetséges hányadosgyűrűjét.

6. Írjuk le $\mathbb{Z}$ összes lokalizáltját.

7. Írjuk le $\mathbb{Z}$ összes faktorgyűrűjét.

8. Mutassuk meg, hogy $\mathbb{Z}$ bármely lokalizáltjában van olyan p elem, hogy minden eleme egyértelműen $r \cdot p^i$ alakba írható, ahol r a gyűrű egy invertálható eleme és $i \geq 0$ egész szám; következésképpen ideáljainak részbenrendezett halmaza lánc.

9. Mutassuk meg, hogy $\mathbb{Z}[x]$-nek van olyan lokalizáltja, amelyikben az ideálok nem alkotnak láncot.

10. Az R gyűrű osztórendszerei a tartalmazásra nézve teljes hálót alkotnak.

11. Az R gyűrűbeli M és N osztórendszert ekvivalenseknek nevezzük, ha $R//M = R//N$. Bizonyítsuk be az alábbiakat:

(1) Ekvivalens osztórendszerek között van legnagyobb. (Hogyan kapható meg?)

(2) Lehetséges, hogy van köztük minimális, de nincs legkisebb.

(3) Lehetséges, hogy van köztük legkisebb.

Definíció. A K test egy R részgyűrűjét értékelésgyűrűnek nevezzük, ha bármely 0-tól különböző $x \in K$ esetén vagy $x \in R$, vagy $x^{-1} \in R$ teljesül. □

12. Bizonyítsuk be, hogy minden értékelésgyűrű lokális gyűrű.

13. Bizonyítsuk be, hogy egy (kommutatív egységelemes) gyűrű pontosan akkor értékelésgyűrű, ha ideáljai a tartalmazásra nézve láncot alkotnak.

14. Bizonyítsuk be, hogy egy értékelésgyűrűben bármely véges sok elem generálta ideál főideál.

15. Legyen Λ egy rendezett halmaz, és $\mathbf{X} = \{\mathbf{x}_\lambda | \lambda \in \Lambda\}$ a $\mathbb{Q}$ feletti határozatlanok halmaza. A $\mathbb{Q}[\mathbf{X}]$-beli normált egytagúakat írjuk $\mathbf{n} = \mathbf{x}_{\lambda_1}^{n_1} \cdot \ldots \cdot \mathbf{x}_{\lambda_r}^{n_r}$ *normált alakba*, ahol $\lambda_1 < \ldots < \lambda_r$ a Λ elemeinek véges (esetleg üres) halmaza. Az ugyancsak normált $\mathbf{k} = \mathbf{x}_{\mu_1}^{k_1} \cdot \ldots \cdot \mathbf{x}_{\mu_s}^{k_s}$ egytagú esetén azt mondjuk, hogy $\mathbf{k}$ megelőzi $\mathbf{n}$-et (jelben $\mathbf{k} \prec \mathbf{n}$), ha van olyan i index, hogy $(j < i)$-re $\lambda_j = \mu_j$ és $n_j = k_j$, míg az i indexre vagy $\mu_i < \lambda_i$, vagy $\mu_i = \lambda_i$ és $k_i < n_i$.

Világos, hogy $\mathbb{Q}[X]$ minden $\mathbf{f}$ eleme (normált alakú) egytagúak (monomok) $\mathbb{Q}$-beli együtthatós lineáris kombinációja. Ezek közül azt amelyik a fenti rendezésben az első, nevezzük $\mathbf{f}$ vezető tagjának és jelöljük $\mathbf{n}(\mathbf{f})$-fel. Jelölje R a $\mathbb{Q}(\mathbf{X})$ azon $\dfrac{\mathbf{f}}{\mathbf{g}}$ elemeinek a halmazát, amelyekre $\mathbf{n}(\mathbf{f}) \preceq \mathbf{n}(\mathbf{g})$. Bizonyítsuk be a következőket:

(1) R a $\mathbb{Q}(\mathbf{X})$-nek a $\mathbb{Q}[\mathbf{X}]$-et tartalmazó részgyűrűje.

(2) R értékelésgyűrű.

(3) R-ben „nagyon sok” ideál és prímideál van; írjuk le ezeket.

(4) R akkor és csak akkor Noether-gyűrű, ha Λ jólrendezett.

16. Legyen V a nemnegatív valós számoknak a természetes számokat és a 0-t tartalmazó olyan additív részfélcsoportja, amelynek nincs legkisebb pozitív eleme és bármely két eleme között van V-beli elem (ilyen például a nemnegatív racionális vagy nemnegatív valós számok félcsoportja). Tekintsük a V-beli „kitevőkkel” képezett $\mathbb{Q}_V[\mathbf{x}]$ „polinomgyűrűt”, amelynek elemei az $\{\mathbf{x}^v | v \in V\}$ bázisvektorok által generált $\mathbb{Q}$ feletti vektortér elemei;

ellátva az $\mathbf{x}^s \cdot \mathbf{x}^r = \mathbf{x}^{s+r}$ $(s, r \in V)$ relációk által értelmezett asszociatív és az összeadásra nézve disztributív szorzással. (Részletek találhatók a csoportalgebrák tárgyalásánál.) Bizonyítsuk be az alábbiakat:

(1) Azok a polinomok, amelyeknek a konstans tagja nem 0, egy M osztórendszert alkotnak $\mathbb{Q}_V[\mathbf{x}]$-ben.

(2) Az $R = \mathbb{Q}_V[\mathbf{x}]//M$ hányadosgyűrűnek tetszőleges $\mathbf{f}$ eleme egyértelműen felírható $v(\mathbf{f}) \cdot \mathbf{m}(\mathbf{f})$ alakban, ahol $v(\mathbf{f}) = \mathbf{x}^v$ $(v \in V)$ alakú és $\mathbf{m}(\mathbf{f})$ R-beli egység (azaz két M-beli elem hányadosa).

(3) R értékelésgyűrű és az $\mathbf{x}^v$ $(v > 0)$ elemek generálta P ideál az egyetlen prímideálja (amely maximális).

(4) Rögzített $v \in V$ esetén az $\mathbf{x}^v$ elemet nem tartalmazó maximális ideál nem végesen generált.

17. Adjuk meg az előző két feladatnak olyan közös általánosítását, amelyben a „kitevők" egy elrendezett kommutatív csoport elemei, és bizonyítsuk be az „analóg" tulajdonságokat.

7.4. Noether-gyűrű, polinomgyűrű

A kommutatív gyűrűk elméletében a Noether-gyűrűk igen jelentős szerepet játszanak. A Noether-gyűrűket nemkommutatív esetben is értelmezhetjük, de mi itt csak a kommutatív esetet vizsgáljuk.

7.40. Definíció. Egy R gyűrűt Noether-gyűrűnek nevezünk, ha ideáljaira teljesül a maximumfeltétel. □

A 3.3. tételből azonnal következik:

7.41. Tétel. *Egy R gyűrű akkor és csak akkor Noether-gyűrű, ha ideáljaira teljesül, hogy minden szigorúan növő lánc véges, vagy minden növő lánc stabilizálódik, illetve érvényes a lefelé menő indukció.* ■

Az 3.32. és 7.17. tételekből azonnal kapjuk:

7.42. Tétel. *Egy gyűrű akkor és csak akkor Noether-gyűrű, ha minden ideálja végesen generált.* ■

A Noether-gyűrűk fontosságát mutatja, hogy a kommutatív testbeli együtthatós polinomok is Noether-gyűrűt alkotnak. A (számtestbeli együtthatós) egy-, illetve többhatározatlanú polinomokat már az I. kötet I. részében definiáltuk (3.1., illetve 4.1. definíció). Az alábbiakban a polinomoknak egy absztrakt definícióját adjuk, amely az I. kötet I. részének 3.20. tételében kimondott jellemző tulajdonságon alapszik:

7.43. Definíció. Legyen X az R gyűrűtől diszjunkt halmaz, amelyet R feletti határozatlanok halmazának nevezünk. Az $R[X] \geq R$ gyűrűt az R feletti, X-ből vett határozatlanok generálta polinomgyűrűnek nevezzük, ha $R[X] = \langle R \cup X \rangle$, továbbá bármely S (kommutatív) gyűrűhöz és olyan $\varphi : (R \cup X) \to S$ leképezéshez, amelynek az R-re való

megszorítása az S gyűrűbe való homomorfizmus, létezik olyan egyértelműen meghatározott $\psi : R[X] \to S$ homomorfizmus, amelynek $R \cup X$-re való megszorítása φ. Ha X véges halmaz, akkor véges sok határozatlanú polinomgyűrűről beszélünk. (Ha $|X| = n$, akkor $R[X]$ n határozatlanú polinomgyűrű.) Az $R[X]$ elemeit R feletti polinomoknak nevezzük. □

Megjegyzés. A definícióból következik, hogy az X halmaz elemei nem lehetnek tetszőlegesek. Az $R = \mathbb{Z}$ és $X = \{\sqrt{2}\}$ eset például nem felel meg. Valóban, ezt nem lehet homomorfizmussal úgy leképezni a valós számokra, hogy minden egész számnak önmagát feleltetjük meg és $\sqrt{2}$-nek $\sqrt{3}$-at. □

7.44. Tétel. *Ha R egységelemes gyűrű, akkor van bármely véges számosságú X halmaz, amelyre létezik az $R[X]$ polinomgyűrű, és ugyancsak egységelemes. Az $|X|$-nél nagyobb $\mathfrak{n}$ számosság esetében létezik olyan $\mathfrak{n}$ számosságú Y halmaz, amelyre $R[X] \leq$ $\leq R[Y]$.*

Hasonló eredmények igazak végtelen számosság esetében is.

A 7.43. *definícióban megadott tulajdonságok a polinomgyűrűt egyértelműen meghatározzák a következő értelemben: Ha $R \leq R'$, $X' \subseteq R'$, $X' \cap R = \emptyset$, S tetszőleges (kommutatív) gyűrű és minden olyan $\varphi : R \cup X' \to S$ leképezés, amelynek R-re való megszorítása homomorfizmus, egyértelműen kiterjeszthető egy $\psi : R' \to S$ homomorfizmussá, akkor van olyan X halmaz, amelyre létezik az $R[X]$ polinomgyűrű és van olyan $\xi : R[X] \to R'$ izomorfizmus, amely R-en az identitás és X-et bijektíven képezi le X'-re.*

Bizonyítás. Először az egyhatározatlanú polinomokkal foglalkozunk. Ezeket fokszám szerinti rekurzióval definiáljuk. Tulajdonképpen elfogadhatjuk az első kötetben található definíciót is. Az itt közölt definíciónak az az előnye, hogy nincsenek benne végtelen sorozatok.

1. Az R elemei polinomok; a nullelemnek nincs foka, az összes többi elem foka 0.

2. Tegyük fel, hogy valamilyen $n \geq 0$ egész számra definiálva vannak az n-edfokú polinomok. Ekkor $(n+1)$-edfokú polinomoknak nevezzük azokat az (a, f) párokat, amelyekben $a \in R$ és f egy n-edfokú polinom. (Ezek az $a + x \cdot f$ polinomot hivatottak jellemezni.)

Ugyancsak rekurzívan definiáljuk a polinomok összeadását és szorzását:

Az R-beli elemeknek mint polinomoknak az összege legyen ugyanaz, mint az R-beli összeg. Ha $a, b \in R$, akkor legyen $a+(b, f) = (b, f)+a = (a+b, f)$. Legyen továbbá $(a, f)+$ $+(b, g) = (a+b, f+g)$. A fokszám szerinti teljes indukcióval belátható, hogy a polinomok a fenti összeadásra nézve kommutatív csoportot alkotnak. (Ezt és a tétel bizonyításában fellépő hosszas, de triviális teljes indukciós bizonyításokat az olvasóra bízzuk.)

Az R-beli elemekre mint polinomokra ugyanúgy értelmezzük a szorzást, mint ahogy az az R-ben értelmezve van. Ha $a, b \in R$, akkor legyen $a \cdot (b, f) = (b, f) \cdot a = (ab, af)$. Legyen továbbá $(a, f) \cdot (b, g) = (ab, ag+bf+(0, fg))$. Itt is a fokszám szerinti teljes indukcióval mutatható ki, hogy kommutatív félcsoportot nyertünk, és a szorzás az összeadásra nézve disztributív. Ezzel tehát valóban gyűrűt kaptunk. Ez a gyűrű egységelemes, ha 1 az R egységeleme, akkor 1 a kapott gyűrűnek is nyilvánvalóan egységeleme.

Válasszuk most az X halmaz egyetlen elemének az $x = (0, 1)$ elemet. Ugyancsak a fokszám szerinti teljes indukcióval látható be, hogy a kapott gyűrű minden eleme egyértelműen előállítható $a_0+a_1x+\cdots+a_nx^n$ alakban, ahol $n = 0$ és $a_0 = 0$ pontosan akkor teljesül,

ha az elemnek nincs foka. Egyébként feltehető, hogy $a_n \neq 0$; amikor e polinomnak a foka n. Ezzel megkaptuk az $R[x]$ gyűrűt. Világos, hogy ez a definíció lényegében megegyezik azzal a definícióval, amelyet (az első kötetben) a számtestből vett együtthatós polinomokra adtunk. Ennek alapján itt is, minden utalás nélkül, használni fogjuk az ottani elnevezéseket.

Ha mármost egy φ leképezés az R elemein homomorfizmus és az x elemet az S gyűrű s elemébe képezi, akkor az $a_0 + a_1x + \cdots + a_nx^n$ elem képe a 7.43. definícióban jellemzett ψ homomorfizmus esetén csak $\varphi(a_0) + \varphi(a_1)s + \cdots + \varphi(a_n)s^n$ lehet. Az $R[x]$-beli elemek egyértelmű előállíthatóságára tekintettel az így definiált „megfeleltetés" egyértelmű; s a fokszámra vonatkozó teljes indukcióval belátható, hogy homomorfizmus. Ezzel az egyetlen határozatlanra vonatkozó esetet beláttuk.

Több határozatlanra ezek számára vonatkozó teljes indukcióval bizonyítunk. Tegyük fel, hogy n számú határozatlanra igaz az állítás és legyen $X = \{x_0, x_1, \ldots, x_n\}$, az x_0 elhagyásával nyert halmazt pedig jelölje Y. Ekkor az R-en megkezdett homomorfizmust a már bizonyítottak szerint kiterjeszthetjük $R[x_0]$-ra, majd erről a teljes indukciós feltétel alapján $R[x_0][Y]$-ra úgy, hogy a határozatlanok képét tetszőlegesen előírhatjuk.

Végtelen sok határozatlan esetén a következőképpen járhatunk el:

Mint a véges esetben láttuk, létezik olyan $X = \{x_1, \ldots, x_n, \ldots\}$ halmaz, amelyre $R = R_0 \leq R_1 \leq R_n \leq \ldots$, ahol $R_i = R_{i-1}[x_i]$ teljesül ($i \in \mathbb{N}$). Jelölje $R[X]$ az R_i gyűrűk egyesítését. Mivel ez gyűrűk növő láncának az egyesítése, ezért ez gyűrű, amely persze részgyűrűként tartalmazza R-t. Mivel $R[X]$ minden eleme benne van valamelyik R_i-ben és a gyűrű minden művelete véges változós, ezért $R \cup X$ e gyűrű generátorrendszere. Ha mármost $\varphi : R \cup X \to S$ olyan leképezés, amelynek R-re való megszorítása homomorfizmus, akkor lépésről lépésre kiterjeszthető olyan $\varphi_i : R_i \to S$ homomorfizmussá, amelynek R_{i-1}-re való megszorítása φ_{i-1} és x_i képe $\varphi(x_i)$. Definiáljuk a $\psi : R[X] \to S$ megfeleltetést úgy, hogy $\psi(t) = \varphi_i(t)$, ha $t \in R_i$. Mint éppen láttuk, ez nem függ az i indextől; továbbá az R_i-re való megszorítása éppen φ_i. Ebből következik, hogy ψ homomorfizmus, mert $R[X]$ a láncot alkotó R_i-k egyesítése és a gyűrűműveletek véges változósak. ψ egyértelműsége abból következik, hogy minden egyes φ_i egyértelmű. Ha a határozatlanok száma nem megszámlálható, akkor transzfinit indukcióval (illetve transzfinit rekurzióval) nyerhető az eredmény.

Legyen végül $R \leq R'$, $X' \subseteq R'$, $X' \cap R = \emptyset$, olyan tulajdonságú, hogy tetszőleges S (kommutatív) gyűrű és minden olyan $\varphi : R \cup X' \to S$ leképezés esetén, amelynek R-re való megszorítása homomorfizmus, létezik egy egyértelmű $\psi : R' \to S$ homomorfizmus kiterjesztés, amely R-en az identitás. Legyen X olyan halmaz, amelyre létezik $R[X]$ és $|X| = |X'|$. Ez utóbbi egyenlőség alapján létezik egy $\zeta : X \to X'$ bijekció. A polinomgyűrű tulajdonsága szerint van olyan $\xi : R[X] \to R'$ homomorfizmus, amelynek R-re való megszorítása az identitás és az X-re való megszorítása ζ. Az R'-re kirótt feltételek miatt viszont van olyan $\xi' : R' \to R[X]$ homomorfizmus, amelynek R-re való megszorítása az identitás és az X'-re való megszorítása ζ^{-1}. Ebből azonnal következik, hogy $\xi\xi'$, illetve $\xi'\xi$ identikusan hat R-en és X'-n, illetve X-en. Az egyértelmű kiterjeszthetőségi tulajdonság alapján tehát mind $\xi\xi'$, mind $\xi'\xi$ identitás, azaz ξ (és ξ') izomorfizmus. ■

Megjegyezzük, hogy az R feletti polinomgyűrűnek akkor is van értelme, ha R nem egységelemes. Ekkor a polinomok $a_0 + (a_1x + k_1x) + \cdots + (a_nx^n + k_nx^n)$ alakúak, ahol $k_1, \ldots, k_n$ egész számok. Ezek gyűrűt alkotnak, de a fenti előállítás nem egyértelmű. Például,

ha R a páros számok gyűrűje, akkor a $2x$ polinomban az együtthatót R-belinek is és $\mathbb{Z}$-belinek is hihetjük.

7.45. Tétel (Hilbert)**.** *Az R egységelemes kommutatív gyűrű akkor és csak akkor Noether-gyűrű, ha $R[x]$ is az.*

Bizonyítás. Az R minden egyes I ideáljának feleltessük meg az $R[x]$ elemeinek azt az $I[x]$ halmazát, amely csupa I-beli együtthatós polinomból áll. Az I ideáltulajdonsága alapján nyilvánvalóan $I[x]$ is ideál, és $I_1[x] \leq I_2[x]$ pontosan akkor teljesül, ha $I_1 \leq I_2$. Ha mármost $R[x]$ Noether-gyűrű, akkor a tekintett speciális ideálok halmazára is érvényes a maximumfeltétel, ami a fenti rendezéstartó megfeleltetés miatt azt jelenti, hogy a maximumfeltétel R ideáljaira is érvényes.

A tétel lényeges része természetesen a fordított irányú következtetés: Azt fogjuk kimutatni, hogy ha R Noether-gyűrű, akkor az $R[x]$ bármely I ideálja végesen generált.

Kiindulva egy $I \lhd R[x]$ ideálból, minden n természetes számhoz rendeljük hozzá az R elemeinek egy I_n halmazát, amely a 0-n kívül az I beli n-edfokú polinomok főegyütthatóját tartalmazza. Mivel az I ideál zárt az $R[x]$-beli elemekkel – speciálisan R elemeivel és az x-szel – való szorzásra, ezért minden egyes I_n zárt az R-beli elemekkel való szorzásra és $I_n \subseteq I_{n+1}$, bármely n természetes szám esetén. Mivel két I-beli n-edfokú polinom különbsége is I-beli, ezért ha két, I_n-beli elemet veszünk, akkor ezek különbsége vagy I_n-beli, vagy 0. Ez utóbbi esetben a különbség – definíció szerint – I_n-ben van, és így I_n ideálja R-nek. Az R-beli ideálokra vonatkozó maximumfeltétel miatt létezik olyan k természetes szám, hogy bármely i természetes számra $I_{k+i} = I_k$. Ezek az ideálok mind végesen generáltak, s mivel véges sokan vannak, generátoraik száma is egy n korlát alatt marad. A kényelem kedvéért feltesszük, hogy mindegyiküket pontosan n elemmel generáljuk (a generátorelemeket többször is számíthatjuk). Legyen $a_{i1}, \ldots, a_{in}$ az I_i ideál egy generátorrendszere, és legyenek $f_{i1}, \ldots, f_{in}$ olyan I_i-beli polinomok, amelyekre f_{ij} együtthatója éppen a_{ij} (ilyen polinomok a feltétel szerint léteznek). Azt bizonyítjuk be, hogy az f_{ij} $(0 \leq i \leq k,\ 0 \leq j \leq n)$ polinomok az I-nek egy (véges !) generátorrendszerét alkotják.

Tekintsük az f_{ij} polinomok generálta ideált, amely eleve része I-nek. Bebizonyítjuk, hogy ez az ideál I minden f elemét tartalmazza. A bizonyítást f fokára vonatkozó teljes indukcióval végezzük. Ha a polinom a 0, vagy egy 0-adfokú polinom, akkor az állítás azonnal következik a 7.19. tételből. Tegyük fel, hogy minden, d-nél alacsonyabb fokú I-beli polinom benne van a generátumban, és legyen $f \in I$ egy tetszőleges, d-edfokú polinom, amelynek a főegyütthatója a. Feltétel szerint $a \in I_d$, és a 7.19. tétel alapján vannak olyan R-beli $b_1, \ldots, b_n$ elemek, amelyekre $a = b_1 a_{d1} + \cdots + b_n a_{dn}$. Az f_{ij} polinomok választása folytán ekkor a $g = b_1 f_{d1} + \cdots + b_n f_{dn}$ polinom – amely benne van a generátumban – ugyancsak d-edfokú és főegyütthatója a. Így $h = f - g$ az I-nek egy d-nél alacsonyabb fokú polinomja, tehát az indukciós feltétel szerint eleme a generátumnak. Mivel az ideálok az összeadásra zártak, ezért $f = g + h$ is eleme a generátumnak. ■

7.46. Következmény. *Noether-gyűrű fölötti véges sok határozatlanú polinomgyűrű is Noether-gyűrű.* ■

Megjegyzés. Ha a határozatlanok száma nem véges, akkor az analóg állítás már nem igaz. Tekintsük például a racionális test feletti $x_1, \ldots, x_n, \ldots$ határozatlanokban vett polinomgyűrűnek azokat az elemeit, amelyeknek a konstans tagja 0. Ezek nyilvánvalóan ideált alkotnak. Megmutatjuk,

hogy ez az ideál nem lehet végesen generált. Tekintsünk ugyanis véges sok $f_1, \ldots, f_k$ polinomot, és tegyük fel, hogy x_n az első olyan határozatlan (indexét tekintve), amelyik e polinomokban nem lép fel. A polinomok definíciója szerint létezik olyan homomorfizmus, amelyik a racionális testen identikus, az x_n határozatlant az 1-be képezi le s az összes többi határozatlant 0-ba. Mivel ez a homomorfizmus a fenti k darab polinomot is a 0-ba képezi, ezért nyilván az általuk generált ideált is. De a homomorfizmusnál x_n képe nem 0, tehát nem lehet a kérdéses generátumban, noha az adott ideálnak eleme. □

Ebben a megjegyzésben úgy is okoskodhattunk volna, hogy az egyik határozatlan helyébe 1-et helyettesítünk és a többiek helyébe 0-t. Ez is mutatja, hogy milyen szoros kapcsolat van a behelyettesítés és a homomorfizmus között.

Valóban, ha az x_i határozatlan helyébe egy R-nél bővebb S gyűrű ξ_i elemét írjuk, akkor a polinomgyűrű definíciója szerint ez a megfeleltetés egyértelműen kiterjeszthető a polinomgyűrű egy olyan homomorfizmusává, amely az R-en injektív.

Fordítva is hasonló a helyzet: ha van egy ilyen homomorfizmus, akkor ez minden egyes x_i határozatlannak megfeleltet egy S-beli ξ_i elemet, és minden polinomot a megfelelő „helyettesítési érték”-re képez le. Ezek indokolják a most következő definíciót, amely előtt még egy megjegyzést teszünk. Általában testbeli együtthatós polinomokkal foglalkozunk, s a behelyettesítendő értékek is egy testből valók. Mivel testbeli együtthatós polinomgyűrű a 7.46. tétel szerint Noether-gyűrű, ezért fogalmazunk Noether-gyűrűre és testre.

7.47. Definíció. Az R Noether-gyűrűnek a K (kommutatív) testbe való φ homomorfizmusát behelyettesítésnek, s a $\varphi(a)$ elemet az R-beli a elem φ helyen vett helyettesítési értékének nevezzük. Ha $\varphi(a) = 0$, akkor azt mondjuk, hogy φ az a-nak gyöke. □

Felhívjuk a figyelmet arra, hogy csupán az R gyűrű rögzített, K is és φ is változhat. Hiszen a polinomgyűrűk esetében is az együtthatókat tartalmazó tetszőleges bővebb test elemeit behelyettesíthetjük a polinomokba.

Érdemes megjegyezni, hogy a 7.34. következmény alapján a fenti definíció lényegében változatlan marad, ha test helyett integritási tartományt mondunk.

7.5. Egyértelmű felbontás

Mind az egész számok, mind a racionális vagy valós együtthatós polinomok körében alapvető jelentőségű az a tény, hogy minden elemet „lényegében egyértelműen” felbonthatunk tovább már nem bonthatóak szorzatára. Ezzel az I. kötetben már foglalkoztunk. Az alábbiakban ennek a tételnek az érvényességi körét fogjuk megvizsgálni. Mindenekelőtt néhány alapvető fogalmat kell definiálnunk.

7.48. Definíció. Ha az R integritási tartomány a és b elemeihez létezik az integritási tartománynak olyan c eleme, amelyre $a = bc$, akkor azt mondjuk, hogy b osztója a-nak, illetve a többszöröse b-nek. Ezt a relációt $b|a$ jelöli.

Azokat az elemeket, amelyek R minden elemének osztói, egységeknek nevezzük. Ha két elem mindegyike osztója a másiknak, akkor ezek asszociáltak. □

Lényegében triviális és az első kötetben vizsgáltak alapján azonnal látható az alábbi

7.49. Tétel. *Az oszthatóság tranzitív, és pontosan akkor reflexív, ha a gyűrű egységelemes. Egységek csak akkor léteznek, ha a gyűrű egységelemes; ezek éppen az egységelem osztói. Két elem pontosan akkor asszociált, ha bármelyik a másiknak egységszerese. A gyűrű egy eleme pontosan akkor többszöröse minden elemnek, ha ez a nullelem. A nullelemnek minden elem osztója; a nullelem csak önmagának osztója.* ■

7.50. Definíció. Az R integritási tartomány a elemét irreducibilisnek nevezzük, ha a nem egység és $a = bc$ esetén b és c valamelyike egység. A gyűrű egy p eleme prímtulajdonságú, ha $p|ab$ esetén $p|a$ vagy $p|b$ valamelyike fennáll. □

Megjegyzés. A definícióból következik, hogy 0 és az egységek prímtulajdonságúak, de általában nem irreducibilisek. Ha $a \in R$ nem egység, akkor a $0 = 0a$ felbontás miatt a 0 nem irreducibilis; míg az egységek a definíció miatt. Minden más prímtulajdonságú elem irreducibilis. Legyen $p \in R$ ilyen. Mivel $p|pp$, ezért $p|p$, a 7.22. tétel szerint tehát R egységelemes, hiszen $p \neq 0$. Ha mármost $p = ab$, akkor a $p|p$ feltételből $p|a$ vagy $p|b$ következik. Mivel $a|p$ és $b|p$ a felírás szerint igaz, ezért p az a és b valamelyikével asszociált, s ekkor a másikuk csak egység lehet. □

Az alábbiakban az oszthatósági tulajdonságokat átfogalmazzuk az ideálok segítségével:

7.51. Tétel. *Az R egységelemes integritási tartományban $b|a$ pontosan akkor teljesül, ha $(b) \supseteq (a)$. Az a elem pontosan akkor egység, ha $(a) = R$; a és b pontosan akkor asszociáltak, ha $(a) = (b)$. Az a elem pontosan akkor irreducibilis, ha (a) az R-től különböző főideálok részbenrendezett halmazában egy maximális elem. A p elem pontosan akkor prímtulajdonságú, ha (p) prímideál.*

Bizonyítás. Az oszthatóságra vonatkozó feltétel azonnal adódik abból, hogy egységelemes gyűrűkben $(a) = Ra$. Ugyanezért az $(a) = R$ feltétel éppen azt fejezi ki, hogy a-nak minden elem többszöröse. Az első tulajdonságot a másik irányba is alkalmazva, azonnal kapjuk az asszociáltakra vonatkozó feltételt is.

Nézzük most meg, mit jelent az, hogy van egy olyan b elem, amelyre $(a) \subset (b) \subset R$. Az első tartalmazás szerint $a = bc$, de $(a) \neq (b)$ miatt c nem egység. Viszont b sem egység, hiszen $(b) \neq R$. Így a nem irreducibilis. Ha viszont a nem irreducibilis, akkor alkalmas elemekkel $a = bc$ alakban írható, ahol a tényezők egyike sem egység. Ebből viszont azonnal következik, hogy a (b) főideál az (a)-t valódi módon tartalmazza, és az R-től különbözik.

A prímideál definíciója szerint (p) pontosan akkor prímideál, ha $ab \in (p)$ esetén vagy $a \in (p)$, vagy $b \in (p)$. Mivel egy ideál bármely eleme olyan ideált generál, amely az adott ideálban benne van és egy kisebb ideál minden eleme a nagyobbnak is eleme, ezért a fenti feltételt így fogalmazhatjuk: Ha $(ab) \subseteq (p)$, akkor vagy $(a) \subseteq (p)$, vagy $(b) \subseteq (p)$. Az oszthatóság átírása szerint ez viszont pontosan azt jelenti, hogy p prímelem. ■

7.52. Definíció. Azt mondjuk, hogy az R integritási tartományban érvényes az egyértelmű faktorizáció, ha R minden, 0-tól és egységtől különböző eleme lényegében egyértelműen bontható fel irreducibilis elemek szorzatára, vagyis, ha bármely két

$$a_1 \cdot a_2 \cdot \ldots \cdot a_n = b_1 \cdot b_2 \cdot \ldots \cdot b_k$$

felbontás esetén létezik olyan $\varphi : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, k\}$ bijekció, hogy a_i és $b_{\varphi(i)}$ asszociáltak $(1 \leq i \leq n)$. □

A feltételből következik, hogy ha van irreducibilis elem, akkor R egységelemes. Ez úgy látható be, hogy erre az elemre az egyértényezős faktorizációt kétszer vesszük. Ha irreducibilis elem nincs, akkor R test, tehát ugyancsak egységelemes.

7.53. Tétel. *Egy R integritási tartományban akkor és csak akkor érvényes az egyértelmű faktorizáció, ha egységelemes, R főideáljaira teljesül a maximumfeltétel és minden R-től különböző maximális főideálja prímideál (azaz minden irreducibilis eleme prím).*

Bizonyítás. Tegyük fel először, hogy R-ben érvényes az egyértelmű faktorizáció. A feltétel szerint $1 \in R$ és minden, egységtől különböző R-beli a elemhez hozzárendelhetünk egy egyértelmű $t(a)$ számot, amely az a felbontásában szereplő irreducibilis faktorok száma. Ugyancsak az egyértelműség alapján kapjuk, hogy $t(ab) = t(a) + t(b)$. Mivel R egységelemes, ez a függvény kiterjeszthető a főideálokra úgy, hogy nagyobb főideálhoz kisebb függvényérték tartozzék. Ha az R-hez 0-t rendelünk, akkor minden 0-tól különböző főideálhoz rendeltünk már egy természetes számot: nagyobbhoz kisebbet. Mármost főideálok bármely adott halmazát tekintjük is, ezek között van olyan, amelyhez minimális szám tartozik (kivéve ha csak a nullideált vettük, amikor ez a maximális), s ez a főideál nyilván maximális (ha csak egy ideált tekintettünk, akkor az állítás triviális).

Legyen továbbá r tetszőleges irreducibilis elem, és legyen $r|ab$. Ez azt jelenti, hogy alkalmas s elemmel $rs = ab$. Az s-nek, a-nak és b-nek egy-egy irreducibilis felbontását véve:

$$rs_1 \dots s_t = a_1 \dots a_i b_1 \dots b_j .$$

Mivel mindkét oldalon csak irreducibilis tényezők szerepelnek, ezért alkalmazhatjuk a felbontás egyértelműségére vonatkozó feltételt. Eszerint a jobb oldalon van olyan tényező, amely r-rel asszociált, és így r valóban osztója a és b valamelyikének.

Most azt kell belátnunk, hogy az ideálokra vonatkozó feltételből következik az egyértelmű felbontás.

Ha R test, az állítás triviális, így feltehető, hogy létezik R-től különböző főideál. Egyébként a lefelé menő indukció formáját alkalmazzuk a maximumfeltételnek (3.3. tétel). Tekintsük azokat az R-től különböző főideálokat, amelyeknek a generátorelemeit fel lehet bontani irreducibilis faktorokra. Ha (a) maximális a főideálok között, akkor a irreducibilis. Ha az (a)-t valódi módon tartalmazó főideálok ilyenek és a nem irreducibilis, akkor $a = bc$, ahol (b) és (c) mindegyike valódi módon tartalmazza (a)-t, tehát mindegyikük felbontható irreducibilis elemek szorzatára, ami egyszersmind a-nak is ilyen felbontását adja. A lefelé menő indukció alapján R minden eleme felbontható irreducibilis elemek szorzatára.

Az egyértelműséget is a lefelé menő indukcióval bizonyítjuk. Ha (a) maximális a főideálok között, akkor irreducibilis, és így $a = a$ az egyetlen felbontása. Ha (a) nem maximális, akkor legyen

$$a = p_1 \dots p_r = q_1 \dots q_s$$

az a elemnek irreducibilis elemek szorzatára való két felbontása. A feltétel szerint az irreducibilis p_1 egyszersmind prímtulajdonságú és így osztója a jobb oldal valamelyik tényezőjének (a prímtulajdonság egy triviális indukciós eljárással átvihető többtényezős szorzatra is). Mivel az indexeknek valamilyen bijekcióját kell megadnunk, ezért feltehető, hogy p_1 a q_1-nek osztója. Ugyancsak az irreducibilitásból következik, hogy ekkor ezeknek asszociáltaknak kell lenniük. p_1-gyel osztva az a egy valódi osztójának két felbontásához jutunk, amire az indukciós feltevés szerint már igaz az egyértelműség és ebből következik a-ra is. ■

7.54. Következmény. *Egységelemes, nullosztómentes Noether-gyűrűben pontosan akkor érvényes az egyértelmű faktorizáció, ha minden irreducibilis eleme prímtulajdonságú.*

Bizonyítás. Mivel az összes ideálra teljesül a maximumfeltétel, ezért teljesül a főideálokra is. ■

7.55. Definíció. Egy integritási tartományt főideálgyűrűnek nevezünk, ha minden ideálja főideál. □

7.56. Tétel. *Ha az R integritási tartomány minden ideálja Ra alakú, akkor R egységelemes főideálgyűrű. Egységelemes főideálgyűrűben érvényes az egyértelmű faktorizáció.*

Bizonyítás. Feltétel szerint $R = Ra$, amiből a 7.22. tétel alapján következik, hogy R egységelemes. Ezért $Ra = (a)$ főideál, így R főideálgyűrű. Mivel minden ideál egy elemmel generált, ezért a gyűrű Noether-gyűrű. Így alkalmazható a 7.54. következmény, amely szerint azt kell még belátni, hogy minden irreducibilis elem prímtulajdonságú.

Tegyük fel, hogy a p irreducibilis elem osztója az ab szorzatnak. Ha $p|a$, akkor az állítás bizonyított. Ha nem, akkor tekintsük a (p, a) ideált, amely feltétel szerint egy (d) főideál. Ez azt jelenti, hogy $d|p$ és $d|a$. Mivel p irreducibilis, ezért d vagy egység, vagy p-nek asszociáltja. Ez utóbbi lehetetlen, mert ekkor $p|a$ volna. Így $(d) = R$, ami azt jelenti, hogy alkalmas $u, v \in R$ elemekkel $1 = up + va$. Ezt az egyenlőséget b-vel szorozva a $b = (bu)p + v(ab)$ összefüggéshez jutunk. Az eredeti oszthatósági feltétel szerint az ab szorzat pq alakú, amiből $b = (bu + vq)p$ következik; tehát $p \mid b$. ■

Most az egységelemes főideálgyűrűk egy fontos speciális esetét, az euklideszi gyűrűket fogjuk tárgyalni.

7.57. Definíció. Egy R integritási tartományt euklideszi gyűrűnek nevezünk, ha létezik olyan φ leképezése a természetes számokra, amely egyedül a 0-t képezi 0-ra és bármely R-beli $b \neq 0$ és a elemekhez létezik az R-nek olyan q és r eleme, hogy

$$\varphi(r) < \varphi(b) \qquad \text{és} \qquad a = bq + r.$$ □

Euklideszi gyűrűkkel már találkoztunk az I. kötetben első részében (Harmadik fejezet 10. pont); ott azt mondtuk, hogy a tétel a polinomok esetéhez hasonlóan bizonyítható. Itt a bizonyítás „nehéz” része már megtörtént, csak azt kell megmutatni, hogy az előző eredmény alkalmazható.

7.58. Tétel. *Euklideszi gyűrűben minden ideál Ra alakú, így érvényes benne az egyértelmű faktorizáció.*

Bizonyítás. Legyen I az R euklideszi gyűrű tetszőleges ideálja. Ha I egyedül a nullelemet tartalmazza, akkor triviálisan Ra alakú. Egyébként tekintsük az I-nek egy olyan $d \neq 0$ elemét, amelyre $\varphi(d)$ minimális. Nyilván $(d) \subseteq I$. Legyen $a \in I$; ekkor a feltétel szerint léteznek olyan R-beli q és r elemek, hogy $a = qd + r$ és vagy $\varphi(r) < \varphi(d)$, vagy $r = 0$. Az ideáltulajdonságok szerint $r = a - qd \in I$; és a d választása miatt csak $r = 0$ lehetséges. Így $a \in (d)$, azaz $I = Rd$. ■

Jól ismert, hogy az egész számok euklideszi gyűrűt alkotnak a $\varphi(a) = |a|$ függvénnyel. Az I. kötetben láttuk, hogy egy számtestbeli együtthatós (egyhatározatlanú) polinomok is euklideszi gyűrűt alkotnak. Ez tetszőleges testbeli együtthatós (egyhatározatlanú) polinomokra is belátható, hozzárendelve például minden $f \neq 0$ polinomhoz a $\mathrm{gr}(f) + 1$ számot (0-hoz 0-t).

A többhatározatlanú polinomokra vonatkozó eredmények is hasonlóak az I. kötetben látottakhoz. Itt is a primitív polinomok játszanak fontos szerepet, de itt nem tehetjük fel, hogy a főegyüttható pozitív. Ennek megfelelően a felbontásban az egységfaktoroktól „el kell tekinteni".

7.59. Definíció. Az R egységelemes, nullosztómentes Noether-gyűrű feletti f polinomot primitívnek nevezzük, ha f együtthatóinak nincs egységtől különböző közös osztója. □

7.60. Tétel. *Legyen K az R egységelemes, nullosztómentes Noether-gyűrű hányadosteste. Ha R-ben érvényes az egyértelmű faktorizáció, akkor minden $f \in K[x]$ polinom (egységfaktortól eltekintve) egyértelműen felírható $f = cg$ alakban, ahol $c \in K$ és $g \in R[x]$ primitív. f pontosan akkor eleme $R[x]$-nek, ha $c \in R$ és pontosan akkor primitív, ha c egység.*

Bizonyítás. Legyen $f = a_0 + \cdots + a_r x^r$. Mivel a hányadostest a_i elemeit alkalmas R-beli elemmel szorozva R-beli elemeket kapunk, ezért ezek $b(\neq 0)$ szorzatával szorozva az f polinomot $bf = b_0 + \cdots + b_r x^r$ adódik, ahol a jobb oldalon levő együtthatók mind R-beliek. Ezeknek az együtthatóknak a faktorizációját figyelembe véve, s a közös tényezőket kiemelve kapjuk, hogy létezik olyan a, amelyre $b_i = ac_i$ $(0 \leq i \leq r)$, és a c_i elemeknek nincs egységtől különböző közös tényezőjük. Így $bf = ag$ $(g = c_0 + \cdots + c_r x^r)$ egy kívánt felbontás, ahol $c = ab^{-1}$. Tegyük most fel, hogy $f = dh$ $(h = u_0 + \cdots + u_r x^r)$ hasonló felbontás, és legyen $d = uv^{-1}$ $(u, v \in R)$. Ez azt jelenti, hogy $avc_i = ubu_i$ $(0 \leq i \leq r)$. Mivel az av szorzat osztója a bal oldalon álló elemeknek, ezért osztója a jobb oldalon álló elemeknek is. Tekintettel arra, hogy az u_i-knek nincs egységtől különböző közös tényezőjük, ezért av osztója ub-nek. Így e két elem csak egységfaktorban különbözhet egymástól; s az a alkalmas megváltoztatásával elérhető, hogy $av = ub$ legyen, ami biztosítja az egyértelműséget. A tétel további állításai ebből triviálisan következnek. ■

7.61. Tétel. *Legyen R egységelemes, nullosztómentes Noether-gyűrű, amelyben érvényes az egyértelmű faktorizáció. Ha az R egy irreducibilis p eleme osztója az $R[x]$-beli f és g elemek szorzatának, akkor p osztója f és g valamelyikének.*

Bizonyítás. Legyen $f = a_0 + \cdots + a_r x^r$ és $g = b_0 + \cdots + b_s x^s$. Ezek $h = fg = c_0 + \cdots$ szorzatát a feltétel szerint osztja a p, ami azt jelenti, hogy p osztója a c_i együtthatók mindegyikének. A $c_0 = a_0 b_0$ feltételből – az egyértelmű faktorizációt felhasználva – következik, hogy az irreducibilis p elem osztója a két tényező valamelyikének, pl. a_0-nak. Ha p minden egyes a_i-nek osztója, akkor a tétel igaz. Ha nem, akkor van egy első indexű az f együtthatói között, amelyik nem osztható p-vel. Legyenek $a_0, \ldots, a_{i-1}$ oszthatók p-vel, de a_i nem. Bebizonyítjuk, hogy ekkor a g minden együtthatója osztható p-vel. A bizonyítás induktíven történik. Tegyük fel, hogy a $b_0, \ldots, b_{j-1}$ együtthatók oszthatók p-vel;

megmutatjuk, hogy b_j is osztható p-vel. Itt a $j = 0$ esetet is megengedjük. Tekintsük h-ban az $(i + j)$-edfokú tag együtthatóját:

$$c_{i+j} = a_0 b_{i+j} + \cdots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \cdots + a_{j+i} b_0.$$

A bal oldal feltétel szerint osztható p-vel. A jobb oldal első i tagjában az első tényező, az utolsó j tagjában a második tényező osztható p-vel, amiből azonnal következik, hogy a fennmaradó $a_i b_j$ tag is p-vel osztható. Mivel az irreducibilis p prímtulajdonságú, ezért p osztója a két tényező valamelyikének, amely feltételünk szerint csak b_j lehet. Így g minden együtthatója, tehát maga g is osztható p-vel. ■

7.62. Tétel. *Ha R egységelemes, nullosztómentes Noether-gyűrű, amelyben érvényes az egyértelmű faktorizáció, akkor $R[x]$ is egységelemes, nullosztómentes Noether-gyűrű, amelyben érvényes az egyértelmű faktorizáció.*

Bizonyítás. A 7.44. és 7.45. tételek alapján $R[x]$ egységelemes Noether-gyűrű. Nullosztómentessége közvetlenül adódik abból, hogy a szorzat főegyütthatója megegyezik a főegyütthatók szorzatával. A 7.54. következményt figyelembe véve azt kell kimutatni, hogy $R[x]$ minden irreducibilis eleme prímtulajdonságú. Ha az irreducibilis elem R-beli, akkor ez pontosan a 7.61. tétel szerint igaz. Ha nem R-beli, akkor a 7.60. tétel alapján ez az elem egy p primitív polinom.

Legyen K az R hányadosteste. Belátjuk, hogy ekkor p a $K[x]$-ben is irreducibilis. Ha $p = fg$, akkor a 7.60. tétel alapján $f = au$, $g = bv$ alakú, ahol $a, b \in K$ és u, v primitív polinomok. A 7.61. tételből triviálisan adódik, hogy esetünkben két primitív polinom szorzata is primitív. Így $p = (ab)(uv)$ egy, a 7.60. tételben adott típusú felbontás. Ugyancsak a 7.60. tételből következik, hogy az ab szorzat R-beli egység, és pl. v helyett a $w = (ab)v$ polinomot tekintve, a $p = uw$ felbontáshoz jutunk. Mivel p $R[x]$-ben irreducibilis, ezért u és w valamelyike konstans; vagyis p valóban irreducibilis $K[x]$-ben.

Tegyük most fel, hogy p osztója az fg szorzatnak. Az oszthatósági kapcsolat természetesen $K[x]$-ben is teljesül, ahol p irreducibilitása alapján már következtethetünk arra, hogy p osztója a két tényező valamelyikének – pl. f-nek –, hiszen test feletti polinomgyűrű euklideszi gyűrű, tehát érvényes benne az egyértelmű faktorizáció. Eszerint létezik egy $f = ph$ felbontás, ahol h természetesen K-beli együtthatós polinom. Ismét a 7.60. tételt használva azt kapjuk, hogy $h = ck$ alakú, ahol c R-beli, és k primitív. Mivel két primitív polinom szorzata primitív, ezért a 7.60. tétel alapján $c \in R$, ami azt jelenti, hogy $h \in R[x]$, vagyis p az $R[x]$-ben is prímtulajdonságú. ■

7.63. Következmény. *Ha egy egységelemes, nullosztómentes Noether-gyűrűben érvényes az egyértelmű faktorizáció, akkor a felette vett akárhány határozatlanú polinomgyűrűben is érvényes.*

Bizonyítás. Véges sok határozatlan esetén az állítás triviális indukcióval következik a 7.62. tételből. Ha a határozatlanok száma végtelen, akkor abból következik az állítás, hogy egy polinomot akárhogyan bontsunk is fel polinomok szorzatára, a tényezőkben csak azok a határozatlanok szerepelhetnek, amelyek az eredeti polinomban (ez következik abból, hogy a szorzat foka minden egyes határozatlanban megegyezik a tényezők fokának összegével). Így bármilyen polinomot tekintünk is, alkalmazhatjuk a véges sok határozatlan esetét. ■

Megjegyezzük, hogy a primitív polinomokra vonatkozó tételekben nem használtuk ki, hogy Noether-gyűrű feletti polinomokról van szó. A változtatás mindossze annyi volna, hogy a 7.62. bizonyításának az első mondatát el kell hagyni.

Könnyen belátható, hogy az egyértelmű faktorizáció az $a+b\varepsilon$ alakú számok körében is érvényes, ahol ε primitív harmadik vagy negyedik egységgyök és a, b racionális egészek. (Mindkét gyűrű euklideszi; φ minden számhoz rendelje hozzá az abszolút érték négyzetét.)

Nem érvényes viszont az egyértelmű felbontás a páros számok körében (nincs egységelem!) vagy az $a+b\sqrt{-3}$ alakú számok körében (a, b racionális egészek). Ez utóbbinak az az oka, hogy a hányadostestből nem vettünk be minden elemet, amit „kellett volna"; például a harmadik egységgyököket. Elvileg más okból nem érvényes az egyértelmű faktorizáció az $a + b\sqrt{-5}$ alakú számok körében (a, b racionális egészek). Belátható, hogy $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, és e tényezők mindegyike irreducibilis: Minden oszthatósági feltételből következtethetünk a konjugáltakra vonatkozó oszthatósági feltételre; és így arra, hogy a megfelelő abszolút értékek négyzeteire is fennáll egy oszthatósági feltétel – de ez már az egész számok körében. Így a fenti négy szám bármelyikének csak olyan $a + b\sqrt{-5}$ alakú osztója lehet, amelyre a^2+5b^2 osztója 4, 6 és 9 valamelyikének. Tekintettel arra, hogy csak valódi osztó jöhet számításba, ezért csak $a^2 + 5b^2 \in \{2, 3\}$ adna valódi osztót. Ilyen a és b pedig triviálisan nem található a racionális egész számok körében.

Feladatok

1. Igaz-e az, hogy Noether-gyűrű részgyűrűje is Noether-gyűrű?

2. Legyen $D \neq 1$ négyzetmentes egész, $D = 4k+1$ alakú és $\xi = \sqrt{D}$. Mutassuk meg, hogy az $\{a+b\xi | a, b \in \mathbb{Z}\}$ alakú számok egy $R = \mathbb{Z}[\xi]$ gyűrűt alkotnak a számokkal végzett műveletekre. Bizonyítsuk be, hogy R Noether-, de nem euklideszi gyűrű. Bizonyítsuk be, hogy a $D = -3, -7, -11$ esetben az R hányadosgyűrűjében levő $a + b\dfrac{1+\xi}{2}$ alakú számok euklideszi gyűrűt alkotnak.

3. Legyen $f(x) \in \mathbb{Z}[x]$ normált irreducibilis polinom és α az $f(x)$ gyöke. Bizonyítsuk be, hogy a $\left\{\sum a_i \alpha^i | a_i \in \mathbb{Z}\right\}$ alakú véges összegek Noether-gyűrűt alkotnak a számokkal végzett műveletekre.

4. Mutassuk meg, hogy $\mathbb{Q}$ minden egységelemes részgyűrűjében igaz az egyértelmű faktorizáció.

5. Adjunk példát olyan euklideszi gyűrűre, amelyben pontosan $n(> 0)$ irreducibilis elem van.

6. Bizonyítsuk be, hogy a K test feletti $K[x]$ gyűrű $a_0 + a_2x^2 + \cdots + a_nx^n$ alakú polinomjainak gyűrűjében nem igaz az egyértelmű faktorizáció.

7. Bizonyítsuk be, hogy ha az R integritási tartományban igaz az egyértelmű faktorizáció, akkor minden nemtriviális prímideálja tartalmaz prímtulajdonságú elemet.

8. Bizonyítsuk be, hogy $\mathbb{Q}[x, y]$-ban azok a polinomok, amelyekben nincs elsőfokú tag, egy olyan R gyűrűt alkotnak, amelyben nem igaz az egyértelmű faktorizáció. Mutassuk meg, hogy R-ben (x^2, xy) prímideál, de nincs benne prímtulajdonságú elem.

9. Legyen P az R Noether-gyűrű prímideálja. Bizonyítsuk be, hogy az $R//P$ lokális gyűrű is Noether-gyűrű. Adjunk meg olyan lokális gyűrűt, amelyben az ideálok nem mind összehasonlíthatók.

10. Bizonyítsuk be, hogy egy (kommutatív) R gyűrű akkor és csak akkor Noether-gyűrű, ha minden valódi faktorgyűrűje is az.

11. Bizonyítsuk be, hogy egy egységelemes kommutatív gyűrű minden valódi ideálja benne van egy valódi prímideálban. Miért „egyszerűbb" a bizonyítás Noether-gyűrűk esetén? Mutassuk meg, hogy nem egységelemes gyűrűkre az állítás nem feltétlenül igaz.

12. Bizonyítsuk be, hogy ha egy egységelemes Noether-gyűrű egy főideálja valódi módon tartalmaz egy prímideált, akkor vagy a prímideál a nullideál, vagy a főideál az egész gyűrű.

13. Bizonyítsuk be, hogy a $\mathbb{Q}[x_1, \ldots, x_n]$ polinomgyűrűben vannak olyan $P_1, \ldots, P_n$ prímideálok, amelyekre $P_1 \subset \ldots \subset P_n$.

14. Bizonyítsuk be, hogy ha egy R integritási tartományban van 0-tól különböző prímtulajdonságú elem, akkor R egységelemes.

15. Tegyük fel, hogy az R integritási tartomány p prímtulajdonságú eleme osztója a $q(\neq p)$ prímtulajdonságú elemnek. Bizonyítsuk be, hogy ha $q \neq 0$, akkor p egység.

16. Adjunk meg $\mathbb{Q}[x, y]$-ban két irreducibilis (tehát prímtulajdonságú) elemet úgy, hogy az általuk generált ideál ne legyen prímideál.

17. Legyen P az R integritási tartomány egy prímideálja és $\varphi : R \to R'$ szürjektív homomorfizmus. Bizonyítsuk be, hogy ha $\operatorname{Ker} \varphi \leq P$, akkor P-nek a φ-nél vett képe ugyancsak prímideál. Mutassunk példát arra, hogy $\operatorname{Ker} \varphi \not\leq P$ esetén ez a kép nem feltétlenül prímideál, még akkor sem, ha $\operatorname{Ker} \varphi$ az.

18. A) Legyen R egységelemes integritási tartomány, és x határozatlan az R felett. Bizonyítsuk be az alábbiakat:

(i) Ha P prímideál $R[x]$-ben, akkor $P \cap R$ prímideál R-ben.

(ii) Ha Q prímideál R-ben, akkor a P-beli polinomok $Q[x]$ halmaza prímideál $R[x]$-ben.

(iii) Ha $Q = R \cap P$, akkor $Q[x] \subseteq P$; s ha $Q[x] \neq P$, akkor van olyan minimális fokú $f(x) \in R[x]$, amelyre $f(x) \in P$, $f(x) \notin Q[x]$ és a $Q[x]$ és $f(x)$ generálta ideál megegyezik P-vel.

B) Legyen K test, $x_1, \ldots, x_n$ határozatlanok K felett, és legyen $R_0 = K$, továbbá minden szóba jövő i-re $R_i = R_{i-1}[x_i]$. Legyen P az R_n egy prímideálja és legyen $P_i = R_i \cap P$. Bizonyítsuk be az alábbiakat:

(i) Tetszőleges i indexre vagy $P_i = P_{i-1}[x_i]$, vagy van olyan R_{i-1} felett irreducibilis $f_i \in P_i \setminus P_{i-1}[x_i]$ hogy a $P_{i-1}[x]$ és f_i generálta ideál megegyezik P_i-vel.

(ii) R_n minden prímideálja generálható legfeljebb n elemmel.

(iii) R_n-ben a prímideálokra teljesül a minimumfeltétel; sőt, mi több, az R_n-beli valódi prímideálok minden tartalmazásra vett láncának legfeljebb n különböző eleme van.

(iv) Ha R_n egy prímideáljában nincs olyan polinom, amelyben n-nél kevesebb határozatlan szerepel, akkor ez a prímideál főideál.

19. Tegyük fel, hogy az R egységelemes integritási tartományban minden végesen generált ideál főideál (ilyen például az algebrai egészek gyűrűje). Bizonyítsuk be, hogy ekkor bármely elem két felbontásának van „közös finomítása”: ha $a_1 \cdot \ldots \cdot a_n = b_1 \cdot \ldots \cdot b_k$, akkor vannak olyan $c_{i,j} \in R$ elemek ($1 \leq i \leq n$, $1 \leq j \leq k$), amelyekre $a_i = \prod_j c_{i,j}$ és $b_j = \prod_i c_{i,j}$.

20. Legyen R az $a_{r_1}x^{r_1} + \cdot + c_{r_n}x^{r_n}$ ($a_r \in \mathbb{Q}$, $r_i \in \mathbb{Q}$) alakú „polinomok” halmaza a természetesen adódó összeadásra és szorzásra. (Részletek találhatók a csoportalgebrák tárgyalásánál.) Bizonyítsuk be, hogy R-ben minden végesen generált ideál főideál, de nem főideálgyűrű.

7.6. Karakterisztika és prímtest, egyszerű testbővítés

A továbbiakban két olyan fontos esetről lesz szó, amelyekben egy test adott részgyűrűjét tartalmazó legkisebb testet vizsgálunk. Ilyen test létezését könnyen beláthatjuk a 3.31. tétel segítségével, bár a tétel nem alkalmazható minden további nélkül, mert a résztest tulajdonságához az is hozzátartozik, hogy minden, 0-tól különböző elemmel együtt annak az inverzét is tartalmazza. Ez azt jelenti, hogy az invertálás nem művelet (csak ún. parciális művelet). Ezen könnyen segíthetünk azonban, ha olyan műveletet vezetünk be, amely 0-hoz önmagát és minden más elemhez az inverzét rendeli hozzá. Ezzel természetesen elvesznek az inverzelem „ismert” tulajdonságai (pl. az $aa^{-1} = 1$ összefüggés), de az adott test részalgebrái éppen a résztestek lesznek, amiből – a 3.31. tétel figyelembevételével – következik az említett test létezése. Az alábbi tétel lehetőséget ad e két test közös elven történő vizsgálatára.

7.64. Tétel. *Legyen φ az R főideálgyűrűnek a K testbe való homomorfizmusa és L az $\mathrm{Im}(\varphi)$-t tartalmazó legkisebb test. Ekkor a következő esetek lehetségesek:*

(1) *Ha $\mathrm{Ker}(\varphi) = 0$, akkor L az $\mathrm{Im}(\varphi)$ hányadosteste.*

(2) *Ha $\mathrm{Ker}(\varphi) = R$, akkor L a K-ban levő legkisebb test, amit K prímtestének nevezünk.*

(3) *Minden más esetben $L = \mathrm{Im}(\varphi)$.*

Bizonyítás. Ha $\mathrm{Im}(\varphi)$ legalább kételemű, akkor integritási tartomány, hiszen K-ban nincsenek nullosztók. Így az $\mathrm{Im}(\varphi)$-t tartalmazó legkisebb test a 7.33. következmény szerint mindenképpen az $\mathrm{Im}(\varphi)$ hányadosteste. Ha $\mathrm{Im}(\varphi)$ egyetlen elemből áll, akkor nyilvánvaló, hogy L a K-ban levő legkisebb test. Azt kell csupán még bizonyítani, hogy ha $\mathrm{Ker}(\varphi)$ nem triviális ideál, akkor $\mathrm{Im}(\varphi)$ test. Mivel K nullosztómentes, ezért $\mathrm{Im}(\varphi)$ integritási tartomány. A 7.36. tétel szerint tehát $\mathrm{Ker}(\varphi)$ prímideál. Mivel R főideálgyűrű, ezért $\mathrm{Ker}(\varphi) = (p)$, alkalmas p elemmel, amely a 7.51. tétel szerint prímtulajdonságú. A 7.50. definíciót követő

megjegyzés alapján p irreducibilis, hiszen ha egység vagy 0 volna, akkor az általa generált ideál triviális volna. Ismét a 7.51. tételt figyelembe véve kapjuk, hogy (p) maximális a nemtriviális főideálok között. Tekintettel arra, hogy R-ben minden ideál főideál, ezért (p) maximális ideál. A 7.26. tétel szerint tehát $\mathrm{Im}(\varphi)$ egyszerű gyűrű, s a kommutativitás miatt nincs benne balideál sem. Figyelembe véve a 7.23. tételt, azt kapjuk, hogy $\mathrm{Im}(\varphi)$ vagy test, vagy zérógyűrű; de ez utóbbi a nullosztómentesség miatt lehetetlen. ■

A 7.64. tétel alkalmazásaként először a prímtesteket vizsgáljuk meg. Ehhez szükségünk van a nullosztómentes gyűrűk additív csoportjának leírására:

7.65. Tétel. *Ha az R gyűrű nullosztómentes, akkor R^+-ban a 0-tól különböző elemek rendje megegyezik.*

Ez a közös rend vagy végtelen, vagy egy p prímszám. Előző esetben a gyűrűt nullkarakterisztikájúnak, az utóbbiban p karakterisztikájúnak nevezzük.

Az egész számok $\mathbb{Z}$ gyűrűje is és a racionális számok $\mathbb{Q}$ teste is nullkarakterisztikájú. Az egész számoknak modulo p vett maradékosztály-gyűrűje egy p elemű $\mathbb{Q}_p$ test, amely p karakterisztikájú.

Bizonyítás. Ha az n természetes számra és az $a \neq 0$ elemre $na = 0$, akkor tetszőleges R-beli b esetén a nullosztómentesség alapján az $a(nb) = (na)b = 0$ összefüggésből $nb = 0$ következik, így b rendje nem lehet nagyobb az a rendjénél. Ha b sem 0, akkor hasonlóképpen kapjuk, hogy a rendje sem nagyobb b rendjénél, tehát a 0-tól különböző elemek rendje megegyezik.

Ha az n természetes számot km alakba írjuk, akkor $n(ab) = 0$ esetén $(ka)(mb) = 0$ miatt kapjuk, hogy a két tényező valamelyike 0. Az előbbiek szerint ez csak úgy lehet, ha n vagy k-nak, vagy m-nek osztója – tehát n prímszám.

A $\mathbb{Z}$ és a $\mathbb{Q}_0$ gyűrűkre vonatkozó állítás triviális. $\mathbb{Q}_p$ a 7.51. tétel alapján egy prímideál szerinti maradékosztály-gyűrű, amely az egyértelmű faktorizáció miatt maximális ideál; így a faktorgyűrű test (zérógyűrű nem lehet, mert prímideál szerinti faktor). E test egységelemének a rendje nyilván p, így a gyűrű valóban p karakterisztikájú. ■

Megjegyezzük, hogy a $\mathbb{Q}_p$ testre általánosan használt a $\mathbb{Z}_p$, a $GF(p)$ vagy a $\mathbb{Z}/p\mathbb{Z}$ jelölés. Mi azért használjuk a fenti jelölést, hogy kihangsúlyozzuk: lényegében a $\mathbb{Q}$-val „egyenrangú” testről van szó.

7.66. Tétel. *Ha a K (kommutatív) test p karakterisztikájú ($p = 0$ vagy prímszám), akkor P prímteste izomorf $\mathbb{Q}_p$-vel.*

Bizonyítás. Legyen $\varphi : \mathbb{Z} \to K$ az a megfeleltetés, amely az n egész számhoz a K test e egységelemének az n-szeresét rendeli hozzá. Ez a megfeleltetés a 7.8. tétel alapján homomorfizmus, amelynek a magja – definíció szerint – nem lehet az egész gyűrű.

Mivel a K test P prímteste tartalmazza a K egységelemét, ezért P éppen az $\mathrm{Im}(\varphi)$-t tartalmazó legkisebb test. Így alkalmazhatjuk a 7.64. tételt. A $\mathrm{Ker}(\varphi)$ azokból az n egész számokból áll, amelyekre $ne = 0$, azaz $\mathrm{Ker}(\varphi) = (p)$, ahol p éppen a K karakterisztikája. Ha $p = 0$, akkor az első eset áll fenn és így P izomorf $\mathbb{Z}$ hányadostestével, vagyis $\mathbb{Q}_0$-lal. Egyébként a harmadik eset lép fel, ami P-nek $\mathbb{Q}_p$-vel való izomorfizmusát adja. ■

A másik fontos eset, amire a 7.64. tételt alkalmazhatjuk, az úgynevezett egyszerű testbővítés esete. (Megjegyezzük, hogy itt nem a struktúra egyszerűségéről van szó, mint a csoportok és gyűrűk esetében, hanem a bővítési eljárás minimális voltáról.)

7.67. Definíció. Az L test az M testnek bővítése, ha $M \leq L$. Ha L a legszűkebb olyan test, amely az M-en kívül egy H elemrendszert is tartalmaz, akkor azt mondjuk, hogy $L = M(H)$ az M-nek H-val való bővítése. Azt, hogy L az M-nek bővítése, $L|M$ is fogja jelölni. Ebben az esetben M-re mint alaptestre utalunk. Ha H egyetlen a elemből áll, akkor egyszerű testbővítésről beszélünk. Ha van olyan M-beli együtthatós, nemnulla polinom, amelynek az a elem gyöke, akkor a az M felett algebrai elem, egyébként a az M felett transzcendens. □

7.68. Tétel. *Egy adott M testnek mindig létezik egyszerű transzcendens bővítése. Az $M(a)$ és $M(b)$ egyszerű transzcendens bővítések között létezik az a elemet b-be vivő és M elemeit fixen hagyó izomorfizmus.*

Az M felett algebrai a elemhez létezik egy egyértelműen meghatározott M-beli együtthatós minimális fokú normált polinom, amely irreducibilis és amelynek az a elem gyöke. (Ezt az a elem főpolinomjának nevezzük.) Bármely M-beli együtthatós, M felett irreducibilis f polinomhoz létezik olyan egyszerű $M(a)$ bővítés, hogy a az f-nek gyöke. Ha $M(b)$ is ilyen bővítés, akkor létezik olyan $\varphi : M(a) \to M(b)$ izomorfizmus, amely az a elemet b-be viszi és az M elemeit fixen hagyja. Az a fokán az f fokát értjük.

Bizonyítás. : Legyen $M \subseteq M(a) = L \subseteq K$. A polinomgyűrű definíciója alapján létezik olyan $\varphi : M[x] \to K$ homomorfizmus, amely az M elemeit fixen hagyja és az x elemet a-ba viszi. $\mathrm{Im}(\varphi) \supseteq M$ miatt itt is csak a 7.64. tétel (1) és (3) esete fordulhat elő. Az első esetben a transzcendens, és $M(a)$ izomorf az $M[x]$ hányadostestével. Ez az izomorfizmus x-et a-ba viszi és M elemeit fixen tartja. Ezzel bizonyítottuk is az egyszerű transzcendens bővítések izomorfizmusára vonatkozó állítást, hiszen az M-et fixen hagyó izomorfizmusok szorzata és inverze is ilyen. Az egyszerű transzcendens bővítés egzisztenciája is nyilvánvaló: Ha van ilyen bővítés, az izomorf az $M[x]$ hányadostestével; és ez a hányadostest triviálisan megfelel a követelményeknek (ez test, és a $\varphi : M[x] \to$ *hányadostest* beágyazás eleget tesz a követelményeknek).

Ha $\mathrm{Ker}(\varphi)$ valódi, akkor $\mathrm{Ker}(\varphi) = (f)$, ahol f az ideál (egy) minimális fokú eleme. Így f minimális fokú azok között a polinomok között, amelyeknek az a elem gyöke. Mivel K-beli elem $K[x]$-ben egység, ezért feltehető, hogy f normált. Mivel polinomok szorzatának a foka a fokok összege (ha a tényezők egyike sem 0), ezért csak a K elemei az egységek a polinomgyűrűben, ami azt jelenti, hogy a normáltsággal f már egyértelműen meghatározott. A prímtulajdonságból azonnal következik f irreducibilitása is. A homomorfizmustétel alapján létezik olyan $\varphi : K[x]/(f) \to K(a)$ izomorfizmus, amely K elemeit fixen hagyja és az x-et tartalmazó maradékosztályt a-ba viszi. Ebből ugyanúgy következik a kívánt izomorfizmus, mint a transzcendens esetben; és ugyanúgy, mint ott, itt is azt kell belátni az egzisztenciához, hogy a fenti maradékosztály-gyűrű a kívánt tulajdonságú. Ehhez csak annyi szükséges, hogy a maradékosztály-gyűrű test legyen. Ez viszont főideálgyűrűk esetében – mint láttuk – az irreducibilitás közvetlen folyománya. Miután az algebrai elem és főpolinomja kölcsönösen meghatározzák egymást, az elem fokának a definíciója egyértelmű. ■

7.7. Műveletek ideálokkal, felbontási tétel

Már az eddigiekben is értelmeztünk műveleteket az ideálokkal. Mivel az ideálok teljes hálót alkotnak, ezért beszélhettünk ideálok egyesítéséről (generátum), illetve metszetéről. Az ideálokkal azonban sokkal több műveletet lehet végezni – és a kommutatív gyűrűk általános elméletében ezekre a műveletekre szükség is van.

7.69. Definíció. Az R gyűrű A és B ideáljainak $A + B$ összegén az $a + b$ ($a \in A, b \in B$) alakú elemek halmazát értjük; ha az előállítás egyértelmű, akkor direkt összegről beszélünk. Az A és B ideálok $A \cdot B$ szorzatán az AB komplexusszorzat generálta additív csoportot értjük. Az A és B ideálok $A : B$ hányadosán a gyűrű ama x elemeinek a halmazát értjük, amelyekre $xB \in A$ teljesül. Az A ideál radikálján azt a $\sqrt{A}$ halmazt értjük, amely elemeinek valamelyik hatványa A-ban van. Egy gyűrű radikálja nullideáljának radikálja. □

Megjegyzések. 1. A direkt szorzatot tetszőleges algebrai struktúrára definiáltuk; ez természetesen gyűrűkre is vonatkozik. Tekintettel arra, hogy a gyűrű additív struktúrája kommutatív csoport, ezért itt érvényesek az Abel-csoportokra vonatkozó eredmények. Így érvényes a direkt szorzatnak a direkt összeggel való kapcsolata. Mivel a 0-val való szorzás eredménye mindig 0, ezért itt a direkt összeadandók ideált alkotnak. Ez indokolja azt, hogy a direkt összegben ne részgyűrű szerepeljen.

2. E fogalmak alkalmas módon átvihetők a nemkommutatív gyűrűk esetére is. A legnagyobb problémát a gyűrű radikáljának a definíciója okozza; a radikált még kommutatív gyűrűk esetében is többféleképpen definiálják. Felhívjuk a figyelmet arra, hogy a fenti radikáldefiníció is csak speciális esetben megfelelő. Ennek ellenére azért választottuk ezt a definíciót, mert ez mutatja, hogy miképpen kapcsolódik össze a gyűrű radikálja a gyökvonás klasszikus értelmezésével. □

7.70. Tétel. *$A + B$ ideál, amely megegyezik a két ideál generátumával. $A \cdot B$ ideál, amelyre $A \cdot B \subseteq A \cap B$ teljesül. $A : B$ ideál; mégpedig minden olyan C ideált tartalmazó ideál, amelyre $C \cdot B \subseteq A$. Minden ideál radikálja is ideál.*

Bizonyítás. Az első állítás azonnal következik a 7.19. tételből. Ha $a \in A$ és $b \in B$, akkor a gyűrű tetszőleges r elemére nyilvánvalóan teljesül az $r(ab) \in AB$ feltétel. Mivel az $A \cdot B$ elemeinek a halmaza a kivonásra eleve zárt, ezért $A \cdot B$ valóban ideál. (A generátumra feltétlen szükség van, mert az AB szorzat általában nem zárt a kivonásra !) A tartalmazási reláció triviálisan következik abból, hogy az ab szorzat mindkét ideálnak eleme. (A szorzat általában nem egyezik meg a metszettel; például egy zérógyűrű esetén a szorzat mindig egyedül a 0-elemből áll, a metszet viszont nem.) Legyen $u, v \in A : B$, ami azt jelenti, hogy minden B-beli b elemre $ub, vb \in A$. Tekintettel arra, hogy A ideál, ezért $(u - v)b = ub - vb \in A$, minden B-beli b esetén, és így $A : B$ zárt a kivonásra. Ha r a gyűrű tetszőleges eleme, akkor tetszőleges B-beli b-re tekintsük az $(ru)b$ szorzatot. Mivel $rb \in B$ és $u \in A : B$, ezért $(ru)b = u(rb) \in A$, és így $A : B$ ideál. A $C \cdot B \subseteq A$ feltételből speciálisan következik az is, hogy $CB \subseteq A$; és így $A : B$ definíciója szerint $C \subseteq A : B$.

Tekintsük végül az A ideál T radikálját. Ha $u \in T$, akkor alkalmas n természetes számra $u^n \in A$; és így a szorzás kommutativitása alapján a gyűrű tetszőleges r elemére $(ru)^n = r^n u^n$ következik, ami A ideáltulajdonsága alapján szintén A-beli elem. Tegyük most fel, hogy a T-nek van egy v eleme, amelynek mondjuk a k-adik hatványa eleme A-nak. Annak a bizonyítására, hogy $u - v \in T$, kimutatjuk, hogy ennek $(n + k - 1)$-edik hatványa eleme A-nak. A disztributivitás alapján ez a hatvány ugyanis olyan összeg alakjában írható, ahol minden egyes tagban vagy legalább n darab u, vagy legalább k darab

v szerepel tényezőként. Mivel ezek a szorzatok mindig A-ban vannak, ezért A ideáltulajdonsága miatt ezeknek más elemekkel való szorzatuk, és ilyenek összege és különbsége is A-beli, ami bizonyítja, hogy $u - v$ eleme a radikálnak.

Azt kell már csupán megmutatni, hogy a fenti ideálok nem üresek, ami triviális, mert 0 nyilvánvalóan eleme mindegyiknek. ■

A továbbiakban Noether-gyűrűk ideáljaival foglalkozunk.

7.71. Definíció. Egy R kommutatív gyűrű M ideálját irreducibilisnek nevezzük, ha nem áll elő két, nála bővebb ideál metszeteként. Egy Q ideál primér, ha $ab \in Q$ esetén vagy $a \in Q$, vagy b egy hatványa eleme Q-nak. □

Felhívjuk a figyelmet arra, hogy a prímerideál definíciója nem fogalmazható úgy, hogy a és b közül valamelyiknek egy hatványa Q-beli, mert lehet, hogy a és b egyike sincs Q-ban, sőt b-nek egyetlen hatványa sincs Q-ban, de a^2 Q-beli. (Lehet is adni olyan példát, amikor e gyengébb feltétel teljesül, de az ideál nem primér.)

7.72. Tétel. *Egy R kommutatív gyűrűben a S ideál radikálja akkor és csak akkor prímideál, ha $ab \in S$ esetén a és b közül valamelyiknek egy hatványa S-beli. A gyűrű egy Q ideálja akkor és csak akkor primér, ha $ab \in Q$ esetén vagy a és b valamelyike Q-beli, vagy a és b mindegyikének egy hatványa benne van Q-ban. Prímerideál radikálja prím.*

Bizonyítás. Tegyük fel, hogy a P prímideál az S radikálja, és legyen $ab \in S$. Ekkor $S \subseteq P$ és P prímtulajdonsága miatt a és b valamelyike P-ben van. Ez viszont a radikál definíciója szerint éppen azt jelenti, hogy ennek az elemnek valamelyik hatványa S-beli. Legyen most S a kirótt tulajdonságú ideál, és tegyük fel, hogy ab eleme az S ideál P radikáljának. Ez azt jelenti, hogy (ab)-nek valamelyik (n-edik) hatványa S-beli; és a feltételek szerint vagy a^n-nek, vagy b^n-nek egy hatványa S-beli. Így a két elem valamelyikének egy hatványa eleme S-nek; ami a radikál definíciója szerint éppen azt jelenti, hogy vagy a, vagy b P-hez tartozik.

Ha a Q ideálra a tételben kirótt feltétel igaz, akkor Q természetesen primér. Legyen most Q primér és tegyük fel, hogy $ab \in Q$, de $a \notin Q$. A prímerideál definíciója szerint ekkor b egy hatványa eleme Q-nak. $ba = ab \in Q$ miatt, ha $b \in Q$ sem igaz, akkor a-nak van olyan hatványa, ami Q-ban van; ez pedig éppen a tételben szereplő állítást adja.

A harmadik állítás most már azonnal adódik abból, hogy a tételben szereplő Q ideálra adott tulajdonságból következik a tételbeli S ideálra kirótt tulajdonság. ■

Megjegyzések. 1. A fenti tétel megmutatja, hogy a „primérség” mennyivel erősebb a „prímradikálúságnál”. Emellett a tételbeli leírás világosabban megfogalmazza a prímerideálok tulajdonságát. Ennek ellenére az eredeti definíciót tartjuk meg, mert a bizonyításokban sokkal kényelmesebb ezt használni.

Megadunk egy példát olyan ideálra, amelyiknek a radikálja prímideál, de az ideál nem primér:

Tekintsük az $S = \mathbb{Q}[x, y]$ polinomgyűrűt és legyen $R = S[\sqrt{xy}]$, amelynek elemei definíció szerint az $S(\sqrt{xy})$ testbővítés $f + g \cdot \sqrt{xy}$ alakú elemei, ahol $f, g \in S$. Az R elemei nyilvánvalóan a fenti test egy részgyűrűjét alkotják. Az is világos, hogy a fenti felírás egyértelmű.

Legyen $P = (x, \sqrt{xy})$ az R-nek e két elem által generált ideálja. Tetszőleges $f, g \in R$ esetén $x \cdot f + g \cdot \sqrt{xy} \in P$, másrészt világos, hogy az ilyen alakú elemek ideált alkotnak; tehát P-nek az elemei pontosan az ilyen alakú elemek. Ha $(f_1 + g_1 \cdot \sqrt{xy}) \cdot (f_2 + g_2 \cdot \sqrt{xy}) \in P$, akkor a felírás

egyértelműsége alapján $f_1 f_2 + g_1 g_2 xy$ osztható x-szel. Ezért f_1 és f_2 valamelyike ugyancsak osztható x-szel, azaz valamelyik tényező P-beli. Tehát P prímideál.

Világos, hogy P^2 egy generátorrendszerét adja a P generátorrendszeréből képezett kétszeres szorzatok rendszere; azaz $P^2 = (x^2, xy, x\sqrt{xy})$. P^2-nek természetesen P a radikálja.

Nyilván $xy \in P^2$. A felírás szerint P^2 elemei $x \cdot f + g \cdot \sqrt{xy}$ alakúak, ahol az f polinom konstans tagja 0. Így $x \notin P^2$, hiszen P^2 elemeiben a „gyökmentes rész" minden tagja legalább másodfokú. De P^2-nek nem lehet eleme y egyetlen hatványa sem, mert a gyökmentes részről azt is láthatjuk, hogy x-szel osztható. (Mindkét esetben figyelembe vettük a felírás egyértelműségét.) Tehát P^2 nem primérideál.

2. Az irreducibilis ideál az irreducibilis elem, míg a primérideál a prímhatvány általánosításának tekinthető. Az egyértelmű faktorizáció ideálokra való általánosításának egy gyenge (de fontos) formája érvényes Noether-gyűrűkben. A későbbiekben látni fogjuk, hogy a „teljes" általánosítás az úgynevezett Dedekind-gyűrűkre érvényes. □

Most a Noether-gyűrűk ideálhálójára vonatkozó alapvető tétel következik. A hálóelméleti vizsgálatoknál látni fogjuk, hogy egy gyűrű ideálhálója egy (speciális) moduláris háló, amelyben igaz a KUROS–ORE-tétel, amit gyűrűkre lefordítva azonnal adódik:

7.73. Tétel. *Egy Noether-gyűrű minden ideálja előállítható véges sok irreducibilis ideál metszeteként úgy, hogy ezeknek bármelyikét elhagyva egy, az eredeti ideált valódi módon tartalmazó ideált nyerünk. Ha*

$$M_1 \cap \ldots \cap M_r \qquad \text{és} \qquad N_1 \cap \ldots \cap N_s$$

egy-egy ilyen felbontás, akkor bármely M_i helyettesíthető egy alkalmas N_j-vel úgy, hogy ezeknek az ideáloknak a metszete is az eredeti ideál legyen. ■

Most a 7.73. tételben adott felbontást fogjuk tovább vizsgálni.

7.74. Tétel. *Noether-gyűrűben minden irreducibilis ideál primér.*

Bizonyítás. Tegyük fel, hogy M az R Noether-gyűrű egy irreducibilis ideálja. A primér tulajdonság bizonyításához legyen $ab \in M$ és $a \notin M$. Azt kell megmutatnunk, hogy b-nek valamelyik hatványa eleme M-nek. Evégett tekintsük mindenekelőtt az

$$M : (b),\ M : (b^2),\ \ldots,\ M : (b^n),\ \ldots$$

ideálsorozatot. Az ideálhányados definíciójából következik, hogy a fenti sorozat mindegyik eleme benne van a következőben, mert ha $rb^n \in M$, akkor $rb^{n+1} \in M$ is fennáll. Mivel R Noether-gyűrű, ezért van olyan k pozitív egész szám, amelyre $M : (b^k) = M : (b^{k+1})$ teljesül. Vegyük ezután az (M, a) és (M, Rb^k) ideálok metszetét. Ez a metszet nyilvánvalóan tartalmazza az M ideált; megmutatjuk, hogy meg is egyezik vele.

A metszetideál tetszőleges eleme – mint (M, Rb^k)-beli elem – felírható $c = m + rb^k$ alakban $(m \in M, r \in R)$. Az $ab \in M$ feltételből azonnal következik, hogy $(M, a) \subseteq$ $\subseteq M : (b)$, és így $c \in (M, a)$ következtében $mb + rb^{k+1} = cb \in M$. Ebből viszont azt kapjuk, hogy $rb^{k+1} = cb - mb \in M$, hiszen mb nyilván eleme M-nek. Ez azt jelenti, hogy $r \in M : (b^{k+1})$, azaz, feltételünk szerint, $r \in M : (b^k)$, és így $rb^k \in M$, tehát $c = m + rb^k$ is eleme M-nek. A metszet így valóban M-mel egyenlő. Mivel M irreducibilis, azaz nem

állítható elő tőle különböző ideálok metszeteként, és $(M, a) \neq M$, így csak $(M, Rb^k) = M$ lehet. Eszerint $Rb^k \subseteq M$, speciálisan $b \cdot b^k \in M$. ■

7.75. Következmény. *Noether-gyűrű minden ideálja előállítható primérideálok metszeteként.* ■

Ha – mint említettük – a prímideálokat a prímelemek általánosításaként tekintjük, akkor a primérideálokra úgy gondolhatunk, mint a prímhatványok általánosítására. Ez persze nem teljesen felel meg a valóságnak. Tekintsük például a $\mathbb{Q}[x_1, \ldots, x_n, \ldots]$ racionális test feletti végtelen határozatlanú polinomgyűrűt. Ebben a $Q = (x_1, (x_2)^2, \ldots, (x_n)^n, \ldots \ldots)$ ideál primér, amelynek P radikálja azoknak a polinomoknak a halmaza, amelyeknek a konstans tagja 0 (ami prímideál). Ezzel szemben P-nek bármely, egynél nagyobb kitevőjű hatványát tekintjük, ez nemcsak nem egyezik meg Q-val, de nincs is benne. Amennyiben azonban egy Noether-gyűrűt vizsgálunk, ebben már minden primérideál tartalmazza radikáljának egy megfelelő hatványát. Ez azon múlik, hogy a radikál végesen generált, és generátorai mindegyikének egy alkalmas hatványa eleme a primérideálnak. Ha e kitevők összege n, akkor biztos, hogy a prímideál elemeiből vett minden n-tényezős szorzat már a primérideálba esik, azaz a prímideál n-edik hatványa már benne van a primérideálban. Az azonban itt sem igaz, hogy bármely primérideál a radikáljának egy hatványa volna.

Az előzőek figyelembevételével a 7.73. tételben adott felbontás esetleg „túl finom". Egy primérideál önmagában ugyanis már „felbontás"-nak tekinthető; de előfordulhatna, hogy ez még tovább bontható – azaz, nem irreducibilis. Például $\mathbb{Q}[x, y]$ esetében ilyen az (x^2, xy, y^2) ideál, amely primér (radikálja az (x, y) ideál); mégis felbontható az (x^2, y) és (x, y^2) ideálok metszetére. E két ideál már irreducibilis – és így primér. Ezeknek a radikálja ugyancsak az (x, y) ideál. (A számolások elvégzését az olvasóra bízzuk.) Ez az eset sugallja, hogy a megegyező radikálú prímideálokat esetleg össze lehetne vonni.

7.76. Tétel. *Egy R Noether-gyűrű véges sok primérideáljának rövidíthetetlen metszete akkor és csak akkor primér, ha radikáljaik megegyeznek.*

Bizonyítás. Legyen a $Q_1, \ldots, Q_r$ primérideálok radikálja ugyanaz a P prímideál, s e primérideálok metszete Q. Tegyük fel, hogy $ab \in Q$ és $a \notin Q$. Azt kell kimutatnunk, hogy b-nek egy alkalmas hatványa Q-ban van.

Mivel Q a $Q_1, \ldots, Q_r$ ideálok metszete, ezért ab eleme ezen ideálok mindegyikének, és a legalább egyiküknek nem eleme. Az általánosság megszorítása nélkül feltehető, hogy $a \notin Q_1$. Mivel Q_1 primér, ezért az $ab \in Q_1$ és $a \notin Q_1$ feltételek alapján b-nek egy alkalmas hatványa Q_1-hez tartozik; vagyis b eleme Q_1 radikáljának, P-nek. Mivel P az összes Q_i-nek $(1 \leq i \leq r)$ radikálja, ezért b-nek egy-egy alkalmas hatványa eleme ezeknek. Ha n a szereplő kitevők maximuma, akkor b^n e primérideálok mindegyikében benne van, és így eleme ezek metszetének, Q-nak is. Ez pedig éppen azt jelenti, hogy Q primér – s a radikálja nyilván ugyancsak a P prímideál.

A metszet rövidíthetetlenségét csak a továbbiakban fogjuk felhasználni. A bizonyítás első része alapján az azonos radikálú primérideálokat helyettesíthetjük a metszetükkel. Így ugyancsak primérideálok metszetét nyerjük, amelyeknek a radikáljai ugyanazok, mint az eredeti metszetben szereplőké. Ha az eredeti metszet rövidíthetetlen volt, akkor nyilván a most kapott metszet is rövidíthetetlen. Így tehát elég a következőket kimutatnunk:

Ha a $Q_1, \ldots, Q_r$ primérideálok $P_1, \ldots, P_r$ radikáljai csupa különböző prímideálok, akkor ezek M metszete nem primér. Evégett az előforduló prímideálok között keressünk egy minimálisat (véges sok különböző halmaz közt ilyen biztosan van), amelyről az általánosság megszorítása nélkül feltehető, hogy éppen P_1. A minimalitás miatt minden i indexre létezik olyan $b_i \in P_i$, amelyre $b_i \notin P_1$ $(2 \leq i \leq r)$. A radikáltulajdonság szerint létezik olyan n (amely a prímideálok számának végessége miatt a prímideáloktól függetlenül választható), amelyre $(b_i)^n \in Q_i$ $(2 \leq i \leq r)$. Így a $b = (b_2 \cdot \ldots \cdot b_r)^n$ elem benne van a $Q_2, \ldots, Q_r$ ideálok mindegyikében. A rövidíthetetlenség miatt $Q_1 \neq M$, és így létezik olyan $a \in Q_1$, amely nem eleme M-nek. Mivel $ab \in Q_1$ és ab eleme a $Q_2, \ldots$ $\ldots, Qr$ ideáloknak is, ezért ab eleme ezek metszetének: $ab \in M$. Az a választása folytán $a \notin M$. Mivel $b_2, \ldots, b_r$ egyike sincs P_1- ben, ezért az ezekből képezett egyetlen szorzat sem lehet P_1-ben – hiszen P_1 prímideál. Így speciálisan b-nek egyetlen hatványa sem lehet benne P_1-ben, tehát nem lehet eleme a P_1 tartalmazta M ideálnak sem. Találtunk tehát egy olyan M-beli ab elemet, amelyre sem a, sem b-nek egyetlen hatványa sem eleme M-nek; azaz M nem primér. ■

7.77. Következmény (Noether–Lasker)**.** *Noether-gyűrűben minden nemtriviális ideál felírható primérideálok metszeteként úgy, hogy a metszetből egyetlen primérideál sem hagyható el, a szereplő primérideálok közül bárhogyan kivéve legalább kettőt, ezek metszete nem primérideál, és bármely két különböző primérideálnak a radikálja különböző prímideál.* ■

A fenti tételben adott felbontás nem mindig teljesen egyértelmű. Be lehet azonban bizonyítani, hogy mind a primérkomponensek száma, mind a megfelelő radikálok egyértelműen meghatározottak.

7.8. Ideálok gyökei

Az alábbiakban célunk az algebrai geometriában fontos, ún. Hilbert-féle speciális nullhelytétel („Nullstellensatz") bebizonyítása. Ennek célja meghatározni, hogy adott polinomok közös gyökei milyen más polinomnak lesznek gyökei. Érdekes módon a speciális nullhelytétel az általánosabb. Erről az általános nullhelytételnél bővebben szólunk.

7.78. Definíció. Az R gyűrűnek a K (kommutatív) testbe való $\varphi \neq 0$ homomorfizmusát az I ideál gyökének nevezzük, ha $I \subseteq \mathrm{Ker}(\varphi)$. □

Ez a definíció megfelel a gyök fogalma 7.47. definícióban szereplő általánosításának. Ha a vizsgált gyűrű egy test feletti polinomgyűrű, akkor az ideál gyökei éppen azok az elem-n-esek, amelyek az ideálhoz tartozó minden polinomnak a gyökei. Ezek a pontok az n-dimenziós tér alakzatai: az úgynevezett algebrai sokaságok. Ezek – durván szólva – olyan alakzatok, amelyeket „algebrai összefüggésekkel" definiálhatunk.

7.79. Definíció. Az R gyűrű A ideáljának a lezártján R azon elemeinek a halmazát értjük, amelyeknek gyöke az A ideál minden gyöke. □

Az a elem tehát pontosan akkor tartozik az A ideál lezártjához, ha benne van minden olyan testbe való homomorfizmus magjában, amely az A ideált tartalmazza. A lezárt tehát

nem más, mint az összes ilyen magnak a metszete. Ez azt jelenti, hogy a lezárt maga is ideál, és az is azonnal látható, hogy tényleg lezárásról van szó. (Hiszen tartalmazza az eredeti ideált és a lezárt lezártja az eredeti lezárt.)

7.80. Tétel (Hilbert)**.** *Egységelemes integritási tartomány bármely ideáljának a lezártja megegyezik ennek az ideálnak a radikáljával.*

Bizonyítás. Mindenekelőtt belátjuk, hogy a radikál benne van a lezártban. Legyen B az A ideál radikálja és φ az A-nak egy tetszőleges gyöke. A radikál definíciója szerint bármely B-beli b elemhez van olyan n pozitív egész szám, amelyre $b^n \in A$. Eszerint $(\varphi(b))^n = 0$; és $\mathrm{Im}(\varphi)$ nullosztómentessége miatt $\varphi(b) = 0$, ami pontosan azt jelenti, hogy b eleme a radikálnak.

A megfordítás bizonyítására először is belátjuk a következőt: Ha az R egységelemes gyűrű egy A ideáljának nincs gyöke, akkor $A = R$. Ezt célszerű úgy fogalmazni, hogy ha $A \neq R$, akkor A-nak van gyöke.

Ennek kimutatása végett tekintsük a vizsgált R gyűrűnek egy R-től különböző A ideálját. A feltételből azonnal következik, hogy $1 \notin A$. Mivel az A-t tartalmazó, de az 1-et nem tartalmazó ideálok növő láncának az egyesítése is ilyen tulajdonságú, ezért – a Zorn-lemma szerint – létezik olyan B ideál, amelyre $A \leq B$, $1 \notin B$ és B az ilyen tulajdonságú ideálok között maximális. Mivel minden B-t tartalmazó ideál eleve tartalmazza A-t, ezért a B-t valódi módon tartalmazó minden ideál tartalmazza 1-et, ami azt jelenti, hogy B az R-nek egy maximális ideálja. A 7.26. tétel szerint ekkor R/B egyszerű. Mivel az egységelem képe egységelem, ezért R/B nem zérógyűrű. A 7.23. tétel szerint tehát R/B (kommutatív) test. Így az R-et R/B-be képező φ természetes homomorfizmus gyöke A-nak, mert $A \leq B = \mathrm{Ker}(\varphi)$.

Ezzel beláttuk, hogy R az egyetlen olyan ideál, amelynek nincs gyöke. (R-nek valóban nincs gyöke, mert ha egy homomorfizmus az R minden elemét 0-ba viszi, akkor a homomorfizmus triviális.)

Legyen most A az R egységelemes gyűrű egy tetszőleges ideálja, és a az A lezártjának egy eleme. Mivel 0 eleve eleme a radikálnak, ezért feltehetjük, hogy $a \neq 0$. Tekintsük az $R[x]$ polinomgyűrűt, amely szintén egységelemes (és kommutatív). Tekintsük e gyűrűnek az $(A, 1 - ax)$ ideálját. Ha φ ennek gyöke, akkor $\varphi(A) = 0$ és az a-ra vonatkozó feltétel miatt $\varphi(a) = 0$ is igaz; továbbá $\varphi(1-ax) = 0$ is teljesül. Ebből a két összefüggésből azonnal kapjuk, hogy $\varphi(1) = 0$, így φ csak a triviális homomorfizmus lehet. A fenti ideálnak tehát nincs gyöke, azaz $(A, 1 - ax) = R[x]$. A bal oldali ideál elemei a 7.19. tétel alapján a következő alakban írhatók:

$$a_1 \cdot f_1(x) + \ldots + a_r \cdot f_r(x) + (1 - ax) \cdot f(x),$$

ahol $a_1, \ldots, a_r$ az A-nak, $f_1(x), \ldots, f_r(x)$ és $f(x)$ az $R[x]$-nek tetszőleges elemei. Mivel a jobb oldal tartalmazza az egységelemet, ezért ez is felírható így:

$$a_1 \cdot g_1(x) + \cdots + a_s \cdot g_s(x) + (1 - ax) \cdot g(x) = 1,$$

alkalmas A-beli $a_1, \ldots, a_s$ és $R[x]$-beli $g_1(x), \ldots, g_s(x), g(x)$ elemekkel. Jelölje n e polinomok fokának a maximumát.

Legyen K az $R[x]$ hányadosteste és $\varphi : R[x] \to K$ az a homomorfizmus, amely R elemeit fixen hagyja és x-et $\frac{1}{a}$-ba viszi ($a \neq 0$). Ez azt jelenti, hogy

$$a_1 \cdot g_1(\frac{1}{a}) + \cdots + a_s \cdot g_s(\frac{1}{a}) = 1.$$

Az n definíciója szerint $b_i = a^n g_i(\frac{1}{a}) \in R$; így a legutóbbi egyenlőséget a^n-nel szorozva az

$$a_1 \cdot b_1 + \cdots + a_s \cdot b_s = a^n$$

összefüggéshez jutunk. Mivel minden egyes a_i eleme az A ideálnak, ezért a valóban eleme A radikáljának. ■

Feladatok

1. Legyen φ az R kommutatív gyűrűnek a K testbe való homomorfizmusa és L az $\mathrm{Im}(\varphi)$-t tartalmazó legkisebb test. Mi az R ideáljaira vonatkozó szükséges és elegendő feltétele annak, hogy a 7.64. tétel R-re igaz legyen?

2. Bizonyítsuk be, hogy ha az R gyűrűben érvényes az egyértelmű faktorizáció, akkor minden lokalizáltjában is érvényes.

3. Bizonyítsuk be, hogy tetszőleges pozitív egész n számra létezik olyan gyűrű, amelyben érvényes az egyértelmű faktorizáció és asszociáltaktól eltekintve pontosan n irreducibilis elem van.

4. Legyen n pozitív egész szám. Adjunk meg olyan euklideszi gyűrűt, amelyben pontosan n irreducibilis elem van.

5. Bizonyítsuk be, hogy $\mathbb{Q}[x, y]$-ban az (x^2, xy) ideál radikálja prím, de az ideál nem primér.

6. Legyen I tetszőleges egységelemes integritási tartomány és tekintsük az I prímideáljainak $\mathcal{P}$ halmazát. Bizonyítsuk be a következőket:

(1) Ha K test és $\varphi : I \to K$ homomorfizmus, akkor $\mathrm{Ker}(\varphi) \in \mathcal{P}$.

(2) Tetszőleges $a \in I$ és $\{\varphi : I \to (I/P) | P \in \mathcal{P}\}$ esetén $\varrho(a, \varphi) \Leftrightarrow \varphi(a) = 0$ Galois-kapcsolat.

(3) ϱ szerint az I-ben zártak a $\mathcal{P}$-beli elemek tetszőleges metszetei.

(4) Az I-beli A ideál ϱ szerinti lezártja ugyanaz, mint a 7.79. definícióban és $\sqrt{A} \subseteq \varrho(A)$ ($\varrho(A)$ az $A \subseteq I$ lezártját jelöli a fenti lezárásban).

(5) $1 \in A \Leftrightarrow 1 \in \varrho(A)$. Miben különbözik ez a bizonyítás a könyvben találhatótól?

7. Legyen α egy normált egész együtthatós n-edfokú polinom gyöke. Bizonyítsuk be, hogy az $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ alakú számok egy Noether-gyűrűt alkotnak (műveletek a szokásosak).

8. Tekintsük a $\sin(x)$ és a $\cos(x)$ függvények racionális (vagy valós) együtthatós kifejezéseit. Bizonyítsuk be, hogy ezek Noether-gyűrűt alkotnak (műveletek a függvényműveletek).

9. Általánosítsuk az előző két feladatot.

10. Az R egységelemes főideálgyűrűben mit jelent az $A : B$, ha A és B nem-0 ideálok?

11. Legyenek $A, B, \ldots$ az R egységelemes kommutatív gyűrű ideáljai. Bizonyítsuk be az alábbi összefüggéseket:

(1) Ideálok szorzása kommutatív és asszociatív.

(2) $A \cdot R = A$ (ha $1 \neq R$, akkor csak $AR \subseteq A$).

(3) $A \cdot (B + C) = A \cdot B + A \cdot C$.

(4) $(A \cap B) \cdot (A + B) \leq A \cdot B$.

(5) $A \leq A : B = A : (A + B)$.

(6) Ha $A \geq B$, akkor $A : C \geq B : C$ és $C : A \leq C : B$.

(7) Ha $A \geq B$, akkor $A : B = R$ és $B : A \geq B$. Lehet-e $B : A = B$, illetve $B : A = R$?

(8) $A : R = A$ (ha $1 \neq R$, akkor csak $A : R \geq A$) és $R : A = R$.

(9) $A : B_1 = A : B_2 = A \iff A : (B_1 \cap B_2) = A \iff A : (B_1 \cdot B_2) = A$.

(10) $(A_1 \cap \ldots \cap A_r) : B = (A_1 : B) \cap \ldots \cap (A_r : B)$.

(11) $A : (B + C) = (A : B) \cap (A : C)$ és $(A : B) \cdot (B : C) \subseteq A : C$.

(12) $(A : B) : C = A : (BC) = (A : C) : B$.

(13) $B \cdot (A : B) \leq A$, $A : (A : B) \geq B$.

12. Legyen A az R kommutatív egységelemes gyűrű egy ideálja. Mely B ideálokra lesz $(A : B) = R$? Melyek azok az A valódi ideálok, amelyekre tetszőleges X ideál esetén $A : X$ két értéket vehet fel?

13. Legyen R egy nullosztómentes Noether-gyűrű és I az R ideálja. Mikor lesz az I szerinti maradékosztály-gyűrű direkt irreducibilis? (Egy gyűrű direkt irreducibilis, ha csak olyan $A \oplus B$ direkt összeggel lehet izomorf, amelyben a két tag valamelyike a nullgyűrű.)

14. Azt mondjuk, hogy a B ideál *relatív prím* az A-hoz, ha $A : B = A$. Mutassuk meg, hogy ez nem szimmetrikus; de bizonyos megszorításokkal az. Milyen megszorítást kell tennünk $\mathbb{Z}$ esetében? Milyen megszorítást kell tennünk általában?

15. Bizonyítsuk be, hogy a Hilbert-féle nullhelytétel a következőket mondja ki: „Az R egységelemes integritási tartomány I ideáljának radikálja megegyezik az I-t tartalmazó összes prímideál metszetével”.

16. Bizonyítsuk be, hogy az R egységelemes integritási tartomány I ideáljának radikálja pontosan akkor egyezik meg az I-t tartalmazó összes maximális ideál metszetével, ha minden R-beli P prímideál előáll maximális ideálok metszeteként.

8. Kommutatív testek

Az algebra „eredeti” feladata az egyenletek és egyenletrendszerek megoldása. Az utóbbival – ha minden egyes egyenlet lineáris – a lineáris algebra foglalkozik. Az előbbi természetesen akkor érdekes, ha a szereplő egyenlet legalább másodfokú. Tekintettel arra, hogy a gyökökkel és az együtthatókkal a „négy alapműveletet” végezhetjük el, ezért e kérdéskörnél egy testből – pontosabban egy kommutatív testből – vett elemekkel dolgozunk. Ennek a fejezetnek a fő célja az egyenletek megoldhatóságának a vizsgálata.

8.1. Algebrai testbővítés

Mindenekelőtt az egyszerű algebrai testbővítésekkel foglalkozunk. Ezekkel már a 7.6. pontban is foglalkoztunk, definíciójuk a 7.67. definícióban szerepel. Az egyszerű testbővítések fontosságát mutatja, hogy e bővítések tulajdonképpen azt adják meg, miképpen lehet egy-egy magasabbfokú egyenlet gyökeivel (formálisan) számolni. Mindenekelőtt egy olyan jellemzést adunk, amely az egyszerű algebrai és az egyszerű transzcendens bővítéseket választja szét:

8.1. Tétel. *A K testnek egy $K(a)$ egyszerű bővítése akkor és csak akkor algebrai, ha $K(a)$ az összeadásra és a K elemeivel való szorzásra a K felett véges dimenziós vektortér. E vektortér dimenziója megegyezik az a elem fokával.*

Ha $K(a)$ transzcendens, akkor – mint vektortér – végtelen dimenziós.

Bizonyítás. Először is megjegyezzük, hogy a K test tetszőleges M bővítése nyilvánvalóan vektortér az M-beli összeadásra és a K elemeivel való szorzásra nézve. Ha az a transzcendens elem K felett, akkor a egyetlen, K-beli együtthatós nemtriviális polinomnak sem gyöke, ami azt jelenti, hogy az $1, a, \ldots, a^n, \ldots$ elemek K felett lineárisan függetlenek, tehát $K(a)$ nem véges dimenziós.

Tegyük most fel, hogy a algebrai elem a K test felett, és legyen $f = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ az a-nak (K feletti) főpolinomja. A 7.68. tétel szerint $K(a)$ izomorf $K[x]/(f)$-fel. Az izomorfizmus úgy adható meg, hogy K elemeit fixen hagyja és x mellékosztályát képezi a-ra. A tétel bizonyításához azt kell tehát még belátnunk, hogy e maradékosztály-gyűrűnek mint K feletti vektortérnek létezik n elemű bázisa. Más szóval, azt kell megmutatni, hogy a $K[x]$ polinomgyűrűben létezik n számú olyan elem, amelyeknek a képe a maradékosztály-gyűrűnek bázisa. A lineáris függetlenség azt jelenti, hogy ezeknek az elemeknek semmilyen K-beli együtthatós lineáris kombinációja nem lehet osztható f-fel; míg a generátorrendszerre vonatkozó feltétel szerint, minden polinomból kivonható ezeknek egy olyan, K-beli együtthatós lineáris kombinációja, hogy a különbség f-fel osztható. E feltételeknek nyilván eleget tesznek az $1, x, x^2, \ldots, x^{n-1}$ polinomok. Ezek K-beli együtthatós lineáris kombinációja csak n-nél alacsonyabb fokú polinom lehet, s így csak akkor osztható f-fel, ha a triviális lineáris kombinációt vettük. A másik feltétel pedig azért teljesül, mert test feletti polinomgyűrűben érvényes a maradékos osztás. ■

Megemlítjük, hogy ha az M test a K-nak olyan bővítése, amely K felett véges dimenziós vektortér, akkor nem feltétlenül igaz, hogy M felírható $K(a)$ alakban. Ennek ellenére

az algebrai bővítések vizsgálatakor nagyon hasznosak a véges dimenziós bővítések. Ennek oka e bővítések „tranzitivitása”:

8.2. Tétel. *Ha a K_2 test a K_1 testnek bővítése, akkor jelölje $(K_2 : K_1)$ a K_2 testnek mint K_1 feletti vektortérnek a dimenzióját. Ha $(L : M)$ és $(M : K)$ véges, akkor $(L : K) = (L : M) \cdot (M : K)$.*

Bizonyítás. Legyen $\alpha_1, \ldots, \alpha_n$ az M-nek K feletti és $\beta_1, \ldots, \beta_k$ az L-nek M feletti bázisa. Kimutatjuk, hogy az $\alpha_i \cdot \beta_j$ elemek $(1 \leq i \leq n, 1 \leq j \leq k)$ az L-nek egy K feletti bázisát alkotják. Tekintsük az L egy tetszőleges β elemét. A feltétel szerint ez felírható $\gamma_1\beta_1 + \cdots + \gamma_k\beta_k$ alakban, ahol $\gamma_1, \ldots, \gamma_k \in M$. Ekkor viszont ezek bármelyike – például γ_j – felírható $c_{1,j}\alpha_1 + \cdots + c_{n,j}\alpha_n$ alakban, alkalmas, K-beli $c_{i,j}$ elemekkel. Ez éppen azt jelenti, hogy a fent megadott elemek generátorrendszert alkotnak. Lineáris függetlenségük a következőképpen látható be. Tegyük fel, hogy ezeknek valamelyik K-beli $d_{i,j}$ együtthatókkal képezett lineáris kombinációja 0. Tekintsük ekkor a $\delta_j = d_{1,j}\alpha_1 + \cdots + d_{n,j}\alpha_n$ elemeket. Ezek – mint M-beli elemek szorzatainak az összegei – maguk is M-beliek; s a disztributivitás alapján teljesül rájuk a $\delta_1\beta_1 + \cdots + \delta_k\beta_k = 0$ feltétel. A β-k M feletti lineáris függetlensége miatt ebből következik, hogy minden egyes $\delta_j = 0$; s az α-k K feletti függetlenségét figyelembe véve kapjuk, hogy minden egyes $d_{i,j}$ is 0-val egyenlő. Így valóban bázist kaptunk; s mivel a bázis elemszáma megegyezik a vektortér dimenziójával, ezért $(L : K) = n \cdot k$. ■

A 8.2. tételnek igen sok fontos következménye van, amelyek kimondásához néhány elnevezésre van szükségünk:

8.3. Definíció. Legyen az M test a K testnek egy bővítése. Ha $(M : K)$ véges, akkor véges bővítésről beszélünk; ha M a K-ból véges sok, K felett algebrai elem bővítéseként áll elő, akkor M-et K felett véges algebrai bővítésnek nevezzük. Ha M minden eleme a K felett algebrai, akkor azt mondjuk, hogy M algebrai bővítés a K felett (vagy K-nak algebrai bővítése). □

8.4. Következmény. *Legyen M a K-nak bővítése.*

(I) *Ha M véges bővítés, akkor algebrai.*

(II) *M akkor és csak akkor véges, ha véges algebrai.*

(III) *Ha M véges, akkor minden, M fölött algebrai elem K fölött is algebrai.*

(IV) *Ha M a K-nak és L az M-nek algebrai bővítése, akkor L algebrai bővítése K-nak is.*

Bizonyítás. (I) Ha $a \in M$, akkor $K(a)$ az M-nek altere. Mivel véges dimenziós tér altere is véges dimenziós, ezért $K(a)$ véges bővítése K-nak. A 8.1. tétel szerint tehát a algebrai a K felett.

(II) Ha M a K-nak véges bővítése, akkor létezik egy $a_1, \ldots, a_n$ véges bázisa a K felett. Erre természetesen teljesül az $M = K(a_1, \ldots, a_n)$ összefüggés. Az (I) tulajdonság szerint ezeknek az elemeknek mindegyike algebrai a K felett, így M valóban véges algebrai bővítés. Legyen $M_0 = K$, $M_1 = M_0(a_1)$, $M_2 = M_1(a_2), \ldots, M = M_k = M_{k-1}(a_k)$. Nyilvánvalóan fennáll a

$$K = M_0 \subseteq M_1 \subseteq \ldots M_{k-1} \subseteq M_k = M$$

összefüggés. Mivel minden a_i algebrai a K felett, ezért algebrai a K-t tartalmazó M_{i-1} felett is. A 8.1. tétel szerint tehát $(M_i : M_{i-1})$ véges; s a 8.2. tétel ismételt alkalmazásával nyerjük, hogy $(M : K)$ is véges.

(III) Legyen a algebrai elem az M felett. A (II) állítás szerint $M(a)$ a K-nak véges algebrai bővítése, mert M is véges algebrai bővítés. Ugyancsak a (II) alapján tehát $M(a)$ véges bővítése K-nak, és (I) szerint ebből következik, hogy a algebrai elem a K felett.

(IV) Legyen $a \in L$. Feltétel szerint a gyöke egy M-beli együtthatós, nemtriviális polinomnak. Legyenek e polinom együtthatói $a_0, \ldots, a_n$; és legyen $T = K(a_0, \ldots, a_n)$. Ekkor T a K-nak véges algebrai bővítése és a algebrai elem a T felett is. (II) és (III) szerint tehát a algebrai elem a K fölött. ■

8.5. Következmény. *Legyen a algebrai elem a K fölött, és legyen $b \in K(a)$. Ekkor:*

(1) *b foka osztója az a fokának.*

(2) *Ha a foka prímszám, akkor vagy $b \in K$, vagy $K(b) = K(a)$.*

Bizonyítás. A 8.4. következmény (I) pontjából és a 8.2. tételből következik, hogy $(K(a) : K) = (K(a) : K(b)) \cdot (K(b) : K)$. Ebből viszont a 8.1. tétel szerint azonnal adódik az első állítás.

Az első állításból következik, hogy a második esetben vagy $(K(b) : K) = 1$, vagy $(K(b) : K) = (K(a) : K)$. Ha az első lehetőség teljesül, akkor b gyöke egy K felett elsőfokú polinomnak, tehát K-ban van. A második lehetőség esetén viszont azt vehetjük figyelembe, hogy egy vektortér valamelyik alterének a dimenziója (véges dimenziós esetben!) csak úgy egyezhet meg az egész tér dimenziójával, ha az altér megegyezik az egész térrel. ■

A 8.5. következmény mutat rá arra, hogy a harmadfokú polinomok gyökeit miért kellett összegalakban keresni. Ugyanis $a \in K$ esetében a $K(\sqrt[3]{a})$ test tartalmazza például a $\sqrt[3]{a} + \sqrt[3]{a^2}$ elemet, amely ugyancsak harmadfokú elem – de köbe nyilván nem feltétlenül eleme K-nak.

8.2. Felbontási test, algebrai lezárt

A 7.68. tétel arra ad választ, hogy „van-e minden polinomnak gyöke?”. A válasz igenlő, bár azt nem mondja meg, hogy – a matematikában eredetileg felvetett kérdésnek megfelelően – racionális együtthatós polinomoknak van-e gyökük a komplex számtestben. E kérdés algebrailag ekvivalens átírásai azt vetik fel, hogy egy polinomnak van-e annyi gyöke, mint amekkora a foka, illetve van-e minden polinomnak „ugyanott” gyöke? Mielőtt e tételeket pontosan megfogalmaznánk, egy segédtételt bizonyítunk be.

8.6. Tétel. *Legyenek $\varphi_0 : K \to K^*$ és $\psi_0 : K^* \to K$ inverz testizomorfizmusok. Ezeknek létezik pontosan egy $\varphi_1 : K[x] \to K^*[x^*]$ és $\psi_1 : K^*[x^*] \to K[x]$ olyan homomorfizmus kiterjesztése, amelyeknek K-ra, illetve K^*-ra való megszorítása φ_0, illetve ψ_0, továbbá x-et és x^*-ot – megfelelően – felcserélik. Ezek a kiterjesztések izomorfizmusok, egymás inverzei, amelyek irreducibilis polinomnak irreducibilis polinomot feleltetnek meg.*

Ezek a homomorfizmusok egyértelműen kiterjeszthetők a hányadostesteknek egy $\varphi_2 : K(x) \to K^*(x^*)$, illetve $\psi_2 : K^*(x^*) \to K(x)$ homomorfizmusává, amelyeknek $K[x]$-re, illetve $K^*[x^*]$-ra való megszorítása φ_1, illetve ψ_1; továbbá ezek is egymás inverzei.

Ha α az $f \in K[x]$ irreducibilis polinomnak egy gyöke és α^* az $f^* = \varphi_1(f)$ polinom tetszőleges gyöke, akkor létezik ezeknek a homomorfizmusoknak pontosan egy olyan $\varphi_3 : K(\alpha) \to K^*(\alpha^*)$, illetve $\psi_3 : K^*(\alpha^*) \to K(\alpha)$ kiterjesztése, amelyeknek K-ra, illetve K^*-ra való megszorítása φ_0, illetve ψ_0; továbbá α-t és α^*-ot – megfelelően – felcserélik. Ezek is izomorfizmusok és egymás inverzei.

Bizonyítás. Legyenek $\iota : K \to K[x]$, illetve $\iota^* : K^* \to K^*[x^*]$ a megfelelő test elemeinek konstansként való beágyazásai a polinomgyűrűbe. Legyenek $\eta : K[x] \to L = K(x)$, illetve $\eta^* : K^*[x^*] \to L^* = K^*(x^*)$ a polinomgyűrűk természetes beágyazásai a megfelelő hányadostestbe. Feltéve, hogy az egymásnak megfelelő $f(x)$, illetve $f^*(x^*)$ polinomok mindegyike irreducibilis és gyökeik a, illetve a^*, legyenek végül $\alpha : K[x] \to K(a)$, illetve $\alpha^* : K^*[x^*] \to K^*(a^*)$ azok a leképezések, amelyek megfelelően K-t (K^*-ot) identikusan önmagára képezve x-et a-ra (x^*-ot a^*-ra) képezik.

A bizonyítást az alábbi kommutatív diagramokon végezzük:

$$\begin{array}{ccccc} K & \xrightarrow{\varphi_0} & K^* & \xrightarrow{\psi_0} & K \\ \iota\downarrow & & \iota^*\downarrow & & \iota\downarrow \\ K[x] & \xrightarrow{\exists!\varphi_1} & K^*[x^*] & \xrightarrow{\exists!\psi_1} & K[x] \\ \eta\downarrow & & \eta^*\downarrow & & \eta\downarrow \\ L & \xrightarrow{\exists!\varphi_2} & L^* & \xrightarrow{\exists!\psi_2} & L \end{array} \qquad \text{és} \qquad \begin{array}{ccccc} K & \xrightarrow{\varphi_0} & K^* & \xrightarrow{\psi_0} & K \\ \iota\downarrow & & \iota^*\downarrow & & \iota\downarrow \\ K[x] & \xrightarrow{\exists!\varphi_1} & K^*[x^*] & \xrightarrow{\exists!\psi_1} & K[x] \\ \alpha\downarrow & & \alpha^*\downarrow & & \alpha\downarrow \\ K[a] & \xrightarrow{\exists!\varphi_3} & K^*[a^*] & \xrightarrow{\exists!\psi_3} & K[a] \end{array}$$

A $\iota^*\varphi_0 : K \to K^*[x^*]$ és a $\iota\psi_0 : K^* \to K[x]$ homomorfizmusok megszorítása az alaptestre megfelelően φ_0, illetve ψ_0, továbbá az x, illetve x^* határozatlant x^*-ba, illetve x-be viszik. A polinomgyűrűk definiáló tulajdonsága alapján tehát pontosan egy olyan φ_1, illetve ψ_1 létezik, amelyre a fenti (mindkét) diagram első két sora kommutatív lesz. A kommutativitás alapján $\psi_1\varphi_1 : K[x] \to K[x]$ a K elemeit is és az x határozatlant is önmagukba képezi le; pontosan ugyanúgy, mint az identitás. Az unicitás alapján tehát $\psi_1\varphi_1 = 1_{K[x]}$. A szimmetria miatt $\varphi_1\psi_1 = 1_{K^*[x^*]}$ is igaz; így e két homomorfizmus inverz izomorfizmusok.

A diagramok további részét külön tárgyaljuk. Az első diagramnál $\eta : K[x] \to L$, illetve $\eta^* : K^*[x^*] \to L^*$ a hányadostestekbe való természetes beágyazás. Itt $\eta^*\varphi_1 : K[x] \to L^*$, illetve $\eta\psi_1 : K^*[x^*] \to L$ a megfelelő polinomgyűrűknek egy testbe való „hányadostartó” homomorfizmusai. A hányadostest egyértelműsége alapján tehát létezik pontosan egy φ_2, illetve ψ_2 homomorfizmus, ami a diagram második sorát kommutatívvá teszi. Az, hogy ezek egymás inverzei, ugyanazon az elven bizonyítható, mint az első sornál.

A második diagram esetében még meg kell említeni, hogy az izomorfizmusok szorzatot szorzatba visznek: Így felbonthatatlan polinom képe is felbonthatatlan, mert egy izomorfizmus inverze is izomorfizmus. Legyen tehát az $f(x) \in K[x]$ irreducibilis polinom képe az $f^*(x^*) \in K^*[x^*]$ ugyancsak irreducibilis polinom; s ezeknek megfelelően legyen

a, illetve a^* egy-egy gyöke. Legyen továbbá $\alpha : K[x] \to K(a)$, illetve $\alpha^* : K^*[x^*] \to \to K^*(a^*)$ az az úgynevezett kanonikus homomorfizmus, amely K, illetve K^* elemeit fixen hagyja és a határozatlant a-ba, illetve a^*-ba viszi.

Ekkor Ker $(\alpha^*) = (f^*)$, és mivel φ_1 bijektív, ezért Ker $(\alpha^*\varphi_1) = (f)$. Tekintettel arra, hogy az α szürjektív homomorfizmusnak a magja ugyancsak (f), ezért létezik pontosan egy olyan φ_3 homomorfizmus (általános homomorfizmustétel!), amire $\varphi_3\alpha = \alpha^*\varphi_1$, azaz a diagram második sorának első oszlopa is kommutatív. Hasonlóan látható be a második oszlop kommutativitása. Az pedig, hogy φ_2 és ψ_2 egymás inverzei, ugyanazon az alapon következnek, mint az előző pontok analóg állításai. ■

A 8.6. tétel biztosítja, hogy minden (irreducibilis) polinomnak „lényegében egyértelmű" gyöke van. Ez persze nem jelenti azt, hogy egy n-edfokú polinomnak „mindent egybevéve" n gyöke van. Hiszen a bővítés elemeinek az indexezésével újabb és újabb testeket tudunk konstruálni, amelyek mindegyikében van a tekintett polinomnak gyöke. Ha azonban egyetlen bővítésre korlátozzuk a vizsgálatokat, akkor már megváltozik a helyzet.

8.7. Tétel. *A K felett n-edfokú f polinomnak K egy tetszőleges, rögzített M bővítésében legfeljebb n gyöke van. Ha a gyöke az f-nek, akkor létezik olyan egyértelműen meghatározott g polinom, amelyre $f = (x - a)g$ teljesül. Ha $f = (x - a_1) \cdot \ldots \cdot (x - a_n)$, akkor $a_1, \ldots, a_n$ az f összes (nem feltétlenül különböző) gyöke.*

Bizonyítás. Az f polinom legfeljebb annyi irreducibilis tényezőre bontható fel, mint amekkora a foka. Ha az f polinomnak az a gyöke, akkor a maradékos osztás alapján a polinom $f = (x - a)g$ alakú, ahol g az egyértelmű faktorizáció miatt egyértelmű. Ebből következik, hogy irreducibilis polinomnak legfeljebb egy gyöke lehet, ez is csak akkor, ha a polinom elsőfokú. Mivel egy polinom bármely gyöke e polinom valamelyik irreducibilis faktorának is gyöke, ezért a gyökök száma valóban nem lehet nagyobb a polinom fokánál. Az utolsó állítás az előzőekből nyilvánvaló. ■

8.8. Definíció. Legyen $\mathcal{P}$ a $K[x]$ legalább elsőfokú polinomjainak egy halmaza. A $K_\mathcal{P}$ testet az $\mathcal{P}$ felbontási testének nevezzük, ha $K_\mathcal{P}$ felett $\mathcal{P}$ minden eleme lineáris faktorokra bomlik és $K_\mathcal{P}$ a K-nak az $\mathcal{P}$ gyökeivel való bővítéseként áll elő. Ha $\mathcal{P}$ az összes, nemkonstans polinomot tartalmazza, akkor $K_\mathcal{P}$ neve a K algebrai lezártja.

Ha K algebrai lezártja önmaga, akkor K-t algebrailag zártnak nevezzük. □

8.9. Tétel. *$K[x]$ tetszőleges $\mathcal{P}$ nemkonstans polinomokból álló polinomhalmazának létezik felbontási teste, amely egy – a K elemeit fixen hagyó – izomorfizmustól eltekintve egyértelmű. Bármely test algebrai lezártja algebrailag zárt, mégpedig az adott testet tartalmazó legkisebb algebrailag zárt test.*

Bizonyítás. Először azt az esetet nézzük, amikor $\mathcal{P}$-nek egyetlen eleme van. A bizonyítást a testtől függetlenül a polinom fokára vonatkozó teljes indukcióval végezzük. A létezéshez elég annyit bizonyítani, hogy van olyan bővítés, amelyben az adott polinom lineáris faktorokra bomlik, mert ekkor a fellépő gyökök generálta test nyilvánvalóan a polinom felbontási teste lesz. Ha a polinom elsőfokú, akkor az eredeti test megfelel. Tegyük most fel, hogy az állítás igaz minden olyan polinomra, amelynek a foka kisebb, mint n és legyen

$f \in K[x]$ egy n-edfokú polinom. Mivel test feletti polinomgyűrű euklideszi gyűrű, ezért f-nek létezik egy K felett irreducibilis p faktora. A 7.68. tétel szerint létezik olyan $K(a)$ test, hogy a gyöke a p polinomnak. Ekkor a természetesen az f polinomnak is gyöke, amiből azt kapjuk, hogy f felbontható a $K(a)[x]$ polinomgyűrűben $f = (x - a)g$ alakba. Mivel g-nek a foka $n - 1$, ezért $K(a)$-nak az indukciós feltevés alapján van olyan M bővítése, amely felett g csupa elsőfokú tényező szorzatára bomlik. Ebből azonnal következik, hogy $M[x]$-ben f is felbomlik elsőfokú faktorok szorzatára.

Az egyértelműséget is teljes indukcióval bizonyítjuk. Az indukciós lépéshez viszont szükség van arra, hogy valamivel többet bizonyítsunk. Legyen $f \in K[x]$ és legyen $\varphi : K \to K^*$ egy izomorfizmus, amelynek $K[x]$-re való egyértelmű kiterjesztésénél f képe f^*. Ha L az f-nek és L^* az f^*-nak a felbontási teste, akkor van φ-nek olyan L-re való izomorfizmus kiterjesztése, amely f gyökeit (valamilyen sorrendben) f^* gyökeibe képezi. Elsőfokú f esetében most is triviális az állítás. Legyen f foka n és tegyük fel, hogy az állítás minden olyan polinomra igaz, amelynek a foka kisebb, mint n. Legyen $f = pg$, ahol p irreducibilis. A polinomgyűrűre való kiterjesztésnél $f^* = \varphi(pg) = \varphi(p)\varphi(g) = p^*g^*$, ahol p^* a 8.6. tételben látottak alapján ugyancsak irreducubilis. Ugyanezen tételből következik, hogy φ kiterjeszthető egy $\varphi_1 : K(a) \to K^*(a^*)$ izomorfizmusra, ahol a a p-nek és a^* a p^*-nak a gyöke. $K(a)$ felett $f = (x - a)h$ és $f^* = (x^* - a^*)h^*$, ahol $h^* = \varphi_1(h)$. Mivel h foka $n - 1$, a teljes indukciós feltétel szerint φ_1 kiterjeszthető a felbontási testre.

A továbbiakhoz megjegyezzük a következőket. Ha a K test számossága $|K| = \alpha$ és $\beta = \max(\alpha, \aleph_0)$, akkor K tetszőleges L algebrai bővítésére $L \leq \beta$.

Mivel a polinomok véges sorozatokkal adhatók meg, ezért a K feletti legfeljebb n-edfokú polinomok száma legfeljebb β. Mivel egy legfeljebb n-edfokú (nemtriviális) polinomnak legfeljebb n gyöke van, ezért ezek gyöke legfeljebb $n \cdot \beta = \beta$. Így a pontosan n-edfokú algebrai elemek száma is legfeljebb β. Mivel $\aleph_0 \cdot \beta = \beta$, ezért valóban $|L| \leq \beta$.

Legyen β, mint az előbb, és válasszunk egy olyan Ω halmazt, amelyre $|\Omega| = \gamma > \beta$, továbbá Ω tartalmazza a K test K_0 alaphalmazát. Tekintsük ezután a következő feltételeknek eleget tevő L testeket (L alaphalmaza Λ):

(1) L a K-nak algebrai bővítése.

(2) L-et $\mathcal{P}$-beli polinomok bizonyos gyökei halmazának adjungálásával nyerjük.

(3) $K_0 \subseteq \Lambda \subseteq \Omega$.

(4) Az L-beli és a K-beli megfelelő műveleteknek K_0-ra való megszorítása megegyezik.

Az előrebocsátottak szerint $\Lambda \subset \Omega$. Tekintettel arra, hogy egy halmazon csak „korlátozott mennyiségben" értelmezhetünk összeadást és szorzást, ezért a fenti L testek számossága korlátozott; beszélhetünk tehát ezek $\mathcal{L}$ halmazáról. Ezen a halmazon bevezetünk egy részbenrendezést a következőképpen:

$L_1 \leq L_2$ pontosan akkor, ha alaphalmazukra $\Lambda_1 \subseteq \Lambda_2$, továbbá ha L_1 és L_2 megfelelő műveleteit Λ_1-re megszorítjuk, akkor mindig ugyanazokat a függvényeket nyerjük.

A fenti tulajdonságokkal rendelkező testeknek a definiált rendezés szerint növő láncának egyesítése is rendelkezik e tulajdonságokkal; ezért a Zorn-lemma alapján létezik e rendezett halmaznak maximális eleme, legyen ez L_0. Tekintsük az $\mathcal{P}$ polinomhalmaz bármely elemének egy $f(x)$ irreducibilis faktorát. Vegyük az $L^* = L_0[x]/(f(x))$ testnek egy tetszőleges olyan bijektív leképezését Ω-ba, amelynek Λ_0-ra való megszorítása az identitás. Tekintettel arra, hogy $|L^*| \leq \beta < |\Omega| = |\Omega \setminus \Lambda_0|$, ezért ilyen leképezés létezik. Eszerint

$L \leq L^*$. Az L maximalitása miatt csak $L^* = L$ lehetséges, ami azt jelenti, hogy a szóban forgó irreducibilis faktor elsőfokú: tehát L_0 az $\mathcal{P}$ felbontási teste.

Az egyértelműség bizonyítására tekintsünk egy K testet, egy K feletti $\mathcal{P}$ polinomhalmazt és egy $\varphi : K \to K^*$ izomorfizmust. Mint láttuk, φ egyértelműen terjeszthető ki egy $\psi : K[x] \to K^*[x^*]$ izomorfizmussá. Legyen $\mathcal{P}^* = \psi(\mathcal{P})$. Jelölje M, illetve M^* a $\mathcal{P}$, illetve $\mathcal{P}^*$ egy-egy felbontási testét. A kívánt izomorfizmushoz elég bizonyítani, hogy φ kiterjeszthető egy $\overline{\varphi} : M \to M^*$ izomorfizmussá. Evégett tekintsük az összes olyan $(\xi, \mathcal{Q}, L)$ hármast, ahol $K \leq L \leq M$, $\mathcal{Q} \subseteq \mathcal{P}$ és $\xi : L \to M$ a φ-nek egy kiterjesztése. E hármasok halmazát a következőképpen rendezhetjük: $(\xi, \mathcal{Q}, L) \leq (\xi', \mathcal{Q}', L')$, ha $\mathcal{Q} \subseteq \mathcal{Q}'$, $L \leq L'$ és ξ' a ξ-nek a kiterjesztése. Ezáltal egy részbenrendezett halmazt nyertünk. Legyen Λ egy jólrendezett halmaz és tekintsük a fenti hármasoknak egy növő láncát: $(\xi_\lambda, \mathcal{Q}_\lambda, L_\lambda) \leq (\xi_\mu, \mathcal{Q}_\mu, L_\mu)$, ha $\lambda < \mu$ a Λ elemei. Definiáljuk a $(\overline{\xi}, \overline{\mathcal{Q}}, \overline{L})$ hármast a következőképpen. Legyen $\overline{\mathcal{Q}}$ az összes szereplő $\mathcal{Q}_\lambda$ halmaznak, $\overline{L}$ az összes szereplő L_λ testnek az egyesítése. Mivel minden egyes szereplő test esetén az összes olyan homomorfizmus, amelyik az adott testen értelmezve van, ugyanúgy hat, ezért az a $\overline{\xi}$ megfeleltetés, amelyre $a \in L_\lambda$ esetén $\overline{\xi}(a) = \xi_\lambda(a)$, egyértelmű, homomorfizmus és az összes ξ_λ kiterjesztése. Ez azt jelenti, hogy $(\overline{\xi}, \overline{\mathcal{Q}}, \overline{L})$ a fenti növő láncnak felső korlátja. A Zorn-lemma szerint tehát a vizsgált hármasok között van maximális elem. Az egyetlen polinom esetét figyelembe véve e maximális elemben a polinomhalmaz csak $\mathcal{P}$, a test csak M és a homomorfizmus φ-nek egy ψ kiterjesztése lehet. Mivel testhomomorfizmus injektív, ezért $\psi(M)$ felbontási teste $\mathcal{P}^*$-nak. Tekintettel arra, hogy a felbontási testet a gyökök generálják, ezért $\psi(M) = M^*$; amiből a kívánt izomorfizmus is adódik. ■

8.3. Véges testek

A 7.65. tételben láttuk, hogy tetszőleges p prímszámhoz található p elemű test. A 7.66. tételben azt is megmutattuk, hogy ez mindig izomorf egy tetszőleges p karakterisztikájú test prímtestével. A következőkben az összes véges testet meghatározzuk, illetve leírjuk ezek szerkezetét.

A véges testek vizsgálatát különösen fontossá teszi alapvető szerepük az algebrai kódelméletben.

8.10. Tétel. *Véges test elemszáma mindig prímhatvány. Ha $q = p^n$ valamely p prímszámra, akkor létezik q elemű test. Ez a test izomorfizmustól eltekintve egyértelmű: megegyezik $x^q - x$ felbontási testével.*

Legyen k természetes szám, $r = p^k$, ekkor a q elemű testben az $a \to a^r$ megfeleltetés izomorfizmus.

Bizonyítás. Legyen P a véges K test prímteste. Mivel P is csak véges lehet, ezért elemszáma egy p prímszám. K vektortér a P test felett, mondjuk n-dimenziós. E vektortér tetszőleges bázisát rögzítve, az n koordinátatengely mindegyikére a P test p számú eleme közül választhatunk egymástól függetlenül egyet-egyet, ami azt jelenti, hogy K-nak p^n darab eleme van.

Most kimutatjuk, hogy a K testben az $a \to a^r$ megfeleltetés minden $r = p^k$ esetben automorfizmus (k természetes szám).

Tekintsük először a $k = 1$ esetet. Mivel véges testről van szó, ahol a kivonás az összeadással és az osztás a szorzással kifejezhető, ezért elég a leképezés összeg- és szorzattartását bizonyítani. A szorzattartás a hatványozás azonosságaiból következik. Azt kell tehát megmutatni, hogy $a, b \in K$ esetén $(a+b)^p = a^p + b^p$ igaz. A binomiális tétel alapján a bal oldal $\binom{p}{i} a^i b^{p-i}$ alakú tagok összege ($0 \le i \le p$). Tekintettel arra, hogy a $\binom{p}{i}$ binomiális együttható az $i = 0$ és $i = p$ esetben 1, minden más esetben p-vel osztható, ezért ebben az összegben éppen csak a két kívánt tag marad meg, hiszen a test p karakterisztikájú. Ez a megfeleltetés tehát egy $\varphi_1 : K \to K$ homomorfizmus. Mivel φ_1 az egységelemet önmagába viszi, ezért φ_1 magja K-tól különbözik. Tekintettel arra, hogy egy testben csak triviális ideál lehet, ezért a fenti homomorfizmus magja egyedül a 0-ból áll, vagyis e homomorfizmus injektív. A test végessége miatt így szürjektívnek is kell lennie, tehát tényleg izomorfizmust kaptunk. A további esetekben k-ra vonatkozó indukciót használunk. Jelölje φ_r azt a megfeleltetést, amelyik minden elemhez annak a p^r-edik hatványát rendeli. Ha már φ_k-ról tudjuk, hogy automorfizmus, akkor tekintsük a $\varphi_{k+1} = \varphi_1 \cdot \varphi_k$ megfeleltetést, amely – mint két automorfizmus szorzata – szintén automorfizmus. Ekkor

$$\varphi_{k+1}(a) = \varphi_1(\varphi_k(a)) = \varphi_1(a^{p^k}) = (a^{p^k})^p = a^{p^k \cdot p} = a^{p^{k+1}},$$

amivel állításunkat bizonyítottuk.

A felbontási test egyértelműsége alapján az egyértelműséghez elég annak a bizonyítása, hogy K az $x^q - x$ felbontási teste. Mivel K test, ezért a 0 elhagyásával egy multiplikatív csoportot kapunk, amelynek $q - 1$ eleme van. E csoport tetszőleges elemére a Lagrange-tétel alapján fennáll az $a^{q-1} = 1$ összefüggés, illetve ebből következően $a^q = a$ is. Tekintettel arra, hogy ez utóbbi a 0-ra is igaz, ezért K minden eleme gyöke az $x^q - x$ polinomnak. Lévén, hogy e polinomnak bármely testben legfeljebb q gyöke lehet, ezért K felett $x^q - x$ elsőfokú faktorokra bomlik fel. Így a p^n elemű K valóban e polinom felbontási teste.

Legyen végül $q = p^n$, ahol p tetszőleges prímszám, és tekintsük $\mathbb{Q}_p$ felett az $x^q - x$ felbontási testét, legyen ez M. Mint láttuk, e testnek endomorfizmusa a $\psi : a \to a^q$ megfeleltetés, amely endomorfizmus egyedül a 0-t viszi 0-ba. (Mivel véges test véges algebrai bővítése véges, ezért ez automorfizmus, a további gondolatmenetben ezt nem használjuk fel.) Tekintsük ennek a ψ endomorfizmusnak a fixpontjait, azaz azokat az a elemeket, amelyekre $\psi(a) = a$ teljesül. Ha $\psi(a) = a$ és $\psi(b) = b$, akkor az endomorfizmustulajdonságból következik, hogy $\psi(a - b) = \psi(a) - \psi(b)$ és $\psi(a/b) = \psi(a)/\psi(b)$. Ez azt jelenti, hogy a fixpontok egy K résztestet alkotnak. Mivel az $x^q - x$ gyökei és ψ fixpontjai megegyeznek, ezért a vizsgált test éppen ennek a polinomnak gyökeiből áll – tehát q eleme van. ■

8.11. Tétel. *Véges test nemnulla elemeinek multiplikatív csoportja ciklikus.*

Bizonyítás. Jelölje G a p^n elemű test 0-tól különböző elemeinek a multiplikatív csoportját, és legyen s a G csoport exponense. s osztója $(p^n - 1)$-nek, és minden $a \in G$ esetén teljesül az $a^s = 1$ összefüggés. Ez azt jelenti, hogy K minden eleme gyöke az $x^{s+1} - x$

polinomnak, ami csak $s = p^n - 1$ esetén lehetséges. Az 5.56. tétel második állítása szerint a csoportnak van s-edrendű eleme, ami pontosan azt jelenti, hogy G ciklikus. ■

Megjegyzés. A fenti bizonyításban valójában nem azt használtuk ki, hogy véges test elemeiről van szó. Pontosan ugyanígy lehet belátni azt, hogy az $x^n - 1$ polinom gyökei a szorzásra nézve ciklikus csoportot alkotnak. Ez nyilván véges Abel-csoport, amelynek exponense megegyezik a rendjével, ha a test karakterisztikája nem osztója n-nek. Az $n = pk$ esetben az eredeti polinom $(x^k - 1)^p$ alakú és a gyökök éppen az $x^k - 1$ gyökei. Ekkor a gyökök száma kevesebb, mint n; de indukcióval ugyancsak belátható a ciklikusság. □

8.12. Tétel. *A K véges, p karakterisztikájú test bármely a elemére az $x^p - a$ polinomnak egyetlen gyöke van.*

Bizonyítás. Mivel az $x \to x^p$ megfeleltetés a 8.10. tétel szerint bijekció, ezért minden elem pontosan egy b-vel írható b^p alakba. ■

Megjegyzés. A fenti tétel szerint p karakterisztikájú véges testek esetében az $x^p - a$ alakú polinomoknak a gyökei többszörös gyökök, pontosabban e polinomnak egyetlen p-szeres gyöke van. Ezek a polinomok sohasem lehetnek irreducibilisek, mert gyökük a 8.10. tétel alapján a konstans tag egy hatványa. Később azt is fogjuk látni, hogy a többszörös gyök léte a karakterisztikafeltételen múlik. □

A fentiekben a véges testekről feltettük, hogy kommutatívak. Erre azonban nincs szükség WEDDERBURN tétele szerint:

8.13. Tétel. *Minden véges test kommutatív.*

Bizonyítás. Legyen P a véges K test p elemű prímteste és Z a K centruma. Ekkor $|Z| = q$ a p egy hatványa és $|K| = q^n$. Tekintsük ezek K^* és Z^* multiplikatív csoportját. Tudjuk, hogy egy $a \in K^*$ elem konjugáltjainak a száma megegyezik az $N(a)$ indexével, így osztója a K^* rendjének, ami $q - 1$. A konjugáltak száma pontosan akkor 1, ha a centrumelem. Így

$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{|N(a)|}, \quad \text{ahol} \quad a \in (K^* \setminus Z^*). \tag{1}$$

Mivel $\{0\} \cup N(a)$ éppen az összes a-val felcserélhető elem halmaza, így egy test; ezért elemszáma $q^d - 1$ az n egy d valódi osztójával. Eszerint az (1) alatti összeg minden tagja $(q^n - 1)/(q^d - 1)$ alakú. Az $F_n(x)$ n-edik körosztási polinom (l. 8.37. tétel bizonyítása) tulajdonságai alapján tehát $F_n(q)$ e tagok mindegyikének osztója. Mivel $F_n(q)$ osztója az (1) bal oldalán álló számnak is, ezért osztója $(q - 1)$-nek is.

Ebből természetesen következik az $|F_n(q)| < q$ összefüggés. Írjuk fel $F_n(x)$-et szorzat alakban. Ebből az adódik, hogy

$$\left\{ \prod |q - \varepsilon| \;\middle|\; \varepsilon \text{ primitív } n\text{-edik egységgyök} \right\} \leq q - 1. \tag{2}$$

Itt a tényezők száma $\varphi(n)$, és minden egyes tényező abszolút értéke legalább $q - 1 \geq 1$. Ha $n > 2$, akkor létezik egy ε nem valós primitív egységgyök. Ekkor – az $|\varepsilon + \overline{\varepsilon}| < 2$

összefüggés alapján – a bal oldalon álló szorzat legalább $(q-\varepsilon)(q-\overline{\varepsilon}) > q^2 - 2q + 1 = (q-1)^2 \geq q-1$, hiszen $q \geq 2$. Ezért az $n > 2$ eset lehetetlen. Az $n = 2$ esetben (2) bal oldalán $q+1$ áll, ami $\not\leq q$. Eszerint csak az $n = 1$ eset lehetséges, azaz $Z = K$. ■

8.4. Hibajavító kódok

Az információközlés egyik legnagyobb gondja az, hogy a csatorna zajossága miatt az információk egy része útközben elvész. Ez ellen úgy védekeznek, hogy az információkat „túlbiztosítják", azaz úgy változtatják meg (úgy kódolják) az eredeti információt, hogy bizonyos számú hiba esetében is következtetni lehessen az eredeti információra. Ennek egyik legegyszerűbb példája a „paritáskontroll", amikor a nyolcbites (tehát nyolc darab 0 és 1 jegyből álló) sorozatban a nyolcadik bitet úgy teszik oda, hogy az 1-ek száma páros legyen. Ha a meghibásodás valószínűsége igen kicsiny, akkor ezáltal legalább az észrevehető, hogy a kapott „kódszó" hibás. A legprimitívebb módszer az, ha minden jelet páratlan sokszor ismételünk meg és a „felvevő állomáson" azt a jelet fogadjuk el, amelyik „többségben van". Ennek a módszernek igen nagy hátránya az, hogy a hosszú jelek küldése költséges, és a csatorna hosszabb zavara esetén az egész adást meg kell ismételni. (Gondoljunk a műholdakkal való kommunikációra.)

A hibajavításban igen fontos szerepet játszanak az algebrai módszerek. Ezek közül az egyik legelső eljárás az úgynevezett *BCH-kódok* segítségével történik. Itt csak vázoljuk ennek az eljárásnak az elemeit. A felépítésben sem szerepeltetünk tételeket és definíciókat, hanem néhány apróbb lépésre bontva tárgyaljuk az eljárást:

Mindenekelőtt rögzítjük a $K = \mathbb{Q}_2$ testet, ennek az r-edfokú L bővítését és az L multiplikatív csoportjának egy α generátorelemét. (Majdnem hasonló eredmények igazak bármely véges testből kiindulva.)

1. Állítás. *Tegyük fel, hogy a $c(x) \in K[x]$ $(2^r - 1)$-nél alacsonyabb fokú polinomnak $(2d+1)$-nél kevesebb együtthatója különbözhet csak 0-tól, és gyöke az $\alpha, \alpha^2, \ldots, \alpha^{2d}$ elemek mindegyike. Ekkor $c(x)$ a 0 polinom.*

Bizonyítás. Feltehető, hogy a megengedett nemnulla együtthatók száma pontosan $d-1$. Behelyettesítve, az együtthatókra egy homogén lineáris egyenletrendszert kapunk, amelynek mátrixa lényegében egy Vandermonde-mátrix, és így csak triviális megoldás van. ■

2. Állítás. *Legyen $g(x) \in K$ az a minimális fokú polinom, amelynek az $\alpha, \alpha^2, \ldots, \alpha^{2d}$ elemek mindegyike gyöke, és legyen $\mathrm{gr}(g) = k$. Ekkor tetszőleges két különböző $a(x)$ és $b(x)$ legfeljebb $(2^r - k - 2)$-fokú polinomra az $a(x)g(x)$ és $b(x)g(x)$ polinomok együtthatói legalább $2d+1$ helyen különböznek.*

Bizonyítás. Az állítás feltételei szerint az $a(x)g(x) - b(x)g(x)$ polinom foka kisebb, mint $2^r - 1$ és gyöke az $\alpha, \alpha^2, \ldots, \alpha^{2d}$ elemek mindegyike. Az 1. állítás szerint tehát legalább $2d+1$ együtthatója nem nulla, azaz a két polinom együtthatói valóban legalább $2d+1$ helyen eltérnek egymástól. ■

3. Állítás. *A 2. állításban megadott polinom foka legfeljebb* $d \cdot r$.

Bizonyítás. Legyen $g_i(x)$ az α^i minimálpolinomja (K felett). Mivel $(L : K) = r$, ezért $\mathrm{gr}(g_i(x)) \leq r$. $g_i(\alpha^{2i}) = (g_i(\alpha^i))^2 = 0$ miatt $g_{2i}(x) \mid g_i(x)$. Így

$$g(x) = \mathrm{lkkt}(g_1(x), g_3(x), \ldots, g_d(x)).$$

A fokokra tett megjegyzés miatt tehát $g(x)$ foka legfeljebb a tételben megadott lehet. ■

4. Állítás. *Tetszőleges* r *és* $2d+1$ *természetes számokhoz létezik olyan* $2^r - 1$ *hosszúságú bináris kód, amellyel* $2^r - k - 1$ *hosszúságú bináris szavakat (ahol* $k = d \cdot r$*) úgy lehet kódolni, hogy legfeljebb* d *hiba kijavítható.*

Bizonyítás. Feleltessük meg az $\mathbf{a} = (a_0, a_1, \ldots, a_{2^r-k-1})$ kódszónak az $a(x) = a_0 + a_1 x + \cdots + a_{2^r-k-1} x^{2^r-k-1}$ polinomot. A fent vizsgált $g(x)$ polinommal elkészítve az $a(x)g(x)$ polinomot, ennek visszafele megfeleltethetünk egy $\mathbf{a}^*$ kódszót, amelynek a hossza $2^r - 1$. Két ilyen áttranszformált kódszó a 2. állítás szerint legalább d helyen különbözik egymástól. Ha tehát egy kódszóba legfeljebb d hiba került, akkor egyértelműen megkeresheto az eredeti kódszó. ■

Megjegyzések. 1. Ezt az eljárást **B**ose, **C**audhuri és **H**ocquenghem egymástól függetlenül, egyidőben fedezték fel. Innét származik az elnevezés.

2.Könnyen belátható, hogy minden kódszóhoz pontosan egy olyan áttranszformált kódszó található, amely az adottól a legkevesebb helyen tér el (ez esetleg d-nél több is lehet). Az eljárás emellett teljesen automatikusan végezhető, például úgynevezett „siftregiszter" segítségével.

3. Általában az is igaz, hogy a $2d$ számú hiba javítására alkalmas kód azt is kimutatja, ha van $2d + 1$ hiba.

4. A BCH-kódok igen rövid vagy igen hosszú kódszavaknál nem jól alkalmazhatók.

5. Több hiba akkor szokott előfordulni, ha a téren keresztül küldve elektromos üzenetet, valami – például egy villámlás – egy viszonylag hosszabb részt „elront". Ezért sem célszerű a jelek ismétlésével ellenőrizni az üzenetet. A BCH-kódok esetében az „ellenőrző jegyek" egymástól távol jelentkeznek, ami az előző problémát is kiküszöböli.

6. Szemléltető példaként szerepeljen az az eset, amikor $r = 7$. Most a küldhető kódszavak hossza $2^7 - 1 = 127$. Ha a javítandó hibák száma mondjuk $i = 0; 1; 2; 3; 4$, akkor az ellenőrző jegyek száma – megfelelően – $0; 7; 14; 21; 28$, míg az „értékes" küldemény $127; 120; 113; 106; 99$ jegyből áll. Tegyük fel, hogy annak a valószínűsége, hogy egy jegy elromlik, 0,1%. Ekkor annak a valószínűsége, hogy pontosan s hibás jegy van, $\binom{r}{s} \cdot 0{,}999^{r-s} \cdot 0{,}0001^s$. Annak a valószínűsége, hogy több mint t jegy elromlik, úgy kapható meg, hogy ezeket $0 \leq s \leq t$ esetre összeadjuk. Így annak a valószínűsége, hogy a fenti i számnál több hiba van (tehát a módszer rosszul működik), százalékban rendre 11,93222858; 0,73642580; 0,03038419; 0,00093636; 0,00002248.

7. Azzal a módszerrel, hogy minden jegyet háromszor írunk le, $126 \approx 127$ jegyet használva annak a valószínűsége, hogy nem veszünk észre egy hibát, mintegy 0,012819%. Igaz, hogy ez alig rosszabb, mint a BCH-kódnál három hiba felfedezése, de itt az értékes jegyek száma nem 106, hanem csupán 42.

8. A megfelelő $\mathbb{Q}_2$ felett irreducibilis polinomok megtalálása elég nehéz, de ezekre táblázatok állnak rendelkezésre; illetve számítógépet lehet használni. □

8.5. Szeparábilis bővítés, tökéletes test

A véges testeknél látottak alapján felmerül a kérdés: nem lehetséges-e, hogy egy irreducibilis polinomnak többszörös gyöke legyen. Megmutatjuk, hogy ez előfordulhat. Tekintsük a p elemű $\mathbb{Q}_p$ prímtestnek az a transzcendens elemmel való K bővítését. Nézzük az $x^p - a$ polinomot. Ha ennek b gyöke, akkor $x^p - a = (x - b)^p$ következtében e polinomnak többszörös gyökei vannak. Tegyük most fel, hogy e polinom a K felett reducibilis. Ez azt jelenti, hogy $(x - b)$-nek már egy, a p-nél alacsonyabb kitevőjű hatványa is K-beli együtthatós polinom. Figyelembe véve, hogy egy prímszám minden nála kisebb természetes számhoz relatív prím, a fentiekből könnyen belátható, hogy $(x - b)$-nek is K-beli együtthatósnak kell lennie. Eszerint volna olyan $\mathbb{Q}_p$-beli együtthatós $u(x)$ és $v(x)$ polinom, amelyekre $(u(a)/v(a))^p = a$ teljesülne. Ez az $(u(a))^p = a \cdot (v(a))^p$ egyenlőséghez vezetne, amelyből a 7.68. tétel szerint az $(u(x))^p = x \cdot (v(x))^p$ összefüggés következne. Ez pedig lehetetlen, mert a bal oldalon álló polinom foka p-vel osztható, a jobb oldalon állóé pedig nem.

8.14. Definíció. A K test feletti $f(x)$ polinomot szeparábilisnek nevezzük, ha nincsenek többszörös gyökei (K egyetlen bővítésében sem). A K felett algebrai a elemet a K fölött szeparábilisnek nevezzük, ha az a elem főpolinomjának nincsenek többszörös gyökei (tehát e polinom szeparábilis). A K test egy L algebrai bővítését szeparábilisnak nevezzük, ha L minden eleme szeparábilis K felett. Ha egy K testnek minden egyszerű algebrai bővítése szeparábilis, akkor K tökéletes test. □

8.15. Tétel. *Minden nullkarakterisztikájú és minden véges test tökéletes.*

Bizonyítás. Az elemi algebrában a derivált polinom definíciójában sehol sem használtuk ki, hogy az együtthatókat számtestből vettük. Így általában érvényes az a tétel is, hogy egy K test felett irreducibilis f polinomnak pontosan akkor van többszörös gyöke, ha deriváltjával vett legnagyobb közös osztója 1-től különbözik. Az f irreducibilitása miatt ez csak akkor lehet, ha az f deriváltja 0. Nullkarakterisztikájú test esetén ez nyilván lehetetlen; elegendő tehát a prímkarakterisztika esetét (vagyis a véges testeket) vizsgálni. A derivált csak akkor lehet 0, ha f-ben csak olyan tagok lépnek fel, amelynek a kitevői oszthatók p-vel, azaz f felírható $g(x^p)$ alakban. Nézzük most a $g = a_0 + \cdots + a_r x^r$ polinomot. A 8.12. tétel alapján minden szóba jövő i-re létezik pontosan egy olyan b_i, amely kielégíti az $a_i = (b_i)^p$ feltételt. Ekkor a K-beli együtthatós $h = b_0 + \cdots + b_r x^r$ polinomra nyilvánvalóan érvényes az $f = h^p$ összefüggés, ami ellentmond az f irreducibilitásának. ■

8.16. Tétel. *Tökéletes test algebrai bővítése is tökéletes.*

Bizonyítás. Legyen L a K tökéletes test algebrai bővítése és legyen a algebrai elem az L felett. A 8.4. tétel szerint a algebrai a K test felett is. Legyen f, illetve g az a elem főpolinomja az L, illetve a K test felett. Ebből következik, hogy f osztója g-nek. Mivel K tökéletes, ezért g-nek nincsenek többszörös gyökei; és így f-nek sem lehetnek. ■

8.17. Tétel. *Legyenek $a_1, \ldots, a_n$ algebrai elemek a K felett, amelyek között legfeljebb egy nem szeparábilis. Ekkor a $K(a_1, \ldots, a_n)$ bővítés egyszerű. Speciálisan tökéletes test véges algebrai bővítése egyszerű algebrai bővítés.*

Bizonyítás. Legyen először K véges, elemszáma q, és legyen az a_i elem foka k_i. Ekkor a 8.1. és a 8.2. tételek alapján a $K(a_1, \ldots, a_n)$ bővítés elemszáma q^k, ahol $k = k_1 + \ldots + k_n$. Ezért $K(a_1, \ldots, a_n)$ véges. Véges test multiplikatív csoportja a 8.11. tétel szerint ciklikus; a bővítés tehát egyszerű. Ezért a továbbiakban feltehető, hogy K végtelen.

Az $n = 1$ eset triviális. Legyen $n = 2$. Legyenek a és b algebrai elemek a K végtelen test felett, és legyen ezeknek főpolinomja – megfelelően – f és g. Legyen L az fg felbontási teste, és legyenek ebben f, illetve g gyökei $a_1(= a), \ldots, a_n$, illetve $b_1(= b), \ldots, b_k$. Tegyük fel továbbá, hogy b szeparábilis. Ez azt jelenti, hogy a $b_1, \ldots, b_k$ elemek különbözőek. (Az lehetséges, hogy valamelyik a_i megegyezik valamelyik a_j-vel vagy b_j-vel.)

Készítsük el minden szóba jövő i, j párra ($i \neq 1, j \neq 1$) az $(a_1 - a_i)/(b_j - b_1)$ elemeket. Feltétel szerint ezek a hányadosok léteznek és számuk nyilvánvalóan véges. A K végtelensége miatt létezik tehát olyan $u \in K$, amely ezektől különbözik. Ez azt jelenti, hogy az L-beli $c = a + ub(= a_1 + ub_1)$ elem minden szóba jövő $a_i + ub_j$ elemtől különbözik.

Azt fogjuk megmutatni, hogy $K(a, b) = K(c)$.

$c \in K(a, b)$ miatt $K(c) \leq K(a, b)$ nyilvánvalóan igaz. Nézzük meg b-nek a $K(c)$ feletti főpolinomját. b eleve gyöke a $g(x)$ polinomnak, amelynek együtthatói $K(c)$-ben vannak, hiszen K minden eleme $K(c)$-ben van. Másrészt b gyöke az $f(c - ux) = h(x)$ polinomnak is, mert $h(b) = f(c - ub) = f(a) = 0$. Mivel $f(x)$ együtthatói is és c, valamint u is $K(c)$-beliek, ezért $h(x)$ is $K(c)$-beli együtthatós polinom. Ez azt jelenti, hogy $x - b$ mindkét polinomnak faktora. Kimutatjuk, hogy több közös faktoruk nincs is. Valóban, ha tekintjük ezek bármely közös faktorát, ez – mint a $g(x)$ egy faktora – előáll $x - b_j$ alakú elemek szorzataként ($1 \leq j \leq k$). Mivel a b_j elemek mind különbözőek, ez azt jelenti, hogy a közös tényezőkben levő minden egyes b_j gyöke $h(x)$-nek is, azaz $0 = h(b_j) = f(c - ub_j)$. Az $f(x)$ polinomnak minden egyes gyöke az a_i-k közül való, a kapott összefüggés tehát azt jelenti, hogy valamely szóba jövő i-re $a_i = c - ub_j$, azaz $c = a_i + ub_j$ teljesül. Az u választása szerint ez csak akkor lehet, ha $i = j = 1$, azaz $x - b$ a két polinom egyetlen közös (normált) faktora. Így $x - b$ e polinomok legnagyobb közös osztója; s mivel a legnagyobb közös osztó együtthatói ugyanabban a testben vannak, mint az eredeti polinomok együtthatói, ezért $x - b$ is $K(c)$-beli együtthatós. Eszerint $b \in K(c)$, amiből már $a = c - ub \in K(c)$ is azonnal következik. Tehát $K(a, b) \subseteq K(c)$ is igaz.

Az $n > 2$ esetben teljes indukcióval bizonyítunk. Tegyük fel, hogy az a_n szeparábilis. Mivel az első $n-1$ elem között legfeljebb egy nem szeparábilis, ezért az indukciós feltevés szerint az ezekkel való bővítés egyszerű. Az a_n szeparábilitását és az $n = 2$ esetet használva kapjuk, hogy az egész bővítés egyszerű.

Mivel tökéletes test esetében minden elem szeparábilis, ezért a most bizonyítottak szerint következik az állítás. ■

8.18. Tétel. *A $K \subseteq L$ testek közötti testek száma akkor és csak akkor véges, ha L a K-nak egyszerű algebrai bővítése.*

Bizonyítás. Legyen $L = K(\vartheta)$ és $f(x) \in K[x]$ a ϑ minimálpolinomja. Tetszőleges M közbülső test (tehát $K \subseteq M \subseteq L$) esetén legyen $f_M(x) \in M[x]$ a ϑ minimálpolinomja M felett ($f_L(x) = f(x)$). $M \subseteq N$ esetén $f_N(x) \mid f_M(x)$. Mivel $f(x)$-nek csak véges sok osztója van, ezért csak véges sok minimálpolinom jöhet szóba. Tegyük fel, hogy ϑ-nak az M és N testek feletti minimálpolinomja ($g(x)$) megegyezik. $g(x) \in M[x] \cap N[x] = (M \cap N)[x]$ alapján $g(x)$ $M \cap N$ felett is a ϑ minimálpolinomja; hiszen reducibilitása

esetén $g(x)$ mindkét közbülső test felett is reducibilis volna. A testfokokra vonatkozó tételek szerint ez csak úgy lehet, ha mindhárom közbülső test megegyezik. Így a közbülső testek száma nem lehet több, mint $f(x)$ faktorainak a száma; azaz véges sok közbülső test van.

Tegyük most fel, hogy a közbülső testek száma véges. Ekkor a bővítés biztosan algebrai, mert egy τ transzcendens elemmel való bővítés esetén – mint láttuk – a $K(\tau) \supset \supset K(\tau^2) \supset \cdots \supset K(\tau^n) \supset \cdots$ egy valódi csökkenő – tehát végtelen – testláncot ad.

Ha K véges, akkor a közbülső testek számának a végessége miatt L is véges, ezért az állítás igaz. Mivel a közbülső testek száma véges, ezért létezik L-ben egy maximális egyszerű bővítés; legyen ez $K(\vartheta)$ (persze $\vartheta \neq 0$). Legyen $\eta \neq 0$ az L tetszőleges eleme. Tekintsük a $\vartheta + u \cdot \eta$ elemeket, ahol u a K elemein fut végig. Mivel K végtelen, de a közbülső testek száma véges, ezért léteznek olyan $u, v \in K$, amelyekre $M = K(\vartheta + u \cdot \eta) = K(\vartheta + v \cdot \eta)$ ugyanaz a közbülső test. M-ben nyilván benne van a két generátorelem, így ezek különbségének $(u - v)$-edrésze: η, és így ϑ is $(u - v \neq 0)$. Ez egy egyszerű bővítés, a $K(\vartheta)$ maximalitása miatt tehát ezzel megegyezik; és így ez az egyszerű bővítés L minden elemét tartalmazza, tehát tényleg egyszerű bővítéssel állunk szemben. ■

8.19. Következmény. *Egyszerű (algebrai) bővítés esetén minden közbülső test is egyszerű (algebrai) bővítés.*

Bizonyítás. Az algebrai bővítés esete a tételnek azonnali folyománya; míg az általános eset a transzcendens bővítésekre vonatkozó Lüroth-tétel (8.25. tétel) figyelembevételével fog azonnal adódni. ■

Most az algebrai bővítések vizsgálatát megszakítva a transzcendens bővítések néhány alapvető tulajdonságát fogjuk megvizsgálni.

8.6. Transzcendens bővítések

A $K[x]$ polinomgyűrű $K(x)$ hányadosteste a K testnek nyilvánvalóan transzcendens bővítése. Ha ezt az $y = \sqrt{x}$ elemmel tovább bővítjük, akkor a $K(x, y) = K(y)$ testet kapjuk, amelyik „szerkezetében” nem különbözik a $K(x)$ testtől. Ha viszont y is határozatlan, akkor a kapott $K(x, y)$ test szerkezete egészen másmilyen lesz. Az eltérés pontos megfogalmazásához az úgynevezett algebrai függésre van szükségünk. Ez – legalábbis alaptulajdonságait tekintve – hasonlít a lineáris függéshez.

8.20. Definíció. Legyenek $u, u_1, \ldots, u_n$ a K test egy L bővítésének elemei. Azt mondjuk, hogy u algebrailag függ az $\{u_1, \ldots, u_n\}$ halmaztól, ha u algebrai $K(u_1, \ldots, u_n)$ felett. □

Az alábbiakban a K testet rögzítjük, és e fölötti algebrai függésről beszélünk.

1. Alaptétel. *Minden elem algebrailag függ egy őt tartalmazó halmaztól.* ■

2. Alaptétel. *Ha u algebrailag függ $\{u_1, \ldots, u_n, v\}$-től, de $\{u_1, \ldots, u_n\}$-től nem függ algebrailag, akkor v algebrailag függ $\{u, u_1, \ldots, u_n\}$-től.*

Bizonyítás. Nyilván eleve feltehetjük, hogy $u_1, \ldots, u_n \in K$. Ekkor feltételünk azt mondja ki, hogy u gyöke egy $K(v)$-beli együtthatós polinomnak, amelynek együtthatói nem mind K-beliek. Az u behelyettesítése után kapott polinomot v hatványai szerint rendezve egy olyan polinomhoz jutunk, amelynek együtthatói $K(u)$-ban vannak. ■

3. Alaptétel. *Ha u algebrailag függ $v_1, \ldots, v_k$-tól, melyek algebrailag függnek $w_1, \ldots, w_n$-től, akkor u algebrailag függ $w_1, \ldots, w_n$-től.*

Bizonyítás. Azonnal következik abból, hogy algebrai bővítés algebrai bővítése ismét algebrai bővítés. ■

8.21. Definíció. Az L test $u_1, \ldots, u_r$ elemeit algebrailag összefüggőknek nevezzük, ha van olyan $f(x_1, \ldots, x_r) \in K[x_1, \ldots, x_r]$ polinom, amelyre $f(u_1, \ldots, u_r) = 0$. □

8.22. Tétel. *Az $u_1, \ldots, u_r$ elemek akkor és csak akkor összefüggők, ha ezek valamelyike a többitől függ.*

Bizonyítás. Ha például u_1 a többitől függ, akkor egy $K(u_2, \ldots, u_r)$-beli együtthatós polinomnak a gyöke. Itt minden egyes u_i elem helyébe az x_i határozatlant írva egy olyan – nemtriviális – polinomot kapunk, amelynek a fenti $(u_1, \ldots, u_r)$ vektor gyöke.

Fordítva, ha egy ilyen polinomunk van, akkor ez legalább az egyik határozatlanban nem triviális; és az ennek megfelelő u_i elem algebrailag függ a többitől. ■

Azt is definiálhatjuk, hogy egy elem algebrailag függ egy végtelen halmaztól; ami azt jelenti, hogy e végtelen halmaznak van olyan véges részhalmaza, amelytől a kiszemelt elem függ. Végtelen részhalmaz algebrai összefüggése azt jelenti, hogy van egy véges algebrailag összefüggő részhalmaza.

Észrevehetjük, hogy a függésre és összefüggésre bizonyított tételek pontosan ugyanolyanok, mint a lineáris összefüggésre vonatkozóak; csupán lineáris helyébe mindig algebrait kell mondani. Ennek megfelelően érvényes a kicserélési tétel, az összes következményével együtt.

Ha $L|K$ véges sok elemmel történő bővítés, akkor L-ben a K felett algebrailag független elemek maximális száma csak az L-től függ. Ezt a számot az L test K feletti *transzcendenciafokának* nevezzük. Egy K feletti maximális független rendszert pedig *transzcendenciabázisnak*. Ezt végtelen bővítésre is általánosíthatjuk, amikor azt kapjuk, hogy a transzcendenciabázisok halmazának a számossága megegyezik.

Könnyen belátható, hogy ha L-nek K feletti transzcendenciafoka nagyobb, mint K számossága, akkor L számossága megegyezik e transzcendenciafokkal. Ez speciálisan azt jelenti, hogy a valós számtestnek a racionális számtest feletti transzcendenciafoka kontinuum. Másképpen fogalmazva létezik a valós számtestnek egy kontinuum számosságú transzcendenciabázisa a racionális számtest felett.

Tekintsünk most a K test felett algebrailag független $u_1, \ldots, u_n$ elemeket és az $x_1, \ldots, x_n$ határozatlanokat. Az algebrai függetlenség miatt az a $\varphi : K[x_1, \ldots, x_n] \to$ $\to K[u_1, \ldots, u_n]$ homomorfizmus, amely K-t elemenként fixen hagyja és minden egyes x_i-t a megfelelő u_i-be visz, feltétlenül injektív. Mivel φ nyilván szürjektív is, ezért ez egy izomorfizmus. Ez az izomorfizmus egyértelműen kiterjeszthető a két hányadostestre:

$K(x_1, \ldots, x_n) \cong K(u_1, \ldots, u_n)$. Eszerint „ezek" a bővítések egyértelműen meghatározottak a transzcendenciafokkal. Most megmondjuk, mi az, hogy „ezek".

Ha az M halmaz K felett algebrailag független, akkor a $K(M)$ bővítést *tiszta transzcendens bővítésnek* nevezzük.

8.23. Tétel. *Ha L a K-nak bővítése, akkor létezik olyan $K \subseteq M \subseteq L$ közbülső test, amelyre M a K-nak tiszta transzcendens bővítése, L pedig algebrai bővítése M-nek.*

Bizonyítás. Legyen $\mathfrak{M}$ L-nek egy K feletti transzcendenciabázisa. Ekkor $M = K(\mathfrak{M})$ nyilván megfelel a feltételeknek. ■

Könnyen belátható az alábbi tétel:

Ha M-nek K feletti transzcendenciafoka n és L-nek M feletti transzcendenciafoka k, akkor L-nek K feletti transzcendenciafoka $n + k$.

Most az egyszerű transzcendens bővítések szerkezetének a vizsgálatára térünk rá.

8.24. Tétel. *Legyen a a K test felett transzcendens elem és $b = f(a)/g(a) \in K(a)$, ahol $f(x), g(x) \in K[x]$ relatív prím polinomok. Ekkor vagy $b \in K$, vagy b transzcendens K felett, és ez utóbbi esetben a algebrai $K(b)$ felett. Ha $n = \max(\mathrm{gr}(f(x)), \mathrm{gr}(g(x))) \neq 0$, akkor $(K(a) : K(b)) = n$. Az n számot a b fokának nevezzük és* $\mathrm{gr}(b)$*-vel jelöljük.*

Bizonyítás. Tegyük fel, hogy $b \notin K$. Az a elem gyöke a $K(b)$-beli együtthatós $h(x) = f(x) - b \cdot g(x)$ polinomnak, amelynek nem lehet minden együtthatója 0 (mert különben $b \in K$ volna). Így a algebrai $K(b)$ felett. Ebből azonnal adódik, hogy b transzcendens K felett, mert egyébként a is algebrai volna K felett. Abból viszont, hogy b transzcendens K felett, azonnal következik, hogy $\mathrm{gr}(h(x)) = n$. Mivel b transzcendens K felett, ezért $h(x)$-nek $K(b)$ feletti irreducibilitása ekvivalens $h(x, y) = f(x) - y \cdot g(x)$ K feletti irreducibilitásával. Mivel $h(x, y)$ az y-ban elsőfokú, ezért csak úgy bontható fel, ha valamelyik tényezője y-ban konstans, és ez ekkor $f(x)$-nek is és $g(x)$-nek is osztója. Mivel e két polinom relatív prím, ezért ez a faktor csak konstans lehet; ami $h(x)$ irreducibilitását bizonyítja. ■

Három következményt mondunk ki:

1. b foka csak a $K(b)$ és $K(a)$ testektől függ, nem $K(a)$ speciálisan választott generátorelemétől.

2. $K(b) = K(a)$ pontosan akkor teljesül, ha $\mathrm{gr}(b) = 1$, azaz ha b az a-nak „tört-lineáris" kifejezése.

3. A $K(a)$-nak a K-t fixen hagyó automorfizmusai a-t ismét $K(a)$ egy generátorelemébe kell, hogy vigyék. Ezek az úgynevezett *relatív automorfizmusok* tehát pontosan az

$$x \mapsto \frac{ax + b}{cx + d} \qquad ad - bc \neq 0, \quad a, b, c, d \in K$$

alakú helyettesítések.

8.25. Tétel (Lüroth)**.** *Legyen a transzcendens a K test felett, és L olyan test, amelyre $K \subset L \subseteq K(a)$ teljesül. Ekkor van olyan K felett transzcendens c, amire $L = K(c)$.*

Bizonyítás. Feltételünk szerint van olyan $b \in L$, amely nincs K-ban. Így b transzcendens K felett és a algebrai $K(b)$ felett. $K(b) \subseteq L \subseteq K(a)$ miatt tehát a algebrai L felett is. Léteznek tehát olyan L-beli $c_0, c_1, \ldots, c_{n-1}$ elemek, hogy a gyöke az

$$f(y) = c_0 + c_1 y + \cdots + c_{n-1} y^{n-1} + y^n \in L[y]$$

irreducibilis polinomnak. Ekkor vannak olyan $c_i(x), d_i(x) \in K[x]$ páronként relatív prím polinomok ($i = 0, 1, \ldots, n-1$), hogy $c_i = c_i(a)/d_i(a)$.

Mivel a nem algebrai K felett, ezért legalább egy $c = c_j$ nem eleme K-nak, amiből következik, hogy a $g(x) = c_j(x)$ és $h(x) = d_j(x)$ polinomok valamelyike nem a 0 polinom. Mivel $c \in L$, ezért a $g(a) = c \cdot h(a)$ egyenlőség alapján a gyöke az ugyancsak L-beli együtthatós $g(y) - c \cdot h(y)$ polinomnak is ($c \notin K$ miatt ez a polinom nem $K[y]$-beli). Az $f(y)$ polinom irreducibilitásából következik, hogy osztója ennek a polinomnak, azaz van olyan $u(y) \in L[y]$ polinom, amelyre $g(y) - c \cdot h(y) = u(y) \cdot f(y)$. $L \leq K(a)$ miatt $u(y)$ felírható $u(a, y)$ alakban, ahol $u(x, y) = (a(x)/b(x)) \cdot v(x, y)$ relatív prím $a(x), b(x) \in K[x]$ és $K[x]$ felett primitív $v(x, y)$ polinomokkal. Tekintsük most az

$$F(x, y) = \frac{c_0(x)}{d_0(x)} + \frac{c_1(x)}{d_1(x)} y + \cdots + \frac{c_{n-1}(x)}{d_{n-1}(x)} y^{n-1} + y^n \in K(x)[y]$$

polinomot. Mivel $K[x]$-ben érvényes az egyértelmű faktorizáció, ezért e polinom

$$F(x, y) = \frac{c(x)}{d(x)} \cdot p(x, y)$$

alakba írható, ahol

$$p(x, y) = p_0(x) + p_1(x) y + \cdots + p_{n-1}(x) y^{n-1} + p_n(x) y^n$$

az y-nak $K[x]$ feletti primitív polinomja, azaz a p_i polinomoknak sincs nemkonstans közös osztójuk; továbbá $c(x)$ és $d(x)$ is relatív prímek. Emellett $d(x)$ osztója a d_i polinomok legkisebb közös többesének. Jelölje k az $f(x, y)$ fokát x-ben. A primitív polinom „elkészítéséből" következik, hogy $g(x)$-nek és $h(x)$-nek a foka sem lehet k-nál nagyobb.

A $g(y) - c \cdot h(y)$, $c = g(x)/h(x)$ és $f(y) = F(a, y)$ összefüggésekből az a transzcendenciája alapján azt kapjuk, hogy

$$(b(x) \cdot d(x)) \cdot (h(x) \cdot g(y) - g(x) \cdot h(y)) = (a(x) \cdot c(x)) \cdot (v(x, y) \cdot p(x, y)).$$

A primitív polinomok szorzatára vonatkozó tétel alapján a bal oldalt osztó $(b(x) \cdot d(x))$ tényező relatív prím a $(v(x, y) \cdot p(x, y))$ szorzathoz, így osztója az $(a(x) \cdot c(x))$ szorzatnak. Egyszerűsítve a

$$h(x) \cdot g(y) - g(x) \cdot h(y) = t(x) \cdot (v(x, y) \cdot p(x, y))$$

egyenlőséget kapjuk. Tekintettel arra, hogy $h(x)$ és $g(x)$ relatív prímek, ezért $t(x)$ konstans, azaz $v(x, y)$ helyébe megfelelő konstansszorosát írva:

$$h(x) \cdot g(y) - g(x) \cdot h(y) = v(x, y) \cdot p(x, y).$$

Itt a bal oldal x-ben legfeljebb k-adfokú, míg a jobb oldalon már $p(x, y)$ pontosan k-adfokú x-ben. Eszerint $v(x, y)$ az x-től független. A bal oldalon viszont nem létezhet csak y-tól függő faktor, hiszen $g(y)$ és $h(y)$ relatív prímek. Ezért $v(x, y) \in K$. Tekintettel arra, hogy a bal oldal x-ben és y-ban szimmetrikus, ezért $p(x, y)$ y-ban is k-adfokú. Végeredményben azt kaptuk, hogy $n = k$, és $\mathrm{gr}(c) = k$ is igaz. Mármost, a kapott

$$(K(a) : K(c)) = (K(a) : L) \cdot (L : K(c)), \qquad (K(a) : K(c)) = (K(a) : L) = n$$

feltételekből azonnal következik $L = K(c)$. ∎

Megjegyzés. E tételnek az alábbi fontos következménye van: Legyen az n-dimenziós tér egy görbéje *racionálisan parametrizált*, azaz a görbe bármely $(\xi_1, \dots, \xi_n)$ pontja előállítható $\xi_1 = f_1(t), \dots$ $\dots, \xi_n = f_n(t)$ alakban, ahol az $f_i(t)$-k racionális törtkifejezések. (Itt és a továbbiakban mindig megengedünk véges sok kivételt.)

Lehetséges, hogy az előállítás túl „bonyolult" és különböző t értékekhez ugyanazok a pontok tartoznak (például ilyen a $(t^2, t^2 + 1, 1/t^2 + 2)$ parametrizálás). Lüroth tétele ekkor lehetőséget ad ennek egyszerűsítésére.

Tekintsük ugyanis K felett a $K(t)$ test $f_1(t), \dots, f_n(t)$ elemei által generált L testet. Ennek t' generátorelemére egyrészt az igaz, hogy $f_i(t) \in K(t')$ alapján $\xi_i = g_i(t')$ ismét az eredeti térgörbe parametrizálása; másrészt létezik olyan n-határozatlanú $\Phi(x_1, \dots, x_n)$ racionális törtkifejezés, amire

$$t' = \Phi(f_1(t), \dots, f_n(t)) = \Phi(\xi_1, \dots, \xi_n)$$

teljesül. Eszerint a $(\xi_1, \dots, \xi_n)$ pont egyértelműen meghatározza a paramétert; tehát valójában egy egyszerűbb parametrizálást kaptunk. □

Feladatok

1. Mutassuk meg, hogy $\sqrt[3]{2} + \sqrt[3]{4} \notin \mathbb{Q}$.

2. Legyen $(K(\alpha) : K) = n$ és $(K(\beta) : K) = k$. Milyen értékeket vehet fel $(K(\alpha, \beta) : K)$ és $(K(\alpha + \beta) : K)$?

3. Legyen $(K(\alpha) : K) = 3$. Bizonyítsuk be, hogy K-nak van olyan L bővítése, amely felett minden másodfokú polinom reducibilis, de $(L(\alpha) : L) = 3$. Általánosítsuk a feladatot.

4. Bizonyítsuk be, hogy bármely nem-0 $c \in \mathbb{K}$ esetén $\mathbb{Q}(\sqrt{2} + c \cdot \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Általánosítsuk a feladatot.

5. Bizonyítsuk be, hogy minden véges nullosztómentes gyűrű kommutatív.

6. Bizonyítsuk be, hogy bármely olyan $f(x) \in \mathbb{Q}_p[x]$ polinomhoz, amelynek nincs többszörös faktora $\mathbb{Q}_p[x]$-ben, van olyan $n > 1$ természetes szám, hogy $f(x)$ osztja az $x^n - 1$ polinomot.

7. Adjunk olyan p karakterisztikájú testet, amelynek a $\varphi : a \mapsto a^p$ endomorfizmus nem automorfizmusa. Bizonyítsuk be, hogy van egy olyan maximális p karakterisztikájú test, amelyben φ minden résztestnek automorfizmusa.

8. Bizonyítsuk be, hogy véges test felett minden algebrai elem egységgyök.

9. Legyen K véges test. Bizonyítsuk be, hogy ha q olyan prímszám, amely osztja a $|K| - 1$ számot, akkor van olyan $a \in K$ elem, amelyre $x^q - a$ irreducibilis K felett.

10. Határozzuk meg az n-edik primitív egységgyökök fokát $\mathbb{Q}_p$ felett.

11. Legyen α a K véges test felett irreducibilis $f(x)$ polinom egy gyöke. Bizonyítsuk be, hogy $K(\alpha)$ az $f(x)$ felbontási teste.

12. Legyenek $f(x)$ és $g(x)$ irreducibilis polinomok a K véges test felett. Bizonyítsuk be, hogy felbontási testük „kapcsolata" csak a fokuk viszonyától függ.

13. Jelölje $\varphi_p(n)$ a $\mathbb{Q}_p$ felett n-edfokú elemek számát. Bizonyítsuk be, hogy $\varphi_p(n) = \sum \mu\left(\frac{n}{d}\right) \cdot p^d$, ahol d az n osztóin fut végig és μ a Möbius-függvény. Bizonyítsuk be, hogy n osztója $\varphi_p(n)$-nek. Mit ad meg a $\varphi_p(n)/n$ szám?

14. „Bizonyítsuk be” (tehát ne csupán számoljuk ki), hogy $x^7 + x + 1$ irreducibilis $\mathbb{Q}_2$ felett.

15. Legyen $p = (K : \mathbb{Q}_2)$ prímszám. Bizonyítsuk be, hogy pontosan akkor lesz $K \setminus \mathbb{Q}_2$ minden eleme a K^* multiplikatív csoport generátoreleme, ha $2^p - 1$ is prímszám. Mutassuk meg, hogy ha $\mathbb{Q}_2$ helyett $\mathbb{Q}_q$ szerepel ($q \notin \{2, p\}$), akkor a bővítésben mindig van olyan elem, amelyik nem generálja a ciklikus csoportot.

16. Legyen α a $\mathbb{Q}_2$ test n-edfokú bővítése multiplikatív csoportjának egy generátoreleme; továbbá p egy páratlan prímszám. Bizonyítsuk be, hogy α^p foka pontosan akkor kisebb, mint n, ha $n = k \cdot \ell$ alakú, és $p = (2^k)^{\ell-1} + \cdots + 2^k + 1$.

17. Készítsünk olyan hibajavító kódot, amelynél az átkódolt szó hossza 15 bit és kettő, illetve három hibát lehet vele javítani.

18. Legyen $\varphi : a \to a^p$ a $\mathbb{Q}_p$ felett p-edfokú K test úgynevezett *Frobenius-automorfizmusa* és ι az identikus automorfizmus. Bizonyítsuk be, hogy $\eta = \varphi - \iota$ a K-nak mint $\mathbb{Q}_p$ feletti vektortérnek endomorfizmusa, amelynek magja $\mathbb{Q}_p$, továbbá $\eta^n \neq 0$, ha $n < p$, de $\eta^p = 0$.

19. Legyen $(K : \mathbb{Q}_p) = p$. Tudjuk, hogy ez a bővítés nem generálható egy $x^p - a$ ($a \in \mathbb{Q}_p$) alakú polinom gyökével, hiszen minden ilyen polinom azonos lineáris faktorokra bomlik. Bizonyítsuk be, hogy van viszont olyan $a \in \mathbb{Q}_p$, amire $x^p - x - a$ irreducibilis, tehát gyöke generálja K-t.

20. Határozzuk meg az alábbi számok $\mathbb{Q}$ feletti fokát:

a) $\sqrt{2} + \sqrt{3}$, b) $\sqrt{5 + 2\sqrt{6}}$, c) $\sqrt{5 + 2\sqrt{6}} + \sqrt{6}$,

d) $\sqrt{2} + \sqrt{3} + \sqrt{6}$, e) $\sqrt{5 + 2\sqrt{6}} + \sqrt{7}$, f) $\sqrt{2} + \sqrt[3]{2}$, g) $\sqrt{2} + \sqrt[3]{1 + \sqrt{2}}$.

21. Legyen $x^2 - a$ irreducibilis a K test felett. Bizonyítsuk be, hogy ha $x^2 - b$ reducibilis $K(\sqrt{a})$ felett, de irreducibilis K felett, akkor van olyan $c \in K$, amire $b = a \cdot c^2$.

22. Bizonyítsuk be, hogy a K test felett algebrai a elem akkor és csak akkor *inszeparábilis* (=nem szeparábilis), ha K karakterisztikája egy p prímszám, a-nak az $f(x)$ főpolinomja $g(x^p)$ alakú; egy ilyen polinom pontosan akkor irreducibilis, ha nem minden együtthatója p-edik hatvány K-ban.

23. Bizonyítsuk be, hogy egy $p(> 0)$ karakterisztikájú K test feletti a elem akkor és csak akkor szeparábilis, ha $K(a^p) = K(a)$.

24. Bizonyítsuk be, hogy egy szeparábilis bővítés felett szeparábilis elem az eredeti test felett is szeparábilis.

25. Bizonyítsuk be, hogy egy elemhalmazzal való (algebrai) bővítés pontosan akkor szeparábilis, ha bármely elemével való bővítés szeparábilis.

26. Legyen L a K-nak algebrai bővítése és $\overline{K}$ a K-nak a K felett szeparábilis L-beli elemekkel való bővítése. Bizonyítsuk be, hogy $\overline{K}$ a K-nak szeparábilis bővítése és L a $\overline{K}$-nak tisztán inszeparábilis bővítése (azaz L egyetlen eleme sem szeparábilis $\overline{K}$ felett).

27. Tegyük fel, hogy L tisztán inszeparábilis (és algebrai) K felett. Bizonyítsuk be, hogy ha L egy automorfizmusa K minden elemét fixen hagyja, akkor ez az identikus automorfizmus.

8.7. Normális bővítés

Az alábbiakban a felbontási testek jellemzése lesz a célunk.

8.26. Definíció. A K test L algebrai bővítésében levő a és b elemeket (K felett) konjugáltaknak nevezzük, ha K feletti főpolinomjaik megegyeznek. Ha az L-beli a elem K feletti főpolinomja az L felett lineáris faktorokra bomlik, akkor azt mondjuk, hogy L tartalmazza a összes konjugáltját. Az L testet K normális bővítésének nevezzük, ha minden elemének összes (K feletti) konjugáltját tartalmazza és K felett algebrai. □

8.27. Tétel. *Egy K test valamely L bővítésére az alábbi feltételek ekvivalensek:*

(1) *L a K-nak algebrai bővítése és bármely $K[x]$-ben irreducibilis polinom $L[x]$-ben megegyező fokú faktorok szorzatára bomlik.*

(2) *L a K-nak normális bővítése.*

(3) *L egy $K[x]$-beli polinomhalmaz felbontási teste.*

Bizonyítás. Ciklikus bizonyítást adunk. Ha (1) teljesül és egy K felett irreducibilis polinomnak van L-ben gyöke, tehát L felett lineáris faktora, akkor a feltétel szerint csupa elsőfokú faktorok szorzatára bomlik. Ez pedig éppen azt jelenti, hogy bármely L-beli elemmel együtt annak minden konjugáltja is L-ben van. Mivel feltettük, hogy algebrai bővítésről van szó, ezért a bővítés valóban normális.

Tegyük most fel, hogy (2) igaz. Ekkor L minden eleme algebrai K felett. Tekintsük az L elemeihez tartozó K feletti főpolinomokat. A feltétel szerint ez a polinomhalmaz csupa elsőfokú tényező szorzatára bomlik L felett, így L tartalmazza e polinomhalmaz felbontási testét. Másrészt e polinomhalmaz gyökei (sőt, választás szerint e gyökök közül már bizonyosak) a test összes elemét kiadják, és így L megegyezik a felbontási testtel.

Végül azt tesszük fel, hogy L egy K feletti $\mathcal{P}$ polinomhalmaz felbontási teste. Tekintsünk egy tetszőleges $g(x) \in K[x]$ irreducibilis polinomot, és tegyük fel, hogy ez $L[x]$-ben felbomlik irreducibilis polinomok szorzatára: $g(x) = g_1(x) \cdot \ldots \cdot g_r(x)$. Az általánosság megszorítása nélkül feltehetjük, hogy a fenti polinomok normáltak, és a tényezők úgy vannak rendezve, hogy a későbbi tényező foka sohasem kisebb az előzőénél.

Az, hogy L a $\mathcal{P}$ polinomhalmaz felbontási teste, azt jelenti, hogy L minden eleme a $\mathcal{P}$-beli polinomok gyökeinek K-beli együtthatós polinomjaként írható fel. Mivel egy polinomban csak véges sok tag, illetve tényező léphet fel, ezért L minden eleme benne van egy véges polinomhalmaz felbontási testében is. Ebből viszont már az is következik, hogy L-nek bármely véges elemhalmaza is egy véges polinomhalmaz felbontási testében van. Mint a 6.9. tétel bizonyításában láttuk, ez azzal ekvivalens, hogy a vizsgált elemhalmaz egyetlen polinom felbontási testében van. Mivel a $g_1(x), \ldots, g_r(x)$ polinomoknak összesen véges sok együtthatója van, ezért ezek a polinomok benne vannak egy olyan M test feletti polinomgyűrűben, amely L-nek része és egyetlen K feletti $f(x)$ polinom felbontási teste. Tekintettel arra, hogy $M \subseteq L$, ezért a fenti polinomok nemcsak L felett, hanem M felett is irreducibilisek.

Nyilván feltehetjük, hogy f normált, és tekintsük lineáris faktorokra bontását:

$$f(x) = (x - a_1) \cdot \ldots \cdot (x - a_n).$$

Ekkor minden egyes szóba jövő $g_i(x)$ együtthatója a fenti a_j elemeknek egy-egy K feletti polinomja. Ez a felírás nem egyértelmű, éppen ezért rögzítsünk egy ilyen előállítást minden

egyes együtthatóra. Csupán egyetlen megkötést teszünk: azt, hogy a legmagasabb fokú tag együtthatójaként az 1 (konstans) polinomot választjuk. Így tehát a következő előállításunk van: minden szóba jövő i indexhez választottunk egy $g_i(y_1, \ldots, y_n, x)$ polinomot úgy, hogy $g_i(a_1, \ldots, a_n, x) = g_i(x)$ teljesül.

Tekintsük most a $g_1(y_1, \ldots, y_n, x)$ polinomot, és az S_n szimmetrikus csoport minden egyes σ permutációjára készítsük el az összes $g_1(y_{\sigma(1)}, \ldots, y_{\sigma(n)}, x)$ alakú polinomot. Jelölje $G(y_1, \ldots, y_n, x)$ e polinomok szorzatát. Ez a polinom az $y_1, \ldots, y_n$ határozatlanok szimmetrikus polinomja, mert e határozatlanok bármely permutálása a megadott tényezőket permutálja csupán. Ha tehát e polinomot x polinomjaként tekintjük, akkor együtthatói mint a többi határozatlan polinomjai, e határozatlanoknak szimmetrikus polinomjai. Ebből viszont a szimmetrikus polinomok alaptétele szerint következik, hogy ezek az együtthatók felírhatók az $y_1, \ldots, y_n$ határozatlanok elemi szimmetrikus polinomjainak K-beli együtthatós polinomjaként. Mivel az $a_1, \ldots, a_n$ elemek elemi szimmetrikus polinomjai előjeltől eltekintve éppen az $f(x)$ együtthatói, ezért a $G(x) = G(a_1, \ldots, a_n, x)$ polinom együtthatói – mint K-beli elemek K-beli együtthatós polinomjai – elemei a K testnek. Ezenkívül még azt is tudjuk a $G(x)$ polinomról, hogy $g(x)$-szel van közös faktora, nevezetesen a $g_1(x)$ polinom. Így $g(x)$-nek és $G(x)$-nek a legnagyobb közös osztója nem konstans. Tekintettel arra, hogy a K test felett $g(x)$ irreducibilis, ez csak úgy lehetséges, hogy $g(x)$ osztója $G(x)$-nek. Térjünk vissza az $M[x]$ polinomgyűrűre. A most megállapított oszthatóság következtében $g(x)$-nek bármely szóba jövő $g_i(x)$ faktora osztója $G(x)$-nek. A feltétel szerint $g_i(x)$ irreducibilis, és így osztója a $G(x)$-ben előforduló tényezők valamelyikének. E tényezők bármelyike $g_1(b_1, \ldots, b_n, x)$ alakú, ahol $b_1, \ldots, b_n$ az $f(x)$ gyökeinek egy permutációja. A konstrukció szerint ennek a polinomnak a foka megegyezik $g_1(x)$ fokával, ami legfeljebb akkora, mint a $g_i(x)$ foka. Az oszthatósági kapcsolat szerint viszont $g_i(x)$ foka nem lehet nagyobb, mint $g_1(b_1, \ldots, b_n, x)$ foka, ami éppen azt adja, hogy a két polinom foka egyenlő. ■

8.28. Tétel. *Legyen N a K test normális bővítése. Ekkor N-nek azok az automorfizmusai, amelyek K minden elemét önmagába képezik le, egy $G(N \mid K)$ csoportot alkotnak. E csoport elemeit (K felett) relatív automorfizmusoknak nevezzük, a csoportot pedig szeparábilis bővítés esetén a bővítés Galois-csoportjának. Amennyiben a bővítést egy polinomrendszer vagy egyetlen polinom felbontási testeként hozzuk létre, akkor a polinomrendszerhez, illetve egyetlen polinomhoz tartozó Galois-csoportról beszélünk.*

Bizonyítás. A tételnek tulajdonképpen egyetlen állítása az, hogy a relatív automorfizmusok csoportot alkotnak. Mivel tetszőleges algebrai struktúra automorfizmusai csoportot alkotnak, ezért elég annak a bebizonyítása, hogy ha két automorfizmus mindegyike önmagába képezi K minden elemét, akkor szorzatuk is és inverzük is ilyen. Ez pedig nyilvánvaló. ■

A relatív automorfizmusoknak igen szoros kapcsolatuk van a bővítés elemeivel:

8.29. Tétel. *A $G = G(N \mid K)$ Galois-csoport bármely σ eleme az N tetszőleges a elemét ennek egy konjugáltjába viszi. Az a elemet fixen hagyó relatív automorfizmusok G-nek egy véges indexű H részcsoportját alkotják, és két relatív automorfizmus pontosan akkor viszi az a elemet ugyanabba az elembe, ha ugyanabban a H szerinti bal oldali mellékosztályban vannak.*

Bizonyítás. Mivel σ művelettartó és K elemeit fixen hagyja, ezért tetszőleges $h(x) \in K[x]$ esetén érvényes a $\sigma(h(a)) = h(\sigma(a))$ összefüggés. Ha tehát f az a elem főpolinomja, akkor $f(a) = 0$ miatt $f(\sigma(a)) = 0$ is teljesül. Így $\sigma(a)$ főpolinomja is f, azaz $\sigma(a)$ valóban konjugáltja a-nak. (Számolás nélkül is kimutathatjuk ezt a következőképpen: Legyen $\varphi : K[x] \to N$ az a homomorfizmus, amely K-t fixen hagyja és x-et a-ba viszi. Mivel σ relatív automorfizmus, ezért $\sigma\varphi$ is fixen hagyja K-t és Ker $(\sigma\varphi)$ = Ker (φ). Ez pedig azt jelenti, hogy $\sigma(a)$-hoz ugyanaz az ideál – tehát ugyanaz a főpolinom – tartozik.)

Az az állítás, hogy H csoport, ugyanúgy látható be, mint a 8.28. tételben a $G(N \mid K)$ csoport volta.

Tekintsük most G-nek egy σ és egy τ elemét. $\sigma(a) = \tau(a)$ pontosan akkor teljesül, ha $\sigma^{-1}\tau(a) = a$, ami ekvivalens a $\sigma^{-1}\tau \in H$, illetve a $\sigma H = \tau H$ feltétellel. Ebből következik már az is, hogy H véges indexű, mert a mellékosztályok száma legfeljebb annyi, mint a konjugáltjainak a száma – tehát véges. ■

Alapvető jelentőségű, hogy a 8.29. tétel állításának a megfordítása is igaz:

8.30. Tétel. *Legyenek a és b a K felett normális és szeparábilis N bővítés konjugált elemei. Ekkor létezik olyan $G(N \mid K)$-beli σ elem, amely az a elemet b-be viszi.*

Bizonyítás. A 8.6. tétel szerint létezik olyan izomorfizmus, amely úgy képezi le $K(a)$-t $K(b)$-re, hogy K elemei fixen maradnak, és a-t b-re képezi le. A 8.9. tétel szerint ez az izomorfizmus kiterjeszthető bármely polinomhalmaz felbontási testére. (A tétel ugyan kevesebbet mond ki, de a bizonyítás során pontosan ezt igazoltuk.) Mivel N a K-nak normális bővítése, ezért N egy K fölötti $\mathcal{P}$ polinomhalmaz felbontási teste (8.27. tétel). Mivel $\mathcal{P}$ egyszersmind $K(a)$-beli és $K(b)$-beli együtthatós polinomok halmazának is tekinthető, mégpedig úgy, hogy a fenti izomorfizmus e polinomhalmazt elemről elemre önmagába viszi, ezért ez az izomorfizmus kiterjeszthető N-re. A kiterjesztésre a tétel feltételei nyilvánvalóan teljesülnek. ■

8.8. A klasszikus Galois-elmélet főtétele

A magasabbfokú polinomok gyökeinek a meghatározásánál lényeges szerepet töltenek be azok az automorfizmusok, amelyek (az együtthatókat fixen hagyva) a gyököket permutálják. A fiatalon meghalt ÉVARISTE GALOIS nevéhez fűződik az a zseniális észrevétel, hogy a végtelen testek szerkezetének a vizsgálata visszavezethető véges csoportok vizsgálatára. (Igaz, ő nem az akkor még nem ismert automorfizmusokkal, hanem a lényegesen bonyolultabb behelyettesítésekkel dolgozott.) Ezzel nem csupán az „egyenletek megoldhatóságának" a kérdését döntötte el, hanem ez volt a kiindulópontja az absztrakt algebrának és az algebrai módszereknek is.

Az előző részben már láttuk, hogy a normális bővítés elemei és a relatív automorfizmusok között szoros kapcsolat van. Tekintsük azt a relációt, amely a test elemei és a relatív automorfizmusok között definiálható: egy testelem és egy automorfizmus akkor legyenek relációban, ha az automorfizmus a testelemet fixen hagyja. Ez a reláció a 3.12. tétel szerint Galois-kapcsolatot létesít a test részhalmazai és a Galois-csoport részhalmazai közt. Valójában a most tárgyalt (és tovább vizsgálandó) kapcsolattípus volt az első fölfedezett

Galois-kapcsolat; és éppen innét ered e kapcsolat neve. Első feladatunk annak a megvizsgálása lesz, hogy e Galois-kapcsolatban melyek lesznek a megfelelő lezárások zárt halmazai.

8.31. Tétel. *A $G(N \mid K)$ által létrehozott Galois-kapcsolatban (tehát abban a Galois-kapcsolatban, amelyet a következő $R \in G(N \mid K) \times N$ reláció hoz létre) $(\sigma, a) \in R$ pontosan akkor, ha $\sigma(a) = a$) az N-beli zárt halmazok K-t tartalmazó, úgynevezett közbülső testek és a G-beli zárt halmazok részcsoportok.*

Ha $X \subseteq N$, illetve $Y \subseteq G(N \mid K)$ tetszőleges részhalmazok, akkor a Galois-kapcsolatban nekik megfeleltetett részcsoportot, illetve közbülső testet $H(X)$, illetve $\Delta(Y)$ fogja jelölni.

Bizonyítás. Nyilván elegendő a tétel állítását egyelemű X, illetve Y halmazra bizonyítani (pl. a 3.8. tétel (4) pontja és a 3.31. tétel miatt). A σ művelettartása miatt $\Delta(\sigma)$ test, és tartalmazza K-t, mert σ relatív automorfizmus. $H(a)$ nyilván tartalmazza az egységelemet és zárt a szorzásra; az inverzképzésre való zártság az $a = \sigma(a)$ figyelembevételével adódik a $\sigma^{-1}(a) = \sigma^{-1}\sigma((a)) = (\sigma^{-1}\sigma)(a) = a$ feltételből. ■

A továbbiakban célunk a 8.31. tétel megfordításának bizonyítása, azaz annak a kimutatása, hogy minden közbülső test, illetve részcsoport zárt. Általában azonban ez nem igaz. Vegyük ismét a p elemű $\mathbb{Q}_p$ prímtest $K = \mathbb{Q}_p(a)$ egyszerű transzcendens bővítését, és legyen N az $x^p - a$ felbontási teste. Ha $a = b^p$, akkor nyilván $N = \mathbb{Q}_p(b)$. Legyen most σ az N-nek olyan automorfizmusa, amely a K test elemeit fixen hagyja. Ekkor $\sigma(b) = (f(b)/g(b))$, alkalmas $\mathbb{Q}_p[x]$-beli f és g polinomokkal. Felhasználva, hogy σ olyan automorfizmus, amely a-t fixen hagyja, valamint az $(f(x))^p = f(x^p)$ és $(g(x))^p = g(x^p)$ összefüggéseket, azt kapjuk, hogy

$$a = \sigma(a) = \sigma(b^p) = (\sigma(b))^p = (f(b)/g(b))^p = f(b^p)/g(b^p) = f(a)/g(a).$$

Tekintettel arra, hogy a transzcendens $\mathbb{Q}_p$ fölött, a fenti összefüggésből $f(x)/g(x) = x$, végül pedig $\sigma(b) = b$ következik. Így a K testet fixen hagyó automorfizmusok az N testet is fixen hagyják, tehát a K test a fenti Galois-kapcsolat esetén nem zárt. Ez az eset nem kerülhető el, ha a bővítés nem szeparábilis. A továbbiakban tehát azt is feltesszük, hogy a vizsgált bővítés szeparábilis. Általában tökéletes testek bővítésével foglalkozunk, de a Galois-csoport meghatározásánál szükségünk lesz olyan szeparábilis bővítésre is, amikor az alaptest nem tökéletes.

8.32. Tétel. *Legyen N a K test szeparábilis normális bővítése. Ekkor*

(1) $\Delta(G(N \mid K)) = K$.

(2) *Tetszőleges Δ közbülső testre N normális bővítése Δ-nak és $H(\Delta) = G(N \mid \Delta)$.*

(3) *Tetszőleges Δ közbülső testre $\Delta(H(\Delta)) = \Delta$.*

Bizonyítás. $K \subseteq \Delta(G(N \mid K))$ a definíció szerint (vagy a 3.12. tétel következtében, a 3.7. definíció (2) pontját figyelembe véve) igaz. Azt kell még belátni, hogy N-nek egyetlen, K-n kívüli elemét sem viszi minden relatív automorfizmus önmagába. Ez viszont azonnal következik a 8.30. tételből, hiszen az $N \mid K$ bővítés szeparábilis és ezért N minden K-n kívüli elemének van önmagától különböző konjugáltja.

A második állítás első része világos a 8.27. tételből, mert N pontosan ugyanannak a polinomhalmaznak a felbontási teste Δ felett is, mint K felett. Az állítás második része

is nagyon könnyen belátható. $G(N \mid \Delta)$ ugyanis a Δ-t fixen hagyó automorfizmusokból áll. Mivel ezek K minden elemét is önmagára képezik (hiszen $K \subseteq \Delta$), ezért ezek a K-t fixen hagyó olyan automorfizmusok, amelyek Δ elemeit sem mozgatják, azaz $G(N \mid \Delta) \subseteq \subseteq H(\Delta)$. Másrészt $H(\Delta)$ elemei N-nek olyan automorfizmusai, amelyek K elemein felül még Δ többi elemét is fixen hagyják – tehát definíció szerint elemei $G(N \mid \Delta)$-nak.

Nézzük most az N egy tetszőleges a elemét. Legyen a-nak a Δ feletti főpolinomja $g(x)$ és a K feletti főpolinomja $f(x)$. Mivel $f(x) \in \Delta[x]$ is igaz, és $f(a) = 0$, ezért a Δ felett irreducibilis $g(x)$ polinom osztója $f(x)$-nek. Tekintettel arra, hogy $N \mid K$ normális és szeparábilis, ezért a K felett irreducibilis $f(x)$ csupa különböző faktorra esik szét $N[x]$-ben. A polinomokra vonatkozó egyértelmű faktorizáció alapján ugyanez történik $g(x)$-szel is. Ez azt jelenti, hogy N a Δ-nak is normális és szeparábilis bővítése. Vegyük most figyelembe azt, hogy $\Delta : Y \to \Delta(Y)$ operáció az alaptesttől függetlenül fogalmazható (nevezetesen úgy, hogy a tekintett automorfizmuscsoport által fixen hagyott elemek halmaza). Ezért az $N \mid \Delta$ bővítésre alkalmazhatjuk e tétel (1) állítását, azaz $\Delta(G(N \mid \Delta)) = \Delta$. A (2) állítás szerint $\Delta(H(\Delta)) = \Delta(G(N \mid \Delta))$, amit az előző egyenlőséggel egybevetve éppen a (3) alatti egyenlőség adódik. ■

A továbbiakban újabb megszorításokat vagyunk kénytelenek tenni. Tekintsük ugyanis a racionális számtestnek, $\mathbb{Q}$-nak a prímszámok négyzetgyökeivel való bővítését. Ez éppen az $\{x^2 - p \mid p = 2, 3, 5, \ldots\}$ polinomhalmaz felbontási teste. Könnyen belátható, hogy a bővítésnek léteznek olyan automorfizmusai, amelyek véges sok négyzetgyököt a negatívjukba visznek s a többieket nem változtatják. Az is nyilvánvaló, hogy ezek a Galois-csoportnak egy részcsoportját alkotják. Ehhez a csoporthoz mint közbülső test, éppen a racionális test tartozik. (Ennek a bizonyítását – az alaptétel felhasználásával – az olvasóra bízzuk.) A racionális testhez tartozó csoport – tehát az egész Galois-csoport – viszont tartalmaz újabb elemeket is, pl. azt, amely minden prímszám négyzetgyökét a negatívjába képezi. Ez a körülmény mindig fellép, ha a bővítés nem véges. Ennek megfelelően a továbbiakban csak véges bővítésekkel foglalkozunk.

8.33. Tétel (Alaptétel)**.** *Legyen N a K test véges szeparábilis normális bővítése, és legyen $G = G(N \mid K)$. Ekkor:*

(1) *A Galois-kapcsolatban minden közbülső test és minden részcsoport zárt.*

(2) *Ha a Δ közbülső test és a H részcsoport a Galois-kapcsolatban egymásnak felelnek meg, akkor $(\Delta : K) = (G : H)$ és $|H| = (N : \Delta)$. Speciálisan $|G| = (N : K)$.*

(3) *Ha Δ_1 és Δ_2 két résztest, akkor*

$$H(\Delta_1 \cap \Delta_2) = \langle H(\Delta_1), H(\Delta_2)\rangle \quad \text{és} \quad H([\Delta_1, \Delta_2]) = H(\Delta_1) \cap H(\Delta_2),$$

ahol $[L_1, L_2]$ ezek generátumát, vagyis az L_1 és L_2 testeket tartalmazó legszűkebb testet jelöli.

Ha H_1 és H_2 két részcsoport, akkor

$$\Delta(H_1 \cap H_2) = [\Delta(H_1), \Delta(H_2)] \quad \text{és} \quad \Delta(\langle H_1, H_2\rangle) = \Delta(H_1) \cap \Delta(H_2).$$

Bizonyítás. Mivel $N \mid K$ véges algebrai, ezért $N = K(a_1, \ldots, a_t)$ alakú. Mivel $N \mid K$ szeparábilis, ezért a 8.17. tétel szerint $N = K(a)$, alkalmas K felett algebrai a elemmel. Legyen $(N : K) = n$; ekkor a-nak N-ben pontosan n darab (különböző) konjugáltja van, hiszen a főpolinomja n-edfokú. Legyenek e konjugáltak $a_1(= a), \ldots, a_n$. A 8.30. tétel szerint ekkor G-nek léteznek olyan σ_i $(1 \leq i \leq n)$ elemei, amelyekre $\sigma_i(a) = a_i$ teljesül.

Tekintettel arra, hogy az a képe ezen automorfizmusok mindegyikénél különböző, ezek az automorfizmusok mind különbözőek. Ha egy automorfizmus az a elemet fixen hagyja, akkor fixen kell hagynia az a generálta N test minden elemét is. Így az a-t fixen hagyó automorfizmusok csoportja egyedül az egységelemből áll. A 8.16. tétel alapján tehát G-nek legfeljebb annyi eleme lehet, ahány konjugáltja van az a-nak, ami a $|G| = (N : K)$ összefüggést bizonyítja.

A 8.32. tétel (2) pontja szerint ebből

$$|H(\Delta)| = (N : \Delta) \tag{I}$$

következik tetszőleges Δ közbülső test esetén. Ekkor Lagrange tétele és a 8.2. tétel alapján kapjuk, hogy

$$(G : H(\Delta)) = (\Delta : K).$$

A Galois-kapcsolatokra általában bizonyítottak következtében $H \subseteq H(\Delta(H))$, amiből

$$|H| \leq |H(\Delta(H))| \tag{II}$$

adódik.

Tekintsük most a G-nek egy k elemű H részcsoportját, és legyenek a H elemei $\sigma_1, \ldots$ $\ldots, \sigma_k$. Tekintsük a

$$g(x) = (x - \sigma_1(a)) \cdot \ldots \cdot (x - \sigma_k(a))$$

polinomot. E polinom foka megegyezik H rendjével. Alkalmazzuk most $g(x)$-re H-nak egy tetszőleges σ elemét (illetve ennek – a 8.6. tétel szerint létező egyértelmű – $N[x]$-re való kiterjesztését):

$$\sigma(g(x)) = (x - \sigma\sigma_1(a)) \cdot \ldots \cdot (x - \sigma\sigma_k(a)).$$

Mivel H csoport, ezért a $\sigma(g(x))$ faktorai – esetleg a sorrendtől eltekintve – ugyanazok, mint $g(x)$ faktorai. Mivel σ tetszőleges H-beli elem, ezért $g(x) \in \Delta[x]$, ahol $\Delta = \Delta(H)$. A H elemei között ott van az identitás is, ami azt jelenti, hogy $g(x)$-nek gyöke az a. Így az a-nak Δ feletti főpolinomja $g(x)$-nek osztója, tehát legfeljebb k-adfokú. A 8.1. tétel szerint tehát $(N : \Delta) \leq k = |H|$, mert $N = \Delta(a)$. Ha ez utóbbi egyenlőtlenséget, valamint az (I) és (II) összefüggéseket egybevetjük, akkor a következőket kapjuk:

$$|H| \leq |H(\Delta(H))| = (N : \Delta(H)) \leq |H|. \tag{III}$$

Itt tehát minden egyenlőtlenség helyén egyenlőségnek kell állnia. A továbbiakban ugyan nem lesz szükségünk rá; de érdemes megnézni a második egyenlőtlenséget. Ha ez egyenlőség, akkor csak az lehetséges, hogy a konstruált $g(x)$ polinom éppen a-nak a Δ feletti főpolinomja. Az első egyenlőtlenség is egyenlőség, amiből az adódik, hogy a szereplő két csoportnak ugyanannyi eleme van. Mivel a Galois-kapcsolat tulajdonságai szerint $H \subseteq$ $\subseteq H(\Delta(H))$, ezért az elemek számának egyenlősége a két csoport egyenlőségét jelenti. Eszerint G minden részcsoportja zárt; s a 8.23. tételt figyelembe véve következik az (1), és így a (2) állítás is, hiszen éppen ezt bizonyítottuk a $H = H(\Delta)$ esetben.

A (3) alatti második és negyedik egyenlőség azonnal következik az 3.8. tétel (4) pontjából.

A második egyenlőségből következik, hogy

$$H_1 \cap H_2 = H(\Delta(H_1)) \cap H(\Delta(H_2)) = H([\Delta(H1), \Delta(H_2)]).$$

Így

$$\Delta(H_1 \cap H_2) = \Delta(H([\Delta(H_1), \Delta(H_2)])) = [\Delta(H_1), \Delta(H_2)],$$

a $\Delta(H(\Delta)) = \Delta$ összefüggés alapján. Ezzel a harmadik egyenlőséget is bizonyítottuk. Az első egyenlőség formálisan ugyanígy bizonyítható. ■

A Galois-elmélet alaptétele tehát egy úgynevezett duális izomorfizmust létesít a részcsoportok és a közbülső testek tartalmazásra vett hálója között. Ez nem csak azt jelenti, hogy nagyobbnak kisebb felel meg, hanem azt is, hogy generátumnak közös rész (és viszont). Emellett még az is igaz, hogy a megfelelően értelmezett „távolságok" is megmaradnak. Ezt a megfeleltetést még tovább lehet „finomítani":

8.34. Tétel. *Legyen N a K test szeparábilis véges normális bővítése. Legyenek továbbá a Δ közbülső test és a $H \leq G = G(N \mid K)$ részcsoport a Galois-kapcsolatban egymásnak megfeleltetett elemek. Δ akkor és csak akkor normális bővítése K-nak, ha H normális részcsoportja G-nek. Ez esetben $G(\Delta \mid K) \cong G/H$.*

Az N-nek egy Δ_1 és egy Δ_2 részteste akkor és csak akkor konjugáltak (azaz, G-nek van olyan eleme, amely egyiküket a másikukba viszi, vagy ezzel ekvivalens módon az egyikük generátorelemének a konjugáltja a másiknak generátoreleme), ha a megfelelő részcsoportok egymás konjugáltjai.

Bizonyítás. Tetszőleges $a \in N$ esetén $H(K(a))$ pontosan azokból a relatív automorfizmusokból áll, amelyek a-t fixen hagyják. Tekintettel arra, hogy $\tau(\sigma(a)) = \sigma(a)$ ekvivalens a $\sigma^{-1}\tau\sigma(a) = a$ feltétellel, ezért $H(K(\sigma(a))) = \sigma H(K(a))\sigma^{-1}$. Mivel normális bővítés generátorelemének bármely konjugáltja is generálja e bővítést, ezért a tétel állításából a kívánt izomorfizmuson kívül mindent beláttunk.

Ha Δ normális bővítése K-nak, akkor – a 8.29. tétel alapján – G minden eleme a Δ testet önmagába képezi. Ez azt jelenti, hogy minden $\sigma \in G$ indukál egy $\overline{\sigma} \in G(\Delta/K)$ automorfizmust. A $\sigma \to \overline{\sigma}$ megfeleltetés nyilvánvalóan homomorfizmus, amelynek a magja pontosan a H. A homomorfizmustétel szerint tehát G/H izomorf $G(\Delta \mid K)$ egy részcsoportjával. Tekintettel arra, hogy e két csoport rendje a 8.33. tétel (2) pontja alapján megegyezik, a kívánt izomorfizmust megkaptuk. (A befejező lépés „újrabizonyítása" annak, hogy az automorfizmusok „kiterjeszthetők".) ■

8.9. Gyökjelekkel való megoldhatóság

A következőkben a Galois-elmélet két fontos alkalmazását, az egyenleteknek gyökjelekkel való megoldhatóságát és a geometriai szerkeszthetőség algebrai elméletét tárgyaljuk.

Az egyenletek megoldása az algebra és az egész matematika egyik legklasszikusabb feladata. Itt most csak polinomok, sőt csak egyhatározatlanú polinomok gyökeinek a meghatározásával foglalkozunk. A „gyök meghatározása" nem egyértelműen definiált fogalom, attól függ, hogy „milyen célból" van szükségünk rá.

Ha – mint a gyakorlati kérdések többségében – az a feladatunk, hogy a gyökben rejlő „numerikus információt" határozzuk meg, akkor valamilyen numerikus eljáráshoz folyamodunk, amely a céltól, illetve a lehetőségektől függően megad egy intervallumot, amelyben a kívánt gyök elhelyezkedik. (Ugyanez történik akkor is, ha számítógépet veszünk igénybe; persze ekkor az eljárás előttünk rejtve marad.)

Ha az a feladatunk, hogy a polinom egyik gyökével „formális számolást" végezzünk – például nevezőt gyöktelenítsünk – mielőtt a numerikus értéket meghatározzuk, akkor a 7.68. tételre hivatkozhatunk, amely lényegében azt mondja ki, hogy egy polinom gyökével való számoláshoz pontosan annyi információnk van, amennyit e gyök főpolinomja nyújt.

Ha azonban visszanyúlunk a „megoldás” eredeti, középkori jelentéséhez, amely szerint a gyököket az együtthatókból „műveletekkel” akarjuk előállítani, akkor a helyzet sokkal bonyolultabbá válik. Mindenekelőtt megemlítjük, hogy akkoriban műveleten az összeadást, kivonást, szorzást, osztást és gyökvonást értették; előállításon pedig azt, hogy e műveleteket véges sokszor alkalmazhatták. (A későbbiekben e fogalmat majd pontosan definiáljuk.) Mint látni fogjuk, az ilyen értelemben vett megoldhatóság kérdésére a Galois-elmélet segítségével nemleges választ adunk. Ez a válasz látszólag érdektelenné teszi a kérdést, hiszen „mi jó van abban, ha egy bonyolult megoldás nem létezik”. Hasonló gondolatokat lehetne leszűrni első pillanatban a szerkeszthetőség algebrai elméletével kapcsolatban is. Ezek ellen talán még az sem elegendő ellenérv, hogy a Galois-elmélet segítségével – legalábbis elvileg – eldönthető, hogy mikor oldható meg egy-egy ilyen feladat. Az itteni módszerek igazi jelentőségét az adja, hogy ezeket tekinthetjük az absztrakt algebra kiindulópontjainak és emellett még ma is az algebra egyik legszebb elméletét alkotják.

A továbbiakban szükségünk lesz az alaptétel alábbi következményére:

8.35. Tétel. *Legyenek Δ_1 és Δ_2 az $N \mid K$ szeparábilis véges normális bővítésében közbülső testek.*

(1) *Ha Δ_2 normális bővítése Δ_1-nek, akkor $G(\Delta_2 \mid \Delta_1) \cong G(N \mid \Delta_1) \mid G(N \mid \Delta_2)$, azaz a $G = G(N \mid K)$ csoport egy részcsoportjának faktora.*

(2) $G([\Delta_1, \Delta_2] \mid \Delta_1) \cong G(\Delta_2 \mid (\Delta_1 \cap \Delta_2))$*, amennyiben az az utóbbi csoport értelmezve van.*

Bizonyítás. 1. Az alaptétel szerint $G(N \mid \Delta_2) = H_2$ és $G(N \mid \Delta_1) = H_1$ a Galois-csoportnak részcsoportjai, amelyekre $\Delta_2 \geq \Delta_1$ miatt $H_2 \leq H_1$ teljesül. Mivel itt normális bővítésről van szó, ezért H_2 normális részcsoport H_1-ben, és a szerinte vett faktorcsoport a 8.34. tétel szerint izomorf a kívánt Galois-csoporttal.

2. Az 1. állítás alapján feltehető, hogy a két közbülső test metszete K. A nyilvánvaló $[\Delta_1, \Delta_2] = \Delta_1(\Delta_2)$ összefüggés miatt ez a test ugyanazon Δ_1 feletti polinom(halmaz) felbontási testének tekinthető, mint Δ_2. Legyen most N a két bővítést tartalmazó (legkisebb) véges, normális bővítés (azaz a generátum egyik generátoreleméhez tartozó főpolinom felbontási teste). Mivel az eredeti bővítés szeparábilis volt, ezért természetesen ez a bővítés is szeparábilis. Jelölje G e bővítés Galois-csoportját, és H_1, H_2, H_3 rendre a Δ_1, Δ_2, $[\Delta_1, \Delta_2]$ közbülső testekhez tartozó részcsoportot. Az 1. szerint a két vizsgált közbülső testhez tartozó részcsoport rendre izomorf a H_1/H_3 és a G/H_2 részcsoportokkal. A 8.33. tétel (3) pontja szerint $G = \langle H_1, H_2 \rangle$ és $H_3 = H_1 \cap H_2$. Ezek után a kívánt izomorfizmus azonnal adódik a (csoportokra vonatkozó) első izomorfizmustételből. ■

A gyökjelekkel való megoldhatóság vizsgálata céljából most definiáljuk a gyökkifejezést. A „naiv definíció”-ból három fontos dolgot figyelhetünk meg: (*a*) E kifejezés adott elemekből épül fel; (*b*) A négy „alapműveletet” használhatjuk. (*c*) Ezen kívül használhatunk gyökvonásokat is.

Az (*a*) alapján valami „feletti” gyökkifejezésről kell beszélni, amihez az eredetileg tekintett elemek hozzátartoznak. A (*b*) alapján ezek testet alkotnak. (*c*) szerint úgy juthatunk tovább, hogy mindig egy-egy $x^n - a$ alakú polinom gyökével bővítünk. Ez utóbbinál azonban a kényelem kedvéért célszerű bizonyos megszorításokat tenni. Először is szorítkozzunk olyan polinomokra, amelyeknek a foka prímszám. Ez nyilvánvalóan nem megy az

általánosság rovására, hiszen prímkitevőjű gyökökkel minden, 1-nél nagyobb egész kitevőjű gyök előállítható. A második korlátozás arra vonatkozik, hogy például az $x^3 - 8$ típusú polinomok gyökeit ne fogadjuk el eleve gyökkifejezésnek. Valóban, ennek a polinomnak az egyik gyöke 2, a másik két gyöke pedig az alacsonyabb fokú $x^2 + 2x + 4$ polinomnak is gyöke. Ez a megszorítás esetleg azt eredményezhetné, hogy a gyökkifejezések számát (esetleg szükségtelenül) csökkentettük, de a bizonyítandó tételek azt is megmutatják, hogy az ilyen módon elmellőzött gyökök is gyökkifejezések.

8.36. Definíció. A K test felett gyökökkel elérhetőnek nevezzük:

(1) A K testet.

(2) Ha az L test a K-nak véges szeparábilis algebrai bővítése, amely K felett gyökökkel elérhető, és $M = L(b)$, ahol b az L felett irreducibilis, prímfokú szeparábilis $x^p - a$ polinom gyöke, akkor M gyökökkel elérhető a K felett.

(3) Csak azokat a testeket nevezzük K felett gyökökkel elérhetőnek, amelyek az előző két lépés véges sokszori alkalmazásával állíthatók elő.

Egy elemet a K felett gyökkifejezésnek nevezünk, ha eleme egy K felett gyökökkel elérhető testnek. □

Az $x^p - a$ alakú úgynevezett *binomok* szerkezetének vizsgálatához – előkészületül – még két tételt bizonyítunk be:

8.37. Tétel. *Legyen L a K test fölött az $x^n - 1$ polinom felbontási teste. Ekkor L/K szeparábilis és Galois-csoportja kommutatív.*

Bizonyítás. Ha a K test p karakterisztikájú és $n = pk$, akkor $x^n - 1 = (x^k - 1)^p$. Ebben az esetben az eredeti polinom helyett tekinthetjük az $x^k - 1$ polinomot, amelynek a felbontási teste megegyezik az eredeti polinom felbontási testével. Így feltehető, hogy n nem osztható a K karakterisztikájával.

Az $x^n - 1 = (x^k - 1) \cdot x^{n-k} + (x^{n-k} - 1)$ összefüggés alapján azonnal látható (például indukcióval), hogy $x^k - 1$ pontosan akkor osztója az $x^n - 1$ polinomnak, ha k osztója n-nek. Legyen most $g_n(x)$ a legkisebb közös többszöröse azoknak az $x^k - 1$ alakú polinomoknak, amelyekre k az n-nek n-nél kisebb osztója. Az elöljáróban mondottak alapján létezik olyan $f_n(x)$ polinom, amelyre $g_n(x) \cdot f_n(x) = x^n - 1$ teljesül. A most definiált $f_n(x)$ polinomot az *n-edik körosztási polinomnak* nevezzük. A definícióból nyilvánvaló, hogy egy a elem pontosan akkor gyöke $f_n(x)$-nek, ha *n-edik primitív egységgyök*, azaz $a^n = 1$, de $k < n$ esetén $a^k \neq 1$. Tekintettel arra, hogy a csak egyetlen n-re lehet n-edik primitív egységgyök, ezért $n \neq k$ esetén $f_n(x)$ és $f_k(x)$ relatív prímek. Ezek után n-re vonatkozó teljes indukcióval bebizonyítjuk, hogy $x^n - 1$ éppen azoknak az $f_k(x)$-eknek a szorzata, amelyekre k osztója n-nek. Az $n = 1$ esetben $x - 1 = f_1(x)$ miatt igaz az állítás. Tegyük most fel, hogy az állítás igaz minden, n-nél kisebb természetes számra. Mivel $k \mid n$ esetén $f_k(x) \mid (x^k - 1)$ és $(x^k - 1) \mid (x^n - 1)$, ezért $x^n - 1$ osztható minden egyes szóba jövő $f_k(x)$-szel, s lévén ezek relatív prímek, szorzatukkal is. Az indukciós feltétel miatt $k < n$ esetén, ha $k \mid n$, akkor $x^k - 1 = \prod_{d \mid k} f_d(x)$. A $k \mid n$ feltétel miatt tehát $(x^k - 1)$ osztója azon $f_d(x)$-ek szorzatának, amelyekre $d < n$ és $d \mid n$. Így a szereplő $x^k - 1$ polinomok legkisebb

közös többszöröse, $g^n(x)$ is osztója e szorzatnak. Ezért $g_n(x) \cdot f_n(x) = x^n - 1$ osztója az összes olyan $f_d(x)$ szorzatának, ahol $d \mid n$, tehát $x^n - 1$ valóban megegyezik e szorzattal. Jelölje $\psi(n)$ az $f_n(x)$ fokát. A feltétel szerint $\psi(1) = 1$, és $\sum_{d \mid n} \psi(d) = n$. Mivel – mint az elemi számelméletből ismeretes – ez a tulajdonsága csak az Euler-féle φ függvénynek van meg, ezért $f_n(x)$ foka éppen $\varphi(n)$.

Ebből következik, hogy az n-edik körosztási polinomnak van gyöke. Legyen ε egy n-edik primitív egységgyök. Ekkor az ε^i (i egész, $1 \leq i \leq n$) elemek mind különbözőek, számuk n, amiből triviálisan adódik, hogy ezek éppen az n darab különböző n-edik egységgyökök. Az is világos, hogy ε a felbontási test egy generátoreleme, s bármely relatív automorfizmus ε-t annak egy hatványába viszi. Ha $\sigma_i(\varepsilon) = \varepsilon^i$ és $\sigma_j(\varepsilon) = \varepsilon^j$, akkor $\sigma_i\sigma_j(\varepsilon) = (\sigma_i(\varepsilon))^j = (\varepsilon^i)^j = \varepsilon^{i \cdot j}$. Ez viszont triviálisan adja, hogy a vizsgált Galois-csoport a modulo n vett redukált maradékosztályok multiplikatív csoportjának részcsoportjával izomorf, tehát kommutatív. ■

A fenti bizonyításban vigyázni kellett, mert egyáltalán nem biztos, hogy a primitív n-edik egységgyökök foka $\varphi(n)$; más szóval nem szükségszerű, hogy ezek az adott K test felett konjugáltak legyenek. Ezt úgy is fogalmazhatjuk, hogy a körosztási polinomok nem mindig irreducibilisek. Más azonban a helyzet akkor, ha a kiindulási test a racionális számok $\mathbb{Q}_0$ teste.

8.38. Tétel (a 8.37. kiegészítése)**.** *A racionális számtest felett a körosztási polinomok irreducibilisek. Az n-edik körosztási polinom Galois-csoportja izomorf a modulo n vett redukált maradékosztályok multiplikatív csoportjával.*

Bizonyítás. Mindenekelőtt megjegyezzük, hogy ha $f_n(x)$-et normáltnak tekintjük, akkor egész együtthatós. (Ez teljes indukcióval belátható, akár a primitív polinomokra vonatkozó eredményekből, akár a maradékos osztás végiggondolásával.) Mivel $x^n - 1$ gyökei ciklikus csoportot alkotnak, amelyek generátorelemei éppen az $f_n(x)$ gyökei, ezért $f_n(x)$ egy ε gyökével együtt ε^i pontosan akkor lesz gyöke az $f_n(x)$-nek, ha i az n-hez relatív prím.

Feladatunk tehát annak a bebizonyítása, hogy ha $g(x)$ az $f_n(x)$ egy ε gyökének a racionális számtest feletti főpolinomja, akkor bármely, az n-hez relatív prím i esetén ε^i-nek ugyancsak $g(x)$ a főpolinomja. Ha ez az állítás i-re és j-re igaz, akkor ε^i főpolinomja ugyanaz, mint ε-é, azaz $g(x)$; és $(\varepsilon^i)^j$-é ugyanaz, mint ε^i-é, vagyis ez is $g(x)$. Tehát azok a kitevők, amelyekre az állítás igaz, multiplikatív félcsoportot alkotnak. Így elegendő az állítást prímkitevőkre bizonyítani, mert minden n-hez relatív prím szám előáll n-hez relatív prím prímszámok szorzataként.

Tekintsük $f_n(x)$ egy ε gyökének a $g(x)$ főpolinomját, és legyen $h(x)$ az ε^p főpolinomja, ahol $(p, n) = 1$. Azt, hogy e két polinom egyenlő, indirekt módon bizonyítjuk. Tegyük fel, hogy különbözőek. Ekkor relatív prímek is, s így $x^n - 1$ osztható a szorzatukkal. Másrészt ε nyilván gyöke $h(x^p)$-nek is (hiszen $h(\varepsilon^p) = 0$), és így $g(x) \mid h(x^p)$.

A bizonyítást folytatva rátérünk a $\mathbb{Z}[x]/(p)$ maradékosztály-gyűrűre, azaz a $\mathbb{Q}_p[x]$ polinomgyűrűre. Itt $g(x)$ nem feltétlen irreducibilis, de biztosan létezik egy $k(x)$ irreducibilis faktora, amelyre tehát teljesül, hogy $k(x) \mid h(x^p)$. Mivel $\mathbb{Q}_p[x]$-ben $h(x)^p = h(x^p)$

(8.10. tétel), ezért $k(x)$ irreducibilitásából következik, hogy $k(x)$ osztója $h(x)$-nek is. Így $g(x) \cdot h(x)$ minden többszöröse – speciálisan $x^n - 1$ is – osztható $k(x)^2$-nel. Ez pedig lehetetlen, mert a 8.37. tétel bizonyításakor láttuk, hogy ha n nem osztható a karakterisztikával, akkor létezik primitív n-edik egységgyök, tehát pontosan n különböző n-edik egységgyök van, azaz $x^n - 1$ nem osztható egyetlen polinom négyzetével sem. Ezzel a körosztási polinom irreducibilitását beláttuk.

A Galois-csoport rendje megegyezik a bővítés fokával, amely esetünkben éppen a szóban forgó maradékosztályok száma. A 8.37. tétel bizonyításakor láttuk, hogy a Galois-csoport a redukált maradékosztályok multiplikatív csoportjának egy részcsoportjával izomorf; a rendek megegyezése miatt tehát a Galois-csoport az egész csoporttal izomorf. ■

Mint a gyökökkel való elérhetőség definíciójánál láttuk, alapvető jelentőségű az $x^p - a$ alakú irreducibilis polinomok gyökével való bővítés. A következő tétel az itt fellépő különböző lehetőségeket írja le:

8.39. Tétel. *A K test feletti prímfokú $x^p - a$ polinom vagy irreducibilis a K felett, vagy pontosan egy lineáris faktora van K felett, vagy csupa lineáris faktor szorzatára bomlik. Ez utóbbi esetben K tartalmazza az összes p-edik egységgyököt.*

Amennyiben K tartalmazza az összes p-edik egységgyököt és $x^p - a$ nem irreducibilis, akkor lineáris faktorokra bomlik.

Bizonyítás. Először nézzük azt az esetet, amikor K-nak a karakterisztikája p. Legyen b az $x^p - a$ gyöke e polinom felbontási testében. Az $(x - b)^p = x^p - a$ összefüggés alapján az adott polinom gyökei egyenlőek. Ha $x^p - a$ reducibilis, akkor valamilyen p-nél kisebb pozitív r mellett $(x - b)^r \in K[x]$, és így $b^r \in K$. Tekintettel arra, hogy r és p relatív prímek, ezért ebből $b \in K$ következik, vagyis a polinom K felett lineáris faktorokra bomlik.

Legyen a továbbiakban K karakterisztikája p-től különböző. A 8.37. tétel szerint ekkor a primitív p-edik egységgyökök száma $p - 1$; és ezek különbözőek. Ha $b^p = a$, akkor bármely ε primitív p-edik egységgyökre $(\varepsilon b)^p = a$ is igaz; és így $x^p - a$ a felbontási testében csupa különböző $x - \varepsilon b$ alakú tényező szorzatára bomlik, ahol ε végigfut a p-edik egységgyökökön. Ha $x^p - a$ reducibilis, akkor e tényezők közül bizonyosaknak a szorzata $K[x]$-ben van. E szorzat konstans tagja εb^k alakú (ε valamelyik p-edik egységgyök). E szorzat $K[x]$-beli, így egy p-nél kisebb pozitív egész k-ra $\varepsilon b^k \in K$. Mivel k és p relatív prímek, ezért léteznek olyan u és v pozitív egészek, amelyekre $ku = pv + 1$ teljesül. Így $(\varepsilon b^k)^u = \varepsilon^u a^v b$; amiből következik, hogy $\varepsilon^u b$ – mint két K-beli elem hányadosa – eleme K-nak, tehát $(x^p - a)$-nak van egy K felett elsőfokú faktora: $x - \varepsilon^u b$. Mivel $\varepsilon^u b$ is gyöke az adott polinomnak, ezért b helyett ezt az elemet is választhatjuk. Így feltehető, hogy az adott polinom $K[x]$-beli lineáris faktora $x - b$. Emellett persze lehetséges, hogy a polinom $K[x]$-ben tovább bomlik; a többi faktorról nem mondunk semmit. Azt az esetet kell még megnézni, amikor a polinomnak van egy másik elsőfokú faktora a K felett. Ekkor a két faktor konstans tagjának a hányadosa is K-beli. Ez az elem egy p-edik primitív egységgyök, amiből azonnal következik a tétel két további állítása.

Végül, ha K tartalmazza a p-edik egységgyököket és a polinom nem irreducibilis, akkor van egy $x - b \in K[x]$ faktora, és ekkor K-ban benne van az összes többi εb alakú gyök is. ■

Alapvető fontosságú a fenti tétel bizonyos fokú megfordíthatósága.

8.40. Tétel. *Legyen N a K test p-edfokú bővítése valamely p prímszámra, amely különbözik a test karakterisztikájától. Ha K tartalmazza a p-edik egységgyököket, akkor a következő két állítás ekvivalens:*

(1) *$N = K(b)$, ahol b az $x^p - a \in K[x]$ irreducibilis polinom gyöke.*

(2) *$G(N \mid K)$ ciklikus.*

Bizonyítás. Ha $N = K(b)$, akkor N az $x^p - a$ felbontási teste, mert K tartalmazza a p-edik egységgyököket. Válasszunk egy ε primitív p-edik egységgyököt. Ekkor annak az automorfizmusnak a hatványai, amely b-t εb-be viszi, előállítják mind a p darab relatív automorfizmust; tehát a Galois-csoport ciklikus.

Tegyük most fel, hogy $G(N \mid K) = [\sigma]$ ciklikus és rögzítsük az N egy K-n kívüli c elemét. Vegyük emellett a K-ban levő tetszőleges ε p-edik egységgyököt és készítsük el az

$$(\varepsilon, c) = c + \varepsilon^{-1}\sigma(c) + \cdots + \varepsilon^{-(p-1)}\sigma^{p-1}(c) \tag{I}$$

úgynevezett *Lagrange-féle rezolvenst.* Tekintsük ezek

$$c' = (\varepsilon, c) + (\varepsilon^2, c) + \cdots + (\varepsilon^p, c) \tag{II}$$

összegét, ahol ε egy primitív p-edik egységgyök. (I) figyelembevételével a (II) alatti összeget az

$$(\varepsilon^{-i} + \varepsilon^{-2i} + \cdots + \varepsilon^{-pi})\sigma^i(c) \tag{III}$$

összegek összegeként írhatjuk fel. (III)-ban az első tényező $i \neq 0$ esetén éppen a p-edik egységgyökök összege, tehát 0. Ha $i = 0$, akkor (III) első tényezője p, ami a karakterisztikára vonatkozó feltétel miatt 0-tól különböző. Így $c' = pc$ sem 0, mert $c \neq 0$, hiszen nem eleme K-nak. Ez utóbbi meggondolás azt is adja, hogy c' sem K-beli elem. Így a (II) alatti összeg tagjai között is van legalább egy, amelyik nincs K-ban. $(1, c)$-t a σ nyilván önmagába viszi, ami azt jelenti, hogy K-ban van, így $b = (\varepsilon, c) \notin K$ valamelyik p-edik primitív egységgyökkel lesz. Mivel $\varepsilon \in K$, ezért

$$\begin{aligned}\sigma(b) =& \sigma(c) + \varepsilon^{-1}\sigma^2(c) + \cdots + \varepsilon^{-(p-1)}\sigma^p(c) = \\ &= \varepsilon(\varepsilon^{-1}\sigma(c) + \varepsilon^{-2}\sigma^2(c) + \cdots + \varepsilon^0 c) = \varepsilon \cdot (\varepsilon, c) = \varepsilon b.\end{aligned} \tag{IV}$$

Ebből következik, hogy az $a = b^p$ elemre

$$\sigma(a) = \sigma(b^p) = (\sigma(b))^p = (\varepsilon b)^p = b^p = a, \tag{V}$$

azaz $a \in K$. Így b az $x^p - a \in K[x]$ polinom gyöke. $b \notin K$ miatt $N = K(b)$, a 8.5. következmény (2) pontja szerint. Ebből következik a fenti polinom irreducibilitása is – figyelembe véve a 8.1. tételt. ■

Megjegyzések. 1. A Lagrange-rezolvens konstrukciója első pillanatban rejtélyesnek tűnik. Valójában azonban egyáltalában nem az. Ha b az irreducibilis $x^p - a \in K[x]$ gyöke, akkor $K(b)$ minden eleme $c = u_0 + u_1 b + \cdots + u_{p-1}b^{p-1}$ alakú, ahol $u_i \in K$. Az $x \to \varepsilon^{-i}\sigma^i(x)$ leképezés az i-edik tagot változatlanul hagyja, míg a többit ε valamelyik hatványával szorozza; mégpedig más kitevő esetén mással. Az összeadás után lényegében egyetlen tag marad meg, valamelyik $u_j b^j$. Tekintettel arra, hogy nem minden u_j lehet 0, ezért valamelyikük (de nem u_0) éppen az a egy hatványának a p-edik gyöke lesz.

2. A szokásnak megfelelően az $x^p - a$ polinom gyökét $\sqrt[p]{a}$ fogja jelölni. Ez az elem nem egyértelmű. A jelölésnél mindig úgy gondoljuk, hogy valamelyik meghatározott gyökről, vagy bármelyik gyökről van szó. Általában ez az utóbbi eset következik be, mert az alaptest rendszerint tartalmazza a p-edik primitív egységgyököket, és ebben az esetben a polinom gyökei „egyenrangúak". □

Ezek után az előkészületek után megadjuk a polinomok megoldhatóságának a karakterizációját. A tételt két részre bontjuk, mert az nem teljesen akkor és csak akkor formájú. Mindenekelőtt azonban bebizonyítunk egy önmagában is érdekes segédtételt:

Lemma. *Legyen M a K-nak olyan véges szeparábilis normális bővítése, amely tartalmazza a p-edik egységgyököket. Ekkor a K-nak az a legkisebb M-et tartalmazó normális bővítése, amely tartalmazza $x^p - a \in M[x]$ egyik gyökét, az M felett gyökjelekkel elérhető, és minden nemtriviális bővítés foka p.*

Bizonyítás. Legyen M az $f(x) \in K[x]$ felbontási teste, és legyenek $a^{(1)}(= a), \ldots, a^{(r)}$ az a összes K feletti konjugáltjai. Legyen $g(x) = \prod\{(x^p - a^{(i)}) \mid i = 1, \ldots, r\}$. A szimmetrikus polinomok alaptétele következtében $g(x) \in K[x]$. Legyen N az $f(x) \cdot g(x)$ felbontási teste. Nyilván $M \leq N$, és persze N normális bővítés. Legyen $M_0 = M$, és $M_{i+1} = M_i(\sqrt[p]{a^{(i)}})$. Mivel a p-edik egységgyökök elemei M_i-nek, ezért a 8.39. tétel szerint $x^p - a^{(i)}$ vagy irreducibilis M_i felett, vagy lineáris faktorokra esik szét. Ennek megfelelően az M_{i+1} mindkét esetben gyökjelekkel elérhető M_i felett. Mivel a gyökjelekkel való elérhetőség tranzitív, ezért $N = M_r$ is gyökjelekkel elérhető M felett. A lemma utolsó állítása triviális. ■

8.41/A. Tétel. *Legyen $f(x) \in K[x]$ irreducibilis, és legyen az $f(x)$ polinom N felbontási teste szeparábilis. Ha $f(x)$ egy α gyöke eleme egy a K felett gyökjelekkel elérhető L testnek, akkor $f(x)$ Galois-csoportja feloldható.*

Bizonyítás. A gyökjelekkel való elérhetőség definíciója szerint létezik egy olyan $K = L_0 \leq L_1 \leq \ldots \leq L_n = L$ testlánc, hogy $L_{i+1} = L_i(\vartheta_i)$, ahol ϑ_i az $x^{p_i} - a_i \in L_i[x]$ irreducibilis prímfokú polinom gyöke. Az $f(x)$ Galois-csoportja a K test L-et tartalmazó legkisebb normális bővítésének a Galois-csoportja. Mivel egy normális bővítés Galois-csoportja egy nagyobb normális bővítés Galois-csoportjának a faktorcsoportja és feloldható csoport faktorcsoportja is feloldható, ezért elegendő találni egy L-et tartalmazó olyan normális bővítést, amelynek a Galois-csoportja feloldható.

Legyen $(L : K) = k$, és M_0 a K-nak az a bővítése, amely úgy áll elő, hogy K-t az összes k-adik egységgyökkel bővítjük. Mint tudjuk, $G(M_0 \mid K)$ kommutatív, tehát feloldható. Emellett $K = L_0 \leq M_0$ is triviálisan teljesül.

A továbbiakat n-re vonatkozó teljes indukcióval bizonyítjuk. Az $n = 0$ esetre a fentiek miatt az állítás igaz. Tegyük most fel, hogy valamely i-re már találtunk olyan M_i testet, hogy:

(1) $M_0 \leq M_i$,

(2) $G(M_i \mid K)$ feloldható,

(3) $L_i \leq M_i$.

Definiáljuk M_{i+1}-et úgy, mint M_i-nek azt a legkisebb normális bővítését, amelyik tartalmazza $x^{p_i} - a_i$ egyik gyökét. M_{i+1}-re (1) és (3) a konstrukció alapján teljesül. A lemma szerint M_{i+1} a K-nak olyan normális bővítése, amely M_i felett gyökjelekkel elérhető és az

egymás utáni bővítések foka mindig p_i: $M_i \leq \ldots \leq M_i^{(j)} \leq \ldots \leq M_{i+1}$. Mivel itt minden egyes $M_i^{(j+1)} \mid M_i^{(j)}$ bővítésnél binom egyenletet használtunk és a p_i-edik egységgyökök az alaptestben vannak, ezért a Galois-csoportok ciklikusak. Ezért $G(M_{i+1} \mid M_i)$ feloldható. A feloldható csoportok tulajdonságai miatt tehát feloldható $G(M_{i+1} \mid K)$ is. ■

8.41/B. Tétel. *Ha f(x) tetszőleges olyan polinom a nullkarakterisztikájú K test fölött, amelynek a Galois-csoportja feloldható, akkor $f(x)$ minden gyöke gyökkifejezés a K fölött, sőt, $f(x)$ felbontási teste része egy K felett gyökökkel elérhető testnek.*

Bizonyítás. Mindenekelőtt megjegyezzük, hogy a tétel olyan prím karakterisztika esetén is igaz, amely nagyobb, mint $(\mathrm{gr}(f))!$. A tételt a Galois-csoport rendjére vonatkozó teljes indukcióval bizonyítjuk. Ha ez 1, az állítás triviálisan igaz. Tegyük fel, hogy bármely, n-nél kisebb fokú normális bővítés esetén igaz az állítás és legyen a K-beli együtthatós $f(x)$ polinom N felbontási testének a K feletti foka n. A 8.37. tétel alapján az $f_n(x)$ körosztási polinom Galois-csoportja feloldható; és a bizonyításban látottak szerint rendje legfeljebb $\varphi(n)$, ami kisebb n-nél. A teljes indukciós feltevés szerint tehát létezik a K-nak olyan M bővítése, amely K-ból gyökökkel elérhető és tartalmazza az összes n-edik egységgyököt. (Ebből a lépésből következik, hogy csak azokat a karakterisztikákat kell kizárni, amelyek az $n, \varphi(n), \varphi(\varphi(n)), \ldots$ sorozat valamelyik elemének osztói – de speciális polinomok esetében még ezek is előfordulhatnak.) A gyökökkel elérhető bővítés definíciója alapján elég annak a bizonyítása, hogy $f(x)$-nek az M feletti N felbontási teste M felett gyökökkel elérhető. A K-nak az N-et tartalmazó legkisebb normális bővítésében tekintsük az $f(x)$ eredeti N_0 felbontási testét, és alkalmazzuk a 8.35. tétel (2) állítását, valamint az alaptételt. Ebből azt kapjuk, hogy $G(N \mid M) \cong G(N_0 \mid N_0 \cap M) \cong G(N \mid K)$, amiből következik, hogy $G(N \mid M)$ feloldható, mert egy feloldható csoport részcsoportjával izomorf, és Lagrange tétele miatt M tartalmazza az összes $|G(N \mid M)|$-edik egységgyököt.

Elég tehát a következő állítás bizonyítása: Ha N a karakterisztikafeltételt kielégítő (például nullkarakterisztikájú) K testnek olyan n-edfokú normális bővítése, amelynek G Galois-csoportja feloldható és K tartalmazza az összes n-edik egységgyököt, akkor N a K fölött gyökökkel elérhető.

Tekintsünk evégett egy

$$G = G_0 \supset \ldots \supset G_i \supset G_{i+1} \supset \ldots \supset G_n = \{1\}$$

kompozícióláncot. A feloldhatóság miatt a G_i/G_{i+1} faktorcsoport prímrendű. A $\Delta_i = \Delta(G_i)$ testekre a 8.35. tétel szerint teljesül, hogy $G(\Delta_{i+1} \mid \Delta_i) \cong G_i/G_{i+1}$. Miután a megfelelő egységgyökök már a Δ_i test K résztestének is elemei, alkalmazhatjuk a 8.40. tételt. Így Δ_{i+1} a Δ_i-nek éppen olyan bővítése, amely biztosítja, hogy N a K felett gyökökkel elérhető legyen. ■

Megjegyzés. A konstrukció „viszonylag nagy” gyökökkel elérhető testet adott. Ez nem véletlen, pontosabban szólva lehetséges, hogy egy normális bővítés része egy gyökökkel elérhető bővítésnek, de maga nem az. (Tehát egy gyökkifejezés olyan gyökökből van felépítve, amelyek „eleve” nem szükségesek.) Tekintsük például a racionális számtest felett az $x^3 - 3x + 1$ polinomot. Ennek racionális gyöke nincs, mert ha volna, akkor az csak egész és 1-nek osztója lehetne; márpedig páratlan helyen e polinom helyettesítési értéke páratlan, így nem lehet 0. Ebből az is következik, hogy ez a polinom irreducibilis, mert ha reducibilis volna, akkor feltétlenül lenne elsőfokú faktora is. Legyen a gyöke a fenti polinomnak, s $N = \mathbb{Q}(a)$. Az $a^3 = 3a - 1$ összefüggés alapján $(a^2 - 2)^3 = a^6 - 6a^4 + 12a^2 - 8 = \ldots = 3(a^2 - 2) - 1$, ami azt jelenti, hogy $a^2 - 2$ is gyöke a fenti polinomnak. A

polinom irreducibilitásából következik, hogy e két gyök különböző, ezért N-ben a fenti polinom lineáris faktorokra bomlik. Így N a racionális számtest normális bővítése, amelynek a Galois-csoportja triviálisan feloldható. Nem lehet azonban ez a test a racionális számtest felett gyökökkel elérhető. Ekkor ugyanis egy köbgyökkel való bővítés volna, amiből a bővítés normalitása és a 8.39. tétel harmadik esete miatt az következne, hogy ez a test tartalmazná a harmadik egységgyököket, amelyek a racionális számtest egy másodfokú bővítésében vannak; s így 2 osztója volna 3-nak. Egyébként pontosan itt érthető meg a Casus irreducibilis. □

8.10. Konkrét polinomtípusok megoldhatósága

Az előzőekben olyan feltételt adtunk a gyökjelekkel való megoldhatóságra, amelynek teljesülését nem tudjuk ellenőrizni, mert nincs általánosan használható módszer egy polinom Galois-csoportjának a meghatározására.

Az alábbiakban konkrét polinomfajtákat vizsgálunk. Mindenekelőtt egy igen fontos speciális esettel foglalkozunk.

8.42. Definíció. A K test feletti általános n-edfokú polinomnak nevezzük az

$$x^n + y_{n-1}x^{n-1} + \cdots + y_1x + y_0$$

polinomot, ahol $y_0, \ldots, y_{n-1}$ határozatlanok a K test felett. □

Megjegyzések. 1. Vegyük észre, hogy az általános n-edfokú polinom tulajdonképpen csak a K test karakterisztikájától függ. Hiszen a K test elemei egyáltalában nem lépnek fel, de ha a határozatlan együtthatókkal műveleteket végzünk, az eredmény a karakterisztikától függően eltérő lehet.

2. A középiskolában az általános másodfokú egyenlet $ax^2 + bx + c = 0$ alakú. A kapott megoldóképletben az a paraméter a nevezőben szerepel. Ez azért okoz gondot, mert az $a = 0$ esetben a képlet értelmetlenné válik. Persze ekkor a másodfokú egyenlet nem is igazán másodfokú. Éppen ezért célszerű a legmagasabbfokú tag együtthatójával végigosztani; amikor pontosan olyan alakhoz jutunk, amilyen a fenti definícióban szerepel. Az egészek tárgyalásakor (10.1. pont) majd észrevehető lesz, hogy a megoldásnál az együtthatókkal nem kell osztani; a nevezőkben csak konkrét – n-től függő – egész számok lehetnek. □

8.43. Tétel. *Az általános n-edfokú polinom Galois-csoportja az n-edfokú szimmetrikus csoport.*

Bizonyítás. Tekintsük a K feletti $x_1, \ldots, x_n$ határozatlanokat, és jelölje $\sigma_i = \sigma_i(x_1, \ldots, x_n)$ e határozatlanok i-edik elemi szimmetrikus polinomját. Tekintsük azt a

$$\varphi : K[y_0, \ldots, y_{n-1}] \to K(x_1, \ldots, x_n)$$

homomorfizmust, amely a K testet fixen hagyja és y_i-t a $(-1)^{n-i}\sigma_{n-i}$-be viszi. Ilyen homomorfizmus a polinomgyűrűk definíciója alapján létezik. A szimmetrikus polinomok alaptétele szerint egyrészt $\operatorname{Im} \varphi = K[\sigma_1, \ldots, \sigma_n]$, másrészt $\operatorname{Ker} \varphi = \{0\}$, vagyis a homomorfizmus injektív. Ekkor viszont ez a homomorfizmus egyértelműen kiterjeszthető a hányadostestekre és létezik kiterjesztése az általános n-edfokú polinom felbontási testére is, továbbá ezek mindegyike ugyancsak injektív. Ez a homomorfizmus az általános n-edfokú polinom $u_1, \ldots, u_n$ gyökeit az $(x-x_1)\cdot\ldots\cdot(x-x_n)$ polinom gyökeire képezi le. Mivel a kiterjesztésben a $K(x_1, \ldots, x_n)$ mindegyik eleme előáll képként, ezért egy $K(u_1, \ldots, u_n) \to K(x_1, \ldots, x_n)$ izomorfizmust kaptunk, amelynél y_i képe $(-1)^{n-i}\sigma_{n-i}$. Ebből pedig következik,

hogy a $K(u_1, \ldots, u_n)$ testnek a $K(y_0, \ldots, y_{n-1})$ feletti, valamint a $K(x_1, \ldots, x_n)$ testnek a $K(\sigma_1, \ldots, \sigma_n)$ feletti Galois-csoportja izomorf. Ez utóbbi Galois-csoport viszont éppen az n-edfokú szimmetrikus csoport: a $K(x_1, \ldots, x_n)$ test minden $K(\sigma_1, \ldots, \sigma_n)$ fölötti relatív automorfizmusa az x_i elemeket permutálja, de minden ilyen permutáció kiterjeszthető relatív automorfizmussá, s a különbözők különböző automorfizmusokká. ■

Megjegyzés. A fenti vizsgálatokat egy igen érthető cél helyezte előtérbe. A másod-, harmad-, illetve negyedfokú egyenletekre adódó megoldóképletek után nemcsak az volt a kérdés, hogy meg lehet-e oldani minden egyenletet, hanem az is, hogy létezik-e valamilyen univerzális megoldóképlet. Nos, világos, hogy ha az n-edfokú általános „egyenlet" gyökjelekkel megoldható, akkor az „általános megoldás" minden konkrét esetben jó lesz, azaz megoldóképletet szolgáltat. Természetesen, ha létezik megoldóképlet az n-edfokú egyenletekre, akkor minden n-edfokú egyenlet (gyökjelekkel) megoldható. Bebizonyítható, hogy ha egy 0 karakterisztikájú test felett minden n-edfokú egyenlet megoldható, akkor az általános n-edfokú egyenlet is megoldható. Ha csak azt tudjuk, hogy a test végtelen, akkor a megoldóképlet létezése esetén bizonyítható, hogy az általános n-edfokú egyenlet megoldható. A felsorolt fogalmak különbözőek: a 61 elemű test esetén például létezik $n = 5$-re megoldóképlet, de az általános ötödfokú egyenlet – mint ezt később látni fogjuk – nem oldható meg. A fenti test algebrai lezártja fölött viszont nem létezik megoldóképlet sem, annak ellenére, hogy bármely ötödfokú egyenlet gyökei előállíthatók az együtthatókból gyökkifejezésként. A továbbiakban azt nézzük meg, hogy milyen n esetén létezik megoldóképlet az általános n-edfokú polinomra. □

8.44. Tétel.

(1) *$n \leq 4$ esetén az általános n-edfokú polinom felbontási teste gyökökkel elérhető.*

(2) (Ruffini-Abel) *$n \geq 5$ esetén az általános n-edfokú polinom felbontási teste gyökökkel nem elérhető.*

Bizonyítás. A 8.41. tétel szerint a gyökökkel való elérhetőség szükséges és elégséges feltétele a polinom Galois-csoportjának a feloldhatósága. A 8.43. tétel szerint az általános n-edfokú polinom Galois-csoportja S_n, amely a 6.31. tétel szerint nem feloldható, ha $n \geq 5$, egyébként pedig feloldható. ■

Megjegyzés. A 6.31. tételben az is szerepel, hogy S_n-nek mindig van 2 indexű részcsoportja (ha $n \geq 2$), nevezetesen az A_n. Mivel ez normálosztó, ezért az általános n-edfokú egyenlet gyökjelekkel való megoldásából egy lépés mindig elvégezhető, hiszen $\Delta(A_n)$ mindig másodfokú bővítést ad, ami a 8.40. tétel miatt mindig egy négyzetgyökkel való bővítést jelent. Ez a négyzetgyök könnyen meghatározható; választható például a határozatlanok generálta Vandermonde-determinánsnak. Ez – mint tudjuk – a határozatlanok alternáló polinomja. Így négyzetét minden relatív automorfizmus fixen hagyja, de őt csak az alternáló csoport elemei. Ezt a polinomot az eredeti n-edfokú polinom D diszkriminánsának nevezzük. Ugyanígy értelmezhetjük a diszkriminánst minden más polinom esetében, s ha a polinom gyökeit gyökkifejezésként akarjuk előállítani, akkor a diszkrimináns meghatározása az első lépés. Másodfokú polinomok esetében a diszkrimináns éppen a négyzetgyök alatt álló kifejezés. Harmadfokú polinomok esetében azonban nem pontosan ez áll a négyzetgyök alatt. Természetesen az is előfordul, hogy egy konkrét polinom esetében a diszkrimináns már benne van a kiindulási testben. □

A gyökképlet meghatározása másod-, harmad-, negyedfokú polinomok esetére elvégezhető a Lagrange-féle rezolvens segítségével. Erre azonban nem térünk ki, mert az első két esetben az ismert gyökképlet adódik, míg a negyedfokú polinomokra itt is túlságosan bonyolult eljárást kaphatunk.

Visszatérünk azonban arra a kérdésre, hogy nem lehetséges-e például minden egyes racionális együtthatós ötödfokú polinomra külön-külön megoldóképletet kapni.

8.45. Tétel. *Van olyan ötödfokú egész együtthatós polinom, amelynek egyetlen gyöke sem gyökkifejezés a racionális test felett.*

Bizonyítás. A 8.41. tétel alapján olyan ötödfokú polinomot kell találnunk, amelynek a Galois-csoportja nem feloldható. Mivel ötödfokú polinomokat vizsgálunk, ezért a Galois-csoport a gyökök egy permutációcsoportja, azaz S_5 egy részcsoportja.

Tekintettel arra, hogy reducibilis ötödfokú polinom megoldhatósága visszavezethető alacsonyabbfokú polinomok megoldhatóságára, ezért csak irreducibilis polinomot kell néznünk. Ez azt jelenti, hogy a polinom gyökei konjugáltak, vagyis bármely gyököt bármely másik gyökbe átvisz egy relatív automorfizmus. Más szóval az irreducibilitás miatt a polinom Galois-csoportja tranzitív. A 6.32. tétel szerint, ha S_5 egy tranzitív részcsoportja feloldható, akkor benne egyedül az identikus permutáció hagy fixen két elemet.

Célunk eléréséhez tehát olyan ötödfokú irreducibilis polinomot kell találni, amelyhez létezik két gyökét fixen hagyó nem identikus permutáció. Legyen N a kérdéses $\mathbb{Q}$ feletti polinom felbontási teste. Ha a két fixen hagyott gyök a és b, akkor a feloldhatóság (megoldhatóság) szükséges feltétele az, hogy $\mathbb{Q}(a,b) = N$. Elég tehát olyan polinomot találni, amelynek valamely két a és b gyökére $\mathbb{Q}(a,b) < N$.

Azt állítjuk, hogy $f(x) = x^5 - 4x + 2$ egy megfelelő ötödfokú polinom. A Schönemann–Eisenstein-tétel alapján ez a polinom irreducibilis. $f(-1) < 0$, $f(2) > 0$, $f(1) < 0$ és $f(2) > 0$ alapján e polinomnak van három valós gyöke. E polinom deriváltja $f'(x) = 5x^4 - 4$; és így a deriváltnak csak két valós gyöke van, tehát az eredeti polinomnak nem lehet háromnál több valós gyöke. Ha vesszük az eredeti polinom (bármely) két valós gyökét, az általuk generált testben nem lehetnek benne a nem valós gyökök; így az ezek által generált test nem lehet az egész felbontási test: a megfelelő egyenlet nem lehet gyökjelekkel megoldható. ■

A következő tételben bemutatunk olyan „tisztán algebrai” eljárást, amelynek a segítségével „tömegesen” készíthetők nem megoldható egyenletek; sőt olyanok, amelyeknek a Galois-csoportja a szimmetrikus csoport.

Az eddigiekben tárgyaltak még nem nyújtottak lehetőséget arra, hogy egy polinomról eldönthessük, hogy gyökei gyökkifejezések-e. Ehhez arra volna még szükség, hogy – legalább elvileg – meghatározhassuk egy tetszőleges polinom Galois-csoportját. A következő tétel ezt teszi lehetővé. A tételnek a teljes kimondása túlságosan bonyolult volna, ezért csak vázlatosan és részekre bontva mondjuk ki.

8.46/A. Tétel. *Egy test feletti egyszeres gyökökkel rendelkező polinom Galois-csoportja mint a gyökök permutációcsoportja előállítható a test feletti többhatározatlanú polinomgyűrű egy irreducibilis polinomját önmagába vivő permutációk csoportjával.*

Bizonyítás. Legyenek az $f(x) \in K[x]$ többszörös gyök nélküli legalább harmadfokú normált polinom gyökei a polinom N felbontási testében $a_1, \ldots, a_n$. Legyenek $u_1, \ldots, u_n$ határozatlanok K felett, továbbá legyen $\overline{K} = K(u_1, \ldots, u_n)$ és $\overline{N} = N(u_1, \ldots, u_n)$. A nyilvánvaló $\overline{N} = \overline{K}(a_1, \ldots, a_n)$ összefüggés alapján a kapcsolatot a következő (kommutatív)

diagrammal szemléltethetjük:

$$\begin{array}{ccc} K & \longrightarrow & \overline{K} = K(u_1, \ldots, u_n) \\ \downarrow & & \downarrow \\ N = K(a_1, \ldots, a_n) & \longrightarrow & \overline{N} = N(u_1, \ldots, u_n). \end{array}$$

A szereplő nyilak a megfelelő természetes beágyazást jelölik.

Az automorfizmusoknak az egyszerű transzcendens bővítésekre való kiterjeszthetősége alapján a $G = G(N \mid K)$ Galois-csoport minden σ eleme egyértelműen kiterjeszthető az $\overline{N}$ egy $\overline{\sigma}$ automorfizmusává, amelyre tetszőleges $b \in N$ esetén $\overline{\sigma}(b) = b$, míg az u_i elemek minden hatványszorzatát önmagába viszi. Speciálisan $\overline{\sigma}\left(\sum b_i u_i\right) = \sum \sigma(b_i) u_i$ (ahol $b_i \in N$). Ezek az automorfizmusok egy G-vel természetes módon izomorf $\overline{G}$ csoportot alkotnak. Mivel G elemei a K testet fixen hagyják, ezért $\overline{G}$ elemei fixen hagyják $\overline{K}$ elemeit. Így $\overline{G}$ elemei az $\overline{N} \mid \overline{K}$ bővítésnek relatív automorfizmusai.

Tetszőleges $\pi \in S_n$ permutációra a polinomgyűrűk definiáló tulajdonsága alapján létezik az $N[u_1, \ldots, u_n]$ polinomgyűrűnek egy olyan π^* automorfizmusa, amely az N elemeit fixen hagyja és az u_i határozatlant az $u_{\pi(i)}$ határozatlanba viszi. Speciálisan $\pi^* : \sum b_i u_i \to \sum b_i u_{\pi(i)}$, ahol $(b_i \in N)$. Ezek a hányadosgyűrűre vonatkozó 7.30. tétel szerint (illetve e tétel bizonyításának elején levő megjegyzés alapján) egyértelműen kiterjeszthetők az $\overline{N}$ hányadostest automorfizmusaivá. Világos, hogy a kapott automorfizmusok egy S_n-nel izomorf S_n^* csoportot alkotnak, amelynek elemei N elemeit fixen hagyják.

Legyen $t_1 = a_1 u_1 + \ldots + a_n u_n$ és tekintsük a $t_\pi = \pi^*(t_1)$ elemeket $(t_\iota = t_1)$. Ezután legyen

$$F(x) = F(x, u_1, \ldots, u_n) = \prod_{\pi \in S_n} (x - t_\pi) \in \overline{N}[x].$$

$F(x)$ az a-kban szimmetrikus, így eleme $\overline{K}[x]$-nek is. Legyen $F(x) = F_1(x) \cdot \ldots \cdot F_r(x)$ a $\overline{K}$ feletti irreducibilis faktorokra való felbontás. $F_1(x)$ együtthatói $\overline{K}$-beliek, ezért $\overline{G}$ elemei fixen hagyják. Ebből következik, hogy $\overline{G}$ bármely $\overline{\sigma}$ eleme az $F_1(x)$ tetszőleges $x - t_\pi$ faktorát ugyancsak az $F_1(x)$ valamelyik faktorára képezi. Legyen $K_1 \leq \overline{K}$ az F_1 együtthatói által a K felett generált test. (Hasonlóképpen definiálható bármely i-re az F_i-hez tartozó K_i test.)

Tekintsük most tetszőleges $\overline{\sigma} \in \overline{G}$ mellett az $x - \overline{\sigma}(t_1)$ polinomok $H(x)$ szorzatát. Mivel ennek együtthatóit $\overline{G}$ minden eleme fixen hagyja, ezért $H(x) \in \overline{K}[x]$.

Tekintettel arra, hogy t_1 mind az $F_1(x)$, mind a $H(x)$ polinomnak gyöke, és $F_1(x)$ irreducibilis $\overline{K}$ felett, ezért $F_1(x)$ osztója $H(x)$-nek. Másrészt $F_1(x) \in \overline{K}[x]$ miatt ezt a polinomot $\overline{G}$ minden eleme önmagába viszi. Vegyük figyelembe, hogy $H(x)$ lineáris faktorai – amelyek mind különbözőek – éppen az $(x - t_1)$-nek $\overline{G}$ elemeivel vett képei. Így $F_1(x)$-nek és $H(x)$-nek ugyanannyi lineáris faktora van felbontási testükben; tehát megegyeznek.

Tekintsük most G-t mint $f(x)$ gyökeinek a permutációit. Minden $\sigma \in G$ meghatároz egy $\pi_\sigma \in S_n$ permutációt, amelyre $\sigma(a_i) = \pi_\sigma(a_i) = a_{\pi(i)}$.

A megfelelő π_σ^* automorfizmusok a szimmetrikus polinomok alaptétele miatt az $F(x)$ polinomot önmagukba viszik.

Nézzük meg, mely π permutációk esetén viszik a π^* automorfizmusok az $F_1(x)$ polinomot önmagába. Ennek természetesen feltétele az, hogy π^* az $x - t_1$ tényezőt valamelyik $x - \overline{\sigma}(t_1)$ tényezőbe vigye. Ha az a_i elemek indexeinek a $\overline{\sigma}$-hoz tartozó permutációja τ, akkor az adódik, hogy $\sum a_{\tau(i)}u_i = \overline{\sigma}\left(\sum a_i u_i\right) = \sum a_i u_{\pi(i)}$. Mivel az u_i elemek N felett határozatlanok, ezért a fenti egyenlőségből $\pi^{-1}(i) = \tau(i)$ következik.

Legyen $\overline{\varrho}(t_1) = \sum a_{\mu(i)}u_i$ az $F_1(x)$ egy tetszőleges (másik) gyöke. Erre alkalmazva π^*-ot a következőket kapjuk:

$$\pi^*(\overline{\varrho}(t_1)) = \sum a_{\mu(i)}u_{\pi(i)} = \sum a_{\mu(\pi^{-1}(i))}u_i = \sum a_{\mu(\varrho(i))}u_i = \overline{\varrho}(\overline{\sigma}(t_1));$$

azaz ez a π^* automorfizmus valóban önmagába viszi az F_1 polinomot. Tekintettel arra, hogy $\pi^*\pi_\alpha$ minden elemet önmagába visz, ezért $\overline{G}$ (és így G is) permutációcsoportként inverz izomorf az $F_1(x)$ polinomot önmagába képező π^*-ok csoportjával. Ez azt jelenti, hogy minden egyes $\sigma \in G$ esetén a megfelelő π^* permutációt úgy kaphatjuk, hogy a szereplő idegen ciklusok elemeit fordított sorrendben írjuk fel. ■

8.46/B. Tétel. *A 8.46/A. tétel eredményei alkalmazhatók egész együtthatós polinomokra is.*

Bizonyítás. Tekintsünk most egy $f(x) \in \mathbb{Z}[x]$ többszörös gyök nélküli legalább harmadfokú normált polinomot. Legyenek ennek a gyökei $a_1, \ldots, a_n$, és legyenek $u_1, \ldots, u_n$ határozatlanok ($\mathbb{Q}$ felett). Legyen $R = \mathbb{Z}[u_1, \ldots, u_n]$ (gyűrűbővítés), $\overline{\mathbb{Z}} = \mathbb{Z}[u_1, \ldots, u_n]$ (polinomgyűrű) és $\overline{R} = R[u_1, \ldots, u_n]$ (polinomgyűrű). A $K = \mathbb{Q}$ esetben tekintve az előző bizonyítást, megkaphatjuk az $f(x)$ Galois-csoportját mint a határozatlanok permutációcsoportját. Az egyetlen kérdés az, hogy az R-be nem kerülnek-e $\mathbb{Q}$-nak olyan elemei, amelyek nincsenek $\mathbb{Z}$-ben. Ezt a gyűrű feletti egész elemek vizsgálatánál fogjuk belátni. ■

8.46/C. Tétel. *Egész együtthatós polinom Galois-csoportja részpermutációkként tartalmazza a modulo p vett polinom Galois-csoportjának elemeit.*

Bizonyítás. Legyen most p tetszőleges prímszám és tegyük fel, hogy $f(x)$-nek $\mathbb{Q}_p$ felett sincsenek többszörös gyökei. A $\mathbb{Q}$ (és $\mathbb{Z}$) felett vizsgált $F(x)$ polinom $F_1(x)$ faktora $\mathbb{Q}_p$ felett nem feltétlenül irreducibilis (nagyon ritkán az). Ezért tovább bomlik $F_1(x) = F_{1,1}(x) \cdot \ldots \cdot F_{1,s}(x)$ szorzattá. Most az eredeti polinom Galois-csoportja a határozatlanok azon permutációiból fog állni, amelyek az $F_{1,1}(x)$ polinomot viszik önmagába. Ezek, az $F_1(x)$ $\mathbb{Q}$ feletti irreducibilitása alapján, az $F(x)$ polinomot is önmagába viszik. A kapott permutációk tehát előfordulnak az $f(x)$ eredeti Galois-csoportjában is. ■

Megjegyzések. 1. Tekintettel arra, hogy itt prímkarakterisztikájú test feletti határozatlanokkal bővítünk, ezért a kapott test nem tökéletes. Emiatt nem elegendő csupán tökéletes test felett vizsgálni

a Galois-elméletet. Az persze világos, hogy a bővítés szeparábilis, mert $\mathbb{Q}_p$-beli polinom gyökeivel bővítünk. (Arra viszont vigyázni kell, hogy e polinomnak ne legyenek többszörös gyökei.)

2. A fenti meggondolás ellentmondani látszik a 8.42. definíció előtti állításnak, mely szerint a Galois-csoport meghatározására nincs általánosan használható módszer. Ha a fenti eljárást másodfokú polinomra alkalmazzuk, nem nyerünk semmit. Ha n-edfokú polinomot tekintünk, akkor a fent kapott polinomban a határozatlanok száma $n+1$, és a polinom foka $n!$. Ez – segédeszközök nélkül – már harmadfokú polinom esetén is elég reménytelen feladat. □

A továbbiakhoz szükségünk van egy, az S_n csoportra vonatkozó segédtételre:

Lemma. *Ha S_n egy G részcsoportja tartalmaz transzpozíciót, n hosszúságú és $n-1$ hosszúságú ciklust, akkor $G = S_n$.*

Bizonyítás. Legyen az $n-1$ hosszúságú ciklus $\tau = (1, 2, \ldots, n-1)$. Mivel G-ben van n hosszúságú ciklus, ezért G tranzitív. Így az eredeti (i, j) transzpozíció áttranszformálható (k, n) alakba, ahol $1 \leq k < n$. Ezt τ hatványaival transzformálva, a $\tau^{-1}(k, n)\tau$ permutációk megadják az összes (i, n) transzpozíciót $(1 \leq i < n)$, amelyek generálják S_n-t. ■

8.47. Tétel. *Konstruálható olyan egész együtthatós polinom, amelynek a Galois-csoportja a szimmetrikus csoport.*

Bizonyítás. Mivel véges test felett egy irreducibilis polinom Galois-csoportja ciklikus, és a ciklus hossza megegyezik a polinom fokával, ezért az $f(x)$ polinomhoz elegendő olyan prímszámokat találni, amelyekre rátérve

(1) $f(x)$ képének egyetlen másodfokú irreducibilis faktora van és a többi irreducibilis faktor foka páratlan,

(2) $f(x)$ képének egyetlen $(n-1)$-edfokú irreducibilis faktora van,

(3) $f(x)$ képe irreducibilis.

Egyedül az első eset szorul némi magyarázatra. Itt ugyanis a kapott ciklusfelbontásban egyetlen transzpozíció lesz, és a többi ciklus páratlan. Világos, hogy ekkor e permutációnak egy hatványa transzpozíció, tehát a csoport tartalmaz transzpozíciót. Természetesen elegendő egy vagy két további tényezőt venni, attól függően, hogy n páratlan vagy páros.

Legcélszerűbb a három legkisebb prímszámot venni. Legyen f_1 n-edfokú irreducibilis $\mathbb{Q}_2$ felett, f_2 egy $(n-1)$-edfokú irreducibilisnek és egy lineárisnak a szorzata $\mathbb{Q}_3$ felett és f_3 egy másodfokú és egy vagy két páratlanfokú irreducibilis polinomnak a szorzata (mind normált). Ekkor könnyen látszik, hogy például az

$$f = -15f_1 + 10f_2 + 6f_3 \in \mathbb{Z}[x]$$

ugyancsak normált polinom lesz, amelynek a Galois-csoportja a szimmetrikus csoport. ■

Megjegyzések. 1. Könnyen belátható, hogy az n-edfokú polinomok $(n > 4)$ „pozitív százalékának” a Galois-csoportja a szimmetrikus csoport. Ezt úgy tehetjük meg, hogy vesszük az összes olyan polinomot (elég a normáltakat nézni), amelyeknek az együtthatói egy N korlát alá esnek, és ezek közül azokat, amelyeknek a Galois-csoportja a szimmetrikus csoport. Ha ez utóbbiak száma a_N, az előbbiek száma b_N, akkor belátható, hogy elég nagy N esetén az a_N/b_N hányados nagyobb, mint egy pozitív konstans. Az is igaz, hogy e hányados határértéke 1, ha N tart a végtelenhez. Ezt úgy értelmezhetjük, hogy „szinte minden” polinom Galois-csoportja a szimmetrikus (következésképpen „szinte egyetlen magasabbfokú polinom sem gyökjelekkel megoldható”).

2. Hosszú idő óta megoldatlan az az EMMY NOETHERtől származó kérdés, hogy minden véges csoport előfordul-e $\mathbb{Z}$ feletti polinom Galois-csoportjaként.

3. Ismeretes a Galois-elméletnek W. KRULLtól való általánosítása, amely végtelen algebrai bővítésekre vonatkozik. Itt egy topológiát vezetnek be: két automorfizmus „közel van" egymáshoz, ha egy véges (normális) bővítésen megegyeznek. Itt a Galois-megfeleltetésben a közbülső testek és a topológiában zárt részcsoportok szerepelnek. Mivel a topológia kompakt, ezért a Galois-csoport számossága legalább kontinuum (ha nem véges). Mivel a $\mathbb{Q}$ felett minden Galois-csoport a bővítés automorfizmuscsoportja, ezért kérdezhető, hogy mi lehet egy test automorfizmuscsoportja. Az egyszerű transzcendens bővítéseknél láttunk példát megszámlálható automorfizmuscsoportra. Be lehet bizonyítani, hogy minden csoport előáll egy alkalmas test automorfizmuscsoportjaként. Még az is igaz, hogy a test valamely résztestének az automorfizmuscsoportja sem függ az eredeti test automorfizmuscsoportjától. □

8.11. A geometriai szerkeszthetőség algebrai elmélete

Ismeretes, hogy a koordinátageometria segítségével lehetőség nyílik a geometriai szerkesztések algebrai megfogására, amely nem mindig „szép" ugyan, de általában eredményes. Ez a módszer arra is alkalmas, hogy egy-egy geometriai feladatról eldöntsük: adott „eljárással" megszerkeszthető-e vagy sem.

Mindenekelőtt tisztáznunk kell az eljárás fogalmát. Ez annak a meghatározását jelenti, hogy milyen szerkesztési eszközöket használhatunk és milyen módon. Geometriai szerkesztéseknél lényegében az úgynevezett *euklideszi szerkesztéseket* szokták vizsgálni, ami a következőket jelenti:

a) *Két adott ponthoz odaillleszthetjük a vonalzót, és meghúzhatjuk a rajtuk átmenő egyenest.*

b) *Egy adott pontba beleszúrhatjuk a körző hegyét, és kinyithatjuk akkorára, hogy a másik vége egy másik adott pontig érjen.*

c) *Kinyitott körzőt beszúrunk egy adott pontba és a másik végével kört rajzolhatunk.*

d) *Ha megrajzolt körök és egyenesek közül kettő metszi egymást, akkor ezt a metszéspontot is adottnak tekinthetjük.*

Ezeket a feltételeket geometriai alakba írjuk át.

8.48. Definíció. Legyen H a síknak egy pontokból, egyenesekből és körökből álló halmaza. H-ból közvetlenül szerkeszthetőnek nevezzük

(1) a H pontjait;

(2) két H-beli ponton átmenő egyenest;

(3) H-beli középpontú kört, ha sugara megegyezik két H-beli pont távolságával;

(4) két, H-ból közvetlenül szerkeszthető egyenesnek vagy körnek a metszéspontjait.

Adott H halmaz esetén H elemeit H-ból 0 lépésben szerkeszthetőnek nevezzük; ha H_i elemei a H-ból i lépésben szerkeszthetők, akkor H-ból $i+1$ lépésben szerkeszthetőnek nevezzük a H_i-ből közvetlenül szerkeszthető H_{i+1} halmazt.

A sík egy pontját, egyenesét vagy körét a H-ból szerkeszthetőnek nevezzük, ha valamely i természetes számra eleme H_i-nek. □

Megjegyzések. 1. A tényleges szerkesztéseknél nem tekintik megszerkesztettnek egy körnek és egy érintőjének a „metszéspontját". A továbbiakban ez nem is fog előfordulni.

2. Tekintettel arra, hogy általában a körök is és az egyenesek is megadhatók két ponttal, ezért csak arra az esetre fogunk szorítkozni, amikor egy ponthalmazból szerkesztünk; és az adott ponthalmazból szerkeszthető pontokat vizsgáljuk. Ha az eredetileg adott ponthalmaznak csak egyetlen pontja van, akkor ebből nyilván nem szerkeszthető semmi; éppen ezért feltesszük, hogy az adott ponthalmaz legalább kételemű. □

A szerkeszthetőség algebrai átfogalmazásához egy fogalomra lesz szükségünk:

8.49. Definíció. A K test 2-bővítésének nevezünk egy testet, ha az K felett gyökökkel elérhető úgy, hogy minden szereplő irreducibilis polinom másodfokú. □

8.50. Tétel. *Legyen egy síkbeli koordináta-rendszer* $(0,0)$ *és* $(1,0)$ *koordinátájú pontja a* H *ponthalmaz egy-egy eleme, és legyen* K *a* H*-beli pontok koordinátái által generált test. A sík egy pontja akkor és csak akkor szerkeszthető meg a* H *pontjaiból, ha e pont mindkét koordinátája eleme a* K *test egy* 2*-bővítésének.*

Bizonyítás. A pontok koordinátái mellett tekinthetjük az egyenesek és a körök „koordinátáit”, azaz ezek egyenleteinek az együtthatóit. Ezek az együtthatók nem egyértelműek ugyan, de a továbbiakban mindig elegendő egy lehetséges esetre gondolni. Ha pontok segítségével előállítunk egyenest vagy kört, akkor feltehető, hogy ezek valamennyi koordinátája – mint az elemi koordinátageometriából ismeretes – ugyanabban a testben lesz, amelyben a pontok koordinátái voltak. Ugyancsak az elemi koordinátageometriai ismeretekre támaszkodva állíthatjuk az alábbiakat:

két egyenes metszéspontjának a koordinátái ugyanabban a testben vannak, mint az egyenesek koordinátái;

egy kör és egy egyenes vagy két kör metszéspontjainak a koordinátái olyan testben vannak, amely az eredeti koordinátáknak egy másodfokú bővítése. Az így megszerkeszthető pontok koordinátái valóban egy 2-bővítésben vannak.

A megfordítás bizonyításához három lépésre van szükség. Először is megszerkesztjük a koordinátatengelyeket (két pont összekötése és egy egyenesre adott pontban merőleges szerkesztése). (Erről tudjuk, hogy a kívánt módon megtehetjük.) A kérdéses koordináták megszerkesztése a következő feladat. (Ezt majd részletesen megvizsgáljuk.) Végül két merőleges szerkesztésével meghatározzuk a kívánt pontot. Azt kell tehát még belátni, hogy adott távolságok ismeretében az ezek generálta test bármely 2-bővítésének bármely eleme megszerkeszthető. Mivel egy koordináta csak valós szám lehet, így csak a 2-bővítés valós elemeinek a megszerkeszthetőségét kell kimutatni. Ennél „többet” mutatunk meg, nevezetesen azt, hogy a 2-bővítésben levő bármely komplex számnak mind a valós, mind a képzetes része megszerkeszthető. Az elemi geometriából tudjuk, hogy távolságok összege, különbsége, szorzata, hányadosa és négyzetgyöke megszerkeszthető. (A hányados szerkesztésekor persze az osztó nem lehet 0; s a szorzat, hányados és négyzetgyök szerkesztése során felhasználjuk, hogy felvettünk egy egységnyi hosszúságú szakaszt.) Ebből természetesen az is következik, hogy a felvett pontok koordinátái generálta test minden eleme megszerkeszthető. Tegyük fel, hogy egy test bármely komplex elemének valós és képzetes része – valamilyen adatokból – megszerkeszthető; elegendő annak a bizonyítása, hogy ugyanez igaz a test minden másodfokú bővítésére. Ha a, b, c, d szerkeszthetők, akkor az $a+bi$ és $c+di$ komplex számok összegére, különbségére, szorzatára és hányadosára triviálisan adódik a szerkeszthetőségi feltétel. Legyen a és b szerkeszthető, és legyen $(u+vi)^2 = a+bi$.

Ebből következik, hogy $u^2 = (a + \sqrt{a^2 + b^2})/2$ és $v^2 = (-a + \sqrt{a^2 + b^2})/2$. A négyzetgyök szerkeszthetőségét is figyelembe véve kapjuk, hogy u is és v is szerkeszthető. ■

Érdemes megjegyezni, hogy K nem függ a koordináta-rendszertől.

A 8.50. tételben kapott eredményt a Galois-elmélet segítségével sokkal hasznosabb formában is meg tudjuk fogalmazni. Az alábbi eredmények egyszerűbb eljárással is megkaphatók, de hiszen a Galois-elmélet már úgyis rendelkezésünkre áll.

8.51. Tétel. *A K számtest felett irreducibilis $f(x)$ polinom valós gyökei akkor és csak akkor szerkeszthetők az $f(x)$ együtthatói generálta testből, ha ez utóbbi test felett az $f(x)$ Galois-csoportjának a rendje 2-hatvány.*

Bizonyítás. Teljesen úgy járhatunk el, mint a 8.41. tételek bizonyításakor. Két dolgot kell csupán figyelembe venni. Egyrészt azt, hogy ha n 2-hatvány, akkor $\varphi(n)$ is az; másrészt azt, hogy 2-hatványrendű csoport p-csoport, tehát feloldható. ■

8.52. Következmény. *Legyen $f(x)$ egy számtestbeli együtthatós polinom, amely irreducibilis az együtthatói generálta test fölött. Annak a szükséges (de nem elégséges!) feltétele, hogy az $f(x)$ valamelyik gyöke a szóban forgó test fölött szerkeszthető legyen, az, hogy $f(x)$ foka 2-hatvány.*

Bizonyítás. Ha valamelyik gyök szerkeszthető, akkor a 8.51. tétel alapján a feltétel szerint $f(x)$ Galois-csoportjának a rendje 2-hatvány. Mivel ez megegyezik $f(x)$ felbontási testének fokával, ezért e test minden elemének a foka 2-hatvány. Mivel $f(x)$ minden gyöke benne van felbontási testében, és egy elem foka egyenlő főpolinomjának a fokával, ezért $f(x)$ foka is 2-hatvány. ■

A következőkben négy nevezetes feladatot tárgyalunk:

1) A szögharmadolás

A feladat annak a megállapítása, hogy létezik-e olyan eljárás, amelynek segítségével – euklideszi szerkesztést használva – bármely szög harmadolható. (Természetesen van olyan szög, ami harmadolható, például a derékszög is.) Ennek lehetetlenségénél többet mutatunk ki, nevezetesen azt, hogy *a 60°-os szög euklideszi szerkesztéssel nem harmadolható.*

Célszerű abból kiindulni, hogy adott az egység sugarú kör, és abban, felmérve egy α nagyságú szög. Egy szög megszerkeszthetősége esetünkben ekvivalens a szög koszinuszának a megszerkesztésével. A trigonometrikus összefüggéseket felhasználva ez a $4x^3 - 3x - a$ polinom gyökének a meghatározására vezet, ahol a az adott szög koszinusza. Esetünkben ez $1/2$; és így a kérdés az, hogy szerkeszthető-e a $8x^3 - 6x - 1$ valamelyik gyöke. Ha e polinomnak volna racionális gyöke, annak kétszerese gyöke lenne az $x^3 - 3x - 1$ polinomnak, amelynek nincs racionális gyöke. Így a vizsgált polinom irreducibilis; ha tehát volna szerkeszthető gyöke, akkor foka 2-hatvány lenne, ami nem igaz. ■

2) Kockakettőzés vagy déloszi probléma Feladatunk körzővel és vonalzóval olyan kockát „szerkeszteni”, amelynek térfogata egy adott kocka térfogatának a kétszerese. Ez azt jelenti, hogy adott kockaélből szerkesztendő az új kocka éle, amely az $x^3 - 2$ polinom

gyökének a megszerkesztésére vezet. Ennek lehetetlensége hasonlóképpen látható be, mint az előző esetben. ■

3) Körnégyszögesítés

Szerkesztendő adott körrel egyenlő területű vagy kerületű négyzet. A kör sugarát egységnek tekintve, feladatunk $\sqrt{\pi}$, illetve $\pi/2$ szerkesztése. Bármelyikük szerkeszthetőségéből azonnal következik, hogy π is szerkeszthető, ami azt jelentené, hogy π eleme volna a racionális számtest egy 2-bővítésének. Így π algebrai lenne a racionális test felett, ami nem igaz. ■

4) Szabályos n-szög szerkesztése

Ez azzal ekvivalens, hogy az n-edik primitív egységgyök valós és komplex részét szerkesztjük. A 8.50., illetve 8.51. tételek alapján ennek szükséges és elégséges feltétele az, hogy az $f_n(x)$ körosztási polinom Galois-csoportjának a rendje 2-hatvány legyen. A 8.38. tételt figyelembe véve a kérdés az, hogy milyen n-re lesz $\varphi(n)$ 2-hatvány. Ezt a φ függvény felírását használva adhatjuk meg: akkor és csak akkor, ha n egy 2-hatványnak és csupa különböző olyan p prímszámnak a szorzata, amelyekre $\varphi(p)$ 2-hatvány. Ez utóbbi pontosan akkor teljesül, ha $p = p_k = 2^{(2^k)} + 1$ alakú – úgynevezett Fermat-féle prím. Nem ismeretes, hogy végtelen sok Fermat-féle prím létezik-e. k első értékeire p_k prímszám: $p_0 = 3$, $p_1 = 5$, $p_2 = 17$, $p_3 = 257$, $p_4 = 65\,537$ prímszámok. Ezzel szemben $p_5 = 2^{32} + 1$ nem prímszám.

Ezt a következőképpen láthatjuk be: A $q = 641$ (prím)számra $641 = 640+1 = 625+16$ alapján $2^7 \cdot 5 \equiv -1 (\mathrm{mod}\ q)$ és $5^4 \equiv -2^4 (\mathrm{mod}\ q)$. Így:

$$2^{32} + 1 = 2^{7\cdot 4+4} + 1 \equiv -2^{7\cdot 4} \cdot 5^4 + 1 = -(2^7 \cdot 5)^4 + 1 \equiv -(-1)^4 + 1 (\mathrm{mod}\ q),$$

vagyis 641 osztója p_5-nek. ■

Ma ez a számolás „feleslegesnek” tűnik, mert egy faktorizálásra képes program azonnal megadja, hogy $2^{32}+1 = 641 \cdot 6\,700\,417$. Annak idején viszont számítógép nem létezett, és a fenti eljárás egy igen hasznos módszernek lett az alapja.

8.12. Az egységgyökök kiszámítása

Az alábbiakban azt írjuk le, miképpen lehet az n-edik egységgyököket $\mathbb{Q}$ felett gyökjelekkel kifejezni. Abban az esetben, ha $\varphi(n)$ 2-hatvány, akkor az eljárás a szabályos n-szög szerkesztését is szolgáltatja.

Ha n felbontható relatív prím tényezők szorzatára, $n = k \cdot \ell$, akkor a feladat nyilvánvaló módon visszavezetődik a k-adik és az ℓ-edik egységgyökök meghatározására. Ha $n = p^k$ alakú, ahol p prímszám és ε egy primitív p-edik egységgyök, akkor

$$\underbrace{\sqrt[p]{\dots \sqrt[p]{\varepsilon}}}_{(k-1)\text{-szer}}$$

a p^k-adik egységgyök megfelelő előállítását adja. (A szereplő $k-1$ számú $x^p - a$ alakú polinom mind irreducibilis.) Elég tehát a p-edik egységgyököket vizsgálni. Legyen p rögzített, ε egy p-edik primitív egységgyök. Mint tudjuk, a racionális számtestnek ε-nal való

bővítése normális és G Galois-csoportja ciklikus $n = (p-1)$-edrendű. Legyen G generátoreleme σ. A G csoport részcsoportjai ugyancsak ciklikusak, és generátorelemeik a σ^k alakú automorfizmusok, ahol k osztója n-nek. Jelölje H_k a σ^k generálta részcsoportot és Δ_k a hozzá tartozó közbülső testet. (Így $G = H_1$, $\mathbb{Q} = \Delta_1$ és $\mathbb{Q}(\varepsilon) = \Delta_n$; továbbá $k_1 \mid k_2$, $H_{k_2} \subseteq H_{k_1}$, valamint $\Delta_{k_1} \subseteq \Delta_{k_2}$ ekvivalensek.)

Mivel ε konjugáltjai a hatványai, ezért $\sigma(\varepsilon) = \varepsilon^g$, valamely pozitív $g < p$ egészre. Így $\sigma(\varepsilon^i) = \varepsilon^{gi}$, amiből azonnal adódik, hogy $\sigma^r(\varepsilon) = \varepsilon^{g^r}$. Tekintettel arra, hogy ε automorf képei között minden konjugáltja szerepel, ezért ε minden hatványa alkalmas r-rel ε^{g^r} alakú. Eszerint g hatványai végigfutnak egy p szerinti redukált maradékrendszeren, ami azt jelenti, hogy g primitív gyök modulo p. Az $\varepsilon_r = \varepsilon^{g^r}$ jelöléssel azt kapjuk, hogy $\sigma^i(\varepsilon_j) = \varepsilon_{i+j}$. Mivel az $\varepsilon_0, \ldots, \varepsilon_{n-1}$ elemek a $\mathbb{Q}(\varepsilon)$ testnek egy $\mathbb{Q}$ feletti bázisát alkotják, ezért a test minden eleme egyértelműen felírható $\alpha = \sum_{i=0}^{n-1} a_i \varepsilon_i$ alakba, ahol $a_i \in \mathbb{Q}$.

Legyen $n = k\ell$. Nézzük meg, hogy az α elemet mikor viszi a σ^k automorfizmus önmagába. Mint láttuk,

$$\sigma^k\left(\sum_{i=0}^{n-1} a_i \varepsilon_i\right) = \sum_{i=0}^{n-1} a_i \varepsilon_{i+k} = \sum_{i=0}^{n-1} a_{i-k} \varepsilon_i,$$

ami pontosan akkor egyezik meg α-val, ha minden i-re $a_{i-k} = a_i$. Ha tehát $\alpha \in \Delta_k$, akkor

$$\alpha = \sum_{j=0}^{k-1} a_j \eta_j, \qquad \text{ahol} \qquad \eta_j = \varepsilon_j + \varepsilon_{j+k} + \ldots + \varepsilon_{j+(\ell-1)k} = \varepsilon_j \sum_{i=0}^{\ell-1} \varepsilon_{ki}.$$

Ezek az η_j elemek lineárisan függetlenek $\mathbb{Q}$ felett, hiszen egyébként ε egy n-nél alacsonyabb fokú polinom gyöke volna. Mivel e számok száma megegyezik a $(\Delta_k : \mathbb{Q})$ testfokkal, ezért a fenti elemek e test egy bázisát alkotják. Az η_j elemeket ℓ hosszúságú Gauss-periódusoknak nevezzük.

A továbbiakban azt nézzük meg, hogy miképpen lehet ezeket az elemeket gyökjelek segítségével konkrétan meghatározni. Pontosabban szólva csak azt nézzük meg, hogy milyen prímfokú polinomok lépnek fel a bővítéseknél; mert a konkrét meghatározásoknál előbb mindig bővíteni kell a megfelelő prímhez tartozó egységgyökkel. (Ez megint hasonló típusú feladathoz vezet, de az eljárás nyilván véges sok lépésben véget ér. Megjegyezzük viszont, hogy a szerkeszthetőség esetében az itt fellépő prímszám egyedül a 2, és ezért újabb egységgyök adjungálására nincs szükség.)

Legyen tehát q egy prímosztója k-nak, $k = qm$, és legyenek $\xi_0, \ldots, \xi_{q\ell-1}$ az m hosszúságú periódusok. Ezek persze generálják $\Delta_{q\ell}$-t, de $\mathbb{Q}$ felett. Válasszuk ki ezek közül azokat, amelyeknek összege η_0, legyenek ezek $\xi_0, \ldots, \xi_{q-1}$. Mivel ezeket (σ^k) egymásba viszi, ezért Δ_k felett konjugáltak. (Hasonlóképpen dolgozhatunk a többiekkel, rendre mindig q darabot összegyűjtve.) Ha meg akarjuk határozni azt a Δ_k feletti irreducibilis q-adfokú polinomokat, amelynek ezek gyökei, akkor elő kell állítani ezek elemi szimmetrikus polinomjait. Világos, hogy ezek a Δ_k testben vannak, csak a konkrét előállításra volna szükség. Ehhez pedig az szükséges, hogy kiszámítsuk két Gauss-féle periódus szorzatát. Itt nem lényeges, hogy milyen hosszúságúakról beszélünk (a végén úgyis olyan elemet fogunk

kapni, amely a megfelelő testhez tartozik); éppen ezért nyugodtan kiindulhatunk az η_i és η_j elemekből.

Mindenekelőtt jegyezzük meg, hogy $\eta_n = \eta_0$ miatt η_i helyett írhatunk η_{i+rn}-et is. Ebből azt kapjuk, hogy

$$\eta_i \cdot \eta_j = \left(\sum_{r=1}^{\ell} \varepsilon_{i+rk}\right) \cdot \left(\sum_{s=1}^{\ell} \varepsilon_{j+sk}\right) = \sum_{s=1}^{\ell} \left(\sum_{r=1}^{\ell} \varepsilon_{i+rk} \cdot \varepsilon_{j+rk+sk}\right).$$

Itt, a jobb oldalon álló belső összegben $j+sk$ helyébe j-t írva, ez a következő alakba írható át:

$$\sum_{r=1}^{\ell} \varepsilon_{i+rk} \cdot \varepsilon_{j+rk} = \sum_{r=1}^{\ell} \varepsilon^{g^{i+rk}} \cdot \varepsilon^{g^{j+rk}} = \sum_{r=1}^{\ell} \varepsilon^{(g^{i+rk}+g^{j+rk})} = \sum_{r=1}^{\ell} \varepsilon^{(g^i+g^j)\cdot g^{rk}}.$$

Most két esetet kell megkülönböztetnünk. Ha $g^i + g^j$ osztható p-vel, akkor minden tag 1; így az összeg ℓ. Egyébként ez az összeg valamilyen m-mel $\sum_{r=1}^{\ell} \varepsilon^{g^m \cdot g^{rk}}$ alakú, tehát ismét egy ℓ hosszúságú periódust kaptunk. Ilyen módon a többszörös szorzatok is visszavezethetők összegekre. (Vigyázat! Az nem igaz, hogy amikor hosszabb periódusokra vezetünk vissza, akkor a kapott periódus mindig ugyanannak a hosszabb periódusnak egy tagja volna, más hosszabb periódus tagjai is felléphetnek.)

Az alábbiakban megmutatjuk, miképpen számolhatjuk ki a 13-adik egységgyököket:

Először egy primitív gyököt kell keresni modulo 13. Mivel 63 és 15 egyike sem osztható 13-mal, ezért 2 primitív gyök modulo 13. A megfelelő 2^i alakú hatványkitevők rendre 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7. Az áttekinthetőbb írás végett az ε hatványainak összegei helyett csak a kitevőket írjuk ki, szögletes zárójelbe téve. Így a 12 hosszúságú periódus

$$[1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7] = -1.$$

Most annak megfelelően, hogy a három egymás utáni lépésben mikor oldunk meg harmadfokú egyenletet, három lehetőségünk van. Mi itt ezt első lépésnek választjuk:

$$\alpha_1 = [1, 8, 12, 5], \qquad \alpha_2 = [2, 3, 11, 10], \qquad \alpha_3 = [4, 6, 9, 7].$$

Ezek összege -1. A kétszeres szorzatokat számítva kezdjük $\alpha_1 \cdot \alpha_2$-vel. A megfelelő periódusból mindig csak az első számot írjuk ki (hiszen ez már egyértelműen meghatározza, hogy melyik periódusról van szó):

$$\alpha_1 \cdot \alpha_2 = [1+2, \ldots] + [1+3, \ldots] + [1+11, \ldots] + [1+10, \ldots] = \alpha_2 + \alpha_3 + \alpha_1 + \alpha_2 = -1 + \alpha_2.$$

Hasonlóképpen kapjuk, hogy $\alpha_2 \cdot \alpha_3 = -1 + \alpha_3$ és $\alpha_3 \cdot \alpha_1 = -1 + \alpha_1$. Ebből azt kapjuk, hogy a kétszeres szorzatok összege -4. A háromszoros szorzatra pedig -1 adódik. Eszerint a három darab 4 hosszúságú periódus az $x^3 + x^2 - 4x + 1$ polinom három gyöke. Az $y = x + \frac{1}{3}$ helyettesítéssel az $y^3 - \frac{13}{3}y + \frac{65}{27}$ polinomhoz jutunk. Ennek a polinomnak a diszkriminánsa:

$$D = \left(\frac{65}{54}\right)^2 - \left(\frac{13}{9}\right)^3 = \frac{13^2}{3^6} \cdot \left(\frac{5^2 - 4 \cdot 13}{4}\right) = \left(\frac{13}{18}\right)^2 \cdot (-3).$$

Mivel a diszkrimináns negatív, ezért mindhárom gyök valós (ez abból is látható, hogy mindhárom periódusban két-két tag egymás konjugáltja). A Cardano-képlettel kiszámítható

ennek a polinomnak mindhárom gyöke, amiből megkapható α_1, α_2 és α_3 is:

$$\alpha_i = \frac{1}{3}\left(-1 + \varrho^i \cdot \sqrt[3]{13 \cdot \left(-1 - 2\sqrt{-3}\right)\varrho^2} + \varrho^{2i} \cdot \sqrt[3]{13 \cdot \left(-1 + 2\sqrt{-3}\right)\varrho}\right), \quad i = 0, 1, 2;$$

ahol $\varrho = \frac{(-1 + \sqrt{-3})}{2}$ harmadik primitív egységgyök. Érdemes megfigyelni, hogy a köbgyök alatt „csúnya" faktorokra $\left(-1 - 2\sqrt{-3}\right) \cdot \left(-1 + 2\sqrt{-3}\right) = 13$ teljesül. Legyenek most:

$$\beta_1 = [1, 12], \quad \beta_2 = [8, 5], \quad \beta_3 = [2, 11], \quad \beta_4 = [3, 10], \quad \beta_5 = [4, 9], \quad \beta_6 = [6, 7].$$

Ekkor az adódik, hogy $\beta_1 + \beta_2 = \alpha_1$, míg $\beta_1 \cdot \beta_2 = \beta_5 + \beta_6 = \alpha_3$. Ez a két szám tehát az $x^2 - \alpha_1 x + \alpha_3$ polinom két gyöke. Végül ε az $x^2 - \beta_1 x + 1$ polinom gyökeként adódik.

Megjegyezzük, hogy annak a meghatározása, hogy a harmadfokú egyenlet gyökei közül melyik az α_1, az lényegtelen. Az viszont, hogy „ehhez képest" melyik az α_3, az már nem kis gondot okoz (a valós részek nagyságrendjét összehasonlítva ez is eldönthető).

Végezetül megadunk egy (illetve sok) példát a $\mathbb{Q}$ olyan bővítésére, amelynek a Galois-csoportja a kvaterniócsoport:

Az alábbiakban mindig csak pozitív elemek négyzetgyökét fogjuk tekinteni. Ha $t > 0$, akkor $\sqrt{t}$ mindig a pozitív négyzetgyököt jelöli. Ezért alkalmazható a $\sqrt{t_1 \cdot t_2} = \sqrt{t_1} \cdot \sqrt{t_2}$ összefüggés.

Mivel $\sqrt{2}$ és $\sqrt{5}$ a $\mathbb{Q}$ felett függetlenek, ezért a $\mathbb{K}_0 = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ bővítésre $(\mathbb{K}_0 : \mathbb{Q}) = 4$. A három közbülső test $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{5})$ és $\mathbb{Q}(\sqrt{10})$. Ennek a bővítésnek a $G(\mathbb{K}_0 \mid \mathbb{Q})$ Galois-csoportja V_4-gyel (a Klein-féle csoport) izomorf; három nemtriviális automorfizmusa van:

$$\alpha : \begin{cases} \sqrt{2} \to \sqrt{2} \\ \sqrt{5} \to -\sqrt{5} \\ \sqrt{10} \to -\sqrt{10} \end{cases} \qquad \beta : \begin{cases} \sqrt{2} \to -\sqrt{2} \\ \sqrt{5} \to \sqrt{5} \\ \sqrt{10} \to -\sqrt{10} \end{cases} \qquad \gamma : \begin{cases} \sqrt{2} \to -\sqrt{2} \\ \sqrt{5} \to -\sqrt{5} \\ \sqrt{10} \to \sqrt{10} \end{cases}.$$

Világos, hogy ezek közül bármely kettőnek a szorzata a harmadik. Tekintsük $\mathbb{K}_0$ következő elemeit:

$$a = 2 - \sqrt{2}, \qquad b = 3 - \sqrt{5}, \qquad c = 10 - \sqrt{10},$$

és legyen:

$$a' = \beta(a) = \gamma(a) = 2 + \sqrt{2}, \quad b' = \alpha(b) = \gamma(b) = 3 + \sqrt{5}, \quad c' = \alpha(c) = \beta(c) = 10 + \sqrt{10}.$$

Vegyük észre, hogy:

$$a^* = \sqrt{aa'} = \sqrt{4 - 2} = \sqrt{2}, \quad b^* = \sqrt{bb'} = \sqrt{9 - 5} = 2, \quad c^* = \sqrt{cc'} = \sqrt{100 - 10} = 3\sqrt{10}$$

mind elemei $\mathbb{K}_0$-nak.

Tekintsük most a következő elemeket:

$$u_1 = \sqrt{abc}, \qquad u_2 = \sqrt{ab'c'}, \qquad u_3 = \sqrt{a'bc'}, \qquad u_4 = \sqrt{a'b'c}.$$

Az u_i^2 elemek mindegyike $\mathbb{K}_0$-ban van. Ezeket az α, β, γ automorfizmusok egyike sem hagyja fixen, és így nincsenek benne egyik közbülső testben sem; tehát bármelyikük gene-

rálja $\mathbb{K}_0$-t. Továbbá:

$$\frac{u_2}{u_1} = \sqrt{\frac{ab'c'}{abc}} = \frac{b'c'}{b^*c^*} = \frac{(3+\sqrt{5})(10+\sqrt{10})}{(2)\cdot(3\sqrt{10})} \in \mathbb{K}_0.$$

Hasonlóképpen adódik, hogy

$$\frac{u_3}{u_1} = \frac{(2+\sqrt{2})(10+\sqrt{10})}{(\sqrt{2})\cdot(3\sqrt{10})} \in \mathbb{K}_0 \qquad \text{és} \qquad \frac{u_4}{u_1} = \frac{(2+\sqrt{2})(3+\sqrt{5})}{(\sqrt{2})(2)\cdot} \in \mathbb{K}_0.$$

Ez azt jelenti, hogy a $\pm u_i$ elemek mindegyike eleme a $\mathbb{K}_1 = \mathbb{K}_0(u_1)$ testnek. Tekintettel arra, hogy u_1^2 és u_i^2 (ahol $i \in \{2,3,4\}$) $\mathbb{K}_0$-ban konjugáltak, ezért u_1-nek konjugáltja $\varepsilon_i u_i$ (ahol $i \in \{2,3,4\}$ és ε_i vagy +1, vagy -1). Eszerint $\mathbb{K}_1 \mid \mathbb{Q}$ normális bővítés. Tekintsük azt a σ_2 relatív automorfizmust, amelyre $\sigma_2(u_1) = \varepsilon_2 u_2$. Erre természetesen $\sigma_2(u_1^2) = u_2^2$ is igaz. Mivel ezek az elemek már $\mathbb{K}_0$-beliek, ezért ezáltal ennek a bővítésnek egy relatív automorfizmusát indukáltuk. A négy automorfizmus közül csak egynek van ilyen hatása, ezért csak $\sigma_2(\sqrt{2}) = \sqrt{2}$ és $\sigma_2(\sqrt{5}) = -\sqrt{5}$ lehet. Ebből a következőket nyerjük:

$$\sigma_2(\varepsilon_2 u_2) = \sigma_2\left(\varepsilon_2 u_1 \cdot \frac{u_2}{u_1}\right) = \sigma_2(\varepsilon_2 u_1)\cdot\sigma_2\left(\frac{u_2}{u_1}\right) = u_2\cdot\sigma_2\left(\frac{u_2}{u_1}\right) = u_1\cdot\frac{u_2}{u_1}\cdot\sigma_2\left(\frac{u_2}{u_1}\right) =$$

$$= u_1\cdot\frac{(3+\sqrt{5})(10+\sqrt{10})}{(2)\cdot(3\sqrt{10})}\cdot\frac{(3-\sqrt{5})(10-\sqrt{10})}{(2)\cdot(-3\sqrt{10})} = -u_1.$$

Ez azt jelenti, hogy σ_2^2 nem az identitás, de σ_2^4 az u_1 generátorelemet fixen hagyja. Így σ_2 negyedrendű elem. Hasonlóképpen negyedrendűek a $\sigma_3 : u_1 \to u_3$ és $\sigma_4 : u_1 \to$ $\to u_4$, valamint a σ_2^3, σ_3^3 és σ_4^3 automorfizmusok. Tekintettel arra, hogy $\sigma_2^2(u_1) = -u_1$, ezért $-u_1$, és hasonlóképpen $-\varepsilon_2 u_2$, $-\varepsilon_3 u_3$, $-\varepsilon_4 u_4$ is konjugáltjai u_1-nek. Eszerint a fenti nyolc elem mindegyikének a foka 8, ezért egymás konjugáltjai (Ezek a számok egyébként mind gyökei az $x^8 - 200x^6 + 11\,120x^4 - 100\,800x^2 + 518\,400$ polinomnak, amely $\mathbb{Q}$ felett irreducibilis.) Ezért a $G = G(\mathbb{K}_1 \mid \mathbb{Q})$ Galois-csoport nyolcelemű. Továbbá a fenti hat automorfizmus mindegyike más-más elembe viszi u_1-et, ezért G-nek hat negyedrendű eleme van. σ_2^2 pedig másodrendű. Könnyen ellenőrizhető, hogy a nyolcadrendű csoportok közül egyedül a kvaterniócsoport ilyen.

Eszerint $G(\mathbb{K}_1 \mid \mathbb{Q}) \cong Q$.

A konstrukció lényege a következő: olyan k_1, k_2, k_3 pozitív egészeket kell találni, amelyekre bármely kettő szorzatát a harmadikkal osztva négyzetszámot kapunk (például két prím és a szorzatuk). Emellett alkalmas x_i, y_i egészekkel $x_i^2 - k_i \cdot y_i^2$ egy esetben négyzetszám, két esetben pedig valamelyik k_i négyzetszámszorosa legyen. Ez legegyszerűbben úgy oldható meg, ha éppen az abban a formulában levő k_i-t választjuk. Tehát alkalmas z_i-kkel $x_1^2 - k_1\cdot y_1^2 = k_1\cdot z_1^2$, $x_2^2 - k_2\cdot y_2^2 = k_2\cdot z_2^2$, $x_3^2 - k_3\cdot y_3^2 = z_3^2$. Ehhez az kell, hogy k_1 és k_2 két négyzet összege legyen, míg k_3 páratlan (vagy annak 4^n-szerese). Például két nem $4k-1$ alakú prím és azok szorzata. Ez a példa a lehető legegyszerűbb ilyen esetet adja.

Feladatok

1. Legyen α a $\mathbb{Q}$ feletti $x^3 - 3x + 1$ polinom gyöke. Bizonyítsuk be, hogy $g(\alpha) \mapsto g(\alpha^2 - 2)$ a $\mathbb{Q}(\alpha)$ testnek egy olyan automorfizmusa, amelyik $\mathbb{Q}$-t fixen hagyja.

2. Legyen α a $\mathbb{Q}$ feletti $x^3 - 3x - 2$ polinom gyöke. Bizonyítsuk be, hogy $g(\alpha) \mapsto g(\alpha^2 - 2)$ a $\mathbb{Q}(\alpha)$ testnek egy olyan automorfizmusa, amelyik $\mathbb{Q}$-t fixen hagyja. Miben különbözik ez a feladat az előzőtől?

3. Bizonyítsuk be, hogy algebrai α esetén a $\mathbb{Q}(\alpha)$ test $\mathbb{Q}$ elemeit fixen hagyó automorfizmusainak a száma legfeljebb $n = (\mathbb{Q}(\alpha) : \mathbb{Q})$. Tetszőleges n-re adjunk olyan példát, amikor csak a triviális automorfizmus létezik.

4. Bizonyítsuk be, hogy tetszőleges G csoporthoz van olyan K test, amelynek automorfizmuscsoportja G-vel izomorf. (Nagyon-nagyon nehéz!)

5. Bizonyítsuk be, hogy egy test minden endomorfizmusa injektív. Hány endomorfizmusa van $\mathbb{Q}(t)$-nek (t transzcendens)? Adjunk ezekről „áttekintést".

6. Fogjuk látni, hogy az $\mathbb{R}$ valós testnek egyetlen automorfizmusa az identitás (ez egyébként könnyű). „Hány" endomorfizmusa van vajon?

7. Legyen $(\mathbb{Q}_2(\alpha) : \mathbb{Q}_2) = n$ és $f(x)$ az α főpolinomja. Határozzuk meg $f(x)$ összes gyökét.

8. Legyen $a_1, \ldots, a_n$ az L test K feletti bázisa. Legyenek $\sigma_1, \ldots, \sigma_k$ L olyan különböző automorfizmusai, amelyek K elemeit fixen hagyják, és jelölje α_i az a_i elemmel való balszorzást. Bizonyítsuk be, hogy a $\alpha_i \cdot \sigma_j$ elemek a $Hom_K(L, L)$ független elemei. (Nagyon nehéz.)

9. Az előző feladatot felhasználva írjuk le egy véges prímtest feletti véges bővítés lineáris transzformációit.

10. Határozzuk meg az alábbi számok $\mathbb{Q}$ feletti konjugáltjait:

a) $\sqrt{2} + \sqrt{3}$, *b)* $\sqrt{5 + 2\sqrt{6}}$, *c)* $\sqrt{5 + 2\sqrt{6}} + \sqrt{6}$,

d) $\sqrt{2} + \sqrt{3} + \sqrt{6}$, *e)* $\sqrt{5 + 2\sqrt{6}} + \sqrt{7}$, *f)* $\sqrt{2} + \sqrt[3]{2}$, *g)* $\sqrt{2} + \sqrt[3]{1 + \sqrt{2}}$.

11. Legyenek $p_1, \ldots, p_r$ különböző prímek és $\alpha = \sqrt{p_1} + \ldots + \sqrt{p_r}$. Határozzuk meg α fokát és konjugáltjait $\mathbb{Q}$ felett. Bizonyítsuk be, hogy $\mathbb{Q}(\alpha)$ normális bővítés; és határozzuk meg a Galois-csoportját, valamint ennek részcsoporthálóját.

Az alábbi három feladatban a Galois-csoportok meghatározása nem konkrét megadást jelent.

12. Határozzuk meg a $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}, \ldots)$ test automorfizmuscsoportját.

13. Határozzuk meg a $\mathbb{Q}(\sqrt{2}, \sqrt[4]{2}, \ldots, \sqrt[2^n]{2}, \ldots)$ test automorfizmuscsoportját.

14. Legyen $\mathbb{A}_p$ a $\mathbb{Q}_p$ algebrai lezártja ($p = 0$ is lehet). Határozzuk meg $\mathbb{A}$ automorfizmuscsoportját.

15. Mi a feltétele annak, hogy a K felett algebrai α elem valamelyik konjugáltja $\alpha + c$, alkalmas $c \in K$ elemmel? Mutassuk meg, hogy ez lehetséges.

16. Legyen q prímszám és K véges test. Mi a feltétele annak, hogy legyen olyan $a \in K$ elem, amelyre $x^q - a$ irreducibilis K felett?

17. Bizonyítsuk be, hogy $x^3 - a \in \mathbb{Q}_5[x]$ minden a-ra reducibilis; így nem létezik $\mathbb{Q}_5(\sqrt[3]{a})$ alakú bővítés. Mutassuk meg, hogy $2+2\sqrt{2}$ harmadik egységgyök $\mathbb{Q}_5$ felett; és az $\alpha = \sqrt[3]{1+\sqrt{2}} + \sqrt[3]{1-\sqrt{2}}$ elem harmadfokú $\mathbb{Q}_5$ felett.

19. Tegyük fel, hogy $x^p - a$ a K felett irreducibilis polinom. Mi a feltétele annak, hogy $K(\sqrt[p]{a})$ a K-nak normális bővítése legyen?

20. Tegyük fel, hogy $x^p - a$ irreducibilis polinom a K test felett. Bizonyítsuk be, hogy ha $b \in K$ és $\sqrt[p]{b} \in K(\sqrt[p]{a})$, akkor van olyan $c \in K$ és olyan i természetes szám, amire $\sqrt[p]{b} = c \cdot (\sqrt[p]{a})^i$. Általánosítsuk a feladatot.

21. Először is bizonyítsuk be, hogy 2 primitív gyök mod 61. Ezután mutassuk meg, hogy $\mathbb{Q}_{61}(\sqrt[61]{2})$ normális bővítése $\mathbb{Q}_{61}$-nek. Végezetül majd mutassuk meg azt is, hogy $\mathbb{Q}_{61}$ felett létezik általános megoldóképlet az ötödfokú egyenletekre. Esetleg az is megmutatható, hogy a $\mathbb{A}_{61}$ algebrai lezárt felett nincs az ötödfokú egyenletekre általános megoldóképlet, de minden konkrét ötödfokú egyenlet gyökjelekkel megoldható.

22. Legyen ε p^2-edik primitív egységgyök (p prím), és legyen $\alpha = \varepsilon + \varepsilon^{-1}$. Bizonyítsuk be, hogy $\mathbb{Q}(\alpha) \mid \mathbb{Q}$ normális bővítés, és Galois-csoportja ciklikus. Mennyi a rendje?

23. Bizonyítsuk be, hogy a 67. primitív egységgyökök gyökjelekkel való kifejezésénél szükség van ötödik gyökökre is.

24. Írjuk fel a 19. egységgyökökhöz tartozó Gauss-féle periódusokat. (2 primitív gyök modulo 19.)

25. Tegyük fel, hogy van olyan szerkezetünk, amivel bármely távolság köbgyökét megszerkeszthetjük. Mik szerkeszthetők körző, vonalzó és a fenti szerkezet segítségével?

26. Igaz-e az, hogy az előző feladatban megengedett szerkesztési lépésekkel minden harmad- és negyedfokú polinom (valós) gyökét is meg tudjuk szerkeszteni?

27. Hogyan kell megváltoztatni a fenti szerkezetet, hogy az előző feladathoz képest még az ötödfokú polinomok gyökei is megszerkeszthetők legyenek? Változtassuk meg ezt a kérdést úgy, hogy „értelmes” legyen.

28. Tekintsük azt az $\mathcal{F} \subseteq \mathbb{Q}[x]$ polinomhalmazt, amely azokból az irreducibilis polinomokból áll, amelyeknek gyökei gyökkifejezések. Bizonyítsuk be, hogy $\mathcal{F}$-nek az $\mathbb{F}$ felbontási teste tartalmazza egész számok (nem $\mathbb{Q}$-beli) köbgyökét is.

29. Határozzuk meg, hogyan állnak elő a $\mathbb{Q}$-nak azok az $\mathbb{N}$ normális bővítései, amelyekre $(\mathbb{N} : \mathbb{Q}) = p$ prímszám. Adjunk minden p esetére példákat.

30. Legyen $f(x) \in \mathbb{Q}[x]$ irreducibilis prímfokú polinom. Írjuk le „minél pontosabban” a felbontási testét.

31. Mutassuk meg, hogy az ötödik körosztási polinom ($f_5(x)$) nem irreducibilis $\mathbb{Q}_{11}$ felett, sőt itt lineáris faktorokra bomlik.

32. Adjuk meg, milyen feltételeknek kell teljesülnie a p és q prímszámokra ahhoz, hogy az $f_q(x)$ körosztási polinom lineáris faktorokra essen szét $\mathbb{Q}_p[x]$-ben.

33. Bizonyítsuk be, hogy az $f_5(x)$ körosztási polinom nem bomlik lineáris faktorokra $\mathbb{Q}_{19}$ felett, de nem is irreducibilis.

34. Adjuk meg, milyen feltételeknek kell teljesülnie a p és q prímszámokra ahhoz, hogy az $f_q(x)$ körosztási polinom irreducibilis legyen $\mathbb{Q}_p[x]$-ben.

35. A 8.38. tételben az $f_n(x)$ $\mathbb{Z}$ feletti irreducibilitásának a bizonyításához azt használtuk fel, hogy ha n nem osztható a karakterisztikával, akkor létezik primitív n-edik egységgyök, tehát pontosan n különböző n-edik egységgyök van, azaz $x^n - 1$ nem osztható egyetlen polinom négyzetével sem. Miért nem használható ez véges testek esetében (ahol ugyancsak nem létezik többszörös gyök, mégsem teljesül az irreducibilitás)?

36. Mutassuk meg, hogy az $x^5 - 2$ polinom a $\mathbb{Q}(\sqrt[5]{2}, \sqrt{5})$ test felett egy elsőfokú és két másodfokú polinom szorzatára bomlik.

37. Adjunk meg végtelen sok olyan ötödfokú polinomot, amelynek Galois-csoportja szimmetrikus.

38. Adjunk meg végtelen sok olyan n-edfokú polinomot ($n > 5$), amelynek Galois-csoportja szimmetrikus.

39. Legyen $\mathbb{R}_n$ a modulo n vett redukált maradékosztályok multiplikatív csoportja. Bizonyítsuk be, hogy minden A véges Abel-csoporthoz van olyan n, hogy A homomorf képe $\mathbb{R}_n$-nek.

40. Bizonyítsuk be, hogy minden Abel-csoport Galois-csoportja $\mathbb{Q}$ egy egyszerű algebrai bővítésének.

41. Bizonyítsuk be, hogy az $x^5 - x - 1$ polinom $\mathbb{Q}$ feletti Galois-csoportja a szimmetrikus csoport.

42. Legyen a $\mathbb{Q}$ felett irreducibilis negyedfokú polinom Galois-csoportja nyolcadrendű. Bizonyítsuk be, hogy akkor ez csak a diédercsoporttal lehet izomorf.

43. Mutassuk meg, hogy az $x^4 + x + 1 \in \mathbb{Q}[x]$ polinom Galois-csoportja S_4.

44. Bizonyítsuk be, hogy az $x^4 - a \in \mathbb{Q}[x]$ polinom Galois-csoportja „általában” a diédercsoport.

45. Mutassuk meg, hogy $x^4 + 1 \in \mathbb{Q}[x]$ Galois-csoportja a Klein-féle csoport.

46. Bizonyítsuk be, hogy egy negyedfokú $\mathbb{Q}$ felett irreducibilis polinom Galois-csoportja nem lehet ciklikus.

47. Milyen n-ekre lehet egy n-edfokú, $\mathbb{Q}$ felett irreducibilis polinom Galois-csoportja ciklikus?

48. Modulo p (prímszám) (kvadratikus) maradéknak nevezünk egy a számot (maradékot), ha van olyan b szám, amire $b^2 \equiv a \pmod{p}$. Ha ilyen b nincs, akkor a „nemmaradék”. Bizonyítsuk be, hogy két maradék vagy két nemmaradék szorzata maradék, míg egy maradék és egy nemmaradék szorzata nemmaradék. Bizonyítsuk be, hogy páratlan p esetén a maradékok és a nemmaradékok száma megegyezik.

49. Általánosítsuk az előző feladatot „kubikus” stb. maradékokra.

NEGYEDIK RÉSZ
ALGEBRÁK

A mátrixok és a polinomok példája mutatja, hogy milyen fontosak azok a vektorterek, amelyekben gyűrűműveletek is vannak. A polinommátrixok és az egész együtthatós polinomok esetében azt is láthattuk, hogy a vektortereknél szereplő test helyett sokszor gyűrűkre is van szükség. Az ilyen struktúrákat „algebrák"-nak nevezik. Célunk a fenti két eset (kommutatív és nemkommutatív) általános vizsgálata. Ehhez mindenekelőtt a modulusokkal foglalkozunk; kissé általánosabban és másképpen, mint az első kötetben.

9. Modulusok

9.1. Moduluselméleti alapfogalmak

Az eddigiekben sok olyan esettel találkoztunk már, ahol egy gyűrű egy másik gyűrű elemein „hat", pontosabban szólva egy gyűrű elemeivel egy másik gyűrű elemeit úgy szorozhattuk, hogy a szorzat a másik gyűrűben volt. Például egy K test egy L bővítésének elemeit K-beli elemmel szorozva ismét L-beli elemet kaptunk. Értelmezhettük adott gyűrű fölötti polinomoknak a gyűrű elemeivel való szorzatát. Beszélhettünk arról, hogy egy integritási tartomány hányadostestének az elemeit az integritási tartomány elemeivel szoroztuk. Olyan eset is előfordult, amikor a szorzat nem egy „nagyobb", hanem egy „kisebb" gyűrű eleme volt – például egy gyűrűelemmel annak egy ideáljába tartozó elemet szorozva, a szorzat is eleme lesz az ideálnak.

A fenti esetekben a „beszorzás" eleve eleget tesz bizonyos összefüggéseknek, amelyek a műveleti azonosságokból következnek. Ilyen összefüggések következhetnek azonban más módon is. Láttuk például, hogy egy Abel-csoport elemeit szorozhatjuk egész számokkal, és ez a szorzás is kielégíti a fenti fontos összefüggéseket. A vektorterek esetében egy – additív – Abel-csoport elemeit szoroztuk egy test elemeivel; és itt a szükséges azonosságok teljesülését axiómákkal mondtuk ki.

Az alábbiakban célunk olyan közös általánosítás megadása, amely a fenti eseteket mind magába foglalja. Ez a közös általánosítás a modulus, amellyel már az első kötetben is találkoztunk. A modulusokat itt most más szempontok figyelembevételével is tárgyaljuk. Emellett néhány eredményt itt ismételten szerepeltetünk.

9.1. Definíció. Az $\mathcal{M}$ additív Abel-csoportot az R gyűrű fölötti bal oldali R-modulusnak nevezzük, ha minden $a \in R$ és minden $\mathbf{u} \in \mathcal{M}$ elemhez értelmezve van az $a \cdot \mathbf{u} = a\mathbf{u} \in \mathcal{M}$ úgynevezett szorzat; és teljesülnek az alábbi összefüggések:

(1) $(a + b)\mathbf{u} = a\mathbf{u} + b\mathbf{u}$,

(2) $(ab)\mathbf{u} = a(b\mathbf{u})$,

(3) $a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$,

tetszőleges $a, b \in R$ és $\mathbf{u}, \mathbf{v} \in \mathcal{M}$ esetén. Az $\mathcal{M}$ Abel-csoportot a modulus tartócsoportjának nevezzük.

Azt a tényt, hogy $\mathcal{M}$ bal oldali R-modulus, ${}_R\mathcal{M}$ jelöli.

Duális módon definiálható a jobb oldali S-modulus, amit $\mathcal{M}_S$ jelöl. Ebben az esetben minden $\mathbf{u} \in \mathcal{M}$ és minden $s \in S$ elemre az $\mathbf{u}s$ szorzat van értelmezve.

Akkor nevezzük $\mathcal{M}$-et bal oldali R- és jobb oldali S-modulusnak (röviden (R–S)-modulusnak), ha $\mathcal{M}$ bal oldali R-modulus, jobb oldali S-modulus, és minden $a \in R$, $\mathbf{u} \in \mathcal{M}$ és $s \in S$ esetén teljesül az

(4) $(a\mathbf{u})s = a(\mathbf{u}s)$

összefüggés.

Az egyedül a nullelemből álló modulus neve triviális modulus, a többieké nemtriviális modulus. □

Megjegyzés. A bal oldali és jobb oldali modulusok között különbség van. Ez a különbség nem abból áll, hogy „melyik oldalra írjuk" a gyűrű elemeit. Tekintsünk egy $\mathcal{M}$ Abel-csoportot, amelyik bal oldali R-modulus és jobb oldali S-modulus. Legyenek $\mathbf{u} \in \mathcal{M}$, $a, b \in R$, és $s, t \in S$. Ekkor az R-beli ab elemre $(ab)\mathbf{u} = a(b\mathbf{u})$, míg az S-beli st elemre $\mathbf{u}(st) = (\mathbf{u}s)t$. Bal oldali R-modulusok esetén a szorzatot úgy alkalmazzuk, hogy *először a második tényezőt* alkalmazzuk, míg jobb oldali S-modulusok esetén *először az első tényezőt.* □

A vektorterekhez hasonlóan az R-modulus definíciója lényegesen különbözik az algebrai struktúrák „szokásos" definíciójától, ugyanis az egyik „művelet" nem az R-modulus elemeire van értelmezve. Ezen azonban könnyen segíthetünk az alábbi triviális tétellel:

9.2. Tétel. *Rögzített R gyűrű esetén a bal oldali R-modulusok algebrai struktúrákká tehetők az alábbi módon. Az R minden a eleméhez hozzárendeljük azt az f_a egyváltozós műveletet, amelyre a modulus tetszőleges $\mathbf{u}$ elemével $f_a(\mathbf{u}) = a\mathbf{u}$ teljesül.* ■

Megjegyzések. 1. Ezáltal a modulusok (esetleg) végtelen sok művelettel rendelkező struktúrákká váltak, de ez semmiféle zavart nem okoz.

2. Teljesen hasonló észrevétel tehető jobb oldali S-modulusokra, illetve R–S-modulusokra is. Ha mást nem mondunk, akkor R-moduluson bal oldali R-modulust értünk.

3. A 9.2. tétel alapján a modulusokat aszerint célszerű osztályozni, hogy melyik gyűrű feletti modulusok. Így – általában – a vizsgált gyűrűt rögzítettnek tekintjük; ellentétben a „kétstruktúraváltozós" szemléletmóddal. □

Nyilvánvalóan igaz az alábbi

9.3. Tétel. *Bármely $\mathcal{M}$ bal oldali R-modulusban teljesülnek az alábbi összefüggések:*

$$a \cdot \mathbf{o} = 0 \cdot \mathbf{u} = \mathbf{o}, \qquad (-a) \cdot \mathbf{u} = a \cdot (-\mathbf{u}) = -(a \cdot \mathbf{u}), \qquad (-a) \cdot (-\mathbf{u}) = a \cdot \mathbf{u},$$

$$(a - b) \cdot \mathbf{u} = a\mathbf{u} - b\mathbf{u}, \qquad a \cdot (\mathbf{u} - \mathbf{v}) = a \cdot \mathbf{u} - a \cdot \mathbf{v},$$

ahol 0 *az R-nek a nulleleme,* $\mathbf{o}$ *az $\mathcal{M}$-nek a nulleleme,* $-a$ *az a-nak,* $-\mathbf{u}$ *az $\mathbf{u}$-nak az ellentettje.* ■

Tetszőleges algebrai struktúrákhoz hasonlóan R-modulusok esetében is beszélhetünk az elemi fogalmakról:

9.4. Definíció. R-modulusok esetében a részalgebrát részmodulusnak, a faktoralgebrát faktormodulusnak, a homomorfizmust R-homomorfizmusnak nevezzük. □

Az R-modulusok esetében is leírhatók a fenti fogalmak a műveletek segítségével.

9.5. Tétel. *$\mathcal{N}$ akkor és csak akkor részmodulusa az $\mathcal{M}$ (bal oldali) R-modulusnak, ha mint Abel-csoport, részcsoportja, és az R-beli elemekkel (balról) való szorzás nem vezet ki belőle. Egy modulus valamely osztályozása akkor és csak akkor kompatibilis osztályozás, ha mint Abel-csoportnak kompatibilis osztályozása, és magja részmodulus. Egy $\varphi : {}_R\mathcal{M} \to {}_R\mathcal{N}$ leképezés akkor és csak akkor R-homomorfizmus, ha Abel-csoport homomorfizmus és $\varphi(a\mathbf{u}) = a\varphi(\mathbf{u})$ teljesül tetszőleges $a \in R$ és $\mathbf{u} \in \mathcal{M}$ esetén.*

Ha félreértésre nem ad okot, akkor $\varphi(\mathbf{u})$ helyett a $\varphi\mathbf{u}$ jelölést is fogjuk használni.

Bizonyítás. Az első állítás egyszerűen a részalgebra tulajdonságainak az átfogalmazása.

A második állításból annyit már tudunk, hogy egy osztályozás pontosan akkor lesz Abel-csoport osztályozásként kompatibilis, ha a magja részcsoport. Azt kell tehát megnézni, milyen feltétel mellett lesz a tetszőleges gyűrűelemmel való szorzás is kompatibilis. Ez azt jelenti, hogy tetszőleges $a \in R$ esetén, ha $\mathbf{u}$ és $\mathbf{v}$ egy osztályban vannak, akkor $a\mathbf{u}$-nak és $a\mathbf{v}$-nek is egy osztályban kell lennie. Más szóval, abból, hogy $\mathbf{u} - \mathbf{v}$ a magban van, annak kell következnie, hogy $a\mathbf{u} - a\mathbf{v}$ is eleme a magnak. A 9.3. tétel utolsó állítása alapján ez nyilván ekvivalens azzal, hogy a mag részmodulus.

Az R-homomorfizmusokra vonatkozó állítás ugyancsak nyilvánvaló átfogalmazása az általános definíciónak. ■

Az általános algebrai fogalmaknak megfelelően itt is beszélhetünk direkt szorzatról és szabad modulusról.

9.6. Definíció. Az $\{\mathcal{M}_i \mid i \in I\}$ modulusok $\prod\{\mathcal{M}_i \mid i \in I\}$ direkt szorzatán azt az $\mathcal{M}$ modulust értjük, amelynek tartóhalmaza az adott modulusok direkt szorzata, s a műveleteket komponensenként végezzük. Az X halmaz generálta szabad $\mathcal{F}_X$ moduluson azt a modulust értjük, amelyet az X halmaz generál, s az X halmazt bármely (bal oldali R-) modulusba akármilyen módon leképezve e leképezésnek létezik egyértelmű homomorfizmus kiterjesztése az $\mathcal{F}_X$-re. □

Tekintettel arra, hogy a modulusok az összeadásra nézve (kommutatív) csoportot alkotnak, ezért direkt szorzataikra teljesülnek az 5.7. pontban tárgyalt eredmények. (Az sem okoz zavart, hogy a csoportműveleteken kívül vannak további egyváltozós műveletek is.) Itt is beszélünk ezek direkt összegéről, amit érdemes külön definiálni.

9.7. Definíció. Az $\{\mathcal{M}_i \mid i \in I\}$ modulusok $\sum\{\mathcal{M}_i \mid i \in I\}$ direkt összegén a $\prod\{\mathcal{M}_i \mid i \in I\}$ direkt szorzatnak azt a részmodulusát értjük, amelynek elemei azok a vektorok, amelyeknek csak véges sok $\mathbf{o}$-tól különböző komponense van. □

Nyilvánvaló, hogy a direkt összeg valóban részmodulus, amely véges indexhalmaz esetén megegyezik a direkt szorzattal.

A csoportokhoz hasonlóan itt is beszélhetünk belső direkt összegről, azaz a direkt összeget az adott részmodulusok által generáltnak tekinthetjük, és bármelyiknek a többiek generátumával való metszete egyedül a nullelemből áll. Véges sok tag esetén a direkt összegre itt is használjuk az $\oplus$ jelölést.

9.8. Tétel. *Az egy elem generálta szabad modulus akármennyi példányának a direkt összege a generátorelemek halmaza által generált szabad modulus.*

Bizonyítás. Avégett, hogy a komponensek indexeiről beszélhessünk, célszerű annyi példányban venni az egy elemmel generált szabad modulust, amennyi példány direkt összegét akarjuk képezni. Legyen $\mathcal{F}_i$ az $\mathbf{x}_i$ elem által szabadon generált modulus. Tekintsünk egy $\mathcal{M}$ modulust, és feleltessük meg az $\mathbf{x}_i$ elemnek e modulus $\mathbf{u}_i$ elemét. Mivel minden egyes $\mathcal{F}_i$ szabad, ezért léteznek olyan egyértelmű $\varphi_i : \mathcal{F}_i \to \mathcal{M}$ homomorfizmusok, amelyekre $\varphi_i(\mathbf{x}_i) = \mathbf{u}_i$ teljesül. Ennek a homomorfizmusnak a direkt összegre egyetlen kiterjesztése lehet; ha az $\mathbf{y}$ vektor i-edik komponense $\mathbf{y}_i$, akkor $\varphi(\mathbf{y})$ az összes $\varphi_i(\mathbf{y}_i)$-k összege. (Ennek az összegnek van értelme, hiszen a komponensek közt csak véges sok $\mathbf{o}$-tól különböző lehet.) A fenti megfeleltetés viszont nyilvánvalóan homomorfizmus, ami bizonyítja, hogy valóban szabad modulust kaptunk. ■

9.2. Unitér modulusok

Az eddigi eredményekből tulajdonképpen még nem is következik, hogy léteznek „igazi" R-modulusok. Elképzelhető ugyanis, hogy az R elemeivel való szorzás minden egyes esetben a modulus nullelemét adja. Ekkor az R-modulusról csupán annyit tudunk, amennyit róla mint Abel-csoportról tudunk. Az eredeti axiómák nem biztosítják, hogy a modulus ne ilyen legyen. Egységelemes gyűrűk esetében azonban könnyen találhatunk olyan feltételt, amely a fenti esetet kizárja, éppen úgy, mint a vektortereknél.

9.9. Definíció. Ha minden R-beli a és minden $\mathcal{M}$-beli $\mathbf{u}$ esetén $a\mathbf{u} = \mathbf{o}$, akkor triviális modulusról beszélünk. Ha R-nek van egy 1 egységeleme és tetszőleges $\mathbf{u} \in \mathcal{M}$ esetén teljesül az $1 \cdot \mathbf{u} = \mathbf{u}$ összefüggés, akkor azt mondjuk, hogy $\mathcal{M}$ unitér R-modulus. □

A fenti két „szélsőséges" eset között még nagyon sok lehetőség léphet fel. A továbbiakban mindenekelőtt azt fogjuk belátni, hogy egységelemes gyűrűk esetén minden modulus e két „véglet" segítségével állítható elő. E tétel egy általánosabb felbontási tételnek, az úgynevezett Peirce-féle felbontási tételnek a következménye.

9.10. Tétel. *Ha e az R gyűrűnek olyan idempotens eleme, amely R minden elemével felcserélhető (azaz $e^2 = e$ és bármely $a \in R$ esetén $ea = ae$), akkor tetszőleges ${}_R\mathcal{M}$ bal oldali modulus felírható részmodulusainak $\mathcal{M}' \oplus \mathcal{M}''$ direkt összegeként, ahol $\mathcal{M}'$ elemein az e-vel való szorzás identikusan hat, míg $\mathcal{M}''$ bármely elemét e-vel szorozva a nullelemet kapjuk. E tulajdonságok a komponenseket egyértelműen meghatározzák.*

Bizonyítás. Legyenek $\mathcal{M}'$ elemei az $e\mathbf{u}$ alakú elemek és $\mathcal{M}''$ elemei az $\mathbf{u} - e\mathbf{u}$ alakú elemek. Az $a(e\mathbf{u}) = e(a\mathbf{u})$ és az $e\mathbf{u} - e\mathbf{v} = e(\mathbf{u} - \mathbf{v})$ feltételekből azonnal következik, hogy mindkét esetben részmodulust kapunk. Az $\mathbf{u} = e\mathbf{u} + (\mathbf{u} - e\mathbf{u})$ összefüggés biztosítja, hogy

e két részmodulus az egész modulust generálja. Azt kell még belátni, hogy a nullelem az egyetlen közös elemük. Tegyük fel, hogy van egy közös elemük, amely ezért kétféleképpen is felírható: $e\mathbf{u} = \mathbf{v} - e\mathbf{v}$. Ebből azt kapjuk, hogy $e\mathbf{u} = e(e\mathbf{u}) = e(\mathbf{v} - e\mathbf{v}) = e\mathbf{v} - e\mathbf{v} = \mathbf{o}$. A bizonyításból az is kiderül, hogy ha $\mathbf{u} \in M'$, akkor $e\mathbf{u} = \mathbf{u}$, és ha $\mathbf{u} \in \mathcal{M}''$, akkor $e\mathbf{u} = \mathbf{o}$. Legyen most $\mathbf{u}+\mathbf{v}$ az $\mathcal{M}$-nek egy olyan eleme, amelyre $\mathbf{u} \in \mathcal{M}'$ és $\mathbf{v} \in \mathcal{M}''$. Ekkor $e(\mathbf{u}+\mathbf{v}) = \mathbf{u}$ alapján a megadott tulajdonságok valóban csak a megfelelő részmodulusok elemeinek vannak meg. ■

9.11. Következmény. *Az R egységelemes gyűrű feletti tetszőleges R-modulus felbontható egy unitér és egy triviális R-modulus direkt összegére.*

Bizonyítás. A gyűrű egységelemére teljesülnek a 9.10. tételben kirótt feltételek. ■

Megjegyzések. 1. A fenti tétel lehetőséget ad arra, hogy egységelemes gyűrűk esetében a triviális modulusoktól eltekintsünk, és mindig csak unitér modulusokat vizsgálhassunk. Ha a gyűrűnek nincs egységeleme, akkor ez természetesen lehetetlen. Akkor lehetne a vizsgálatokat hasonló módon redukálni, ha az eredeti gyűrűt „ki lehetne cserélni" egy egységelemes gyűrűre úgy, hogy ezzel a modulusok és modulushomomorfizmusok ne változzanak meg.

Egy ilyen kicserélés el is végezhető. Tekintsük az (n, a) párok halmazát, ahol n egész szám és a eleme az adott R gyűrűnek. Ezekre definiáljuk az összeadást komponensenként és a szorzást az $(n, a) \cdot (k, b) = (nk, nb + ka + ab)$ összefüggéssel. Így egységelemes gyűrűt kapunk, amely tartalmaz egy, az R-rel izomorf gyűrűt. Könnyen belátható, hogy ha $\mathbf{u}$ valamely bal oldali R-modulus egy eleme, akkor az $(n, a)\mathbf{u} = n\mathbf{u} + a\mathbf{u}$ definícióval az eredeti modulus a bővebb gyűrű feletti modulussá válik, és minden R-homomorfizmus a bővebb gyűrű feletti homomorfizmus lesz.

2. Amennyiben az összes R-modulust tekintjük, akkor természetesen „többet" kapunk, mintha csupán az unitéreket vesszük figyelembe. Az unitér R-modulusok közti R-homomorfizmusok azonban nem változnak meg. Megváltoznak viszont a szabad R-modulusok. Például az egy elemmel generált szabad R-modulus elemeit $(n, \mathbf{u})$ párok alakjában írhatjuk fel, ahol n egész szám és $\mathbf{u}$ az $\mathbf{x}$ elem generálta szabad unitér R-modulus egy eleme. Az elempárok közötti összeadást komponensenként végezzük, míg R egy a elemével szorozva az $a(n, \mathbf{u}) = (0, na\mathbf{x} + a\mathbf{u})$ elemet kapjuk. Ennek az R-modulusnak a generátoreleme az $(1, \mathbf{o})$ elem. □

9.3. Az R-homomorfizmusok csoportja

A vektorterek lineáris leképezéseihez hasonlatosan, bizonyos esetekben az R-modulusoknál is végezhetünk műveleteket az R-homomorfizmusokkal. Erre általában – mint látni fogjuk – sokkal korlátozottabbak a lehetőségek.

9.12. Tétel. *Legyen $\mathcal{M}$ és $\mathcal{N}$ két R-modulus, és $\varphi : {}_R\mathcal{M} \to {}_R\mathcal{N}$, valamint $\psi : {}_R\mathcal{M} \to {}_R\mathcal{N}$ két R-homomorfizmus. Definiáljuk ezek összegét a $(\varphi+\psi)\mathbf{u} = \varphi\mathbf{u}+\psi\mathbf{u}$ összefüggéssel. Erre az összeadásra nézve az $\mathcal{M}$-et $\mathcal{N}$-be képező R-homomorfizmusok egy Abel-csoportot alkotnak, amelyet* $\mathrm{Hom}_R({}_R\mathcal{M}, {}_R\mathcal{N})$ *vagy* $\mathrm{Hom}_R(\mathcal{M}, \mathcal{N})$ *jelöl.*

Ha $\mathcal{N} = \mathcal{M}$, akkor az $\mathrm{End}_R({}_R\mathcal{M}) = \mathrm{Hom}_R({}_R\mathcal{M}, {}_R\mathcal{N})$ *jelölést is fogjuk használni.*

Bizonyítás. Először belátjuk, hogy $\varphi+\psi$ is az $\mathcal{M}$-et $\mathcal{N}$-be képező R-homomorfizmus. Ha $\mathbf{u}, \mathbf{v} \in \mathcal{M}$, akkor a homomorfizmusok összegének a definíciója szerint

$$(\varphi + \psi)(\mathbf{u} + \mathbf{v}) = \varphi(\mathbf{u} + \mathbf{v}) + \psi(\mathbf{u} + \mathbf{v}) = \varphi(\mathbf{u}) + \varphi(\mathbf{v}) + \psi(\mathbf{u}) + \psi(\mathbf{v}) =$$

$$= (\varphi\mathbf{u} + \psi\mathbf{u}) + (\varphi\mathbf{v} + \psi\mathbf{v}) = (\varphi + \psi)\mathbf{u} + (\varphi + \psi)\mathbf{v},$$

ami igazolja az összegtartást. Ha $a \in R$, akkor

$$(\varphi + \psi)(a\mathbf{u}) = \varphi(a\mathbf{u}) + \psi(a\mathbf{u}) = a(\varphi\mathbf{u}) + a(\psi\mathbf{u}) = a(\varphi\mathbf{u} + \psi\mathbf{u}) = a((\varphi + \psi)\mathbf{u}),$$

bizonyítva a másik azonosságot.

Az R-modulusokban értelmezett összeadás kommutativitásából, illetve asszociativitásából azonnal következik, hogy az R-homomorfizmusok összeadása is kommutatív, illetve asszociatív. Így az $\mathcal{M}$-et $\mathcal{N}$-be vivő R-homomorfizmusok egy kommutatív félcsoportot alkotnak.

Tekintsük most azt a leképezést, amely $\mathcal{M}$ minden eIeméhez az $\mathcal{N}$ nullelemét rendeli hozzá. Erre a 0 leképezésre és tetszőleges $\varphi : \mathcal{M} \to \mathcal{N}$ R-homomorfizmusra nyilvánvalóan teljesül a $0+\varphi = \varphi$ összefüggés. Ezen felül triviálisan teljesül az is, hogy a 0 leképezés R-homomorfizmus. Könnyen belátható az is, hogy a $(-\varphi)\mathbf{u} = -(\varphi\mathbf{u})$ összefüggéssel definiált leképezés is R-homomorfizmus, amelyre teljesül a $(-\varphi) + \varphi = 0$ összefüggés. Így valóban egy Abel-csoportot kaptunk. ■

Megjegyzés. A vektorterek esetében a fenti homomorfizmusokról azt is be lehet látni, hogy maguk is vektorteret alkotnak az $(a\varphi)\mathbf{u} = a(\varphi\mathbf{u})$ összefüggéssel definiált szorzásra mint skalárral való szorzásra. Ez modulusokra általában nem igaz, mert az $(a\varphi)(b\mathbf{u})$ kifejezést kétféleképpen meghatározva, egyrészt $a(\varphi(b\mathbf{u})) = ab(\varphi(\mathbf{u}))$, másrészt $b((a\varphi)(\mathbf{u})) = b(a(\varphi(\mathbf{u}))) = ba(\varphi(\mathbf{u}))$ adódik, és ebből az $(ab - ba)(\varphi\mathbf{u}) = 0$ összefüggéshez jutunk, ami nem mindig teljesül. Ha R kommutatív, akkor a fenti összefüggés igaz, amiből kimutatható, hogy Hom $(\mathcal{M}, \mathcal{N})$ szintén R-modulus. Ha viszont R nem kommutatív, akkor nem kaphatunk mindig R-modulust. Ha ugyanis φ egy modulusnak önmagára való identikus leképezése, akkor az $(ab - ba)\mathbf{u} = \mathbf{o}$ összefüggést kapjuk. Márpedig belátható, hogy ez nem mindig igaz; például a szabad modulusok generátorelemeit R egyetlen nemnulla eleme sem képezi le a nullelemre. □

9.13. Tétel. *Legyenek $\varphi : \mathcal{A} \to \mathcal{B}$ és $\psi : \mathcal{B} \to \mathcal{C}$ R-homomorfizmusok. Ekkor ezek $\psi\varphi : \mathcal{A} \to \mathcal{C}$ szorzata is R-homomorfizmus. Az R-homomorfizmusok szorzata asszociatív és a 9.12. tételben definiált összeadásra nézve mindkét oldalról disztributív. Ennek következtében* End $_R(\mathcal{M})$ *gyűrűt alkot a fenti műveletekre.*

Bizonyítás. $\psi\varphi(\mathbf{u}+\mathbf{v}) = \psi(\varphi\mathbf{u}+\varphi\mathbf{v}) = \psi\varphi(\mathbf{u})+\psi\varphi(\mathbf{v})$, valamint $\psi\varphi(a\mathbf{u}) = \psi(a(\varphi\mathbf{u})) = a(\psi(\varphi(\mathbf{u})))$ bizonyítják az első állítást. A szorzat asszociativitása tetszőleges leképezésekre teljesül. A disztributivitás igazolásakor természetesen két esetet kell megkülönböztetni. Tegyük fel, hogy létezik a $\varphi + \psi$ összeg. Ha létezik az $\mathcal{U}$ vektortéren ható $\alpha(\varphi + \psi)$ szorzat, akkor minden $\mathbf{u} \in \mathcal{U}$ elemre

$$(\alpha(\varphi + \psi))\mathbf{u} = \alpha(\varphi\mathbf{u} + \psi\mathbf{u}) = \alpha\varphi\mathbf{u} + \alpha\psi\mathbf{u} = (\alpha\varphi + \alpha\psi)\mathbf{u}$$

bizonyítja az egyik disztributivitást. Ha viszont a $\mathcal{V}$ vektortéren ható $(\varphi + \psi)\beta$ szorzat létezik, akkor a másik oldali disztributivitás a $\mathcal{V}$-beli $\mathbf{v}$-re felírt

$$((\varphi + \psi)\beta)\mathbf{v} = (\varphi + \psi)(\beta\mathbf{v}) = \varphi\beta\mathbf{v} + \psi\beta\mathbf{v} = (\varphi\beta + \psi\beta)\mathbf{v}$$

összefüggésből adódik. A tétel utolsó állítása abból következik, hogy End $_R(\mathcal{M})$ bármely két elemének létezik a szorzata. ■

Ennek a pontnak a további részében egyetlen rögzített R-modulust tekintünk. Tulajdonképpen ez egy $\mathcal{M}$ Abel-csoport, amely „sok” R gyűrű felett lehet akármelyik oldali R-modulus. Az első kötet 151. oldalán szereplő következő szinte triviális tétel e gyűrűk közötti bizonyos kapcsolatról szól:

Tétel. *Legyen $\varphi : S \to R$ egy tetszőleges gyűrűhomomorfizmus, és $\mathcal{M}$ egy R-modulus. Ekkor $\mathcal{M}$ az*

$$s \cdot \mathbf{x} = \varphi(s) \cdot \mathbf{x} \qquad (s \in S) \quad (\mathbf{x} \in \mathcal{M})$$

definícióval S-modulussá válik.

Ott, mint az egyik legfontosabb eset van említve, amikor $S \leq R$ és φ a természetes beágyazás. Ez felveti azt a kérdést, hogy nem létezik-e olyan R gyűrű, amelyben minden másik szóba jövő S gyűrű „benne van”. Tekintettel arra, hogy minden modulushomomorfizmus homomorfizmusa $\mathcal{M}$-nek mint Abel-csoportnak, ezért erre az univerzális szerepre az Abel-csoport endomorfizmusai a legszembetűnőbb jelöltek.

Jelölés. Az egész számok $\mathbb{Z}$ gyűrűje esetén $\mathrm{Hom}_{\mathbb{Z}}(\mathcal{M},\mathcal{N})$ helyett a $\mathrm{Hom}\,(\mathcal{M},\mathcal{N})$, továbbá $\mathrm{End}_{\mathbb{Z}}(\mathcal{M})$ helyett az $\mathrm{End}\,(\mathcal{M})$ jelölést (is) fogjuk használni.

9.14. Tétel. *Legyen $\mathcal{M}$ tetszőleges R-modulus, és minden $a \in R$ elemnek feleltessük meg a $\varphi_a : \mathbf{u} \mapsto a\mathbf{u}$ függvényt. Az $a \mapsto \varphi_a$ megfeleltetés egy $\Phi : R \to \mathrm{End}\,(\mathcal{M})$ gyűrűhomomorfizmust létesít. Φ pontosan akkor injektív, ha R egyetlen 0-tól különböző eleme sem képezi $\mathcal{M}$ minden elemét $\mathbf{o}$-ba. Ez az eset például akkor, ha $\mathcal{M}$ szabad R-modulus.*

Bizonyítás. Az $a(\mathbf{u}+\mathbf{v}) = a\mathbf{u}+a\mathbf{v}$ összefüggés biztosítja, hogy Φ az R-et $\mathrm{End}\,(\mathcal{M})$-be képezi le. $(a+b)\mathbf{u} = a\mathbf{u}+b\mathbf{u}$ miatt φ összegtartó és $(ab)\mathbf{u} = a(b\mathbf{u})$ következtében szorzattartó. $0\mathbf{u} = \mathbf{o}$ miatt $\Phi(0)$ a null-leképezés és $(-a)\mathbf{u} = -a\mathbf{u}$ miatt az ellentett képe a kép ellentettje. Φ tehát gyűrűhomomorfizmus. Tekintettel arra, hogy Φ magja R-nek pontosan azokból az elemeiből áll, amelyek minden elemet $\mathbf{o}$-ra képeznek, ezért az injektivitásra vonatkozó állítás is igaz. Tekintsük végül az $\ldots, \mathbf{x}_i, \ldots$ elemek generálta szabad R-modulust. Azt fogjuk kimutatni, hogy tetszőleges $a \in R$ esetén, ha $a \neq 0$, akkor $a\mathbf{x}_i \neq \mathbf{o}$. Tekintsük evégett az (n, r) alakú elemek halmazát, ahol $n \in \mathbb{Z}$ és $r \in R$. Ezek az elemek elemei a $\mathbb{Z} + R$ additív Abel-csoport összegnek; ezért ezek az összeadásra csoportot alkotnak. Legyen tetszőleges $a \in R$ esetén $a \cdot (n, r) = (0, na+br)$. Ezáltal e párok halmaza R-modulussá vált. Mivel szabad modulusból indultunk ki, ezért van olyan φ R-homomorfizmus, amely az $\mathbf{x}_i$ elemet $(1, 0)$-ba viszi (s a többi generátort például $\mathbb{Z} + R$ nullelemébe: $(0, 0)$-ba). Ekkor $a \neq 0$ esetén $\varphi(a \cdot \mathbf{x}_i) = a \cdot (\varphi\mathbf{x}_i) = a \cdot (1, \mathbf{o}) = (0, a) \neq (0, 0)$ miatt $a \cdot \mathbf{x}_i$ nem eleme φ magjának, így $a\mathbf{x}_i \neq \mathbf{o}$. ■

Megjegyzés. A fenti eredmény természetesen vonatkozik a jobb oldali S-modulusokra is. Ha S egyetlen eleme sem „annullálja” a modulus elemeit, akkor S is tekinthető a tartócsoport endomorfizmus-gyűrűje részének. □

Az általános elvnek megfelelően az egyedül a nullelemből álló részmodulust, illetve az egész modulust *triviális részmodulusnak* nevezzük. A többi részmodulus neve *nemtriviális részmodulus.*

9.15. Definíció. Ha egy nemtriviális modulusnak nincs nemtriviális részmodulusa, akkor minimális vagy egyszerű modulusnak nevezzük. □

9.16. Tétel (Schur-lemma)**.** *Ha $\mathcal{M}$ minimális bal oldali R-modulus, akkor $\Delta = \mathrm{End}_R(\mathcal{M})$ test, amelyre nézve $\mathcal{M}$ egy $R-\Delta$-modulus.*

Bizonyítás. Legyen $\eta \neq 0$ tetszőleges R-endomorfizmus. Ez azt jelenti, hogy $\mathrm{Ker}\,\eta \neq \mathcal{M}$ és $\mathrm{Im}\,\eta \neq \{\mathbf{o}\}$. Tekintettel arra, hogy mind $\mathrm{Ker}\,\eta$, mind $\mathrm{Im}\,\eta$ részmodulus, és $\mathcal{M}$-nek csupán két részmodulusa van, csak $\mathrm{Ker}\,\eta = \{\mathbf{o}\}$ és $\mathrm{Im}\,\eta = \mathcal{M}$ lehetséges. Ez azt jelenti, hogy η bijekció. Létezik tehát az η^{-1} inverz leképezés, amely nyilvánvalóan ugyancsak műveletartó. Így Δ valóban test. A második állítás tüstént következik az R-homomorfizmus definíciójából. ■

9.17. Tétel. *Tetszőleges $\mathcal{M}$ Abel-csoportra legyen $E = \mathrm{End}(\mathcal{M})$. Ekkor $\mathcal{M}$ bal oldali E-modulus. Ha $\mathcal{M}$ bal oldali R-modulus, akkor $\mathrm{End}_R(\mathcal{M})$ az $\mathrm{End}(\mathcal{M})$ azon elemeiből áll, amelyek $\Phi(R)$ elemeivel felcserélhetőek, ahol Φ a 9.14. tételben definiált homomorfizmus.*

Bizonyítás. Az, hogy $\mathcal{M}$ bal oldali E-modulus, abból következik, hogy $\varphi, \psi \in E$ esetén tetszőleges $\mathbf{u} \in \mathcal{M}$ mellett $(\varphi\psi)(\mathbf{u}) = \varphi(\psi(\mathbf{u}))$. Az R-homomorfizmus definíciója szerint $\varphi \in \mathrm{End}_R(\mathcal{M})$ pontosan akkor, ha minden $a \in R$ esetén $\varphi(a\mathbf{u}) = a\varphi(\mathbf{u})$ teljesül tetszőleges $\mathbf{u} \in \mathcal{M}$ mellett. Ennek az a feltétele, hogy a bal oldali és jobb oldali függvény ugyanaz legyen, azaz $\varphi\Phi(a)$ és $\Phi(a)\varphi$ megegyezzenek. ■

Megjegyzés. A fenti tétel azt mutatja, hogy „R-homomorfizmus az, ami az R-beli szorzással felcserélhető". Ennek viszont látszólag nincs értelme akkor, ha nem endomorfizmusról van szó. Éppen ezért célszerű a 9.2. tételt „átfogalmazni". Ott minden $a \in R$ elemhez egyetlen egyváltozós műveletet rendeltünk hozzá. Valójában ez a művelet minden modulusra más és más. (Csoportok esetén is van „csoportszorzás", ami minden egyes csoportban másképpen „realizálódik".) Így itt is az $a \in R$ elemmel való beszorzást az R feletti $\mathcal{M}$ modulusban célszerű $a_{\mathcal{M}}$-mel jelölni. Ekkor tetszőleges ${}_R\mathcal{N}$-re képező $\varphi : \mathcal{M} \to \mathcal{N}$ Abel-csoport homomorfizmus pontosan akkor lesz R-homomorfizmus, ha minden $a \in R$ esetén $\varphi a_{\mathcal{M}} = a_{\mathcal{N}}\varphi$. □

9.18. Tétel. *Tekintsük az R gyűrű elemei és az ${}_R\mathcal{M}$ elemei között azt a relációt, amelynél $a \in R$ és $\mathbf{u} \in \mathcal{M}$ akkor állnak relációban, ha $a\mathbf{u} = \mathbf{o}$. Tudjuk, hogy minden heterogén reláció egy Galois-kapcsolatot hoz létre. Legyen $\mathcal{H} \subseteq \mathcal{M}$ és $H \subseteq R$. Jelölje $\ell(\mathcal{H})$, illetve $r(H)$ az R-nek, illetve az $\mathcal{M}$-nek azt a részhalmazát, amelyet a megfelelő Galois-kapcsolat az $\mathcal{M}$-beli $\mathcal{H}$, illetve az R-beli H részhalmazához hozzárendel.*

$\ell(\mathcal{H})$ mindig balideál, $r(H)$ mindig bal oldali $\mathrm{End}_R(\mathcal{M})$-modulus. Ha $\mathcal{H}$ részmodulus, akkor $\ell(\mathcal{H})$ az R-nek jobbideálja is, ha H az R-nek jobbideálja, akkor $r(H)$ az $\mathcal{M}$-ben részmodulus is.

Bizonyítás. Legyenek $a, b \in \ell(\mathcal{H})$ és $c \in R$. Ekkor $\mathcal{H}$ tetszőleges $\mathbf{u}$ elemére $(a-b)\mathbf{u} = a\mathbf{u} - b\mathbf{u} = \mathbf{o} - \mathbf{o} = \mathbf{o}$ és $(ca)\mathbf{u} = c(a\mathbf{u}) = c\mathbf{o} = \mathbf{o}$, tehát $\ell(\mathcal{H})$ balideál. Legyenek $\mathbf{u}, \mathbf{v} \in r(H)$ és φ tetszőleges R-homomorfizmus. Ha $a \in H$, akkor $a(\mathbf{u} - \mathbf{v}) = a\mathbf{u} - a\mathbf{v} = \mathbf{o} - \mathbf{o} = \mathbf{o}$ miatt $r(H)$ részcsoport; $a\varphi(\mathbf{u}) = \varphi(a\mathbf{u}) = \varphi(\mathbf{o}) = \mathbf{o}$ miatt bal oldali $\mathrm{End}_R(\mathcal{M})$-modulus is.

Legyen most $\mathcal{H}$ az $\mathcal{M}$ részmodulusa, $a \in \ell(\mathcal{H})$ és $x \in R$. Ekkor tetszőleges $\mathbf{u} \in \mathcal{H}$ esetén $x\mathbf{u} \in \mathcal{H}$ miatt $(ax)\mathbf{u} = a(x\mathbf{u}) = a\mathbf{o} = \mathbf{o}$, vagyis $ax \in \ell(\mathcal{H})$. Legyen H jobbideál R-ben. Ekkor $a \in H$ és $x \in R$ esetén $ax \in H$. Így $r(H)$ tetszőleges $\mathbf{u}$ elemére $a(x\mathbf{u}) = (ax)\mathbf{u} = \mathbf{o}$, vagyis H bármely a eleme $\mathbf{o}$-ra képez minden $x\mathbf{u}$ elemet; tehát ezek az elemek is $r(H)$-ban vannak. ■

A továbbiakban fel fogjuk használni a vektorterekben a generálásra, a lineáris függésre és függetlenségre, valamint a bázisra vonatkozó ismereteket; mégpedig abban az erősebb formában, hogy az alaptest kommutativitását sem tételezzük fel. Ennek átgondolását az olvasóra bízzuk.

9.19. Tétel. *Legyen $\mathcal{M}$ minimális nemtriviális bal oldali R-modulus és legyen $\Delta = \mathrm{End}_R(\mathcal{M})$. Az $\mathcal{M}$-nek mint bal oldali Δ-vektortérnek egy $\mathbf{v}$ eleme akkor és csak akkor lineárisan függő az $\mathcal{M}$-nek $\mathbf{u}_1, \dots, \mathbf{u}_n$ elemeitől, ha bármely R-beli a elemre az $a\mathbf{u}_1 = \dots = a\mathbf{u}_n = \mathbf{o}$ feltételből következik $a\mathbf{v} = \mathbf{o}$. (Azaz, ha $\mathbf{v} \in r(\ell(\langle \mathbf{u}_1, \dots, \mathbf{u}_n \rangle))$.)*

Bizonyítás. Tegyük fel először, hogy fennáll a lineáris függés, azaz alkalmas Δ-beli elemekkel $\mathbf{v} = \eta_1\mathbf{u}_1 + \dots + \eta_n\mathbf{u}_n$, és legyen $a \in \ell(\langle \mathbf{u}_1, \dots, \mathbf{u}_n \rangle)$. Ekkor $\mathbf{o} = \eta_1(a\mathbf{u}_1) + \dots + \eta_n(a\mathbf{u}_n) = a(\eta_1\mathbf{u}_1 + \dots + \eta_n\mathbf{u}_n) = a\mathbf{v}$ igazolja az állítást.

A fordított irányú állítást az n-re vonatkozó teljes indukcióval bizonyítjuk be. Ha $n = 0$, akkor a feltétel azt mondja, hogy az üres halmazt annulláló, minden R-beli elem annullálja $\mathbf{v}$-t. Mivel az üres halmazt minden elem annullálja, ezért $\mathbf{v}$-t is minden elem annullálja. Így $\mathbf{v} \in r(R)$. A 9.19. tétel szerint $r(R)$ részmodulus. Mivel $\mathcal{M}$ nemtriviális, ezért $r(R) \neq \mathcal{M}$; így a minimalitás miatt $r(R) = \{\mathbf{o}\}$, azaz $\mathbf{v} = \mathbf{o}$. Márpedig $\mathbf{o}$ valóban függ az üres halmaztól.

Tegyük most fel, hogy az állítás igaz valamely n természetes számra és igazoljuk $(n+1)$-re. Legyenek a kiindulásul vett vektorok $\mathbf{u}_1, \dots, \mathbf{u}_{n+1}$ és $\mathbf{v}$. Legyen $B = \ell(\mathbf{u}_1, \dots, \mathbf{u}_n)$; ha $\mathbf{u}_{n+1} \in r(B)$, akkor az indukciós feltevés miatt $\mathbf{v}$ lineárisan függ már az első n elemtől is. Tegyük fel tehát, hogy $\mathbf{u} = \mathbf{u}_{n+1} \notin r(B)$.

Ez azt jelenti, hogy a $B\mathbf{u} = \{b\mathbf{u} \mid b \in B\}$ halmaz nem csupán a nullelemből áll. Kimutatjuk, hogy $B\mathbf{u}$ részmodulus. Valóban, ha $a, b \in B$, akkor $a\mathbf{u} - b\mathbf{u} = (a-b)\mathbf{u} \in B\mathbf{u}$, és tetszőleges R-beli c-vel $c(a\mathbf{u}) = (ca)\mathbf{u} \in B\mathbf{u}$. A minimalitás szerint tehát $\mathcal{M} = B\mathbf{u}$.

Definiáljuk most az η megfeleltetést az $\eta : a\mathbf{u} \mapsto a\mathbf{v}$ összefüggéssel, ahol a végigfut B elemein. Mindenekelőtt azt kell belátni, hogy η leképezés, azaz egy elemhez egyértelműen rendel hozzá egy elemet: ha $a\mathbf{u} = b\mathbf{u}$, akkor $(a-b) \in B$, és így $a\mathbf{v} = b\mathbf{v}$. Az $\mathcal{M} = B\mathbf{u}$ feltétel miatt η-t az egész $\mathcal{M}$-re értelmeztük. Így valóban $\mathcal{M}$-nek egy leképezését kaptuk. Tetszőleges $c \in R$ esetén $cB \subseteq B$, mert B balideál; így $\eta(cb\mathbf{u}) = (cb)\mathbf{v} = c(b\mathbf{v})$, tehát η R-homomorfizmus. Tekintsük most a $\mathbf{w} = \mathbf{v} - \eta(\mathbf{u})$ elemet. Ha $a \in B$, akkor $a\mathbf{w} = a\mathbf{v} - \eta(a\mathbf{u}) = \mathbf{o}$, azaz $\mathbf{w} \in r(B)$. Az indukciós feltevés alapján tehát $\mathbf{w}$ lineárisan függ az $\mathbf{u}_1, \dots, \mathbf{u}_n$ elemektől; és így $\mathbf{v}$ lineárisan függ az $\mathbf{u}_1, \dots, \mathbf{u}_n, \mathbf{u}$ elemektől. ■

9.20. Tétel (sűrűségi tétel)**.** *Legyen $\mathcal{M}$ minimális, nemtriviális R-modulus, legyen $\Delta = \mathrm{End}_R(\mathcal{M})$, legyenek $\mathbf{u}_1, \dots, \mathbf{u}_n$ a ${}_\Delta\mathcal{M}$ független elemei és $\mathbf{v}_1, \dots, \mathbf{v}_n$ tetszőleges elemei $\mathcal{M}$-nek. Ekkor létezik olyan $a \in R$, amelyre $\mathbf{v}_i = a\mathbf{u}_i$, teljesül, minden $1 \leq i \leq n$ esetén.*

Bizonyítás. Mivel minden egyes $\mathbf{u}_i$ lineárisan független a többi $\mathbf{u}_j$-től, ezért – mint azt a 9.19. tétel bizonyításában láttuk – a $B_i = \ell(\mathbf{u}_1, \dots, \mathbf{u}_{i-1}, \mathbf{u}_{i+1}, \dots, \mathbf{u}_n)$ balideálra $B_i\mathbf{u}_i = \mathcal{M}$ teljesül. Így léteznek olyan R-beli a_i elemek $(a_i \in B_i)$, amelyekre $a_i\mathbf{u}_i = \mathbf{v}_i$ és $a_i\mathbf{u}_j = \mathbf{o}$, ha $j \neq i$. Az $a = a_1 + \dots + a_n$ elem nyilvánvalóan kielégíti a kívánt feltételt. ■

Megjegyzés. Ha $\mathcal{M}$ véges dimenziós a Δ felett, akkor a sűrűségi tétel elég pontosan leírja a modulus szerkezetét, mint ezt a Wedderburn–Artin-struktúratételnél, majd később a csoportalgebráknál látni fogjuk. A végtelen dimenziós esetben a sűrűségi tétel egy interpolációs tételnek fogható fel.

Az R-homomorfizmusok segítségével általánosíthatjuk a 9.10. tételt úgy, hogy a direkt felbonthatóságnak szükséges és elégséges feltételét kapjuk.

9.21. Tétel. *Ha $\varepsilon \in End_R({}_R\mathcal{M})$ idempotens (azaz $\varepsilon^2 = \varepsilon$), akkor $\mathcal{M}$ felírható az*

$$\mathcal{M} = \mathrm{Im}\ \varepsilon \oplus \mathrm{Ker}\ \varepsilon$$

direkt összeg alakban, és az $\mathcal{M}$ minden kéttagú direkt felbontása alkalmas idempotens ε-nal a fenti alakba írható.

Bizonyítás. A Ker ε elemei definíció szerint azok az $\mathbf{u}$ elemek, amelyekre $\varepsilon\mathbf{u} = \mathbf{o}$ teljesül. Az ε idempotenciája következtében Im ε éppen azokból a $\mathbf{v}$ elemekből áll, amelyekre $\varepsilon\mathbf{v} = \mathbf{v}$. Így Ker ε és Im ε metszete egyedül a nullelemet tartalmazza. (A homomorfizmus definíciójából következik, hogy mindketten részmodulusok.) Mivel tetszőleges $\mathbf{u}$ elem esetén $\varepsilon(\mathbf{u} - \varepsilon\mathbf{u}) = \mathbf{o}$, ezért az $\mathbf{u} = \varepsilon\mathbf{u} + (\mathbf{u} - \varepsilon\mathbf{u})$ felbontás azt adja, hogy a szereplő két részmodulus generálja $\mathcal{M}$-et.

Legyen most $\mathcal{M} = \mathcal{A} \oplus \mathcal{B}$ egy direkt felbontás. Ekkor $\mathcal{M}$ minden $\mathbf{u}$ eleme egyértelműen felírható $\mathbf{u} = \mathbf{a} + \mathbf{b}$ alakban, ahol $\mathbf{a} \in \mathcal{A}$ és $\mathbf{b} \in \mathcal{B}$. Triviális számolással megmutatható, hogy az $\varepsilon : (\mathbf{a} + \mathbf{b}) \mapsto \mathbf{a}$ megfeleltetés kielégíti a feltételeket. ■

Megjegyzés. Ez valóban általánosítása a 9.10. tételnek. Ott az R egy olyan e idempotens elemét tekintettük, amely R minden elemével felcserélhető. A 9.14. tételben szereplő Φ homomorfizmusra nézve ez azt jelenti, hogy $\Phi(R)$ elemei mind felcserélhetők az $\varepsilon = \Phi(e)$ elemmel, azaz e képe egy idempotens R-homomorfizmus. □

9.22. Tétel. *Rögzített R gyűrű feletti modulusokra és R-homomorfizmusokra érvényesek az alábbiak:*

a) *Az $\mathcal{M}$ modulus $\mathcal{A}$ és $\mathcal{B}$ részmodulusaira ekvivalens az alábbi három állítás:*

(1) $\mathcal{A} \leq \mathcal{B}$.

(2) *Bármely $\mathcal{M}$-be képező ψ homomorfizmusra* Im $\psi \subseteq \mathcal{A}$*-ból következik* Im $\psi \subseteq \mathcal{B}$.

(3) *Bármely $\mathcal{M}$-et leképező φ homomorfizmusra $\mathcal{B} \subseteq$ Ker φ-ből következik $\mathcal{A} \subseteq$ Ker φ.*

b) Im $\alpha \leq$ Im β *pontosan akkor teljesül, ha $\varphi\beta = 0$-ból mindig következik $\varphi\alpha = 0$.* Ker $\alpha \leq$ Ker β *pontosan akkor teljesül, ha $\alpha\psi = 0$-ból mindig következik $\beta\psi = 0$.*

c) *Ha létezik az $\alpha\beta$ szorzat, akkor* Ker $\beta \leq$ Ker $\alpha\beta$ *és* Im $\alpha\beta \leq$ Im α *teljesül.*

Bizonyítás. (1)-ből triviálisan következik (2) is és (3) is. Legyen $\psi : \mathcal{A} \to \mathcal{M}$ a természetes beágyazás és $\varphi : \mathcal{M} \to \mathcal{M}/\mathcal{B}$ a faktormodulusra való természetes homomorfizmus. Ekkor $\mathcal{A} =$ Im ψ és $\mathcal{B} =$ Ker φ; és most ezekre (2), illetve (3) biztosítja (1) teljesülését.

A b) alatti első állítás bizonyítására legyen $\mathcal{A} =$ Im α és $\mathcal{B} =$ Im β. Az (1) és (3) ekvivalenciájából éppen a kívánt állítás adódik. A másik állítás hasonlóan kapható (1) és (2) ekvivalenciájából.

A c) alatti állítást a következőképpen láthatjuk be b)-ből. Ha létezik az $\alpha\beta$ szorzat, akkor a $\varphi\alpha = 0$, illetve a $\beta\psi = 0$ feltételből nyilvánvalóan következik a $\varphi\alpha\beta = 0$, illetve a $\alpha\beta\psi = 0$ feltétel. ■

9.23. Tétel. *A $\varphi : \mathcal{U} \to \mathcal{M}$ R-homomorfizmus akkor és csak akkor képezi le $\mathcal{U}$-t bijektíven $\mathcal{M}$ egy direkt összeadandójára, ha létezik olyan $\varphi^* : \mathcal{M} \to \mathcal{U}$ R-homomorfizmus, amelyre $\varphi^*\varphi$ az $\mathcal{U}$ identitása. A $\psi : \mathcal{M} \to \mathcal{V}$ R-homomorfizmus akkor és csak akkor képezi le $\mathcal{M}$ egy direkt faktorát bijektíven $\mathcal{V}$-re, ha létezik olyan $\psi^+ : \mathcal{V} \to \mathcal{M}$ R-homomorfizmus, amelyre $\psi\psi^+$ a $\mathcal{V}$ identitása.*

Bizonyítás. Tegyük fel először, hogy a kívánt homomorfizmusok léteznek, és legyen $\mathcal{A} = \operatorname{Im}\ \varphi$, $\mathcal{B} = \mathcal{M}$, és α az $\mathcal{A}$-nak $\mathcal{M}$-be való beágyazása, illetve $\mathcal{A} = \operatorname{Ker}\ \psi$, $\mathcal{B} = \mathcal{M}$, és β a $\mathcal{B}$-nek $\mathcal{M}$-be való beágyazása. Ez mindkét esetben azt jelenti, hogy van olyan $\alpha : \mathcal{A} \to \mathcal{B}$ és $\beta : \mathcal{B} \to \mathcal{A}$ alakú R-homomorfizmus, amelyre $\beta\alpha = 1_{\mathcal{A}}$ az $\mathcal{A}$ identitása. Mindenekelőtt megmutatjuk, hogy α injektív és β szürjektív. Valóban, tetszőleges $\mathbf{a} \in \mathcal{A}$ esetén, ha $\alpha\mathbf{a} = \mathbf{o}$, akkor $\mathbf{a} = \beta\alpha\mathbf{a} = \beta\mathbf{o} = \mathbf{o}$, és $\mathbf{a} = \beta\alpha\mathbf{a} \in \operatorname{Im}\ \beta$. A $\beta\alpha = 1_{\mathcal{A}}$ egyenlőségből azonnal következik, hogy $\alpha\beta\alpha = \alpha$ és $\beta\alpha\beta = \beta$, továbbá az $\varepsilon = \alpha\beta \in \operatorname{End}\ \mathcal{B}$ idempotens, hiszen $\varepsilon^2 = \alpha\beta\alpha\beta = \alpha 1_{\mathcal{B}}\beta = \alpha\beta = \varepsilon$. A 9.22. tétel c) pontja szerint

$$\operatorname{Im}\ \alpha = \operatorname{Im}\ \alpha\beta\alpha = \operatorname{Im}\ \varepsilon\alpha \leq \operatorname{Im}\ \varepsilon = \operatorname{Im}\ \alpha\beta \leq \operatorname{Im}\ \varepsilon \quad \text{és}$$

$$\operatorname{Ker}\ \beta = \operatorname{Ker}\ \beta\alpha\beta = \operatorname{Ker}\ \beta\varepsilon \geq \operatorname{Ker}\ \varepsilon = \operatorname{Ker}\ \alpha\beta \geq \operatorname{Ker}\ \beta.$$

A 9.21. tétel szerint $\mathcal{B} = \mathcal{B}_1 \oplus \mathcal{B}_2$, ahol $\mathcal{B}_1 = \operatorname{Im}\ \varepsilon$. Ebből azt kapjuk, hogy α az $\mathcal{A}$-t $\mathcal{B}_1$-re képezi le izomorf módon és β a $\mathcal{B}_1$-t képezi le izomorf módon $\mathcal{A}$-ra.

A fordított irányú állításnál ismét ugyanúgy járhatunk el mindkét esetben. Adott egy $\mathcal{B} = \mathcal{B}_1 \oplus \mathcal{B}_2$ direkt összeg és az $\alpha : \mathcal{A} \to \mathcal{B}$, valamint $\beta : \mathcal{B} \to \mathcal{A}$ R-homomorfizmusok úgy, hogy α injektív és $\operatorname{Im}\ \alpha = \mathcal{B}_1$, továbbá β szürjektív, magja $\mathcal{B}_2$, és $\mathcal{B}_1$-re való megszorítása izomorfizmus. Jelen esetben csak annyi következik azonnal a feltételekből, hogy $\eta = \beta\alpha$ az $\mathcal{A}$-nak izomorfizmusa. Ez azt jelenti, hogy létezik az η^{-1} R-homomorfizmus. Legyen $\alpha^* = \eta^{-1}\beta$ és $\beta^+ = \alpha\eta^{-1}$. Ezekre azonnal látható, hogy $\alpha^*\alpha = \beta\beta^+ = 1_{\mathcal{A}}$. ■

Érdemes megfigyelni, hogy a részmodulus és a faktormodulus „nagyon hasonló módon” viselkedik, de nem „teljesen” ugyanúgy. Kimutatható közöttük bizonyos fokú dualitás; amit kategóriaelméleti módszerekkel lehet megfogalmazni.

Feladatok

1. Láttuk, hogy ha $e \in R$ az R elemeivel felcserélhető idempotens, akkor ${}_R\mathcal{M}$ felírható $\mathcal{M}' \oplus \mathcal{M}''$ alakban (9.10. tétel). Található-e alkalmas idempotens az $\mathcal{M}'' \oplus \mathcal{M}'$ felíráshoz?

2. Mi a válasz az előző kérdésre akkor, ha $\mathcal{M}$ unitér?

3. A 9.14. tétel alapján határozzuk meg, hogy egy Abel-csoport direkt felbontása mikor lesz modulusfelbontás.

4. Tetszőleges R gyűrűben vezessünk be egy „új” szorzást: $a \circ b = b \cdot a$. Bizonyítsuk be, hogy az eredeti összeadásra és erre a szorzásra ismét gyűrűt kaptunk, amit R^* jelöl. Bizonyítsuk be, hogy ${}_R\mathcal{M} = \mathcal{M}_{R^*}$.

5. Mit kell megváltoztatnunk az R-homomorfizmusok definíciójában, ha a 9.14. tétel megfelelőjét akarjuk bizonyítani?

6. Tetszőleges ${}_R\mathcal{M}$ és $\mathcal{M}_S$ modulusnál nézzük azt a $\varrho \subseteq R \times S$ relációt, amelynél $r\varrho s$ pontosan akkor, ha minden $\mathbf{u} \in \mathcal{M}$ esetén $(r\mathbf{u})s = r(\mathbf{u}s)$. Melyek az indukált Galois-kapcsolat zárt részhalmazai?

7. Mit jelent az, hogy ${}_R\mathcal{M}_S$, ha $\mathcal{M}_S$ helyett az ${}_{S^*}\mathcal{M}$-et tekintjük?

8. Bizonyítsuk be, hogy egy minimális R-modulus mindig direkt felbonthatatlan.

9. Adjunk meg olyan direkt felbonthatatlan modulust, amelyik nem minimális.

10. Adjunk meg olyan direkt felbonthatatlan modulust, amelynek nincs minimális (nemtriviális) részmodulusa.

11. Bizonyítsuk be, hogy tetszőleges R gyűrűre $R = {}_RR_R$. Melyek a részmodulusok?

12. Van-e olyan R gyűrű, amelyre ${}_RR$ minimális modulus, de R_R nem az.

13. Bizonyítsuk be a vektortér-tulajdonságok „alapjait”, ha Δ nem kommutatív.

9.4. Diagramok

Sok olyan bizonyításban, amely elsősorban a homomorfizmusok tulajdonságait használja fel, egyszerűbb és szemléletesebb a bizonyítás menete, ha a modulusok (vagy akár tetszőleges algebrák) helyett egy-egy „pontot” rajzolunk, a homomorfizmusok helyett pedig csak megfelelő „nyilakat”. Ilyen esetekben diagramokról beszélünk. A diagramok esetén egy-egy pont között több nyíl is mehet, és egy-egy modulus vagy homomorfizmus a rajz más helyén is szerepelhet. Diagramokról és kommutatív diagramokról már az előzőekben is volt szó. A most következőkben a diagramokkal kapcsolatos legalapvetőbb fogalmakat ismertetjük az eddigieknél precízebben.

Mindenekelőtt definiáljuk az irányított gráf fogalmát (persze ez nem algebrai fogalom, de szükségünk van rá).

Definíció. Irányított gráfnak nevezünk egy $\mathcal{G} = (X, E)$ párt, ahol $E \subseteq X \times X$. Az X elemei a gráf csúcsai (vagy szögpontjai), az E elemei a gráf (irányított) élei. Az (a, b) élhez hozzárendeljük a $k(a, b) = a$ kezdőpontját és a $v(a, b)$ végpontját. Azt, hogy $(a, b) \in E$, úgy is jelöljük, hogy $a \to b$. □

9.24. Definíció. Diagramnak nevezünk egy $\Phi = (\Phi_X, \Phi_E)$ függvénypárt, amely egy $\mathcal{G} = (X, E)$ gráfhoz R-modulusokat, illetve R-homomorfizmusokat rendel úgy, hogy $\Phi_X(a)$ egy R-modulus, $\Phi_E(a, b)$ egy olyan R-homomorfizmus, amelyre $\Phi_E(a, b) : \Phi_X(a) \to \to \Phi_X(b)$.

A diagramokat tehát a következőképpen képzelhetjük el:

$$a \xrightarrow{(a,b)} b \quad \Longrightarrow^{\Phi} \quad \Phi_X(a) \xrightarrow{\Phi_E(a,b)} \Phi_X(b).$$

A diagramokat tehát úgynevezett címkézett gráfoknak tekinthetjük, ahol a csúcsok rögzített R gyűrűhöz tartozó R-modulusok, az élek pedig olyan R-homomorfizmusokkal vannak címkézve, amelyek a kezdőpontot a végpontba képezik. A fenti definíciót valójában nem fogjuk használni; megelégszünk a szemléletes elképzeléssel. A kategóriaelméletben viszont szükséges a precíz definíció. □

9.25. Definíció. Az $\mathcal{A} \xrightarrow{\alpha} \mathcal{B}$ diagram esetén azt mondjuk, hogy $\mathcal{A}$ az α kezdőpontja és $\mathcal{B}$ a végpontja. Élek olyan $\alpha_1, \ldots, \alpha_r$ sorozatát, amelyben mindegyiknek a végpontja a következőnek a kezdőpontja, olyan útnak nevezzük, amely az első (α_1) kezdőpontjából az utolsó (α_r) végpontjába vezet. A fenti út szorzatán az $\alpha_r \cdot \ldots \cdot \alpha_1$ szorzatot értjük. (A szorzat tehát a kezdőpontból a végpontba mutató homomorfizmusnak feleltethető meg.) Ha egy pontból a másikba mutató bármely két út szorzata megegyezik, akkor a két pont között a diagram kommutatív. Ha a diagram bármely két pontja között kommutatív, akkor kommutatív diagramnak nevezzük. □

Ha valamelyik homomorfizmus az identitás, akkor ott $\rightarrow$ helyett az = jel is szerepelhet.

Az

$$\begin{array}{ccc} \mathcal{U} & \xrightarrow{\varphi} & \mathcal{V} \\ \| & & \downarrow{\scriptstyle \psi} \\ \mathcal{U} & \xleftarrow{\chi} & \mathcal{W} \end{array}, \qquad \text{illetve} \qquad \begin{array}{ccccc} \mathcal{A} & \xrightarrow{\alpha} & \mathcal{B} & \xrightarrow{\beta} & \mathcal{C} \\ \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \varepsilon} \\ \mathcal{A}_1 & \xrightarrow{\alpha_1} & \mathcal{B}_1 & \xrightarrow{\beta_1} & \mathcal{C}_1 \end{array}$$

diagramok kommutativitása az első esetben azt jelenti, hogy $\chi\psi\varphi$ az identitás, míg a második esetben nem csak a $\delta\alpha = \alpha_1\gamma$ és $\varepsilon\beta = \beta_1\delta$ egyenlőségeket, hanem (az ezekből egyébként következő) $\varepsilon\beta\alpha = \beta_1\alpha_1\gamma$ egyenlőséget is.

9.26. Definíció. Ha egy diagramban bármely csúcs legfeljebb egy él kezdőpontja és legfeljebb egy él végpontja; továbbá bármely két csúcs esetén pontosan az egyikből vezet út a másikba, akkor sorozatról beszélünk. A sorozat hosszán a benne levő élek számát értjük. □

Egy sorozat tehát az alábbi módon adható meg:

$$\cdots \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \cdots$$

Elvileg mindkét irányban akármeddig elmehetünk. Ha a sorozat hossza végtelen, az lehet úgy is, hogy a sorozatban van első elem, de lehet úgy is, hogy a sorozatban van utolsó elem. Ha azonban a sorozatban mind első, mind utolsó elem van, akkor a sorozat természetesen csak véges hosszúságú lehet.

A sorozatok közül is igen fontos két speciális típusú:

9.27. Definíció. Egy sorozat egy csúcsában félig egzakt, ha a pontba mutató, illetve az onnan kiinduló élek (illetve a megfelelő homomorfizmusok) szorzata 0. Egy sorozat félig egzakt, ha minden csúcsában félig egzakt. □

9.28. Tétel. *Az* $\cdots \xrightarrow{\alpha} \mathcal{A} \xrightarrow{\beta} \cdots$ *sorozat* $\mathcal{A}$*-ban akkor és csak akkor félig egzakt, ha* $\operatorname{Im} \alpha \leq \operatorname{Ker} \beta$.

Bizonyítás. $\beta\alpha = 0$ azt jelenti, hogy minden szóba jövő $\mathbf{u}$ elemre teljesül a $\beta\alpha\mathbf{u} = \mathbf{o}$ összefüggés. A függvények szorzásának definíciója szerint ez azzal ekvivalens, hogy minden szóba jövő $\mathbf{u}$ elemre $\beta(\alpha\mathbf{u}) = \mathbf{o}$ teljesül; ami viszont éppen azt jelenti, hogy $\operatorname{Im} \alpha \leq \operatorname{Ker} \beta$. ■

A fenti tétel alapján látható, hogy az alábbi definíció a félig egzakt sorozatok egy speciális esetét adja.

9.29. Definíció. Az $\cdots \xrightarrow{\alpha} \mathcal{A} \xrightarrow{\beta} \cdots$ sorozat $\mathcal{A}$-ban egzakt, ha Im α = Ker β. Egy sorozat egzakt, ha minden csúcsában egzakt. □

A következőkben azt nézzük meg, hogy mit jelent egy olyan – lehetőleg rövid – egzakt sorozat, amelynek egyik vagy mindkét végén a nullmodulus (a csak a nullelemet tartalmazó modulus) áll. Mindenekelőtt megjegyezzük, hogy egy egzakt sorozat hossza legalább kettő.

Tekintsük a

$$\mathcal{O} \xrightarrow{\alpha} \mathcal{A} \xrightarrow{\beta} \mathcal{B}$$

sorozatot. Ennek egzaktsága az Im $\alpha = \{\mathbf{o}\}$ miatt azt jelenti, hogy Ker $\beta = \{\mathbf{o}\}$; vagyis azt, hogy β injektív. Érdemes megfigyelni, hogy az α kiírása teljesen felesleges, mert azzal, hogy a nullmodulust képezi le, egyértelműen meghatározott. Már ezt megjegyezve írjuk fel a következő egzakt sorozatot:

$$\mathcal{A} \xrightarrow{\varphi} \mathcal{B} \longrightarrow \mathcal{O}.$$

Mivel a második homomorfizmus magja $\mathcal{B}$, ezért az egzaktság azzal ekvivalens, hogy φ szürjektív.

Most olyan egzakt sorozatokat vizsgálunk, amelyeknek mindkét végén $\mathcal{O}$ áll. Az első két esetben ezek triviálisak:

$$\mathcal{O} \longrightarrow \mathcal{A} \longrightarrow \mathcal{O}, \qquad \text{illetve} \qquad \mathcal{O} \longrightarrow \mathcal{B} \xrightarrow{\varphi} \mathcal{C} \longrightarrow \mathcal{O}.$$

Az első egzaktsága azt jelenti, hogy $\mathcal{A} = \mathcal{O}$. A másodiké pedig – az előbb elmondottakat figyelembe véve – azt, hogy φ izomorfizmus.

Nézzük most az alábbi egzakt sorozatot:

$$(*) \qquad \mathcal{O} \longrightarrow \mathcal{A} \xrightarrow{\alpha} \mathcal{B} \xrightarrow{\beta} \mathcal{C} \longrightarrow \mathcal{O}.$$

Az $\mathcal{A}$-ban, illetve a $\mathcal{C}$-ben való egzaktság azt jelenti, hogy α injektív, illetve β szürjektív. A $\mathcal{B}$-ben való egzaktság szerint Im α = Ker β, amiből a következő eredményt kapjuk:

9.30. Tétel. *A (*) alatti sorozat egzaktsága azt jelenti, hogy β olyan szürjektív homomorfizmus, amelynek magja éppen az α injekció képe.* ■

9.5. Kapcsolatok az algebrai topológiával

A modulusok egzakt és féligegzakt sorozatainak a vizsgálata az algebrai topológiához nyúlik vissza. Az itteni alkalmazások felfedezése után derült ki, hogy e sorozatok segítségével nagyon sok minden tulajdonság kideríthető arról a gyűrűről, amely feletti modulusokat vizsgáljuk. Ezek a vizsgálatok a homologikus algebra tárgykörébe tartoznak. A következő pontokban majd ezekről mutatunk be néhány elemi eredményt. Ebben a pontban most csak arról fogunk szólni, hogy mi az egzakt sorozatoknak a kapcsolata az algebrai topológiával.

Az *algebrai topológia* centrális kérdése a topológiai alakzatok „összefüggési viszonyai”-nak a vizsgálata. Ezeket a vizsgálatokat az n-dimenziós (euklideszi) térben folytatják. (Az algebrai topológiát kombinatorikus topológiának is nevezik.)

Egy n-dimenziós testet „jól megközelítenek” n-dimenziós „poliéderekkel”, azaz „síklapú” testekkel; és ezeknek a topológiai viszonyait nézik. A geometriai térben „igazi” testek és poliéderek, a síkban síkidomok és poligonok szerepelnek.

Itt felléphetnek „lyukas” testek vagy lapok; vagy „önmagába metszések”; szóval rendkívül bonyolult helyzet alakulhat ki. Topológiailag bizonyítható, hogy elég általános esetben egy bizonyos finomítás után a topológiai jellemzők már nem változnak meg, ezért elegendő poliéderekkel foglalkozni. A poliédereket úgy tekintik, hogy ezek a legegyszerűbb poliéderekből állnak össze; a síkban háromszögekből, a térben tetraéderekből, az n-dimenziós térben (tehát általában) úgynevezett *szimplexekből*. Egy ilyen felbontás tehát magában hordozza az eredeti test topológiai jellemzőit. A vizsgált testhez hozzátartoznak annak lapjai, élei és csúcsai is. A poliéderek tehát „kis” „térelemek”-ből állnak össze egymáshoz fűzéssel. A térelemeket alapobjektumoknak tekintve az egymáshoz fűzés úgy jelentkezik, mint ezeknek formális összege. A térelemeket „szabad generátoroknak” tekintve egy ($\mathbf{Z}$ feletti) modulust kapunk.

Az algebrai leíráshoz még ez is túlságosan „konkrét”.

Az absztrakt kombinatorikus topológia a poliéder pontjaiból indul ki. Ezek közül bizonyos párok a poliéder élei. Bizonyos hármasok a poliéder lapjai és így tovább. Vigyázni kell arra, hogy mi történjék például egy négyszöglappal; hiszen ilyet nem soroltunk fel. Nos, ilyen esetben a poliédert kicsit „deformáljuk” úgy, hogy a négyszöglap két csatlakozó háromszöglappá váljon. A test „belső” topológiai szerkezete ezáltal sem fog megváltozni.

Ezek után az absztrakt poliédert lehet úgy tekinteni, mint amit egy $\mathbf{P} = \{P_1, \ldots, P_r\}$ ponthalmaz határoz meg. Maga a poliéder ezek bizonyos részhalmazainak $\mathfrak{P}$ halmazából áll. A hozzá tartozó $s+1$ elemű részhalmazokat s-dimenziós szimplexeknek nevezik (ilyenek a pontok, szakaszok, háromszögek, tetraéderek stb.). Arra kell vigyázni, hogy a $\mathfrak{P}$-hez tartozó minden halmazzal együtt annak minden részhalmaza is $\mathfrak{P}$ eleme legyen (egy tetraéder minden lapja, minden éle és minden csúcsa is a tetraéderhez tartozik). A poliéder algebrai jellemzésére a $\mathfrak{P}$ generálta szabad modulust, $\mathcal{P} = \mathbf{Z}(\mathfrak{P})$-t tekintjük. E modulus elemeit *láncoknak* nevezik. Minden szimplex csak egyszer szerepelhet. Ha két szimplexnek ugyanazok a csúcsai, akkor a két szimplexet nem tekinthetjük „lényegesen” különbözőnek. Megengedhetjük viszont azt, hogy szerepeltetjük a szimplexet felcserélt csúcsokkal. Ilyen esetben a kapott „új” szimplex vagy az eredeti legyen, vagy annak a negatívja, attól függően, hogy a végzett permutáció páros vagy páratlan. A permutációk paritására vonatkozó eredmények alapján ez egyértelmű. A poliédert „realizáló” láncnál arra kell vigyázni, hogy a szimplexek csatlakozó lapjai a két szimplexnél különböző előjellel szerepeljenek.

Igen alapvető fogalom a testek „határa”. A $\mathcal{P}$ modulusra definiálunk egy δ additív *határfüggvényt*. Az additivitás miatt elegendő ezt szimplexekre definiálni.

Definíció. Legyen $\mathbf{Q} = (A_1, A_2, \ldots, A_s)$ egy s-dimenziós szimplex. Legyen $\mathbf{Q}_i$ az a szimplex, amit az eredetiből úgy nyerünk, hogy elhagyjuk az A_i pontot. Mármost $\mathbf{Q}$ határa:

$$\delta(\mathbf{Q}) = \sum_{i=1}^{s} (-1)^{i-1} \mathbf{Q}_i. \qquad \square$$

Így $\delta(AB) = B - A$; $\delta(ABC) = (BC) - (AC) + (AB)$; $\delta(ABCD) = (BCD) - (ACD) + (ABD) - (ABC)$, és így tovább. Az (AB) irányított szakasz határa olyan, hogy a végpont pozitív, a kezdőpont negatív. Az (ABC) (így) irányított háromszög határa éppen az a „vektorlánc”, amely például B-ből kiindulva „körbejárja” a háromszöget. Ha két háromszög megfelelő irányítással van egymás mellé téve, akkor határuk pontosan a

kapott négyszög határa lesz. Mivel a határképzés láncokra is értelmezett, ezért beszélhetünk egy poliéder határának a határáról. Az $(ABC\ldots)$ szimplex határa $\delta(ABC\ldots) = (BC\ldots) - (AC\ldots) + \ldots$ A fenti szimplex határának határát nézve két olyan eset adódik, amikor sem A, sem B nem lép fel:

$$\delta(BC\ldots) = (C\ldots) + \ldots \qquad \text{és} \qquad \delta(-(AC\ldots)) = -(C\ldots).$$

Általában is bizonyítható, hogy egy poliéder határának a határa mindig 0. Azért kell a csatlakozó szimplexek lapjait különböző előjellel venni, hogy ezek a határképzésnél „kiessenek"; hiszen ezek nem a határon, hanem a poliéder belsejében vannak.

Nem csak egy határ határa lehet 0. Azokat a láncokat, amelyeknek a határa 0, *ciklusoknak* nevezik. Például egy lyukas háromszög külső határolóvonala nem határ, de ciklus. Egy Möbius-szalag határolóvonala ugyancsak nem határ, de a kétszerese már határ (ennek az az oka, hogy a Möbius-szalagnak egy oldala van). A határok a ciklusoknak egy részmodulusát alkotják, és a képezett faktormodulus szerkezete sok mindent megad az alakzat topológiájáról.

Korlátozódjunk a rögzített (mondjuk s-) dimenziós láncokra, jelölje ezek modulusát $\mathcal{L}_s$. Ezeknek a határa $(s-1)$-dimenziós, legyen a határképző homomorfizmus δ_s. Ez azt jelenti, hogy a következő diagram adódik:

$$\ldots \longrightarrow \mathcal{L}_{s+1} \xrightarrow{\delta_{s+1}} \mathcal{L}_s \xrightarrow{\delta_s} \mathcal{L}_{s-1}.$$

Tekintettel arra, hogy minden határ ciklus, ezért a fenti diagram félig egzakt. A $H_s = \operatorname{Ker}\delta_s / \operatorname{Im}\delta_{s+1}$ csoport (modulus) neve *homológiacsoport*.

Célszerű megjegyezni, hogy az algebrai struktúrákra való átfogalmazás a matematika sok más ágában is általában sokat elárul az eredeti problémákban fennálló struktúrákról, éppen az algebrai struktúrák egyszerűbb felépítése miatt.

Feladatok

1. Határozzuk meg az (ABC) háromszög H_1 homológiacsoportját.

2. Az (ABC) háromszögbe helyezzünk el egy $(A_1B_1C_1)$ háromszög alakú lyukat. (Tekinthetjük ezt egy szalagnak is, amelynek egyik „széle" az (ABC) háromszög, a másik az $(A_1B_1C_1)$ háromszög.) Bontsuk fel az alakzatot az $(ABA_1) + (BB_1A) + (BCB_1) + (CC_1B) + (CAC_1) + (AA_1C)$ háromszögek alkotta láncra. Határozzuk meg az ezek összegéből álló lánc határát. Mutassuk meg, hogy az két ciklus összege. Mi a H_1 homológiacsoport?

3. Nézzük meg az előző kérdést, ha a háromszögből egy másik (az elsőtől diszjunkt) $(A_2B_2C_2)$ háromszöget is kivágunk.

4. „Csavarjuk meg" az előbbi szalagot (Möbius-szalag), ami azt jelenti, hogy a szereplő lánc utolsó két tagja ne $(CAC_1) + (AA_1C)$, hanem $(CA_1C_1) + (A_1AC)$ legyen. Most (ABC) nem széle a szalagnak, csak $(ABCA_1B_1C_1)$ (azaz $(AB) + (BC) + (CA)$ nem szerepel ciklusként – hiszen (CA) ellenkező előjellel áll –, csak $(AB) + (BC) + (CA_1) + (A_1B_1) + (B_1C_1) + (C_1A)$). Hogy változik meg a homológiacsoport?

5. Határozzuk meg egy lyukas tetraéder homológiacsoportját; illetve egy olyanét, amelyikben több lyuk is fellép.

9.6. A Hom_R funktor

A $\mathrm{Hom}_R(\mathcal{A},\mathcal{B})$ kétváltozós „függvénynek” képzelhető, amely minden moduluspárhoz egy Abel-csoportot rendel. A következőkben az lesz a célunk, hogy e „függvényt” vizsgáljuk, mégpedig úgy, hogy vagy az egyik, vagy a másik modulust rögzítjük. Így tehát két, egyváltozós függvényt kapunk. (Valójában a függvény elnevezés nem jogos, mert a modulusok összessége „túl nagy”.) A Hom funktor vizsgálata már szerepelt az első kötetben is. Itt most részletesebb vizsgálatok következnek.

A továbbiakban egy rögzített $\mathcal{M}$ és egy rögzített $\mathcal{N}$ modulus esetére a $\mathrm{Hom}_R(\mathcal{M},-)$, illetve $\mathrm{Hom}_R(-,\mathcal{N})$ Abel-csoportokat fogjuk tekinteni. A $-$ jel helyébe bármelyik R-modulust beírhatjuk.

9.31. Definíció. Rögzített $\mathcal{M}$, illetve rögzített $\mathcal{N}$ modulus esetén a $\mathrm{Hom}_R(\mathcal{M},\mathcal{A})$, illetve a $\mathrm{Hom}_R(\mathcal{A},\mathcal{N})$ Abel-csoportokra az $\mathcal{A}_*$, illetve $\mathcal{A}^*$ jelölést fogjuk használni. □

9.32. Tétel. *Tetszőleges $\alpha:\mathcal{A}\to\mathcal{B}$ R-homomorfizmus természetes módon indukál egy $\alpha_*:\mathcal{A}_*\to\mathcal{B}_*$ és egy $\alpha^*:\mathcal{B}^*\to\mathcal{A}^*$ csoporthomomorfizmust a következő definíció szerint:*

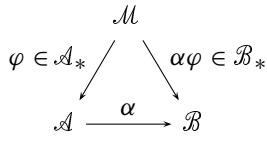
$$\text{1. Ha}\quad \varphi:\mathcal{M}\to\mathcal{A},\quad \text{akkor}\quad \alpha_*:\varphi\mapsto\alpha\varphi,$$
$$\text{2. Ha}\quad \psi:\mathcal{B}\to\mathcal{N},\quad \text{akkor}\quad \alpha^*:\psi\mapsto\psi\alpha.$$

Bizonyítás. Az egyetlen állítás az, hogy a szereplő sorozatok léteznek, és a megfelelő Abel-csoportnak az elemei. Ez pedig azonnal leolvasható az

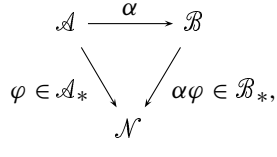
$$\mathcal{M}\xrightarrow{\varphi}\mathcal{A}\xrightarrow{\alpha}\mathcal{B},\qquad\text{illetve}\qquad \mathcal{A}\xrightarrow{\alpha}\mathcal{B}\xrightarrow{\psi}\mathcal{N}$$

diagramokról. ■

A definiált két homomorfizmus hatását az alábbi diagramok mutatják:



és



ahol $\varphi\xmapsto{\alpha_*}\alpha\varphi$ és $\psi\alpha\xmapsto{\alpha^*}\psi$.

Ezekről a diagramokról az is látszik, hogy a „lent-csillag” miért tartja meg a nyíl irányát, és miért változtatja meg az irányát a „fent-csillag”.

9.33. Definíció. A

$$\mathrm{Hom}_R(\mathcal{M},-):\begin{cases}\mathcal{A}\to\mathcal{A}_*\\ \alpha\to\alpha_*\end{cases}\qquad\text{és}\qquad \mathrm{Hom}_R(-,\mathcal{N}):\begin{cases}\mathcal{A}\to\mathcal{A}^*\\ \alpha\to\alpha^*\end{cases}$$

megfeleltetéseket funktoroknak nevezzük. Az első esetben kovariáns, a második esetben kontravariáns funktorról beszélünk. □

Megjegyezzük, hogy a fenti definíció csak azt mondja ki, hogy ezek funktorok, és nem azt, hogy mi a funktor. A funktorok általános definíciójában szereplő tulajdonságot majd a 9.36. tételben fogjuk kimondani.

A jelöléssel összhangban α_*, illetve α^* helyett sokszor használatos $\mathrm{Hom}_R(\mathcal{M}, \alpha)$, illetve $\mathrm{Hom}_R(\alpha, \mathcal{N})$. Szeretnénk felhívni a figyelmet arra, hogy ily módon a jelölés egyértelművé válik. Mi csak azért használjuk a csillagot, mert az $\mathcal{M}$ és $\mathcal{N}$ modulusokat eleve rögzítettnek tekintettük. (És természetesen a jelölés rövidebb volta növeli az áttekinthetőséget.) Ez a kétféle „csillag"-funktor valójában természetesen igen sok, hiszen a választott modulusok változtatásával ezek is változ(hat)nak.

A fenti funktorok további vizsgálatához szükségünk lesz két összefüggésre.

9.34. Tétel. *Ha $\alpha : \mathcal{A} \to \mathcal{B}$ injektív (szürjektív) R-homomorfizmus, akkor vele balról (jobbról) lehet egyszerűsíteni. Az ilyen tulajdonságú R-homomorfizmus neve monomorfizmus (epimorfizmus).*

Bizonyítás. Tegyük fel, hogy α injektív, és legyen $\alpha\varphi = \alpha\psi$. Tetszőleges szóba jövő $\mathbf{x}$ elemre teljesül tehát az $\alpha\varphi(\mathbf{x}) = \alpha\psi(\mathbf{x})$ összefüggés. Az α injektivitása alapján ebből már következik, hogy $\varphi(\mathbf{x}) = \psi(\mathbf{x})$. Szürjektív α esetén olyan R-homomorfizmusokat vegyünk, amelyekre $\varphi\alpha = \psi\alpha$ áll fenn. Most $\mathcal{B}$ tetszőleges $\mathbf{b}$ elemét felírhatjuk $\alpha(\mathbf{a})$ alakban, hiszen α szürjektív. Így $\varphi(\mathbf{b}) = \varphi\alpha(\mathbf{a}) = \psi\alpha(\mathbf{a}) = \psi(\mathbf{b})$, vagyis a két homomorfizmus valóban megegyezik. ■

Megjegyzés. Felhasználva a homomorfizmusokról azt, hogy $\mathrm{Hom}_R(\mathcal{A}, \mathcal{B})$ Abel-csoport, és azt, hogy a részmodulusok és faktormodulusok kölcsönösen meghatározzák egymást, kimutatható a következő: Ha egy R-homomorfizmus monomorfizmus (epimorfizmus), akkor injektív (szürjektív). Ez azonban tetszőleges algebrák esetében már nem igaz. □

A másik összefüggés a 9.22. tétel c) pontjának a megfordítása egy speciális esetben:

9.35. Tétel. *Ha az α injektív és β szürjektív R-homomorfizmusokra, valamint a φ, illetve ψ R-homomorfizmusokra* $\mathrm{Im}\ \varphi \subseteq \mathrm{Im}\ \alpha$, *illetve* $\mathrm{Ker}\ \beta \subseteq \mathrm{Ker}\ \psi$ *teljesül, akkor léteznek olyan σ, illetve τ R-homomorfizmusok, amelyekre $\varphi = \alpha\sigma$, illetve $\psi = \tau\beta$.*

Bizonyítás. Legyen először $\alpha : \mathcal{A} \to \mathcal{B}$ és $\varphi : \mathcal{M} \to \mathcal{B}$. Tetszőleges $\mathbf{m} \in \mathcal{M}$ elemhez létezik olyan $\mathbf{a} \in \mathcal{A}$ elem, amelyre $\alpha(\mathbf{a}) = \varphi(\mathbf{m})$, hiszen $\mathrm{Im}\ \varphi \subseteq \mathrm{Im}\ \alpha$. Mivel α injektív, ezért $\mathbf{m}$ egyértelműen meghatározza $\mathbf{a}$-t. Így $\sigma : \mathbf{m} \mapsto \mathbf{a}$ leképezés, amelyre $\varphi = \alpha\sigma$ igaz. Ebből pedig α injektivitását figyelembe véve, nyilvánvalóan következik az is, hogy σ R-homomorfizmus.

Tekintsük most a $\sigma : \mathcal{B} \to \mathcal{C}$ és $\psi : \mathcal{B} \to \mathcal{N}$ R-homomorfizmusokat. A $\mathcal{C}$ tetszőleges $\mathbf{c}$ eleméhez β szürjektivitása miatt található olyan $\mathcal{B}$-beli $\mathbf{b}$ elem, amelyre $\beta(\mathbf{b}) = \mathbf{c}$. Definiálja most τ-t $\tau(\mathbf{c}) = \psi(\mathbf{b})$. Ez minden $\mathbf{c}$-re definiálva van, és a $\mathrm{Ker}\ \beta \subseteq \mathrm{Ker}\ \psi$ feltétel következtében egyértelmű. A művelettartás bizonyítása itt is nyilvánvaló. ■

A 9.33. definícióban megadott két funktor alapvető tulajdonságait mondjuk ki:

9.36. Tétel. $1_* = 1^*$ *identitás;* $(\alpha\beta)_* = \alpha_*\beta_*$ *és* $(\alpha\beta)^* = \beta^*\alpha^*$.

Bizonyítás. Az első állítás abból következik, hogy φ-nek az első esetben $(1 \cdot \varphi)$-t, a második esetben $(\varphi \cdot 1)$-et feleltetjük meg. A második állításpár azonnal adódik az $(\alpha\beta)\varphi = \alpha(\beta\varphi)$, illetve a $\psi(\alpha\beta) = (\psi\alpha)\beta$ összefüggésekből. ■

9.37. Tétel. *Ha*

$$\mathcal{O} \longrightarrow \mathcal{A} \xrightarrow{\alpha} \mathcal{B} \xrightarrow{\beta} \mathcal{C} \longrightarrow \mathcal{O}$$

egzakt sorozat, akkor egzakt az alábbi két sorozat is:

$$\mathcal{O} \longrightarrow \mathcal{A}_* \xrightarrow{\alpha_*} \mathcal{B}_* \xrightarrow{\beta_*} \mathcal{C}_* \qquad \text{és} \qquad \mathcal{A}^* \xleftarrow{\alpha^*} \mathcal{B}^* \xleftarrow{\beta^*} \mathcal{C}^* \longleftarrow \mathcal{O}.$$

Bizonyítás. Tekintettel arra, hogy mind 0_*, mind 0^* nyilvánvalóan a nullhomomorfizmust adja, ezért a 9.36. tétel következtében mindkét funktor félig egzakt sorozatot félig egzakt sorozatba visz.

A 9.34. tétel szerint α_* is és β^* is injektív.

Azt kell most már csak bizonyítani, hogy $\mathrm{Ker}\ \beta_* \subseteq \mathrm{Im}\ \alpha_*$, és $\mathrm{Ker}\ \alpha^* \subseteq \mathrm{Im}\ \beta^*$.

Ha valamilyen φ-re $\beta\varphi = 0$, akkor az eredeti sorozat egzaktsága miatt $\mathrm{Im}\ \varphi \subseteq \mathrm{Im}\ \alpha$. A 9.35. tétel szerint tehát létezik olyan σ, hogy $\varphi = \alpha\sigma$, azaz $\varphi \in \mathrm{Im}\ \alpha^*$. Tegyük most fel, hogy egy ψ homomorfizmusra $\psi\alpha = 0$, amiből ismét az eredeti sorozat egzaktságát kihasználva $\mathrm{Ker}\ \beta \subseteq \mathrm{Ker}\ \psi$ következik. A 9.35. tétel másik állítása szerint tehát alkalmas τ R-homomorfizmussal $\psi = \tau\beta$; ami éppen azt jelenti, hogy $\psi \in \mathrm{Im}\ \beta^*$. ■

Természetesen felmerül a kérdés, hogy a 9.37. tételben szereplő két sorozatot nem lehet-e $\mathcal{O}$-val befejezni úgy, hogy a nyert sorozatok még mindig egzakt sorozatok legyenek. Erre a válasz általában nemleges. A további vizsgálatok előtt célszerű a felvetett modulustulajdonságot átfogalmazni.

A β_* szürjektivitása azt jelenti, hogy bármely $\varphi : \mathcal{M} \to \mathcal{C}$ homomorfizmus alkalmas σ-val $\varphi = \beta\sigma$ alakba írható. Az α^* szürjektivitása pedig azt, hogy minden $\psi : \mathcal{A} \to \mathcal{N}$ homomorfizmushoz található olyan τ homomorfizmus, amelyre $\psi = \tau\alpha$ teljesül. Különösen fontosak azok a modulusok, amelyekre a fentiek bármely egzakt sorozat esetében fennállnak.

9.38. Definíció. A $\mathcal{P}$, illetve a $\mathcal{Q}$ R-modulust projektív, illetve injektív modulusnak nevezzük, ha tetszőleges $\beta : \mathcal{B} \to \mathcal{C}$ szürjektív, illetve $\alpha : \mathcal{A} \to \mathcal{B}$ injektív R-homomorfizmushoz és tetszőleges $\varphi : \mathcal{P} \to \mathcal{C}$, illetve $\psi : \mathcal{A} \to \mathcal{Q}$ R-homomorfizmusokhoz léteznek olyan $\sigma : \mathcal{P} \to \mathcal{B}$, illetve $\tau : \mathcal{B} \to \mathcal{Q}$ R-homomorfizmusok, amelyekre $\varphi = \beta\sigma$, illetve $\psi = \tau\alpha$.

Most a projektív modulusok egy jellemzését adjuk:

9.39. Tétel. *Egy modulus pontosan akkor projektív, ha egy szabad modulus direkt összeadandója.*

Bizonyítás. Tegyük fel, hogy $\mathcal{P}$ projektív, és legyen $\mathcal{F}$ a $\mathcal{P}$ elemei által generált szabad modulus. A szabad modulus definíciója szerint létezik olyan $\varphi : \mathcal{F} \to \mathcal{P}$ homomorfizmus, amely $\mathcal{P}$ minden elemét önmagára képezi le. Ez a leképezés tehát szürjektív. Így a $\mathcal{P}$-nek önmagára való identikus leképezéséhez található olyan σ R-homomorfizmus, hogy a

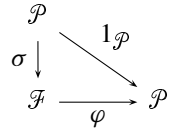
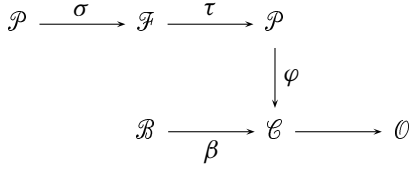


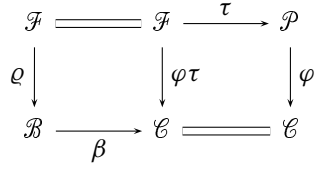
diagram kommutatív. Ez viszont a 9.23. tétel következtében azt jelenti, hogy $\mathcal{P}$ az $\mathcal{F}$-nek direkt összeadandója. A fordított irányú következtetést két lépésben bizonyítjuk.

Először azt mutatjuk ki, hogy minden szabad modulus projektív. Legyen $\beta : \mathcal{B} \to \mathcal{C}$ tetszőleges szürjektív R-homomorfizmus és φ az $\mathcal{F}$ szabad modulust $\mathcal{C}$-be vivő tetszőleges R-homomorfizmus. Legyen $\mathbf{X}$ az $\mathcal{F}$ szabad generátorrendszere, és tetszőleges $\mathbf{x} \in \mathbf{X}$ elemhez rendeljünk hozzá egy olyan $\mathbf{b} \in \mathcal{B}$ elemet, amelyre $\beta(\mathbf{b}) = \varphi(\mathbf{x})$. Ilyen $\mathbf{b}$ elem a β szürjektivitása alapján biztosan létezik. Mivel $\mathbf{X}$ szabad generátorrendszer, ezért a megadott hozzárendelés kiterjeszthető egy $\sigma : \mathcal{F} \to \mathcal{B}$ R-homomorfizmussá. Erre nyilvánvalóan igaz, hogy $\varphi(\mathbf{x}) = \beta\sigma(\mathbf{x})$ teljesül a generátorrendszer tetszőleges $\mathbf{x}$ elemére. Így a φ és $\beta\sigma$ R-homomorfizmusok a szabad generátorrendszeren ugyanúgy hatnak; s a kiterjeszthetőség egyértelműsége alapján meg kell egyezniük.

Második lépésként azt mutatjuk meg, hogy projektív modulus direkt összeadandója is projektív. Legyen most $\mathcal{P}$ az $\mathcal{F}$ projektív modulus direkt összeadandója, és tekintsünk egy tetszőleges φ szürjektív R-homomorfizmust. Ismét a 9.23. tételre hivatkozva a következő diagramot kapjuk:



ahol az alsó sor egzakt, és a felső sorban $\tau\sigma = 1_{\mathcal{P}}$. A $\psi = \varphi\tau$ homomorfizmushoz az előbb bizonyítottak szerint található olyan ϱ R-homomorfizmus, hogy az alábbi diagram kommutatív legyen:



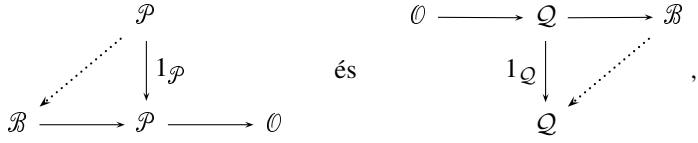
A bal oldali négyszög kommutativitását, azaz a $\beta\varrho = \varphi\tau$ összefüggést felhasználva kapjuk, hogy $\varphi = \varphi 1 = \varphi\tau\sigma = \beta\varrho\sigma = \beta(\varrho\sigma)$. ■

Megjegyzés. A második lépéshez hasonlóan kimutatható, hogy injektív modulus direkt összeadandója (vagy inkább direkt faktora) ugyancsak injektív. Az injektív modulusok jellemzése viszont lényegesen bonyolultabb, mint a projektívaké. Egyszerűbb a helyzet az Abel-csoportoknál, ahol az injektívek pontosan az osztható csoportok. (Ezt nem bizonyítjuk; tekinthető feladatnak.) □

A fenti tétel bizonyításában láttuk, hogy projektív modulus direkt összeadandója is projektív. Ennek a „megfordítása” is igaz; és a projektív modulusok egy igen fontos tulajdonságát adja. E tulajdonság „duálisa” az injektív modulusokra teljesül.

9.40. Tétel. *Egy projektív (injektív) modulus minden olyan modulusnak direkt összeadandója, amelynek faktormodulusa (részmodulusa).*

Bizonyítás. Tekintsük az alábbi diagramokat:



ahol a vízszintes sorokban egzakt sorozatok állnak. $\mathcal{P}$ projektivitásából, illetve $\mathcal{Q}$ injektivitásából azonnal következik, hogy a pontokkal jelzett nyilak helyére olyan homomorfizmusokat írhatunk, amelyekkel a diagramok kommutatívvá tehetők. Ez pedig a 9.23. tétel alapján éppen a kívánt állítást bizonyítja. ■

Megjegyzés. A 9.39. tételt figyelembe véve azt kapjuk, hogy a 9.40. tételben megadott tulajdonsága pontosan a projektív modulusoknak van meg. A 9.39. tétel utáni megjegyzés alapján az is igaz, hogy a 9.40. tételben megadott tulajdonság „duálisa" éppen az injektív modulusokat jellemzi. Ezeket a modulusokat sokszor pontosan az említett tulajdonsággal definiálják. Ehhez az volna szükséges, hogy minden modulus beágyazható legyen egy injektívbe. Ez a tulajdonság viszont valóban igaz. (Ezt nem bizonyítjuk.) □

A fentiekben egy-egy rögzített $\mathcal{M}$ modulus segítségével funktorokat definiáltunk. E funktorok egzakt sorozatokat nem mindig vittek át egzakt sorozatokba. Azt vizsgáltuk, hogy milyen speciális szerkezetű modulusok esetén visznek a megfelelő funktorok minden egzakt sorozatot egzakt sorozatba. Ezzel az $\mathcal{M}$ modulust jellemeztük. Ha azt kérdezzük, hogy mikor teljesül a most leírt tulajdonság minden egyes $\mathcal{M}$ R-modulusra, akkor már az R gyűrű jellemzését kapjuk. Esetünkben tehát úgy vethető fel a kérdés, hogy mely R gyűrűre lesz minden modulus injektív, illetve projektív.

9.41. Tétel. *Az R gyűrűre vonatkozó alábbi három állítás ekvivalens:*

(1) *Minden R-modulus injektív.*

(2) *Minden R-modulus projektív.*

(3) *Tetszőleges R-modulus minden részmodulusa direkt összeadandó.*

Bizonyítás. A 9.23. tételt figyelembe véve, a 9.40. tétel alapján mind az (1), mind a (2) feltételből következik (3).

Tegyük most fel, hogy (3) igaz. Feltételünk és a 9.23. tétel alapján az $\alpha : \mathcal{A} \to \mathcal{B}$ injektív és $\beta : \mathcal{B} \to \mathcal{A}$ szürjektív R-homomorfizmusok úgy rendelhetők egymáshoz, hogy a megfeleltetettekre $\beta\alpha = 1$ teljesül. Mivel itt a 9.38. definícióbeli $\mathcal{C}$ helyét is $\mathcal{A}$ tölti be, azt kell kimutatnunk, hogy tetszőleges $\varphi : \mathcal{M} \to \mathcal{A}$ és $\psi : \mathcal{A} \to \mathcal{N}$ R-homomorfizmusokhoz található olyan $\sigma : \mathcal{M} \to \mathcal{B}$ és $\tau : \mathcal{B} \to \mathcal{N}$ R-homomorfizmus, hogy $\varphi = \beta\sigma$ és $\psi = \tau\alpha$ teljesül. E feltételeknek nyilvánvalóan eleget tesz $\sigma = \alpha\varphi$ és $\tau = \psi\beta$. ■

Megjegyzés. Világos, hogy vektorterek esetén az e tételben megfogalmazott harmadik tulajdonság teljesül. Könnyen belátható az is, hogy a test kommutativitására nincs szükség. Majd látni fogjuk, hogy a (3) tulajdonság teljesül akkor is, ha féligegyszerű gyűrűket tekintünk. Sőt, ez a feltétel szükséges is. □

A továbbiakban azt nézzük meg, hogy mi az, ami „meggátolja” a 9.37. tételben szereplő sorozatoknak a $\mathcal{O}$-val való folytatását. Azt kell tehát megnézni, hogy a

$$\begin{array}{ccccccccc} & & & & & & \mathcal{M} & & \\ & & & & & & \downarrow & & \\ \mathcal{O} & \longrightarrow & \mathcal{A} & \longrightarrow & \mathcal{B} & \longrightarrow & \mathcal{C} & \longrightarrow & \mathcal{O} \end{array}$$

diagramban, ahol a vízszintes sor egy egzakt sorozat, miért nem található egy $\mathcal{M}$-et $\mathcal{B}$-be képező R-homomorfizmus, amely a diagramot kommutatívvá teszi, illetve mikor található ilyen.

9.42. Tétel. *Adott* $\mathcal{O} \longrightarrow \mathcal{A} \xrightarrow{\alpha} \mathcal{B} \xrightarrow{\beta} \mathcal{C} \longrightarrow \mathcal{O}$ *egzakt sorozathoz és* $\varphi : \mathcal{C}' \to \mathcal{C}$ R*-homomorfizmushoz elkészíthető egy*

$$\begin{array}{ccccccccc} \mathcal{O} & \longrightarrow & \mathcal{A}' & \xrightarrow{\alpha'} & \mathcal{B}' & \xrightarrow{\beta'} & \mathcal{C}' & \longrightarrow & \mathcal{O} \\ & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \varphi} & & \\ \mathcal{O} & \longrightarrow & \mathcal{A} & \xrightarrow{\alpha} & \mathcal{B} & \xrightarrow{\beta} & \mathcal{C} & \longrightarrow & \mathcal{O} \end{array}$$

kommutatív diagram, amelynek az első sora is egzakt sorozat.

Bizonyítás. Mindenekelőtt megadunk egy – a feltételeknek megfelelő – $\mathcal{B}'$ modulust, amely álljon a $\mathcal{B} \oplus \mathcal{B}'$ direkt összeg azon $(\mathbf{b}, \mathbf{c}')$ elemeiből, amelyekre $\beta\mathbf{b} = \varphi\mathbf{c}'$. Könnyen belátható, hogy ezek valóban R-modulust alkotnak. A megfelelő R-homomorfizmusokat definiálja $\alpha'\mathbf{a} = (\alpha\mathbf{a}, \mathbf{o})$, $\beta'(\mathbf{b}, \mathbf{c}') = \mathbf{c}'$ és $\psi(\mathbf{b}, \mathbf{c}') = \mathbf{b}$. Triviális, hogy ezek R-homomorfizmusok, valamint az is, hogy α' injektív és β' szürjektív. Ugyancsak triviálisan látható be a felső sor egzaktságához az Im α' = Ker β' egyenlőség és a diagram kommutativitása is. ■

A 9.42. tétel egy fontos speciális esetét nézzük:

9.43. Tétel. *Ha a 9.42. tételben* $\varphi = 1$*, akkor* ψ *izomorfizmus.*

Bizonyítás. Először ψ injektivitását bizonyítjuk. Legyen $\psi\mathbf{b}' = \mathbf{o}$. Ekkor $\beta'\mathbf{b}' = 1\beta'\mathbf{b}' = \beta\psi\mathbf{b}' = \mathbf{o}$. A felső sor egzaktsága miatt tehát létezik olyan $\mathbf{a} \in \mathcal{A}$, amelyre $Bb' = \alpha'\mathbf{a}$. Így $\mathbf{o} = \psi\mathbf{b}' = \psi\alpha'\mathbf{a} = \alpha 1\mathbf{a} = \alpha\mathbf{a}$. Az α injektivitása alapján ebből $\mathbf{a} = \mathbf{o}$, azaz $\mathbf{b}' = \alpha'\mathbf{o} = \mathbf{o}$ következik. A szürjektivitás bizonyítására vegyünk egy $\mathcal{B}$-beli $\mathbf{b}$ elemet. β' szürjektivitása miatt létezik olyan $\mathbf{b}' \in \mathcal{B}'$, amelyre $\beta\mathbf{b} = 1\beta'\mathbf{b}' = \beta\psi\mathbf{b}'$; azaz $\beta(\mathbf{b} - \psi\mathbf{b}') = \mathbf{o}$. Az alsó sor egzaktságát figyelembe véve kapjuk, hogy létezik olyan $\mathcal{A}$-beli $\mathbf{a}$ elem, amelyre $\mathbf{b} - \psi\mathbf{b}' = \alpha\mathbf{a} = \alpha 1\mathbf{a} = \psi\alpha'\mathbf{a}$; azaz $\mathbf{b} = \psi(\mathbf{b}' + \alpha'\mathbf{a})$, ami éppen a szürjektivitást jelenti. ■

Megjegyzés. A tételben alkalmazott módszert „diagramvadászatnak” nevezik. Ez azt jelenti, hogy a felvett elemet addig „zavarjuk” a helyes irányba, amíg megkapjuk a kívánt eredményt. □

9.44. Tétel. *Tekintsük a 9.42. tételben szereplő két sorozat között azt a relációt, amelyet a 9.43. tétel definiál (vagyis a $\varphi = 1$ esetet). Ez egy ekvivalenciareláció. Ettől a relációtól eltekintve a 9.42. tételben megadott alsó egzakt sorozat és a φ R-homomorfizmus a felső egzakt sorozatot egyértelműen meghatározza.*

Bizonyítás. A relációban három adat szerepel. Egy ψ izomorfizmus és két egyenlőség: $\beta' = \beta\psi$, valamint $\alpha = \psi\alpha'$. A reláció reflexivitásához $\beta' = \beta$ és $\alpha' = \alpha$ esetén $\psi = 1$ választandó. A szimmetriát úgy láthatjuk be, hogy izomorfizmusnak ψ^{-1}-et választjuk; míg a tranzitivitásnál a szereplő két izomorfizmus megfelelő szorzatát kell tekinteni.

Tegyük most fel, hogy a 9.42. tételben kirótt feltételeknek a

$$\mathcal{O} \longrightarrow \mathcal{A} \xrightarrow{\alpha''} \mathcal{B}'' \xrightarrow{\beta''} \mathcal{C}' \longrightarrow \mathcal{O}$$

egzakt sorozat is eleget tesz. Legyen a „középen" álló homomorfizmus $\psi'' : \mathcal{B}'' \to \mathcal{B}$. A 9.42. tétel bizonyításában definiált $\mathcal{B}'$-re legyen $\sigma : \mathcal{B}'' \to \mathcal{B}'$ a következőképpen definiálva: $\sigma\mathbf{b}'' = (\psi''\mathbf{b}'', \beta''\mathbf{b}'')$. Annak a kiszámolását, hogy σ a fenti ekvivalenciarelációnál megkívánt azonosságoknak eleget tevő R-homomorfizmus, az olvasóra bízzuk. ■

Most adjuk meg azt, hogy mi gátolja a 9.37. tételben szereplő első sorozatban a $\mathcal{O}$-val való folytatást, illetve, hogy mikor lehetséges a folytatás. A második sorozat esetében is hasonló jellemzés adható; csupán az eddig tárgyaltak „duális" meggondolását kell végigvinni.

9.45. Tétel. *A*

$$\begin{array}{ccccccccc}
\mathcal{O} & \longrightarrow & \mathcal{A}' & \xrightarrow{\alpha'} & \mathcal{B}' & \xrightarrow{\beta'} & \mathcal{C}' & \longrightarrow & \mathcal{O} \\
 & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \varphi} & & \\
\mathcal{O} & \longrightarrow & \mathcal{A} & \xrightarrow{\alpha} & \mathcal{B} & \xrightarrow{\beta} & \mathcal{C} & \longrightarrow & \mathcal{O}
\end{array}$$

kommutatív diagramban, amelynek sorai egzaktak, akkor és csak akkor létezik egy olyan $\sigma : \mathcal{C}' \to \mathcal{B}$ R-homomorfizmus, amelyre $\varphi = \beta\sigma$ teljesül, ha létezik egy olyan $\gamma : \mathcal{C}' \to \mathcal{B}'$, amelyre $\beta'\gamma$ a $\mathcal{C}'$ identitása.

Bizonyítás. Ha $\beta'\gamma = 1$, akkor $\varphi = \varphi 1 = \varphi\beta'\gamma = \beta\psi\gamma$ alapján választható $\sigma = \psi\gamma$. Tegyük most fel, hogy létezik a kívánt tulajdonságú σ, és legyen $\mathcal{B}'$ a 9.42. tételben konstruált modulus. Definiálja γ-t a $\gamma\mathbf{c}' = (\sigma\mathbf{c}', \mathbf{c}')$ összefüggés. Ez nyilvánvalóan homomorfizmus, amelyre $\beta\sigma\mathbf{c}' = \varphi\mathbf{c}'$ következtében Im $\gamma \subseteq \mathcal{B}'$ teljesül. A $\beta'\gamma = 1$ összefüggés triviálisan igaz. Ugyancsak triviális, hogy a fenti tulajdonságú γ akkor is található, ha a felső egzakt sorozatot vele ekvivalenssel helyettesítjük, hiszen „középen" izomorfizmus áll. A zárójelbe tett állítás a 9.23. tételből következik. ■

Megjegyzés. A 9.45. tétel esetében $\mathcal{B}'$ az $\mathcal{A}$ és $\mathcal{C}'$ direkt összegével izomorf. Ennél több is igaz; nevezetesen $\mathcal{B}'$ pontosan az Im α'-nek és a Ker β'-nek a (belső) direkt összege. □

Térjünk most vissza a $\mathcal{C}' = \mathcal{M}$ esetre. A 9.42. tétel szerint minden $\mathcal{C}_*$-beli elemhez egyértelműen hozzárendelhető egy $\mathcal{B}'$ modulus (és alkalmas homomorfizmusok), amelynek az $\mathcal{A}$ modulus részeként tekinthető, és az e szerinti faktor izomorf az $\mathcal{M}$-mel. Ez a $\mathcal{B}'$

úgy fogható fel, mint $\mathcal{A}$-nak $\mathcal{M}$-mel való bővítése. A $\mathcal{B}_*$-beliek képeként előálló megfeleltetett bővítés a 9.45. tétel alapján éppen a direkt összeg lesz. Ez sugallja, hogy a 9.37. tételben szereplő első sorozatot úgy lehet folytatni, hogy a $\mathcal{C}_*$ után az *$\mathcal{A}$-nak $\mathcal{M}$-mel való bővítései* következnek. Sőt, azt is látjuk, hogy a „bővítések nulleleme" a direkt összeg. De értelmezhető-e a bővítések „összege"? Kimutatható, hogy igen. Diagramokkal például a következőképpen adhatjuk meg. Tekintsünk két bővítést:

$$\mathcal{O} \longrightarrow \mathcal{A} \xrightarrow{\alpha_1} \mathcal{B}_1 \xrightarrow{\beta_1} \mathcal{C} \longrightarrow \mathcal{O}$$

és

$$\mathcal{O} \longrightarrow \mathcal{A} \xrightarrow{\alpha_2} \mathcal{B}_2 \xrightarrow{\beta_2} \mathcal{C} \longrightarrow \mathcal{O}.$$

Ebből elkészíthetjük az alábbi sorozatot:

$$\mathcal{O} \longrightarrow \mathcal{A} \oplus \mathcal{A} \xrightarrow{\alpha_1 + \alpha_2} \mathcal{B}_1 \oplus \mathcal{B}_2 \xrightarrow{\beta_1 + \beta_2} \mathcal{C} \oplus \mathcal{C} \longrightarrow \mathcal{O}.$$

ahol a morfizmusok úgy értendők, hogy a direkt összeg első komponensén az első homomorfizmus, a másodikon a második hat. Könnyen belátható, hogy így egy egzakt sorozatot kapunk. A 9.42. tétel segítségével ez kommutatív diagrammá egészíthető ki:

$$\begin{array}{ccccccccc}
\mathcal{O} & \longrightarrow & \mathcal{A} \oplus \mathcal{A} & \longrightarrow & \bullet & \longrightarrow & \mathcal{C} & \longrightarrow & \mathcal{O} \\
 & & \Big\downarrow 1 & & \Big\downarrow & & \Big\downarrow \Delta & & \\
\mathcal{O} & \longrightarrow & \mathcal{A} \oplus \mathcal{A} & \longrightarrow & \mathcal{B}_1 \oplus \mathcal{B}_2 & \longrightarrow & \mathcal{C} \oplus \mathcal{C} & \longrightarrow & \mathcal{O}
\end{array}$$

ahol Δ a $\mathbf{c}$ elemet $(\mathbf{c}, \mathbf{c})$-re képezi. Kimutatható, hogy érvényes a 9.42. tétel duálisa, amikor a $\mathcal{C}$-nél van identitás, és az $\mathcal{A}$-beli nyíl irányában következtetünk. Így egy

$$\begin{array}{ccccccccc}
\mathcal{O} & \longrightarrow & \mathcal{A} \oplus \mathcal{A} & \longrightarrow & \bullet & \longrightarrow & \mathcal{C} & \longrightarrow & \mathcal{O} \\
 & & \Big\downarrow \nabla & & \Big\downarrow & & \Big\downarrow 1 & & \\
\mathcal{O} & \longrightarrow & \mathcal{A} & \longrightarrow & \mathcal{B}_3 & \longrightarrow & \mathcal{C} & \longrightarrow & \mathcal{O}
\end{array}$$

kommutatív diagramot nyerünk, amelyben ∇-t $\nabla(\mathbf{a}_1, \mathbf{a}_2) = \mathbf{a}_1 + \mathbf{a}_2$ definiálja. Az eredeti két bővítés összege az alsó sorban kapott sorozat lesz, vagyis $\mathcal{B}_3$ a megfelelő homomorfizmusokkal együtt. Ezt a csoportot $\mathrm{Ext}_R(\mathcal{C}, \mathcal{A})$ jelöli. E csoportot – $\mathcal{C}$ helyébe rögzített $\mathcal{M}$ modulust írva – jelöljük $\mathcal{A}_{**}$-gal. A 9.42. tételben konstruált megfeleltetésről kimutatható, hogy ez egy χ_* homomorfizmus, amelynek a magja éppen β_* képe. A 9.42. tétel említett duálisa azt is biztosítja, hogy α természetes módon indukálja $\mathcal{A}_{**}$-nak a $\mathcal{B}_{**}$-ba való α_{**} homomorfizmusát. Ezzel a vizsgált sornak egy folytatását találhatjuk:

$$\mathcal{O} \longrightarrow \mathcal{A}_* \xrightarrow{\alpha_*} \mathcal{B}_* \xrightarrow{\beta_*} \mathcal{C}_* \xrightarrow{\chi_*} \mathcal{A}_{**} \xrightarrow{\alpha_{**}} \mathcal{B}_{**} \xrightarrow{\beta_{**}} \mathcal{C}_{**} \longrightarrow \ldots$$

E sorozat általában tovább folytatható. Mindig egymás után az $\mathcal{A}$-tól, $\mathcal{B}$-től és $\mathcal{C}$-től függő csoportok, illetve a megfelelő R-homomorfizmusoktól függő csoporthomomorfizmusok lépnek fel. Analóg módon folytatható a másik képzett sorozat:

$$\ldots \longleftarrow \mathcal{A}^{**} \xleftarrow[\alpha^{**}]{} \mathcal{B}^{**} \xleftarrow[\beta^{**}]{} \mathcal{C}^{**} \xleftarrow[\chi^{**}]{} \mathcal{A}^{*} \xleftarrow[\alpha^{*}]{} \mathcal{B}^{*} \xleftarrow[\beta^{*}]{} \mathcal{C}^{*} \longleftarrow \mathcal{O}.$$

Általában ez a sorozat is „igen hosszú”. Érdemes megemlíteni azonban, hogy ha R főideálgyűrű (amit mi csak integritási tartományokra definiáltunk), akkor a fenti sorozat már mindig $\mathcal{O}$-val zárható. Igen sokat elárulnak e sorozatok a vizsgált R gyűrű szerkezetéről. E sorozatok hossza mintegy a gyűrű „dimenziójának” tekinthető. Lényeges szerepet játszanak például a Noether-gyűrűk vizsgálatában is.

9.7. Modulusok tenzorszorzata

Az első kötetben a Hom funktor mellett vizsgáltuk a tenzorszorzatot is, mert a lineáris algebrában szükség van a tenzor fogalmára, és ezt akartuk precízen megalapozni. Ott a két funktor közti különbség megmutatása végett nem csak vektortereket, hanem kommutatív gyűrűk feletti modulusokat is megengedtünk. Ennek az volt az oka, hogy véges dimenziós vektorterek esetében a konstruált vektorterek izomorfak. (Igaz, hogy a *Hom* funktor az első változóban kontravariáns, de ez „nehezen érzékelhető”.) Az alábbiakban a tenzorszorzatot olyan gyűrűk fölötti modulusokra nézzük, amely gyűrűkről nem kötjük ki, hogy kommutatívak.

Az R-homomorfizmusok vizsgálatánál láttuk, hogy az ${}_R\mathcal{A}$-t ${}_R\mathcal{B}$-be vivő R-homomorfizmusok általában nem alkottak R-modulust. Ennek az az oka, hogy ha egy R-homomorfizmust értelemszerűen megszorzunk egy R-beli elemmel, akkor a kapott leképezés nem lesz minden esetben R-homomorfizmus. Ez már akkor sem teljesül, ha egyetlen modulust nézünk. A 9.17. tétel szerint ez ugyanis lényegében az R kommutativitásával volna ekvivalens. Azt azonban könnyen beláthatjuk, hogy a kapott szorzat mindig összegtartó. Éppen ezért érdemes megnézni, hogy ha R-modulusoknak az Abel-csoport homomorfizmusait nézzük, vajon ezek nem tekinthetők-e egy R-modulus elemeinek. A válasz erre a kérdésre valóban igenlő:

9.46. Tétel. *Legyen $\mathcal{A}$ bal oldali S-modulus és $\mathcal{B}$ bal oldali R-modulus. Ekkor $Hom_{\mathbb{Z}}(\mathcal{A},\mathcal{B})$ bal oldali R-modulus, jobb oldali S-modulus, sőt kettősmodulus az alábbi természetes definícióval:*

Tetszőleges $\varphi \in \mathrm{Hom}\,(\mathcal{A},\mathcal{B})$, $r \in R$, $s \in S$ és $\mathbf{a} \in \mathcal{A}$ elemekre legyen $(r\varphi)(\mathbf{a}) = r(\varphi\mathbf{a})$ és $(\varphi s)(\mathbf{a}) = \varphi(s\mathbf{a})$.

Bizonyítás. A 9.14. tétel szerint „hatásukat tekintve” $r \in \mathrm{Hom}\,(\mathcal{B},\mathcal{B})$, $s \in \mathrm{Hom}\,(\mathcal{A},\mathcal{A})$. Ekkor a ($\mathbb{Z}$-)homomorfizmusok szorzatának definíciója szerint $r\varphi, \varphi s \in \mathrm{Hom}\,(\mathcal{A},\mathcal{B})$ és a szorzat asszociativitása alapján $(r\varphi)s = r(\varphi s) \in \mathrm{Hom}\,(\mathcal{A},\mathcal{B})$. ■

Megjegyzés. Hasonló (illetve duális) tétel igaz jobb oldali modulusokra is. □

A további célunk kétváltozós modulushomomorfizmusok vizsgálata. Ha eltekintünk a gyűrűelemekkel való szorzástól, akkor Abel-csoportokra vonatkozó kétváltozós homomorfizmusokról van szó. Ha olyan kétváltozós függvényt vizsgálunk, amelynek egyik változója az $\mathcal{A}$, a másik változója a $\mathcal{B}$ Abel-csoport elemein fut végig, akkor valójában az $\mathcal{A} \times \mathcal{B}$ halmazelméleti direkt szorzat elemein értelmezett függvényeket tekintünk. Technikai szempontból előnyösebb a függvényeket kiterjeszteni a direkt szorzat által szabadon generált

Abel-csoport additív leképezéseire. Mint tudjuk, a szabad generátorokon értelmezett tetszőleges függvénynek van ilyen kiterjesztése; s e kiterjesztést a függvény egyértelműen meghatározza. Az alábbi definícióban ilyen függvényeket tekintünk:

9.47. Definíció. Jelölje $\mathcal{A} \circ \mathcal{B}$ az $\mathcal{A}$ és $\mathcal{B}$ Abel-csoportokkal képezett $\mathcal{A} \times \mathcal{B}$ halmazelméleti direkt szorzat elemei által generált szabad Abel-csoportot; és legyen $f \in \in \mathrm{Hom}\,(\mathcal{A} \circ \mathcal{B}, \mathcal{M})$.

Tetszőleges $\mathbf{a} \in \mathcal{A}$, illetve $\mathbf{b} \in \mathcal{B}$ esetén jelölje $\mathbb{F}_{f,\mathbf{a}}$, illetve $\mathbb{F}_{f,\mathbf{b}}$ azt a függvényt, amelyet

$$\mathbb{F}_{f,\mathbf{a}} : \mathbf{b} \mapsto f(\mathbf{a}, \mathbf{b}), \qquad \text{illetve} \qquad \mathbb{F}_{f,\mathbf{b}} : \mathbf{a} \mapsto f(\mathbf{a}, \mathbf{b})$$

definiál. Legyen végül $\mathbb{F}_{f,\mathcal{A}}$, illetve $\mathbb{F}_{f,\mathcal{B}}$ az a függvény, amelyre

$$\mathbb{F}_{f,\mathcal{A}} : \mathbf{a} \mapsto \mathbb{F}_{f,\mathbf{a}}, \qquad \text{illetve} \qquad \mathbb{F}_{f,\mathcal{B}} : \mathbf{b} \mapsto \mathbb{F}_{f,\mathbf{b}}. \qquad \square$$

9.48. Definíció. Legyen a 9.47. definícióbeli $\mathcal{A}$ jobb oldali és $\mathcal{B}$ bal oldali R-modulus. Ha $\mathbb{F}_{f,\mathbf{a}} \in \mathrm{Hom}\,(\mathcal{B}, \mathcal{M})$ és $\mathbb{F}_{f,\mathbf{a}} \in \mathrm{Hom}\,(\mathcal{A}, \mathcal{M})$, akkor f-et biadditívnak nevezzük. Ha ezenfelül $\mathbb{F}_{f,\mathcal{A}}$ és $\mathbb{F}_{f,\mathcal{B}}$ még jobb oldali, illetve bal oldali R-homomorfizmus is, akkor azt mondjuk, hogy f R-bihomomorfizmus. $\square$

Megjegyzés. A 9.46. tétel alapján a fenti homomorfizmusok valóban lehetnek R-homomorfizmusok, hiszen $\mathrm{Hom}\,(\mathcal{A}, \mathcal{M})$ bal oldali és (a 9.46. tétel utáni megjegyzés szerint) $\mathrm{Hom}\,(\mathcal{B}, \mathcal{M})$ jobb oldali R-modulus. Felesleges volt azonban kikötni, hogy mindkettő R-homomorfizmus legyen, mert – mint az alábbi tételben látni fogjuk – ha az egyikük R-homomorfizmus, akkor a másik is az. $\square$

9.49. Tétel. *Egy $f \in \mathrm{Hom}\,(\mathcal{A} \circ \mathcal{B}, \mathcal{M})$ csoporthomomorfizmus akkor és csak akkor biadditív, ha*

$$f(\mathbf{a}_1 + \mathbf{a}_2, \mathbf{b}) = f(\mathbf{a}_1, \mathbf{b}) + f(\mathbf{a}_2, \mathbf{b}) \qquad \text{és} \qquad f(\mathbf{a}, \mathbf{b}_1 + \mathbf{b}_2) = f(\mathbf{a}, \mathbf{b}_1) + f(\mathbf{a}, \mathbf{b}_2).$$

Az f biadditív homomorfizmus akkor és csak akkor R-bihomomorfizmus, ha a szereplő R gyűrű tetszőleges r elemére $f(\mathbf{a}r, \mathbf{b}) = f(\mathbf{a}, r\mathbf{b})$.

Bizonyítás. $\mathbb{F}_{f,\mathbf{a}} \in \mathrm{Hom}\,(\mathcal{B}, \mathcal{M})$ azt jelenti, hogy a leképezés összegtartó, ami $\mathbb{F}_{f,\mathbf{a}}$ definíciója szerint éppen a második egyenlőséggel ekvivalens. Hasonlóképpen, az első egyenlőség azt fejezi ki, hogy $\mathbb{F}_{f,\mathbf{b}} \in \mathrm{Hom}\,(\mathcal{A}, \mathcal{M})$. Annak a feltétele, hogy $\mathbb{F}_{f,\mathcal{A}}$ jobb oldali R-homomorfizmus legyen, az, hogy tetszőleges $r \in R$ mellett fennálljon az $\mathbb{F}_{f,\mathcal{A}}(\mathbf{a}r) = \mathbb{F}_{f,\mathbf{a}}(\mathbf{a})r$ egyenlőség. Ez azzal a követelménnyel ekvivalens, hogy e két függvény ugyanúgy hasson $\mathcal{B}$ minden $\mathbf{b}$ elemén. Definíció szerint $\mathbb{F}_{f,\mathcal{A}}(\mathbf{a}r) : \mathbf{b} \mapsto f(\mathbf{a}r, \mathbf{b})$ és $[\mathbb{F}_{f,\mathbf{a}}(\mathbf{a})r](\mathbf{b}) = [\mathbb{F}_{f,\mathbf{a}}](r\mathbf{b}) = f(\mathbf{a}, r\mathbf{b})$. Hasonlóképpen látható be, hogy ez annak is a feltétele, hogy $\mathbb{F}_{f,\mathcal{B}}$ bal oldali R-homomorfizmus legyen. ■

Egy csoporthomomorfizmusnál két elemnek a képe pontosan akkor egyezik meg, ha különbségük a homomorfizmus magjában van. Így a 9.49. tételből azonnal adódik:

9.50. Következmény. *Egy* $f \in \mathrm{Hom}\,(\mathcal{A}\circ\mathcal{B},\mathcal{M})$ *homomorfizmus akkor és csak akkor* R*-bihomomorfizmus, ha* $\mathrm{Ker}\,(f)$ *tartalmazza az*

$$(\mathbf{a}_1+\mathbf{a}_2,\mathbf{b})-(\mathbf{a}_1,\mathbf{b})-(\mathbf{a}_2,\mathbf{b}),$$

$$(\mathbf{a},\mathbf{b}_1+\mathbf{b}_2)-(\mathbf{a},\mathbf{b}_1)-(\mathbf{a},\mathbf{b}_2),$$

$$(\mathbf{a}r,\mathbf{b})-(\mathbf{a},r\mathbf{b})$$

elemek által generált $\mathcal{L}=\mathcal{L}(R)=\mathcal{L}(R)_{\mathcal{A},\mathcal{B}}$ *részmodulust* ($r\in R$)*, amelynek elemeit linearitásoknak nevezzük.* ■

9.51. Definíció. Adott $\mathcal{A}_R$ és ${}_R\mathcal{B}$ R-modulusok $\mathcal{A}\otimes_R\mathcal{B}$ tenzorszorzatán értjük az $(\mathcal{A}\circ\mathcal{B})/\mathcal{L}$ faktorcsoportot, ellátva azzal a $\mathfrak{t}:\mathcal{A}\circ\mathcal{B}\to\mathcal{A}\otimes_R\mathcal{B}$ természetes homomorfizmussal, amely minden elemhez az őt tartalmazó mellékosztályt rendeli. ($\mathcal{L}$ a 9.50. következményben definiált linearitások részcsoportja.) □

9.52. Tétel. *Tetszőleges* $\mathfrak{f}:\mathcal{A}\circ\mathcal{B}\to\mathcal{C}$ R*-bihomomorfizmushoz létezik egy olyan egyértelműen meghatározott* $F:\mathcal{A}\otimes_R\mathcal{B}$ *csoporthomomorfizmus, amellyel az*

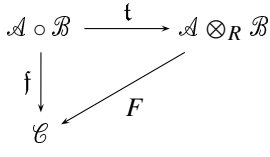


diagram kommutatívvá válik. Ez a tulajdonság a tenzorszorzatot egyértelműen meghatározza a következő értelemben. Ha létezik olyan $\mathfrak{t}':\mathcal{A}\circ\mathcal{B}\to\mathcal{T}$ R*-bihomomorfizmus, amelyet* $\mathfrak{t}$ *helyébe téve a tétel állítása igaz marad, akkor létezik olyan egyértelmű* $T:\mathcal{A}\otimes_R\mathcal{B}$ *izomorfizmus, amellyel az*

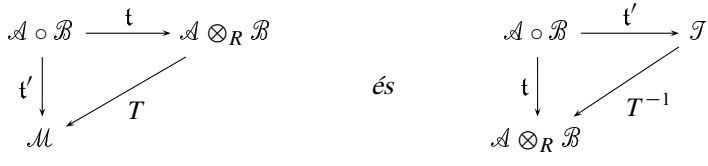


diagram kommutatív.

Bizonyítás. $\mathfrak{t}$ és $\mathfrak{f}$ csoporthomomorfizmusok. $\mathfrak{t}$ definíciója szerint szürjektív, és a 9.50. következmény alapján $\mathrm{Ker}\,(\mathfrak{t})\subseteq\mathrm{Ker}\,(\mathfrak{f})$. A 9.35. tétel szerint tehát létezik a kívánt tulajdonságú F homomorfizmus; s a 9.34. tétel szerint ez egyértelműen meghatározott. Tegyük fel, hogy egy $\mathfrak{t}'$ R-bihomomorfizmus is eleget tesz a kívánalmaknak. A most bizonyítottakat e két homomorfizmus mindegyikére alkalmazva azt kapjuk, hogy léteznek olyan (egyértelműen meghatározott) S és T homomorfizmusok, amelyekre $\mathfrak{t}'=F\mathfrak{t}$ és $\mathfrak{t}=S\mathfrak{t}'$ teljesül. Azt kell csupán belátni, hogy a kapott két homomorfizmus izomorfizmus és egymás inverzei. Elég ez utóbbit belátni, hiszen csak izomorfizmusnak van kétoldali inverze.

A kapott összefüggésekből $\mathfrak{t}=ST\mathfrak{t}$ és $\mathfrak{t}'=TS\mathfrak{t}'$ adódik. Ez ismét két kommutatív diagramnak fogható fel. Mármost az egyértelműséget felhasználva, a triviálisan fennálló

$\mathfrak{t} = 1 \cdot \mathfrak{t}$ és $\mathfrak{t}' = 1 \cdot \mathfrak{t}'$ összefüggésekből $ST = 1$ és $TS = 1$ következik, tehát ezek valóban egymás inverzei. ■

Mivel az $(\mathbf{a}, \mathbf{b})$ párok generálják $(\mathcal{A} \circ \mathcal{B})$-t, ezért képeik generálják a tenzorszorzatot. Azaz, a tenzorszorzat minden eleme előállítható ezek összegei, illetve különbségei alakjában. (Természetesen a tenzorszorzat elemei nem csak a generátorelemek képei!) A generátorelemekkel végzett műveletek a 9.50. következményben felírt azonosságok megfelelőjének tesznek eleget. Így érvényes az alábbi:

9.53. Tétel. *A* $\mathfrak{t}(\mathbf{a}, \mathbf{b}) = \mathbf{a} \otimes \mathbf{b}$ *elemek az* $\mathcal{A} \otimes_R \mathcal{B}$ *Abel-csoport egy generátorrendszerét alkotják. E generátorrendszer elemeire az*

$$(\mathbf{a}_1 + \mathbf{a}_2) \otimes \mathbf{b} = \mathbf{a}_1 \otimes \mathbf{b} + \mathbf{a}_2 \otimes \mathbf{b},$$

$$\mathbf{a} \otimes (\mathbf{b}_1 + \mathbf{b}_2) = \mathbf{a} \otimes \mathbf{b}_1 + \mathbf{a} \otimes \mathbf{b}_2,$$

$$\mathbf{a}r \otimes \mathbf{b} = \mathbf{a} \otimes r\mathbf{b}$$

összefüggések teljesülnek $(r \in R)$. ■

Megjegyzés. A 9.53. tétel következményeként beláthatjuk, hogy a tételben szereplő generátorrendszer nem független. Például a tenzorszorzat nullelemét is többféleképpen felírhatjuk: mind a $\mathbf{o} \otimes \mathbf{b}$, mind az $\mathbf{a} \otimes \mathbf{o}$ alakú elemek a nullelemet adják, mint ez a $\mathbf{o} \otimes \mathbf{b} + \mathbf{a} \otimes \mathbf{b} = (\mathbf{o} + \mathbf{a}) \otimes \mathbf{b} = \mathbf{a} \otimes \mathbf{b}$ összefüggésből azonnal következik, tekintettel arra, hogy kommutatív csoportban a kivonás egyértelmű. □

Hasonlóképpen ahhoz, amint a homomorfizmusok vizsgálatakor tettük, a tenzorszorzatot is értelmezhetjük leképezésekre is. Felhívjuk a figyelmet arra, hogy ez a definíció nem „eleve egyértelmű". Ennek bemutatását megtalálhatjuk az első kötet 314–315. oldalain a 10.13. tétel előtti bekezdéstől e tétel bizonyítása utáni megjegyzésig bezárólag. Itt is a szokásos definíciót adjuk.

9.54. Tétel. *Ha* $\varphi : \mathcal{A} \to \mathcal{B}$ *jobb oldali* R*-modulusok,* $\psi : \mathcal{C} \to \mathcal{D}$ *pedig bal oldali* R*-modulusok homomorfizmusa, akkor a* $(\varphi \otimes \psi) : (\mathbf{a} \otimes \mathbf{c}) \mapsto (\varphi\mathbf{a} \otimes \psi\mathbf{c})$ *összefüggéssel definiált leképezés csoporthomomorfizmus. Homomorfizmusok fent definiált tenzorszorzatára teljesül, hogy szürjektív homomorfizmusok tenzorszorzata is szürjektív.*

Bizonyítás. Mindenekelőtt azt kell belátni, hogy a fent definiált leképezés valóban létezik (eleve az sem világos, hogy egy elem képe egyértelmű volna). Feleltessük meg az $(\mathbf{a}, \mathbf{c}) \in \mathcal{A} \times \mathcal{C}$ párnak a $\varphi\mathbf{a} \otimes \psi\mathbf{c}$ elemet. Ez a leképezés $\mathcal{A} \circ \mathcal{C}$-nek a $\mathcal{B} \otimes_R \mathcal{C}$-re való homomorfizmusaként tekinthető. Nyilvánvaló számolással belátható, hogy ez egy R-bihomomorfizmus. A 9.52. tétel következtében e bihomomorfizmus $F \cdot \mathfrak{t}$ alakú, és F éppen a tételben definiált tulajdonsággal rendelkezik. Tegyük most fel, hogy mindkét adott homomorfizmus szürjektív. Ekkor tetszőleges $\mathbf{b} \otimes \mathbf{d}$ elemhez található olyan $\mathbf{a}$ és $\mathbf{c}$ elem, amelyekre $\mathbf{b} = \varphi\mathbf{a}$ és $\mathbf{d} = \psi\mathbf{c}$ teljesül. Ebből pedig $(\varphi \otimes \psi)(\mathbf{a} \otimes \mathbf{c}) = \mathbf{b} \otimes \mathbf{d}$ következik. A 9.53. tétel szerint tehát egy generátorrendszer minden eleme előáll képként, amiből következik, hogy minden elem előáll képként. ■

9.55. Tétel. *Ha az alábbi összegek, illetve szorzatok léteznek, akkor érvényesek a felírt összefüggések:*

$$(\varphi_1 + \varphi_2) \otimes \psi = \varphi_1 \otimes \psi + \varphi_2 \otimes \psi,$$

$$\varphi \otimes (\psi_1 + \psi_2) = \varphi \otimes \psi_1 + \varphi \otimes \psi_2,$$

$$(\varphi_1\varphi_2) \otimes (\psi_1\psi_2) = (\varphi_1 \otimes \psi_1)(\varphi_2 \otimes \psi_2).$$

Fennáll továbbá a $\varphi \otimes 0 = 0 \otimes \psi = 0$ *összefüggés.*

A tételben felírt összefüggések kiszámolását az olvasóra bízzuk. ■

A következő tételben megmutatjuk, hogy bármilyen R gyűrűt tekintünk is, mindig létezik olyan tenzorszorzat, amelyik nem a nullcsoportot adja. Egyúttal egy olyan eljárást is láthatunk, amelynek a segítségével a tenzorszorzatok esetében izomorfizmust bizonyíthatunk.

9.56. Tétel. *Legyen* $\mathcal{A}$ *az* $\mathbf{a}$ *elemmel generált jobb oldali* R*-modulus; és tegyük fel, hogy létezik olyan* R*-beli* r*, hogy* $\mathbf{a}$*-t csak az* r *által generált jobbideál elemei annullálják. Tetszőleges* $\mathcal{B}$ *bal oldali* R*-modulus esetén legyen* $r\mathcal{B} = \{r\mathbf{b} \mid \mathbf{b} \in \mathcal{B}\}$*. Ekkor* $r\mathcal{B}$ *a* $\mathcal{B}$ *részcsoportja és* $\mathcal{A} \otimes_R \mathcal{B} \cong \mathcal{B}/r\mathcal{B}$*. Ha* $\mathcal{A}$*-t speciálisan egy elemmel generált szabad modulusnak vesszük, akkor a tenzorszorzat* $\mathcal{B}$*-vel izomorf.*

Bizonyítás. Az $\mathcal{A}$ elemei $\mathbf{a}x$ alakban írhatók, ahol x az R egységelemes bővítésének egy eleme. A továbbiakban mindig az R egységelemes bővítését tekintjük. Mindenekelőtt megjegyezzük, hogy $r\mathcal{B}$ triviálisan részcsoport. Így van értelme annak az állításnak, hogy $\mathcal{A} \circ \mathcal{B}$ tetszőleges $(\mathbf{a}x, \mathbf{b})$ generátorelemének megfeleltetjük az $x\mathbf{b}$ elemet tartalmazó mellékosztályt. Ez a megfeleltetés egyértelmű, hiszen $\mathbf{a}x_1 = \mathbf{a}x_2$ esetén $x_1 - x_2$ felírható ry alakban, amiből nyilvánvalóan adódik, hogy $x_1\mathcal{B}$ és $x_2\mathbf{b}$ ugyanabba a mellékosztályba esnek (itt y az R egységelemes bővítésének egy eleme). A definiált $\mathfrak{f} : \mathcal{A} \circ \mathcal{B} \to \mathcal{B}/r\mathcal{B}$ nyilvánvalóan R-bihomomorfizmus. Így $\mathfrak{f} = F\mathfrak{t}$ alakú (a 9.52. tételbeli jelöléseket használva). Azt fogjuk bebizonyítani, hogy F izomorfizmus. Mivel F homomorfizmus, ezért elég a bijektivitás bizonyítása. A szürjektivitás triviálisan adódik abból, hogy az $Ff(\mathbf{a}, \mathbf{b})$ mellékosztály tartalmazza a $\mathbf{b}$ elemet. Az injektivitás bizonyításához felhasználjuk, hogy a tenzorszorzatnak esetünkben létezik egy igen egyszerű generátorrendszere: a 9.53. tétel alapján a tenzorszorzat minden eleme $\mathbf{a} \otimes \mathbf{b}$ alakba írható. Ha mármost egy ilyen elem benne van F magjában, akkor a következőket kapjuk: $\mathbf{o} = F(\mathbf{a} \otimes \mathbf{b}) = F\mathfrak{t}(\mathbf{a}, \mathbf{b}) = \mathfrak{f}(\mathbf{a}, \mathbf{b}) = \mathbf{b}$; és így $\mathbf{a} \otimes \mathbf{b} = \mathbf{a} \otimes \mathbf{o} = \mathbf{o}$. A speciális esetben – mint már láttuk – $r = 0$, amiből triviálisan következik a tétel utolsó állítása is. ■

Most a tenzorszorzatnak az egzakt sorozatokra való hatását nézzük meg.

9.57. Tétel. *Legyen* $\mathcal{O} \longrightarrow \mathcal{A} \xrightarrow{\alpha} \mathcal{B} \xrightarrow{\beta} \mathcal{C} \longrightarrow \mathcal{O}$ *bal oldali* R*-modulusokból álló egzakt sorozat és* $\mathcal{M}$ *egy jobb oldali* R*-modulus. Ekkor az*

$$\mathcal{M} \otimes_R \mathcal{A} \xrightarrow{1 \otimes \alpha} \mathcal{M} \otimes_R \mathcal{B} \xrightarrow{1 \otimes \beta} \mathcal{M} \otimes_R \mathcal{C} \longrightarrow \mathcal{O}$$

sorozat is egzakt.

Bizonyítás. A félig egzaktság következik a 9.55. tételből; s az $\mathcal{M} \otimes \mathcal{C}$ modulusnál való egzaktságot a 9.54. tétel biztosítja.

Azt kell még bizonyítani, hogy $\mathrm{Ker}\,(1\otimes\beta)\subseteq\mathrm{Im}(1\otimes\alpha)$. Evégett válasszunk egy olyan $\varphi:\mathcal{M}\otimes_R\mathcal{B}\to\mathcal{D}$ szürjektív homomorfizmust, amelynek a magja $\mathrm{Im}(1\otimes_R\alpha)$. Ezzel a választással egy

$$\mathcal{M}\otimes_R\mathcal{A}\xrightarrow{1\otimes\alpha}\mathcal{M}\otimes_R\mathcal{B}\xrightarrow{\varphi}\mathcal{D}\longrightarrow\mathcal{O}$$

egzakt sorozatot kapunk. Ker $\varphi\subseteq\mathrm{Ker}\,(1\otimes\beta)$ alapján olyan szürjektív ψ homomorfizmus is létezik, amelyre $1\otimes\beta=\psi\varphi$ teljesül. Azt fogjuk bebizonyítani, hogy az így megadott ψ izomorfizmus. Evégett megkonstruáljuk az inverzét.

Tetszőleges $\mathbf{m}\in\mathcal{M}$ és $\mathbf{b}\in\mathcal{B}$ esetén az $(\mathbf{m},\beta\mathbf{b})$ elemnek feleltessük meg a $\varphi(\mathbf{m}\otimes\mathbf{b})$ elemet. Ez a megfeleltetés egyértelmű: ha $\beta\mathbf{b}_1=\beta\mathbf{b}_2$, akkor az eredeti sorozat egzaktsága alapján létezik egy $\mathbf{b}_2=\mathbf{b}_1+\alpha\mathbf{a}$ felírás, ahol $\mathbf{a}\in\mathcal{A}$. Így

$$\varphi(\mathbf{m}\otimes\mathbf{b}_2)=\varphi(\mathbf{m}\otimes\mathbf{b}_1)+\varphi(1\otimes\alpha)(\mathbf{m}\otimes\mathbf{a})=\varphi(\mathbf{m}\otimes\mathbf{b}_1).$$

Ez a megfeleltetés nyilvánvalóan R-bihomomorfizmus, és így létezik olyan $\eta:\mathcal{M}\otimes_R\mathcal{C}\to$ $\to\mathcal{D}$ csoporthomomorfizmus, amelyre $\eta(\mathbf{m}\otimes\beta\mathbf{b})=\varphi(\mathbf{m}\otimes\mathbf{b})$. A

$$\psi\eta(\mathbf{m}\otimes\beta\mathbf{b})=\psi\varphi(\mathbf{m}\otimes\mathbf{b})=(1\otimes\beta)(\mathbf{m}\otimes\mathbf{b})=(\mathbf{m}\otimes\beta\mathbf{b})$$

egyenlőség alapján $\psi\eta$ identitás, és

$$\eta\psi(\varphi(\mathbf{m}\otimes\mathbf{b}))=\eta(1\otimes\beta)(\mathbf{m}\otimes\mathbf{b})=\eta(\mathbf{m}\otimes\beta\mathbf{b})=\varphi(\mathbf{m}\otimes\mathbf{b})$$

pedig azt jelenti, hogy $\eta\psi$ is identitás. ■

A Hom funktorra vonatkozó vizsgálatokhoz hasonlóan itt is megkérdezhetjük, hogy a konstruált sorozat mikor folytatható „bal oldali $\mathcal{O}$-val”. Azt a meglepő eredményt kapjuk, hogy az ottani feltétel itt is elegendő:

9.58. Tétel. *Ha minden bal oldali R-modulusnak bármely részmodulusa direkt összeadandó, akkor a 9.57. tételben konstruált sorozat elejére $\mathcal{O}$-t írva, egzakt sorozatot kapunk.*

Bizonyítás. A 9.23. tétel szerint a feltételből következik egy olyan $\psi:\mathcal{B}\to\mathcal{A}$ homomorfizmus létezése, amelyre $\psi\alpha=1$ teljesül. A 9.55. tétel alapján tehát $(1\otimes\psi)(1\otimes\alpha)=$ $=1\otimes\psi\alpha=1\otimes1$, ami nyilván éppen $\mathcal{M}\otimes_R\mathcal{A}$ identitása. ■

Megjegyzés. A 9.58. tételben kimondott eredmény igaz lehet a szereplő feltétel nélkül is. Bebizonyítható, hogy az egzakt sorozatokra vonatkozó tétel igaz például akkor is, ha R-nek a valós függvények gyűrűjét választjuk (összeadás és szorzás a szokásos), annak ellenére, hogy például ${}_RR$-ben azok a függvények, amelyek véges sok helytől eltekintve a 0 értéket veszik fel, olyan részmodulust alkotnak, amely nem direkt összeadandó. □

Megmutatjuk még, hogy a tenzorszorzás is funktor abban az értelemben, ahogy azt a Hom_R funktornál láttuk.

9.59. Tétel. *Rögzített $\mathcal{M}$ jobb oldali R-modulus esetén feleltessük meg az $\mathcal{A}$ bal oldali R-modulusnak az $\mathcal{M}\otimes_R\mathcal{A}$ Abel-csoportot, és a bal oldali R-modulusok közti α R-homomorfizmusnak az $1\otimes\alpha$ Abel-csoportok közötti homomorfizmust. Ez a megfeleltetés a homomorfizmusokon szorzattartó, identitásnak identitást feleltet meg, s ha egy homomorfizmus $\mathcal{A}$-ból $\mathcal{B}$-be képez, akkor képe az $\mathcal{A}$ képéből a $\mathcal{B}$ képébe.*

Bizonyítás. A tétel utolsó állítása a homomorfizmusok tenzorszorzatának a definíciójából következik. A szorzattartást már a 9.55. tételben kimondottuk; a hiányzó állítás pedig $(1\otimes1)(\mathbf{m}\otimes\mathbf{a})=\mathbf{m}\otimes\mathbf{a}$ alapján triviális. ■

A 9.59. tétellel analóg állítás mondható ki a jobb oldali R-modulusokra is. Ennek bizonyítása a „bal oldali”-nak duálisa.

Megjegyzés. Világos, hogy a Hom funktorral szemben a tenzorszorzat mindkét változójában kovariáns funktor.

9.8. Összefüggések ⊗ és Hom között

A Hom_R funktor és a $\otimes_R$ tenzorszorzat között igen mély kapcsolat van. Ennek a kimondása és kimutatása az általános esetben igen körülményes. Éppen ezért a következőkben az S kommutatív gyűrű feletti modulusokat tekintjük. Mivel a vektortereket kommutatív testek feletti modulusoknak tekinthetjük, ezért az itt bizonyított eredmények a vektorterekre vonatkozó eredmények általánosításaként foghatók fel. Ezt a kapcsolatot az első kötet 10. fejezetében a 2. pontban (311–315. oldal) már részletesen megvizsgáltuk. Itt most csak a lényeges tételeket fogjuk kimondani. Ezek bizonyítása a fenti helyen (vagy még előtte) megtalálható; esetleg az olvasó saját maga is elvégezheti. Ugyancsak javasoljuk az első kötetben található feladatokat (316–317. oldal).

9.60. Tétel. *Tetszőleges $\mathcal{A}$ S-modulusra mind* $\mathrm{Hom}\,(S,\mathcal{A})$*, mind $S\otimes\mathcal{A}$ természetes módon izomorf $\mathcal{A}$-val. Ezen azt értjük, hogy léteznek olyan $\varphi_{\mathcal{A}}$:* $\mathrm{Hom}\,(S,\mathcal{A})\to\mathcal{A}$ *és $\varphi_{\mathcal{B}}$:* $\mathrm{Hom}\,(S,\mathcal{B})\to\mathcal{B}$ *izomorfizmusok, hogy bármely $\alpha:\mathcal{A}\to\mathcal{B}$ homomorfizmusra az*

$$\begin{array}{ccc} \mathcal{A}_* & \xrightarrow{\alpha_*} & \mathcal{B}_* \\ {\scriptstyle\varphi_{\mathcal{A}}}\downarrow & & \downarrow{\scriptstyle\varphi_{\mathcal{B}}} \\ \mathcal{A} & \xrightarrow{\alpha} & \mathcal{B} \end{array} \qquad \text{és} \qquad \begin{array}{ccc} S\otimes\mathcal{A} & \xrightarrow{1\otimes\alpha} & S\otimes\mathcal{B} \\ {\scriptstyle\varphi_{\mathcal{A}}}\downarrow & & \downarrow{\scriptstyle\varphi_{\mathcal{B}}} \\ \mathcal{A} & \xrightarrow{\alpha} & \mathcal{B} \end{array}$$

diagramok kommutatívak, ahol $\mathcal{A}_* = \mathrm{Hom}\,(S,\mathcal{A})$ *és* $\mathcal{B}_* = \mathrm{Hom}\,(S,\mathcal{B})$. ■

9.61. Tétel. *A tenzorszorzat kommutatív és asszociatív; azaz $\mathcal{A}\otimes\mathcal{B}$ és $\mathcal{B}\otimes\mathcal{A}$, illetve $(\mathcal{A}\otimes\mathcal{B})\otimes\mathcal{C}$ és $\mathcal{A}\otimes(\mathcal{B}\otimes\mathcal{C})$ (természetes módon) izomorfak.* ■

9.62. Tétel. *Ha $\alpha:\mathcal{A}'\to\mathcal{A}$ és $\beta:\mathcal{B}\to\mathcal{B}'$ S-homomorfizmusok, akkor az a* $\mathrm{Hom}\,(\alpha,\beta)$ *megfeleltetés, amely* $\mathrm{Hom}\,(\mathcal{A},\mathcal{B})$ *tetszőleges φ elemének a* $\mathrm{Hom}\,(\mathcal{A}',\mathcal{B}')$ *modulus $\beta\varphi\alpha$ elemét felelteti meg, S-homomorfizmus.* ■

9.63. Tétel. $\mathrm{Hom}(\mathcal{A}\otimes\mathcal{B},\mathcal{C})$ *és* $\mathrm{Hom}\,(\mathcal{A},\mathrm{Hom}\,(\mathcal{B},\mathcal{C})$ *természetes módon izomorfak.* ■

9.64. Tétel. *Létezik egy* $\mathrm{Hom}\,(\mathcal{A},\mathcal{B})\otimes\mathcal{C}\to\mathrm{Hom}\,(\mathcal{A},\mathcal{B}\otimes\mathcal{C})$ *természetes homomorfizmus.* ■

10. Algebrák

Ez a fejezet két részre oszlik. Az első három pontban kommutatív algebrákkal foglalkozunk. Kommutatív algebra az algebra egy igen nagy fejezete, amely az algebrai geometria nélkülözhetetlen bevezető tudományága. Itt viszont csak azt akarjuk kifejezni, hogy olyan algebrákról beszélünk, amelyek kommutatívak. Igaz, a kapott eredmények alapvetőek. Az algebra – mint algebrai struktúra – valójában egy olyan gyűrű, amely egy másik gyűrű feletti modulus. Tekintettel arra, hogy egyelőre az algebra fogalmára nincs szükség, ezért ezt csak az 5. pontban fogjuk definiálni.

10.1. Egész elemek kommutatív gyűrűk felett

10.1. Definíció. Az R egységelemes integritási tartomány egy r elemét az R egy S részgyűrűje felett egésznek nevezzük, ha r gyöke egy S-beli együtthatós normált polinomnak. □

Megjegyzés. A definícióból nem következik, hogy S is egységelemes. Mint a 7.44. tétel után megjegyeztük, ilyen esetben is definiálható polinomgyűrű, ilyen esetben a polinom együtthatóit az S egységelemes bővítéséből vesszük. □

10.2. Tétel. *Az R egységelemes integritási tartomány egy r elemére az alábbi állítások ekvivalensek:*

(1) *r egész egy S részgyűrű felett.*

(2) *Az r generálta $S[r]$ részgyűrű végesen generált S-modulus.*

(3) *Létezik olyan $S \leq T \leq R$ részgyűrű, amely végesen generált S-modulus és $r \in T$.*

Bizonyítás. Legyen r egész az S felett. Ez azt jelenti, hogy létezik olyan $x^n + s_{n-1}x^{n-1} + \ldots + s_1x + s_0$ S-beli együtthatós polinom, amelynek r gyöke. Ebből következik, hogy r^n eleme az $\{1, r, \ldots, r^{n-1}\}$ generálta S-modulusnak. Ebből viszont indukcióval nyilvánvalóan belátható, hogy r-nek n-nél nagyobb hatványai is e részmodulus elemei. Márpedig ez a részmodulus végesen generált.

Ha az $S[r]$ részgyűrű végesen generált S-modulus, akkor a $T = S[r]$ választásra teljesül a (3) alatti állítás.

Tegyük most fel, hogy $S \leq T \leq R$ olyan részgyűrűk, hogy T végesen generált S-modulus és $r \in T$. Legyen $t_1, \ldots, t_n$ a T-nek egy S feletti generátorrendszere. A gyűrűtulajdonság miatt minden egyes rt_i $(i = 1, \ldots, n)$ eleme T-nek. A generátorrendszer tulajdonsága szerint tehát ezek mind előállíthatók a t_i-knek S-beli lineáris kombinációiként: $rt_i = \sum s_{i,j} \cdot t_j$ $(s_{i,j} \in S,\ 1 \leq i, j \leq n)$.

Így a $\sum (s_{i,j} - \delta_{i,j})x_j = 0$ homogén lineáris egyenletrendszernek $(t_1, \ldots, t_n)$ egy nemtriviális megoldása, és ezért az $[s_{i,j} - r\delta_{i,j}]$ mátrix determinánsa zérus ($\delta_{i,j}$ a Kronecker-féle szimbólum). Ez azt jelenti, hogy r gyöke a $\det[s_{i,j} - x\delta_{i,j}] = 0$ egyenletnek. Ennek az egyenletnek a bal oldalán egy olyan polinom áll, amelynek az együtthatói S-ből valók és a főegyütthatója $+1$ vagy -1. Ez pedig pontosan azt jelenti, hogy r egész az S felett. ■

10.3. Tétel. *Az R gyűrűnek az S részgyűrű felett egész elemei az R-nek egy S-et tartalmazó részgyűrűjét alkotják.*

Bizonyítás. Azt kell csupán bizonyítani, hogy ha r_1 és r_2 egészek az S felett, akkor S felett egész az összegük és a szorzatuk is. Mivel ezek elemei az $S[r_1, r_2]$ részgyűrűnek, ezért elég belátni, hogy ennek minden eleme egész. A 10.2. tétel (3) szerint ennek elégséges feltétele az, hogy $S[r_1, r_2]$ végesen generált S-modulus. Legyen $a_1, \ldots, a_n$ egy véges generátorrendszere $S[r_1]$-nek S felett. Ilyen létezik, mert r_1 egész az S felett. Tekintettel arra, hogy r_2 is egész az S felett, ezért eleve egész $S[r_1]$ felett is (ugyanaz a normált polinom választható, mint S felett). Így viszont $S[r_1, r_2]$ végesen generált $S[r_1]$-modulus egy $b_1, \ldots, b_k$ generátorrendszerrel. Ebből pedig azonnal következik, hogy az összes $a_i b_j$ elemek a szóban forgó gyűrűnek egy S feletti generátorrendszerét adják. Így ez valóban egy végesen generált S-modulus. ■

Mint a hányadostestek vizsgálatánál láttuk, egy S integritási tartomány hányadostestének bármely eleme felírható két S-beli elem hányadosaként. Most ezt az eredményt általánosítjuk:

10.4. Tétel. *Az S hányadosteste fölötti bármely algebrai elem felírható egy S felett egész elemnek és egy S-beli elemnek a hányadosaként.*

Bizonyítás. Legyen az S felett algebrai α elem (S-beli együtthatós) főpolinomja $a_n x^n + \ldots + a_0$. Ekkor az $a_n\alpha = \beta$ elem gyöke az

$$x^n + a_{n-1}x^{n-1} + a_n a_{n-2}x^{n-2} + \cdots + a_n^{n-2}a_1 x + a_n^{n-1}a_0$$

polinomnak – és így egész. ■

Megjegyzések. 1. A definíció alapján egy integritási tartomány felett egész elem eleve algebrai elem az integritási tartomány felett.

2. Láthatjuk, hogy ha az eredeti polinom minden együtthatója S-beli, akkor is előfordulhat, hogy a fent kapott polinom főegyütthatója (= 1) nincs S-ben. □

10.5. Definíció. Egy integritási tartományt (hányadostestében) integrálisan zártnak nevezünk, ha a hányadostestében levő bármely (felette) egész elem benne van. □

Megjegyzések. 1. Az $x - 1$ polinom együtthatói mind elemei egy gyűrű egységelemes bővítésének. Mivel e polinomnak gyöke az 1, ezért integrálisan zárt gyűrű csak egységelemes lehet.

2. Ismeretes, hogy ha egy egész együtthatós polinomnak van racionális gyöke, amelyet tovább nem egyszerűsíthető tört alakban írtunk fel, akkor a nevező osztója a polinom főegyütthatójának. Ha tehát a főegyüttható 1, akkor ez a racionális gyök egész. Az egész számok tehát a racionális számok gyűrűjének egy integrálisan zárt részgyűrűjét alkotják.

3. A racionális számok egy részgyűrűje pontosan akkor integrálisan zárt, ha tartalmazza az egész számokat.

4. Ha egy integritási tartományban érvényes az egyértelmű prímtényezős felbontás, akkor integrálisan zárt. Valóban, a második megjegyzés gondolatmenete erre az esetre is szó szerint átvihető.

5. Test feletti polinomgyűrű integrálisan zárt. Ez az előző megjegyzés speciális eseteként adódik. □

Az algebrai bővítések vizsgálatakor láttuk, hogy ha az $a_1, \ldots, a_n$ elemek a K test felett algebrai elemek, akkor a $K[a_1, \ldots, a_n]$ gyűrűbővítés test. Most ennek a megfordítását is bebizonyítjuk:

10.6. Tétel. *Ha a K test feletti $K[a_1, \dots, a_n]$ gyűrűbővítés test, akkor minden egyes a_i algebrai K felett.*

Bizonyítás. A tételt n szerinti teljes indukcióval bizonyítjuk. Ha egy testet egyetlen transzcendens elemmel bővítünk, akkor a test feletti polinomgyűrűt kapjuk, ami nem test. Így $n = 1$ esetén igaz az állítás. Tegyük most fel, hogy az állítás igaz $n - 1$ elemmel való bővítés esetén. Mivel $K[a_1, \dots, a_n]$ test, ezért tartalmazza az $L = K(a_1)$ testet. Ebből azonnal következik, hogy $L[a_2, \dots, a_n] = K[a_1, \dots, a_n]$, tehát feltevéseink szerint $L[a_1, \dots, a_n]$ is test. Az indukciós feltevés alapján tehát minden egyes a_i algebrai L felett (természetesen a_1 is). A 10.4. tétel következtében minden a_i megszorozható úgy egy alkalmas $K[a_1]$-beli elemmel, hogy a szorzat $K[a_1]$ felett egész legyen. Mivel egészek szorzata is egész és az a_i-k száma véges, ezért feltehető, hogy mindegyik esetben ugyanazt a rögzített $K[a_1]$-beli b elemet választjuk. Mivel $K[a_1, \dots, a_n]$ minden eleme az a_i elemek szorzatainak K-beli együtthatós lineáris kombinációjaként írható fel, ezért e test minden eleme olyan, hogy b alkalmas hatványával szorozva $K[a_1]$ felett egészet kapunk. Tegyük fel most azt, hogy a_1 transzcendens a K felett. Az 5. megjegyzés szerint $K[a_1]$ integrálisan zárt $K(a_1)$-ben. Ez azt jelentené, hogy létezik olyan $b(a_1)$ polinom, amelynek valamely hatványával a hányadostest bármely elemét megszorozva egy polinomot kapunk. Ez pedig lehetetlen. ■

A 10.6. tétel lehetőséget ad a Hilbert-féle nullhelytétel teljes bizonyítására. A speciális nullhelytétel (7.80. tétel) azt mondja ki, hogy ha egy Noether-gyűrű egy ideáljának minden gyöke egyszersmind egy adott elemnek is gyöke, akkor ez az elem benne van a szóban forgó ideál radikáljában. A Hilbert-féle nullhelytétel természetesen akkor igazán fontos, amikor a vizsgált Noether-gyűrű egy rögzített test feletti többhatározatlanú polinomgyűrű. Ekkor a feltétel úgy szól, hogy ha egy polinomideálnak valamely testben van gyöke, és e gyökök mindegyike gyöke egy előre megadott polinomnak, akkor a megadott polinom a vizsgált polinomideál radikáljában van. Tényleges vizsgálatok esetén azonban a polinomoknak csak olyan gyökeit nézik, amelyek az alaptest algebrai lezártjába tartozó elemekből állnak. Természetesen a gyökök „nagyon ritkán" ilyenek: például az $x^2 + y^2 - z^2 \in \mathbb{Q}[x, y, z]$ polinomnak egy általános gyöke az $(u^2 - v^2, 2uv, u^2 + v^2)$. Ez a gyök $(\mathbb{Q}[u, v])^3$-ben van. Specializálással nyerhetjük ebből a $(\mathbb{Q}[t])^3$-beli $(t^2 - 9, 6t, t^2 + 9)$ gyököt (de sok mást is). Újabb specializálással – többek közt – a $(7, 24, 25) \in \mathbb{Q}^3$ gyökhöz juthatunk.

Persze vannak gyökök $\mathbb{Q}$-nál bővebb testekben is. Nem célszerű azonban speciális gyöknek tekinteni algebrailag független $\alpha, \beta \in \mathbb{C}$ esetén az $(\alpha^2 - \beta^2, 2\alpha\beta, \alpha^2 + \beta^2)$ megoldást; hiszen ez semmivel sem árul el többet, mint az először adott megoldás. Értelmes viszont a $(t^2 - 2, 2\sqrt{2}t, t^2 + 2)$ specializálásról beszélni, vagy mondjuk $(1, 2\sqrt{6}, 5)$-ről.

A most adott megfogalmazás szerint a speciális nullhelytétel valami olyat mond ki, hogy ha az adott polinom minden olyan „összefüggésnek" eleget tesz, mint aminek az ideálba tartozó polinomok, akkor beletartozik az ideál radikáljába. Ebből viszont – eleve – nem következik például az, hogy ha a polinomnak gyöke minden olyan algebrai számokból álló rendszer, amely az ideálok minden elemének gyöke, már akkor is benne van a radikálban. Ezt az általános esetet fogjuk most bizonyítani.

10.7. Tétel. *Legyen K (kommutatív) test, $R = K[x_1, \ldots, x_n]$ polinomgyűrű és I egy ideál R-ben. Legyen továbbá L a K-nak az algebrai lezártja. Ha I-nek minden (L^n)-ben levő gyöke az előre megadott f polinomnak is gyöke, akkor f benne van az I radikáljában.*

Bizonyítás. A 7.80. tétel bizonyítása két részből állt. Az első lépésben azt láttuk be, hogy ha az ideálnak nincs gyöke, akkor az ideál megegyezik az egész gyűrűvel. Mindenekelőtt ennek azt az általánosítását látjuk be, hogy ha a tételben megadott ideálnak nincs gyöke (L^n)-ben, már akkor is megegyezik az egész polinomgyűrűvel. Itt is – mint a 7.80. tételben – elég maximális ideálokra bizonyítani az állítást. Ha I maximális, akkor az I szerinti maradékosztály-gyűrűről tudjuk, hogy test. Legyenek e testben a határozatlanoknak megfelelő elemek az a_i-k. Ez azt jelenti, hogy a $K[a_1, \ldots, a_n]$ gyűrű test. A 10.6. tétel szerint tehát minden a_i algebrai K felett, amiből következik, hogy az adott ideálnak van gyöke (L^n)-ben, hiszen L a K algebrai lezártja.

A 7.80. tétel bizonyításának a további része szinte szó szerint átvihető esetünkre is; csupán ahelyett, hogy van gyöke, azt kell mondani, hogy van gyöke (L^n)-ben (illetve, amikor egy új határozatlant vezetünk be, akkor a kitevőt is 1-gyel növelni kell). Ennek az ellenőrzését az olvasóra bízzuk. ■

Megjegyzés. Legyen M az $R = K[x_1, \ldots, x_n]$ tetszőleges maximális ideálja, és $\varphi : R \to R/M$ a természetes homomorfizmus. Mint tudjuk, a maximalitás alapján $L = R/M$ test, és a fentiekhez hasonlóan feltehető, hogy $K \leq L$, továbbá azt is tudjuk, hogy L az $a_i = \varphi(x_i)$ K felett algebrai elemekkel való bővítésként jön létre $(i = 1, \ldots, n)$. Eszerint L részteste a K test Ω algebrai lezártjának. A 10.7. tétel szerint a beágyazáskor kapott $(\xi_1, \ldots, \xi_n)$ elemek éppen az R ideáljainak az Ω^n-ben levő gyökhelyei. Egy olyan Galois-kapcsolatot létesítettünk a polinomok és a „helyek" között, amely akkor áll fenn, ha a hely gyöke a polinomnak. Egy polinomhalmaz lezártja az általa generált ideál radikálja. A zárt polinomhalmazok pedig pontosan azok az ideálok, amelyeknek lezártja önmaga. A „másik oldalon" álló zárt halmazok neve *algebrai varietás.* Ezek az algebrai geometria kiindulópontjai. Rögtön a következő lépés, amikor a törtfüggvényekre vagy az algebrai képben a $K(x_1, \ldots, x_n)$ testre terjesztik ki a Galois-kapcsolatot. Itt persze gondot okoz az, ha a nevezőben 0 áll; ezért aztán e testnek lokális gyűrűit nézik. A fentiekből világos, hogy a „pontokat" (helyeket) azonosíthatjuk a maximális ideálokkal. Minden varietás pontokból áll össze. A Noether–Lasker-tétel szerint minden varietás prímideálokhoz tartozó – úgynevezett irreducibilis – varietások „irredundáns" uniója. □

10.2. Dedekind-gyűrűk

Mint fent említettük, a kommutatív gyűrűk lényeges szerepet töltenek be az algebrai geometria bevezetésénél. A másik fontos szerepük az *algebrai számelméletben* (az algebrai számok elméletében) van. Itt is az ideálok jelentik az alapfogalmat, de itt a középponti kérdés az, hogy hogyan lehetne általánosítani az egyértelmű faktorizációt. Mindenekelőtt szükségünk lesz a prímideálok alábbi tulajdonságára:

10.8. Tétel. *Egy S kommutatív gyűrű egy P ideálja akkor és csak akkor prímideál, ha bármely A és B ideálokra az $AB \subseteq P$ feltételből vagy $A \subseteq P$, vagy $B \subseteq P$ következik.*

Bizonyítás. Ha a feltétel teljesül, és $ab \in P$, akkor $(a)(b) \subseteq P$ is igaz, és így például $(a) \subseteq P$, amiből $a \in P$ következik.

Tegyük most fel, hogy P prímideál és $AB \subseteq P$. Ha $A \subseteq P$, akkor készen vagyunk. Ha nem, akkor van olyan $a \in A$, amelyre $a \notin P$. Mivel tetszőleges $b \in B$ esetén $ab \in P$, ezért a kapott feltételből – a prímtulajdonság alapján – következik, hogy B minden eleme P-nek is eleme. ■

Megjegyzés. A fenti tételben az AB ideálszorzatot akár halmazelméleti, akár ideálelméleti szorzatnak is tekinthettük. A továbbiakban mindig ideálelméleti szorzat fog szerepelni. Amikor ezt ki akarjuk hangsúlyozni, akkor kitesszük a szorzásjelet. □

Rögzítsünk most egy S egységelemes integritási tartományt, és legyen K ennek a hányadosteste. Célunk annak a megvizsgálása, hogy milyen feltételek mellett érvényes S-ben az egyértelmű felbontási tételnek ideálokra vonatkozó analogonja. Ez tulajdonképpen a 7.77. Noether–Lasker-tétel egy további finomításának felel meg.

Először az S-beli ideálfogalmat szeretnénk általánosítani a K részhalmazaira. Az S-nek egy részhalmaza pontosan akkor ideál, ha S-modulus. Ez átvihető volna szó szerint, de célszerűbb nem minden ilyen részhalmazt megengedni. Indoklásul gondoljunk a racionális számok $\mathbb{Q}$ testében az egyértelmű felbontásra. Itt minden elem olyan, hogy valamilyen egészszámszorosa egész szám. Vannak azonban $\mathbb{Q}$-ban olyan $\mathbb{Z}$-modulusok, amelyek nem felelnek meg törtszámoknak. Tekintsük például a 2-hatvány nevezőjű vagy mondjuk a páratlan nevezőjű törteket. Bármelyik esetben egy $\mathbb{Z}$-modulust kapunk. Mindkét esetben az okozza a gondot, hogy a nevezőkben a prímtényezők száma „összességében” nem korlátos. Ezt a lehetőséget célszerű kizárni.

10.9. Definíció. Az egységelemes S integritási tartomány K hányadostestének egy I részhalmazát akkor nevezzük törtideálnak, ha olyan S-modulus, amelyet egy alkalmas fix (a modulustól függő) S-beli elemmel szorozva csupa S-beli elemet kapunk. □

A K ideáljaira a műveleteket ugyanúgy értelmezzük, mint a 7.69. definícióban.

Megjegyzések. 1. Egy törtideál elemeinek a szorzata nincs feltétlenül e törtideálban. Gondoljunk például arra a törtideálra, amelyben a szereplő törtek rövidített alakjában a nevező 2 vagy 1. Ebben benne van $\frac{1}{2}$, de $\frac{1}{2} \cdot \frac{1}{2}$ nincs benne. Ezért volt célszerű az, hogy az ideált nem mint részgyűrűt definiáltuk.

2. Nyilvánvaló, hogy a K-beli ideálok összege, szorzata és metszete is K-beli ideál. Az ideálhányados azonban nem mindig létezik (a kapott halmaz természetesen mindig S-modulus lesz, de nem mindig rendelkezik a külön kirótt tulajdonsággal). Az is világos, hogy az ideálok a szorzásra nézve kommutatív monoidot alkotnak, amelynek egységeleme S.

3. Némely könyvben a törtideál elnevezés helyett ideál szerepel. Ezt esetenként itt is megtesszük; természetesen testeknél ennek csak akkor van értelme, ha ezt egy adott integritási tartomány hányadostesteként vizsgáljuk. □

10.10. Tétel. *Ha az ideálok félcsoportjának egy eleme invertálható, akkor az inverz egyértelmű. Az invertálható A ideál inverze $S : A$. Invertálható ideál végesen generált S-modulus. Ha minden S-beli ideálnak van inverze (a K-beliek között), akkor minden K-belinek is van, és így az ideálok monoidja csoport.*

Bizonyítás. Legyen $AB = S$. Ebből azonnal következik, hogy B része az $S : A$ modulusnak. Másrészt

$$S : A \subseteq (S : A) \cdot S = (S : A) \cdot A \cdot B \subseteq S \cdot B \subseteq B,$$

amiből $B = S : A$ következik.

Ha A invertálható, és inverze B, akkor $AB = S$ miatt $1 \in AB$ teljesül. Ez $1 \in S$ miatt azt jelenti, hogy léteznek olyan A-beli a_i és B-beli b_i elemek, amelyekre $a_1b_1 + \cdots + a_rb_r = 1$. Ha a az A-nak tetszőleges eleme, akkor $AB = S$ miatt minden $1 \leq i \leq r$ mellett érvényes az $ab_i \in S$ összefüggés. Így $a = a_1(ab_1) + \cdots + a_r(ab_r)$ éppen azt fejezi ki, hogy $a_1, \ldots, a_r$ generátorrendszere A-nak.

Tekintsünk végül egy tetszőleges A_1 törtideált. Feltétel szerint létezik olyan $b \in S$, amelyre $b \cdot A_1 \subseteq S$. Mivel $B = b \cdot A_1$ is S-modulus, ezért (S-beli) ideál. Ha mármost C a B inverze, azaz $BC = S$, akkor $A_1 \cdot (b \cdot C) = S$. Mivel C-vel együtt nyilvánvalóan $b \cdot C$ is törtideál, ezért A is invertálható. Márpedig, ha egy monoid minden eleme invertálható, akkor csoport. ■

10.11. Tétel. *Ha S-beli ideálok egy rendszerének a szorzata invertálható, akkor mindegyikük külön-külön is invertálható. Speciálisan ez a helyzet áll elő, ha a szorzat főideál. Invertálható ideáloknak prímideálokra való felbontása egyértelmű.*

Bizonyítás. Legyen B egy invertálható S-beli ideál, és legyen $B = AC$, ugyancsak S-beli ideálokkal. Legyen továbbá B^{-1} a B inverze. Ekkor $A(CB^{-1}) = BB^{-1} = S$ bizonyítja az A invertálhatóságát. A tétel második állítása azonnal következik abból, hogy egy főideál nyilvánvalóan invertálható (egy elemmel generált S-modulusnak nyilván megvan a külön kirótt tulajdonsága).

Legyen az A invertálható ideálnak prímideálokra való felbontása $P_1 \cdot \ldots \cdot P_r = Q_1 \cdot \ldots \cdot \ldots \cdot Q_s$. A tétel már bizonyított állítása szerint ekkor minden egyes P_i és Q_j invertálható. Legyen e prímideálok között valamelyik, például P_1 minimális. A prímideálok tulajdonsága alapján ekkor valamelyik Q_i, például Q_1 része P_1-nek. Ugyancsak a prímideálok tulajdonságát kihasználva kapjuk, hogy valamelyik P_i viszont a Q_1-nek része. A P_1 minimalitása szerint ez viszont csak a $P_i = P_1$ esetben lehetséges. A felírt egyenlőséget P_1 inverzével szorozva hasonló típusú, eggyel kevesebb tényezőjű szorzatot kapunk. Így a bizonyítást teljes indukcióval befejezhetjük. ■

10.12. Definíció. Az S gyűrűt Dedekind-gyűrűnek nevezzük, ha minden nemtriviális ideálja felbontható nemtriviális prímideálok szorzatára. □

10.13. Tétel. *Dedekind-gyűrűben minden valódi invertálható prímideál maximális, és minden valódi prímideál invertálható.*

Bizonyítás. Legyen P az S Dedekind-gyűrűnek egy invertálható prímideálja, és $a \in S$ egy P-hez nem tartozó elem. Mivel P prímideál, ezért a^2 sem eleme P-nek. Legyen továbbá $A = (P, a)$, és $B = (P, a^2)$. Amennyiben P nem volna maximális, és $(P, a) \neq S$, akkor mind A, mind B felbomlik prímideálok szorzatára. Tekintsük most a P szerinti S' maradékosztály-gyűrűt. Ez integritási tartomány, mert P prímideál, és S' ideáljai egy-egyértelműen megfelelnek az S P-t tartalmazó ideáljainak. A megfeleltetés az, amelynél minden S-beli ideálhoz a természetes homomorfizmusnál kapott képét rendeljük. Az is világos, hogy ha a megfelelő ideálok közül az egyik prím, akkor a másik is az. A művelettartásból az is következik, hogy az ideálok képének a szorzata a megfelelő képek szorzatával egyezik meg. Tekintettel arra, hogy S Dedekind-gyűrű, ezért az A és B ideálok

mindegyike felbontható prímideálok szorzatára: $A = \prod P_i$, $B = \prod Q_j$. Az ideálok szorzatának a definíciójából következik, hogy a tényezők mindegyike tartalmazza az a^2 elemet és így mindegyik nagyobb P-nél. Az S/P faktorra térve kapjuk, hogy $(a') = A' = \prod P_i'$ és $(a'^2) = B' = \prod Q_j'$ nem-0 prímideálokra való felbontás. Mivel A', B' mindketten főideálok, ezért a 10.11. tétel szerint *egyértelműen* bonthatók (invertálható) prímideálok szorzatára. Tekintettel arra, hogy $(a'^2) = (a')^2$, ezért a B' felbontásában a Q_j' prímideálok között minden P_i' kétszer akkora multiplicitással lép fel, mint az A' felbontásában. Az egyértelmű megfeleltetés következtében tehát ugyanez a kapcsolat a B és A felbontásában; következésképpen $B = A^2$.

Mivel A minden eleme $p + x \cdot a$ alakba írható ($p \in P$, $x \in S$), ezért A^2 elemeit felírhatjuk $pq + ya$ alakban, ahol mind p, mind q P-beli elemek. Tekintettel arra, hogy $P \subseteq B = A^2$, ezért P tetszőleges u elemét is így írhatjuk fel. Most azonban $ya = u - pq \in P$, amiből $a \notin P$ alapján $y \in P$ következik – hiszen P prímideál. Így a $P = P^2 + Pa = PA$ eredményhez jutottunk. Ez viszont P invertálhatósága alapján az $A = S$ eredményhez vezet, ellentmondva a $B \neq S$ feltételnek, ami éppen P maximalitását jelenti.

Tekintsünk most egy tetszőleges P prímideált, és annak egy tetszőleges p elemét. Ezt az elemet – illetve a (p) ideált – feltétel szerint felírhatjuk prímideálok szorzataként: $(p) = P_1 \cdot \ldots \cdot P_r$. Ezek a prímideálok a 10.11. tétel szerint invertálhatóak; a most bizonyítottak alapján tehát maximálisak. Mivel szorzatuk benne van a P prímideálban, ezért közülük valamelyik szintén része ennek az ideálnak, ami a maximalitás miatt csak úgy lehet, hogy egyenlő is vele. Ez pedig éppen a P ideál invertálhatóságát – és egyben maximalitását – adja. ■

10.14. Következmény. *Dedekind-gyűrűkben az ideálok felbontása prímideálok szorzatára egyértelmű. Dedekind-gyűrű hányadostestének minden ideálja egyértelműen felbontható prímideálok egész kitevős hatványára. Jelölje $n_P(A)$ azt a kitevőt, amely egy rögzített P prímideálhoz tartozik az A ideál felbontásában. Ekkor:*

A pontosan akkor osztója B-nek, ha $(\forall P)(n_P(A) \leq n_P(B))$;

$$n_P(A + B) = \min(n_P(A), n_P(B)); \qquad n_P(A \cap B) = \max(n_P(A), n_P(B));$$

$$n_P(AB) = n_P(A) + n_P(B); \qquad n_P(A : B) = n_P(AB^{-1}) = n_P(A) - n_P(B).$$

Bizonyítás. Az első állítás azonnal következik a 10.11. és 10.13. tételekből. A további állítások kiszámolását az olvasóra bízzuk. ■

10.15. Tétel. *S akkor és csak akkor Dedekind-gyűrű, ha hányadostestének (nem 0) ideáljai a szorzásra nézve csoportot alkotnak.*

Bizonyítás. A 10.14. következményből azonnal kapjuk, hogy egy Dedekind-gyűrű hányadostestének (nem-0) ideáljai csoportot alkotnak az ideálszorzásra.

Induljunk ki most abból, hogy az S gyűrű ideáljaira a feltétel teljesül. A 10.10. tétel szerint ebből következik, hogy minden ideál végesen generált (azaz S Noether-gyűrű).

Ezért használhatjuk a lefelé menő indukciót annak a bizonyítására, hogy S minden ideálja felbontható prímideálok szorzatára. Tegyük fel, hogy az állítás igaz az A valódi ideált valódi módon tartalmazó minden ideálra. Ha A az S-nek maximális ideálja, akkor a szerinte vett faktor test, mert S egységelemes. Mivel minden test nullosztómentes, ezért A prímideál, ami bizonyítja az állítást. Ha A nem maximális, akkor van egy őt tartalmazó P maximális ideál (S Noether-gyűrű), amely az előzőek szerint prím. A-nak a hányadostestben van triviális felbontása: $A = P \cdot (P^{-1}A)$. Az $A \subseteq P$ feltétel szerint $P^{-1}A \subseteq P^{-1}P = S$, ami azt jelenti, hogy $P^{-1}A$ is az S-nek ideálja. $S \subseteq S : P = P^{-1}$ alapján azt kapjuk, hogy $A = SA \subseteq P^{-1}A$. E két ideál különböző, hiszen az $A = P^{-1}A$ egyenlőségből a csoporttulajdonság alapján $P^{-1} = S$ következne, feltevésünkkel ellentétben. Az indukciós feltevés alapján tehát $P^{-1}A$ felírható prímideálok szorzataként; így ugyanez igaz A-ra is. ■

Megjegyzés. A 10.10. tételben láttuk, hogy minden Dedekind-gyűrű Noether-gyűrű. A 10.13. tételből az is kiderült, hogy Dedekind-gyűrű minden prímideálja maximális. Tekintsük most az S Dedekind-gyűrű hányadostestének egy a elemét, amely egész az S felett. Ez azt jelenti, hogy $S[a]$ végesen generált S-modulus, és így létezik olyan $b \in S$, amelyre k-tól függetlenül $ba^k \in S$. Ebből kapjuk, hogy a fenti elemek prímideálokra való felbontásában bármely rögzített prímideálnak pozitív kitevője van, azaz (elhagyva a P indexet) a 10.14. tételben megadott összefüggések szerint $n(b \cdot a^k) = n(b) + k \cdot n(a)$ bármely k természetes számra pozitív. Ez viszont csak úgy lehetséges, ha $n(a)$ is pozitív. Így csak $a \in S$ lehetséges. Ez azt jelenti, hogy bármely Dedekind-gyűrű integrálisan zárt. Kimutatható, hogy e három feltétel (Noether-gyűrű, minden valódi prímideál maximális és az integrális zártság) elegendő is ahhoz, hogy a gyűrű Dedekind-gyűrű legyen. □

Dedekind-gyűrűkre fontos példát adnak a főideálgyűrűk algebrai bővítései. Ha az egész számokból indulunk ki, akkor az algebrai egészek vizsgálatához jutunk. Ezekkel az algebrai számelmélet foglalkozik. A következő pontban megmutatjuk, hogy ezek a bővítések valóban Dedekind-gyűrűk.

Az az eset, amikor a kiinduló gyűrű a komplex együtthatós polinomok gyűrűje, igen fontos az algebrai geometriában. Itt nem bizonyítjuk, hogy az így nyert gyűrűk valóban mindig Dedekind-gyűrűk.

Megemlítjük, hogy a fenti példákban általában olyan gyűrűket nyerünk, amelyekben az elemek egyértelmű prímtényezős felbontása nem érvényes. Fordított példát is mondhatunk. A test feletti többhatározatlanú polinomgyűrűkben érvényes az egyértelmű prímtényezős felbontás. Ezzel szemben ezek nem Dedekind-gyűrűk. Például a $\mathbb{Q}[x, y]$-ban az (x) ideál prímideál, de nem maximális, mert benne van az (x, y) ideálban.

Nem nagyon nehéz annak a bebizonyítása, hogy egy Dedekind-gyűrű bármely valódi ideál szerinti faktorában minden ideál főideál (ez a faktor azonban általában nem nullosztómentes!). Ennek segítségével kimutatható, hogy egy Dedekind-gyűrűben bármely ideál generálható két elemmel.

Feladatok

1. Legyen K az S egységelemes integritási tartomány hányadosteste és L a K algebrai lezártja. Vezessük be L elemeire a következő feltételnek eleget tevő E tulajdonságot: Az E tulajdonságú elemek egy R gyűrűt alkotnak; E tulajdonságú elem konjugáltja is E tulajdonságú; és K egy eleme pontosan akkor E tulajdonságú, ha S-ben van. Bizonyítsuk be, hogy R hányadostestében pontosan az S feletti egészeknek van meg az E tulajdonsága.

2. Bizonyítsuk be, hogy a 10.5. definíció után szereplő megjegyzések példáiban valóban fennáll az integrális zártság.

3. A következőkben legyen R egy Dedekind-gyűrű. Bizonyítsuk be az alábbiakat:

(1) Ha $P_1, \ldots, P_r$ az R prímideáljai, akkor $P_1^{i_1} \cdot \ldots \cdot P_r^{i_r} = P_1^{i_1} \cap \ldots \cap P_r^{i_r}$.

(2) R minden faktora is Dedekind-gyűrű.

(3) Ha $I = P_1^{i_1} \cap \ldots \cap P_r^{i_r}$ az R ideálja, akkor $R/I \cong R/P_1^{i_1} \oplus \cdots \oplus R/P_r^{i_r}$.

(4) Ha P az R prímideálja és $P^i \neq \{0\}$, akkor bármely $t \in P \setminus P^2$ esetén $t^i \in P^i \setminus P^{i+1}$ $(i = 2, \ldots)$.

(5) Ha $P \neq (0)$ az R prímideálja, akkor R/P^i főideálgyűrű.

(6) Főideálgyűrűk direkt összege is főideálgyűrű.

(7) Ha $I \neq (0)$ az R ideálja, akkor R/I főideálgyűrű.

(8) Ha $I \neq (0)$ az R ideálja, akkor bármely $a \in I$ esetén van olyan $b \in I$, hogy az $R/(a)$ gyűrűben b képe generálja az I ideál képét.

(9) Az előző pontbeli a és b elemek generálják az I ideált.

10.3. Algebrai egészek felett

Az alábbiakban legyen $f(x)$ a $\mathbb{Q}$ felett n-edfokú egész ϑ minimálpolinomja, $\mathbb{K} = \mathbb{Q}(\vartheta)$ és $\mathbb{E}$ a $\mathbb{K}$ egészeinek a gyűrűje. (Általában $\mathbb{E}$ nem egyezik meg $\mathbb{Z}[\vartheta]$-val.)

Mint említettük, a $\mathbb{Q}$ test egyszerű algebrai bővítésének egészei Dedekind-gyűrűt alkotnak. Noha ezekkel az algebrai számelmélet foglalkozik, mégis érdemes róluk legalább ezt bebizonyítani. Már csak azért is, mert ezek indították el a Dedekind-gyűrűkkel foglalkozó kutatásokat.

10.16. Tétel. *$\mathbb{E}$ minden ideálja legfeljebb n elem által generált szabad $\mathbb{Z}$-modulus.*

Bizonyítás. Minden $\alpha \in \mathbb{E}$ egyértelműen felírható

$$\alpha = c_0 + c_1 \cdot \vartheta + \cdots + c_{n-1} \cdot \vartheta^{n-1} \qquad (c_i \in \mathbb{Q}) \tag{1}$$

alakban. ϑ-nak ϑ_j konjugáltjaira $(j = 1, \ldots, n)$ áttérve, az α-k konjugáltjait kapjuk, amelyek ugyancsak algebrai egészek, bár általában nem elemei $\mathbb{K}$-nak:

$$\alpha_j = c_0 + c_1 \cdot \vartheta_j + \cdots + c_{n-1} \cdot \vartheta_j^{n-1} \qquad (c_i \in \mathbb{Q}). \tag{2}$$

Mivel a rendszer determinánsa Vandermonde-féle, ezért nem 0. A (2) alatti egyenletrendszert Cramer-szabállyal megoldva a $c_i = \dfrac{\Delta_i}{\Delta}$ összefüggéshez jutunk. A fenti összefüggést $c_i \cdot \Delta^2 = \Delta_i \cdot \Delta$ alakba írhatjuk. D a ϑ_i-kben szimmetrikus, Δ elemei egészek, így $D = \Delta^2$ racionális és egész, ezért $c_i \cdot D$ racionális. A jobb oldalon levő mindkét tényező algebrai egészekből álló mátrix determinánsa, tehát algebrai egész. Tekintettel arra, hogy $\mathbb{Z}$ integrálisan zárt $\mathbb{Q}$-ban, ezért a $c_i = \dfrac{x_i}{D}$ felíráshoz jutottunk, ahol minden egyes $x_i \in \mathbb{Z}$. Eszerint $\mathbb{E}$ minden eleme felírható

$$x_0 \cdot \frac{1}{D} + x_1 \cdot \frac{\vartheta}{D} + \cdots + x_{n-1} \cdot \frac{\vartheta^{n-1}}{D} \qquad (x_i \in \mathbb{Z}) \tag{3}$$

alakban. Így $\mathbb{E}$, és $\mathbb{E}$-nek minden ideálja a $\mathbb{Q}$ felett független $\frac{1}{D}, \frac{\vartheta}{D}, \ldots, \frac{\vartheta^{n-1}}{D}$ elemek generálta – így szabad – $\mathbb{Z}$-modulus részmodulusa. Az ezekről tanultak alapján tehát mindegyikük legfeljebb n elemmel generált szabad $\mathbb{Z}$-modulus. ■

A továbbiakban az ideálokra vonatkozó alapvető, HURWITZtól származó tételnek a STEINITZ által adott bizonyítását tárgyaljuk.

10.17. Tétel. *Legyenek*

$$A(x) = \alpha_p \cdot x^p + \cdots + \alpha_0 \quad \text{és} \quad B(x) = \beta_q \cdot x^q + \cdots + \beta_0 \tag{4}$$

algebrai egész együtthatós polinomok ($\alpha_p \neq 0$, $\beta_q \neq 0$). Ha a

$$C(x) = A(x) \cdot B(x) = \gamma_{p+q} \cdot x^{p+q} + \cdots + \gamma_0 \tag{5}$$

polinom minden együtthatója osztható a δ algebrai egésszel, akkor δ ugyancsak osztója minden egyes szóba jövő $\alpha_i \cdot \beta_j$ szorzatnak is.

Megjegyzés. A ξ algebrai egész osztója az η algebrai egésznek, ha az $\frac{\eta}{\xi}$ tört is algebrai egész. □

A 10.17. tétel bizonyításához két lemmát használunk fel:

A. Lemma. *Legyen ξ gyöke az algebrai egész együtthatós*

$$D(x) = \delta_m \cdot x^m + \cdots + \delta_0 \qquad (\delta_m \neq 0) \tag{6}$$

polinomnak. Ekkor $\frac{D(x)}{x - \xi}$ is algebrai egész együtthatós.

Bizonyítás. Mivel $\delta_m \cdot \xi$ egy normált algebrai egész együtthatós polinom gyöke, ezért maga is algebrai egész (bizonyítás?). A lemma állítását most már m szerinti teljes indukcióval végezzük.

Az $m = 1$ esetben a hányados δ_1, ami algebrai egész.

Az indukciós lépéshez tekintsük a $D_1(x) = D(x) - \delta_m \cdot x^{m-1} \cdot (x - \xi)$ polinomot. Az előzetes megjegyzés szerint $D_1(x)$ ugyancsak algebrai egész együtthatós, ξ nyilván gyöke és a foka kisebb, mint m. Az indukciós feltevés alapján tehát algebrai egész együtthatós a $\frac{D(x)}{x - \xi} = \frac{D_1(x)}{x - \xi} + \delta_m \cdot x^{m-1}$ polinom is. ■

B. Lemma. *Legyen $\xi_1, \ldots, \xi_m$ az A lemmában adott polinom összes gyöke. Ekkor tetszőleges $1 \leq k \leq m$ esetén $\delta_m \cdot \xi_1 \cdot \ldots \cdot \xi_k$ is algebrai egész.*

Bizonyítás. Az A. lemma ismételt alkalmazásával azt kapjuk, hogy a

$$\delta_m \cdot (x - \xi_1) \cdot \ldots \cdot (x - \xi_k) = \frac{D(x)}{(x - \xi_{k+1}) \cdot \ldots \cdot (x - \xi_m)} \tag{7}$$

ugyancsak egész együtthatós. Ennek a konstans tagja pedig éppen a kérdéses szám vagy annak a negatívja. ■

A 10.17. tétel bizonyítása. Tekintsük az $A(x)$ és $B(x)$ polinomoknak lineáris faktorokra való felbontását:

$$A(x) = \alpha_p \cdot (x - \xi_1) \cdot \ldots \cdot (x - \xi_p), \quad B(x) = \beta_q \cdot (x - \eta_1) \cdot \ldots \cdot (x - \eta_q).$$

Feltétel szerint a

$$\frac{C(x)}{\delta} = \frac{\alpha_p \cdot \beta_q}{\delta} \cdot [(x-\xi_1)\cdot\ldots\cdot(x-\xi_p)]\cdot[(x-\eta_1)\cdot\ldots\cdot(x-\eta_q)] \tag{8}$$

polinom egész együtthatós. A B. lemma alapján tehát minden

$$\frac{\alpha_p \cdot \beta_q}{\delta} \cdot [\xi_\square \cdot \ldots \cdot \xi_\square] \cdot [\eta_\square \cdot \ldots \cdot \eta_\square] \tag{9}$$

alakú szorzat algebrai egész. (Itt $\xi_\square$, illetve $\eta_\square$ azt jelenti, hogy ezeket az elemeket valamilyen módon indexezzük úgy, hogy egy zárójelen belül minden index különböző.) Az

$$\frac{\alpha_i \cdot \beta_j}{\delta} = \frac{\alpha_i \cdot \beta_j}{\alpha_p \cdot \beta_q} \cdot \frac{\alpha_p \cdot \beta_q}{\delta} \tag{10}$$

összefüggésben a jobb oldal első tényezője $\frac{\alpha_i \cdot \beta_j}{\alpha_p \cdot \beta_q} = \frac{\alpha_i}{\alpha_p} \cdot \frac{\beta_j}{\beta_q}$. A gyökök és együtthatók közti összefüggés alapján ez a szorzat bizonyos ξ_i-k és bizonyos η_j-k szorzata. (9) miatt tehát a (10) jobb oldalán mindig egész áll. ■

10.18. Tétel (Főtétel)**.** *Az $\mathbb{E}$ gyűrű minden I ideáljához található olyan J ideál, hogy $I \cdot J$ főideál.*

Bizonyítás. Az $I = (\alpha_1, \ldots, \alpha_r)$ ideálhoz tekintsük a $g(x) = \alpha_1 \cdot x + \cdots + \alpha_r \cdot x^r$ algebrai egész együtthatós polinomot. Ekkor ugyancsak algebrai egész együtthatósak lesznek ennek a

$$g^{(i)}(x) = \alpha_1^{(i)} \cdot x + \cdots + \alpha_r^{(i)} \cdot x^r \quad (i = 1, \ldots, n) \tag{11}$$

alakú konjugáltjai; amelyek között például $g^{(1)}(x) = g(x)$ is szerepel. Képezzük most ezek

$$G(x) = \prod_{i=1}^{n} g(i)(x) = \sum_{j=1}^{r\cdot n} c_j x^j \tag{12}$$

szorzatát. A szimmetrikus polinomok alaptételét felhasználva azt kapjuk, hogy $G(x) \in \in \mathbb{Z}[x]$, hiszen az együtthatók egészek is. Ekkor viszont a $h(x) = \frac{G(x)}{g(x)}$, mint két $\mathbb{K}$-beli együtthatós polinom hányadosa, szintén $\mathbb{K}$-beli együtthatós. Mivel $h(x) = \prod_{i=2}^{n} g^{(i)}(x)$ egy olyan szorzat, amelyben minden egyes tényező egész algebrai együtthatós, ezért ugyanez igaz $h(x)$-re is. Eszerint

$$h(x) = \beta_1 \cdot x + \cdots + \beta_s \cdot x^s \in \mathbb{E}[x] \qquad (s = r \cdot (n-1)). \tag{13}$$

Tekintsük a $G(x)$ polinom c_i együtthatóit, és legyen N ezeknek a legnagyobb közös osztója ($\mathbb{Z}$-ben vagyunk!). A 10.17. tétel szerint minden egyes $\alpha_i \cdot \beta_j$ szám osztható N-nel: $\alpha_i \cdot \beta_j = \lambda_{i,j} \cdot N$. Mivel $\mathbb{Z}$ euklideszi gyűrű, ezért léteznek olyan $n_\ell \in \mathbb{Z}$ számok, amelyekre $\sum c_\ell \cdot n_\ell = N$. A c_ℓ számok mindegyike felírható az $\alpha_i \cdot \beta_j$ szorzatok közül bizonyosoknak az összegeként. Így maga N is $\mu_{i,j} \cdot (\alpha_i \cdot \beta_j)$ alakba írható egész (sőt racionális egész!) $\mu_{i,j}$ számokkal.

Azt kaptuk tehát, hogy minden $\alpha_i \cdot \beta_j$ szorzat osztható N-nel és N egész együtthatós lineáris kombinációja e szorzatoknak. Eszerint ennek az $\mathbb{E}$ gyűrűbeli $(\ldots, \alpha_i \cdot \beta_j, \ldots)$ ideálnak minden eleme osztható N-nel és N eleme ennek az ideálnak. Ez viszont pontosan azt jelenti, hogy ennek az ideálnak az elemei éppen az N-nel osztható számok; azaz ez éppen az (N) főideál. Ennek az ideálnak a generátorelemei pontosan az $(\ldots, \alpha_i, \ldots)$ és $(\ldots, \beta_j, \ldots)$ ideálok generátorelemeinek a szorzatai, ami azt jelenti, hogy

$$(\ldots, \alpha_i, \ldots) \cdot (\ldots, \beta_j, \ldots) = (N),$$

mint állítottuk. ■

A 10.18. tétel szerint a $\mathbb{Q}(\vartheta)$ egészeinek S gyűrűjében minden valódi I ideálhoz van olyan valódi J ideál, amelyre az IJ szorzat nem-0 főideál. Tekintettel arra, hogy ezek a szorzásra nézve egy H csoportot alkotnak, ezért a valódi ideálok is; következésképpen a $K(\vartheta)$ egészeinek S gyűrűje Dedekind-féle. (Egyébként $H \cong \mathbb{Q}(\vartheta)^*$.) Az ideálok G csoportjának tehát H részcsoportja. Ha $G = H$, akkor a S-ben minden ideál főideál, tehát érvényes az elemek egyértelmű faktorizációja. Egyébként – mint említettük – minden ideál két elemmel generálható.

A vizsgált testek egészeinek létezik egy „finomabb" megkülönböztetése a G/H faktorcsoport segítségével. A geometriában ismert, a rácspontokkal kapcsolatos Minkowski-tétel segítségével kimutatható, hogy G/H véges. Ezt a számot a $K(\vartheta)$ osztályszámának nevezik. Az osztályszám meghatározása az algebrai számelmélet egyik fontos feladata. A végességből következik, hogy minden I ideálnak egy alkalmas hatványa főideál. Ha $I^k = (a)$, akkor úgy tekinthetjük, hogy I nem más, mint a $\sqrt[k]{a}$ „ideális szám" (ebből ered az ideál elnevezés). Valójában ez a szám létezik, csak nem a vizsgált testben. Ha az osztályszám 2, akkor egyetlen ideális számmal bővítve e bővítésben minden S-beli párnak lesz legnagyobb közös osztója. Természetesen – mint várható – a bővebb testben olyan újabb párok keletkeznek, amelyeknek nincs legnagyobb közös osztójuk. Ha azonban ezt tovább visszük, akkor az algebrai számok $\mathcal{A}$ testjének egy $\mathcal{E}$ részgyűrűjét – az algebrai egészek gyűrűjét – kapjuk. $\mathcal{E}$-ben bármely két egésznek létezik legnagyobb közös osztója:

Ha $\alpha, \beta \in \mathcal{E}$, akkor van olyan $\delta \in \mathcal{E}$, amelyre α/δ és β/δ mindegyike algebrai egész, s ha α/γ és β/γ mindegyike algebrai egész, akkor δ/γ is az. Emellett léteznek olyan ξ és η algebrai egészek, amelyekre $\delta = \xi\alpha + \eta\beta$.

Ebből mégsem következik az, hogy $\mathcal{E}$-ben érvényes az egyértelmű faktorizáció, ugyanis nincs benne irreducibilis elem, mert $\alpha = (\sqrt{\alpha})^2$.

Feladatok

1. Bizonyítsuk be, hogy ha α algebrai egész, akkor $\sqrt{\alpha}$ is az.

2. Világos, hogy $\mathcal{E}$-ben bármely véges sok elemnek van legnagyobb közös osztója, tehát főideált generálnak. Főideálgyűrűben viszont érvényes az egyértelmű faktorizáció. Keressük meg a gondolatmenetben azt a hiányosságot, amelyből ezt az „ellentmondást" kaptuk.

3. Mutassuk meg, hogy $\mathcal{E}$-ben létezik valódi prímideál.

4. Mutassuk meg, hogy az egyértelmű faktorizáció sem $\mathbb{Z}[\sqrt{-3}]$-ban, sem $\mathbb{Z}[\sqrt{-5}]$-ben nem igaz. Bizonyítsuk be, hogy ezek egyike nem is integrálisan zárt és integrális lezártjában igaz az egyértelmű faktorizáció.

5. Határozzuk meg, hogy milyen négyzetmentes D (nem feltétlen pozitív) számokra lesz $\mathbb{Z}[\sqrt{D}]$ integrálisan zárt.

6. Határozzuk meg, hogy milyen $\mathbb{Z}$-beli polinomok gyökei egységek a megfelelő algebrai bővítésben.

7. Határozzuk meg, hogy négyzetmentes D esetén hány egységgyök lehet $\mathbb{Q}(\sqrt{D})$ egészei között.

8. Bizonyítsuk be, hogy negatív négyzetmentes D esetén $\mathbb{Q}(\sqrt{D})$ egészei között minden egység egységgyök.

9. Bizonyítsuk be, hogy ha $\mathbb{Q}(\sqrt{D})$ egészei között van olyan egység, amelyik nem egységgyök, akkor van végtelen sok ilyen egység.

10. Bizonyítsuk be, hogy $\mathbb{Z}[\sqrt{2}]$-ben $\varepsilon = -1 + \sqrt{2}$ egység, és e gyűrű minden egysége $\pm\varepsilon^k$ alakú, ahol k tetszőleges egész szám.

11. Bizonyítsuk be, hogy $\mathbb{Z}[\sqrt{-5}]$-ben az osztályszám 2.

12. Legyen K a $\mathbb{Q}(x)$ egy integrálisan zárt részteste. Bizonyítsuk be, hogy ha K tartalmaz egy legalább elsőfokú polinomot, akkor az összeset tartalmazza. Adjunk példákat arra az esetre, amikor $K \neq \mathbb{Q}$ és egyetlen polinomot sem tartalmaz.

13. Bizonyítsuk be, hogy az általános n-edfokú polinom gyökei egészek az együtthatók generálta polinomgyűrű felett.

14. Jellemezzük azokat a $\mathbb{Q}$-beli $\mathbb{Z}$-modulusokat, amelyek törtideálok.

15. Legyenek A és B az S egységelemes kommutatív gyűrű ideáljai. Bizonyítsuk be, hogy $A = (A : S)$ és $A \cdot (S : B) \subseteq (A : B)$.

16. Tekintsük az (integrálisan zárt) $R = \mathbb{Z}[\sqrt{-5}]$ gyűrű egy $I \neq \{0\}$ ideálját. Bizonyítsuk be:

(1) I tartalmaz pozitív n egész számot.

(2) I végesen generált.

(3) I minden $\mathbb{Z}$-n kívüli eleme $b \cdot (c + \sqrt{-5})$ alakú – rögzített c-vel.

(4) I két elemmel generált.

(5) I minden eleme $b \cdot \alpha$ alakú, ahol α egy I_1 ideál elemein fut végig, amelyet egy $n_1 \in \mathbb{Z}$ és $c + \sqrt{-5}$ generálnak.

(6) $|c| < n_1$ és n osztója $(c^2 + 5)$-nek.

17. Legyen $\vartheta_1 = \sqrt{2}$, $\vartheta_2 = \sqrt{10}$, $\vartheta \in \{\vartheta_1, \vartheta_2\}$. Bizonyítsuk be, hogy $\mathbb{Q}(\vartheta)$ egészei pontosan $\mathbb{Z}[\vartheta]$ elemei, $\mathbb{Z}[\vartheta]$ egységei (alkalmas $\alpha \in \mathbb{Z}[\vartheta]$ elemmel) $\pm\alpha^n$ $(n \in \mathbb{Z})$ alakúak. $\mathbb{Z}[\vartheta_1]$ euklideszi gyűrű, $\mathbb{Z}[\vartheta_2]$-ben nem érvényes az egyértelmű faktorizáció.

18. Adjunk meg végtelen sok olyan pozitív D egész számot, amelyre $\mathbb{Q}(\sqrt{D})$ egészei éppen $\mathbb{Z}(\sqrt{D})$ elemei; itt sem érvényes az egyértelmű faktorizáció és ez hasonlóképpen bizonyítható, mint $\mathbb{Z}[\vartheta_2]$-ben.

10.4. Féligegyszerű gyűrűk

Most azokra a gyűrűkre kívánunk struktúratételt adni, amelyek esetében a Hom funktor egzakt sorozatot egzakt sorozatba visz. Struktúratételen olyan tételt értünk, amely bizonyos algebrai struktúrák szerkezetét más, egyszerűbb struktúrák segítségével írja le. Ilyen struktúratétel például a véges Abel-csoportok alaptétele. De struktúratételnek nevezhető egy olyan tétel, amely például bizonyos félcsoportok szerkezetét csoportokra vezeti vissza még akkor is, ha a fellépő csoportok szerkezete a csoportelméletben nincs kielégítően leírva. Az algebrában igen kevés struktúratétel ismeretes.

Esetünkben nem feltétlenül kommutatív gyűrűk struktúrájáról van szó. Ilyen struktúrát egyet ismerünk jól; a négyzetes mátrixok, illetve más felfogásban a lineáris transzformációk gyűrűjét. A struktúratétel előkészítéseképpen ezeket a fogalmakat „újradefiniáljuk" anélkül, hogy az alapgyűrű kommutativitását feltennénk.

10.19. Definíció. Egy R gyűrű feletti R_n $(n \times n)$-es teljes mátrixgyűrűn azokat az $(n \times n)$-es mátrixokat értjük, amelyeknek az elemei az R gyűrűből valók. Ha $\mathbf{A} = (a_{i,j})$ és $\mathbf{B} = (b_{i,j})$ ilyen mátrixok, akkor ezek $(c_{i,j})$ összegét és $(d_{i,j})$ szorzatát a $c_{i,j} = a_{i,j} + b_{i,j}$, illetve $d_{i,j} = a_{i,1}b_{1,j} + \cdots + a_{i,n}b_{n,j}$ összefüggés definiálja. Ha $a \in R$, akkor az $a\mathbf{A}$, illetve az $\mathbf{A}a$ mátrixokban az i-edik sor j-edik eleme $aa_{i,j}$, illetve $a_{i,j}a$. □

A mátrixműveletekre vonatkozó elemi azonosságok itt is könnyen igazolhatók (ugyanúgy, mint amikor a mátrix elemei számok), kivéve azt, hogy $a\mathbf{A}$ és $\mathbf{A}a$ általában különböznek, hiszen R nem feltétlenül kommutatív. Ezeknek a bizonyítását az olvasóra bízzuk.

10.20. Tétel. *R_n a 10.19. definícióra nézve gyűrűt alkot, amelyben érvényes az* $(ab)\mathbf{A} = a(b\mathbf{A})$, *valamint az* $\mathbf{A}(ab) = (\mathbf{A}a)b$ *összefüggés.*

Az R tetszőleges a elemének megfeleltetve azt az $\mathbf{M}_a$ mátrixot, amelyben a főátlóban az összes elem a, és a többi elem 0, az R-nek a teljes mátrixgyűrűbe való injektív homomorfizmusát kapjuk, amelynél $\mathbf{M}_a\mathbf{A} = a\mathbf{A}$ *és* $\mathbf{A}\mathbf{M}_a = \mathbf{A}a$ *teljesül.* ■

Célunk R-nek mátrixokkal való ábrázolása. Tekintettel arra, hogy ${}_RR$ bal oldali R-modulus, ezért a 9.14. tétel szerint rendelkezésünkre áll R-nek az $\mathrm{End}_R({}_RR)$-be való homomorfizmusa. A 9.14. tétel szerint ez beágyazás, ha a homomorfizmus magja csak a 0-ból áll. Általában az endomorfizmusokat jellemző mátrixok nem csak végtelenek, de bonyolultak is. Akkor lehet a mátrixok szerkezetéből valamit „látni", ha e mátrixok végesek. Az alábbi definíció pontosan a 10.20. tételbeli injektivitás és a végesség megragadását szolgálja:

10.21. Definíció. Az R gyűrűt radikálmentesnek nevezzük, ha nincs nemnulla nilpotens balideálja, azaz, ha nincs olyan $B \neq 0$ balideálja, amelyre BB a nullideál.

Az R gyűrűt bal oldali Artin-gyűrűnek nevezzük, ha balideáljaira teljesül a minimumfeltétel.

Az R gyűrűt féligegyszerűnek nevezzük, ha radikálmentes és bal oldali Artin-gyűrű. □

Megjegyzések

1. A nilpotens balideál tulajdonképpen olyan B balideál, amelynek valamelyik hatványa a nullideál. Ha azonban például $B^n \neq 0$, de $B^{n+1} = 0$, akkor $(B^n)^2 = 0$. Így tehát a nilpotenciát esetünkben elég így értelmezni.

2. A 10.21. definícióban elvileg bal oldali radikálmentességről, illetve bal oldali féligegyszerűségről kellene beszélni. Ha $B \neq 0$ és $B^2 = 0$, akkor kimutatható, hogy $J = B + BR$ olyan, 0-tól különböző jobbideál, amelynek a négyzete 0. (A triviális számolást az olvasóra bízzuk.)

3. Ami a bal, illetve a jobb oldali féligegyszerűséget illeti, arról a későbbiekben majd bebizonyítjuk, hogy ugyanazt jelentik. Így felesleges ezekre külön elnevezést bevezetni. □

10.22. Tétel (Wedderburn–Artin). *Tetszőleges R gyűrűre az alábbi állítások ekvivalensek:*

(1) *R egységelemes, és bal oldali unitér R-modulusok minden részmodulusa direkt összeadandó.*

(2) *R jobbegységelemes, és minden balideálja (mint R-modulus) R-nek direkt összeadandója.*

(3) *R féligegyszerű.*

(4) *R véges sok, test feletti teljes mátrixgyűrű direkt összege. (A testek nem feltétlenül kommutatívak és nem feltétlenül izomorfak.)*

(5) *R egységelemes, és ${}_RR$ véges sok minimális balideáljának a direkt összege.*

Bizonyítás. Az állítások ekvivalenciáját ciklikusan bizonyítjuk.

(1)-ből következik (2) Mivel R maga is bal oldali R-modulus, ezért (2) az (1)-nek speciális esete.

(2)-ből következik (3) Legyen e az R jobb oldali egységelemeleme, legyen $B \neq (0)$ tetszőleges balideál, és legyen $B \oplus C$ az ${}_RR$-nek direkt összegre való felbontása. E felbontásban $e = f + g$ adódik ($f \in B$, $g \in C$), amiből tetszőleges $a \in R$ esetén azt kapjuk, hogy $a = ae = af + ag$. A balideál-tulajdonság miatt ez éppen az a felbontása. Amennyiben tehát a-t speciálisan B-ből választottuk, akkor az $af = a$ összefüggéshez jutunk (és azt is kapjuk, hogy $ag = 0$). Így $B \subseteq B^2$, tehát a nem (0) direkt összeadandó balideál nem lehet nilpotens. Feltételünk szerint minden balideál direkt összeadandó – így R radikálmentes.

Legyenek most B és C az R-nek olyan balideáljai, amelyekre $B \supseteq C$ teljesül. Mivel minden balideálról tudjuk, hogy jobbegységelemes, ezért legyen f a B-nek és g a C-nek jobbegységeleme. Tekintsük most a B azon x elemeinek a D halmazát, amelyekre $xg = 0$. Ilyen elem van, például $0g = 0$. Világos, hogy D balideál. Ha $a \in B$, akkor $a = (a - ag) + ag$, valamint $(a - ag)g = 0$ következtében azt kapjuk, hogy a C és D balideálok generálják a B balideált. Ha $x \in C \cap D$, akkor egyrészt $xg = 0$, másrészt $xg = x$ teljesül, ami azt jelenti, hogy C direkt összeadandója B-nek.

Legyen most $R = B_0 \supseteq B_1 \supseteq \ldots \supseteq B_n \supseteq \ldots$ az R balideáljainak egy csökkenő lánca. Az előzőek szerint B_{i-1} felírható $B_i \oplus C_i$ (balideál-) direkt összeg alakban. Legyen C a $C_1, \ldots$ balideálok generálta balideál. Ehhez található – mint láttuk – egy olyan C_0 balideál, amelyre $R = C \oplus C_0$. Ebből következik, hogy az összes szóban forgó C_i balideál generálja az R gyűrűt. Azt állítjuk, hogy a balideálok bármelyikének az összes többi generátumával való metszete egyedül a 0-ból áll. Ez az $i = 0$ esetben a C_0 definíciójából következik. Mivel $C \cap C_0$ csak a 0-t tartalmazza, ezért minden C_i-beli elem ($i \neq 0$) egyértelműen írható fel egy C-beli és egy C_0-beli elem összegeként; de egy felírásnál a C_0-beli komponens 0, és így elegendő a 0-tól különböző indexekkel foglalkozni. Mivel a generátum minden eleme már véges sok balideál generátumában benne van, ezért a feladatot a következőképpen fogalmazhatjuk: ha $c_1 + \cdots + c_n = 0$ ($c_i \in C_i$), akkor minden egyes $c_1 = 0$. Ezt pedig lépésenként bizonyíthatjuk $i = 1, 2, \ldots, n$ esetére, felhasználva a $B_{i-1} = B_i + C_i$ felbontást

és a $C_j \subseteq B_i$ $(j \geq i)$ összefüggést. Tekintsük az R gyűrű e jobbegységelemét. Ez eleme a C_i-k generátumának. Így eleme már véges sokénak is: $e \in C_0 \oplus C_1 \oplus \cdots \oplus C_n$. Ha mármost az e-nek a C_i-be eső komponense e_i, akkor $e_i e = e_i$ miatt e_i eleme a fenti direkt összegnek. Mint láttuk, ebből $i > n$ esetén $e_i = 0$, vagyis $C_i = \{0\}$ következik. A fenti lánc tehát stabilizálódik, vagyis érvényes a balideálokra a minimumfeltétel.

(3)-ból következik (4) Ennek a bizonyításához felhasználjuk a Schur-lemmát (9.16. tétel) és a sűrűségi tételt (9.20. tétel), de előbb az ott kimondott tételekből adódó újabb eredményeket bizonyítunk be speciálisan bal oldali Artin-gyűrűkre.

1. Állítás. *Ha R bal oldali Artin-gyűrű, $\mathcal{M}$ minimális nemtriviális R-modulus és $\Delta = \mathrm{End}_R(\mathcal{M})$, akkor $\mathcal{M}$ véges dimenziós a Δ test felett.*

Bizonyítás. Definiáljuk az $\mathbf{u}_1, \ldots, \mathbf{u}_n, \ldots$ vektorokat úgy, hogy mindegyik legyen lineárisan független az előzőektől, ha ez egyáltalán lehetséges. A 9.19. tétel szerint ekkor a $B_i = \ell(\mathbf{u}_1, \ldots, \mathbf{u}_i)$ balideálokra egy $B_1 \supset B_2 \supset \ldots$ szigorúan csökkenő láncot kapunk, amely a minimumfeltétel következtében véges. Így $\mathcal{M}$ valóban véges dimenziós. ■

2. Állítás. *Ha az $\mathcal{M}$ minimális, nemtriviális bal oldali R-modulus véges dimenziós, $\Delta = End_R(\mathcal{M})$, akkor $R/\ell(\mathcal{M}) \cong End_\Delta(\mathcal{M})$.*

Bizonyítás. A 9.14. tételben szereplő Φ gyűrűhomomorfizmus magja éppen $\ell(\mathcal{M})$. Így $\mathrm{Im}(\Phi) \cong R/\ell(\mathcal{M})$. Azt kell még belátni, hogy Φ szürjektív. Ez viszont azonnal következik a sűrűségi tételből, mert $\mathcal{M}$ véges dimenziós Δ-vektortér. ■

3. Állítás. *Ha $\mathcal{M}$ n-dimenziós vektortér a Δ test felett, akkor* $\mathrm{End}_\Delta(\mathcal{M}) \cong \Delta_n$.

Bizonyítás. Legyen $\mathbf{u}_1, \ldots, \mathbf{u}_n$ a vektortér egy bázisa, és α egy Δ-endomorfizmus. Ha $\alpha\mathbf{u}_i = a_{1,i}\mathbf{u}_1 + \cdots + a_{n,i}\mathbf{u}_n$, akkor rendeljük hozzá azt az $(n \times n)$-es $\mathbf{A}$ mátrixot, amelyben az i-edik sor j-edik eleme $a_{i,j}$. Világos, hogy az endomorfizmusok összegéhez tartozó mátrix a megfelelő mátrixok összege. A szorzat vizsgálatához legyen egy másik Δ-endomorfizmus $\beta\mathbf{u}_i = b_{1,i}\mathbf{u}_1 + \cdots + b_{n,i}\mathbf{u}_n$. Az ehhez tartozó $\mathbf{B}$ mátrixban legyen az i-edik sor j-edik eleme $b_{i,j}$. Legyen e két endomorfizmus szorzata $\gamma = \alpha\beta$ és legyen $\mathbf{C}$ a hozzájuk tartozó mátrix. Mivel α Δ-endomorfizmus, ezért:

$$\alpha\beta\mathbf{u}_i = \alpha\left(\sum_j b_{i,j}\mathbf{u}_j\right) = \sum_j b_{i,j}\alpha\mathbf{u}_j = \sum_j b_{i,j}\sum_k a_{j,k}\mathbf{u}_k = \sum_k \left(\sum_j b_{i,j}a_{j,k}\right)\mathbf{u}_k.$$

Ez pedig azt jelenti, hogy $\mathbf{C} = \mathbf{BA}$; ami duálisan izomorf Δ_n-nel (azaz sor–oszlop szorzás helyett oszlop–sor szorzás szerepel). ■

4. Állítás. *Tetszőleges Δ testre Δ_n egyszerű.*

Bizonyítás. Legyen adva egy tetszőleges $\mathbf{A} \in \Delta_n$ mátrix, amelynek valamelyik eleme nem 0. Mivel $(\delta_{i,j})$ a Δ egységeleme és az egységelem által generált ideál az egész gyűrű,

ezért elegendő annak a megmutatása, hogy $(\delta_{i,j})$ eleme az **A** generálta ideálnak. Az **A** mátrix előáll úgy, hogy olyan mátrixokat adunk össze, amelyeknek egyetlenegy eleme 1, a többi pedig 0. Világos, hogy ezek bármelyikéből megkapható akármelyikük úgy, hogy alkalmas mátrixszal balról és jobbról szorozzuk (l.: lineáris algebra). Ha az eredeti mátrix egy eleme nem 0, akkor ugyancsak alkalmas mátrixokkal való szorzás után elérhető, hogy ez az elem ne változzék, és a többi mind 0 legyen. Szorozzuk meg a kapott mátrixot a nem-0 elem inverzével, és máris kapunk egy kívánt alakú mátrixot. Δ-beli elemmel való szorzás megengedett a 10.20. tétel alapján. ■

Ezek után térjünk vissza a 10.22. tétel bizonyításához. Tekintsünk egy R féligegyszerű gyűrűt. A minimumfeltétel következtében R-nek van egy minimális B balideálja. B bal oldali R-modulus, s a minimalitás szerint minimális R-modulus. Mivel $BB \neq 0$, ezért $RB \neq 0$, azaz B nemtriviális. Ekkor $\ell({}_RB)$ ideál, így $r(\ell({}_RB))$ is ideál. Nyilvánvalóan $B \subseteq r(\ell(B))$. A $\ell(B) \cap r(\ell(B))$ balideál nilpotens, R radikálmentessége miatt tehát a metszet csak a nullelemet tartalmazza. Ebből következik, hogy az R-et az $R/\ell(B)$-be képező természetes homomorfizmus $r(\ell(B))$-t injektíven képezi 1e a maradékosztály-gyűrű egy 0-nál nagyobb ideáljára. Ez a maradékosztály-gyűrű viszont az 1. és 2. állítások miatt egyszerű; amiből azonnal következik, hogy $R = \ell(B) \oplus r(\ell(B))$. Emellett azt is tudjuk, hogy a 3. és 4. állítások következtében $r(\ell(B))$ olyan egyszerű gyűrű, amely egy test feletti teljes mátrixgyűrűvel izomorf. A bizonyítás következő lépését ugyancsak érdemes külön állításban megfogalmazni.

5. Állítás. *Ha egy féligegyszerű gyűrű két ideáljának a direkt összege, akkor mindkét ideál féligegyszerű.*

Bizonyítás. Ha egy gyűrű valamely ideáljának minden balideálja az eredeti gyűrűnek is balideálja volna, akkor az állítás triviálisan teljesülne. Ez viszont általában nem igaz. Ha azonban az ideál direkt összeadandó, akkor igaz ez a tulajdonság. Legyen $R = A \oplus B$, ahol mind A, mind B ideál. Mivel $BA, AB \subseteq B \cap A$, ezért egy B-beli és egy A-beli elem szorzata mindig 0. Ha mármost C az A-nak balideálja, akkor természetesen additív csoport. Azt kell még belátni, hogy ha $r \in R$ és $c \in C$, akkor $rc \in C$ is igaz. A direkt összeg tulajdonság szerint $r = a + b$ $(a \in A, b \in B)$ és így $rc = ac + bc$. Itt $ac \in C$, mert C balideálja A-nak; és $bc \in C$, mert – mint láttuk – $bc = 0$. ■

Most ismét visszatérünk a struktúratétel bizonyításához. Készítsük el az R ideáljainak (tehát balideáljainak) egy szigorúan csökkenő láncát. Legyen $R_0 = R$. Tegyük fel, hogy már megkonstruáltuk az $R_0 \supset R_1 \supset \ldots \supset R_n$ láncot úgy, hogy mindegyik ideál R-ben, és mindegyik direkt összeadandó is. Az 5. állítás miatt R_n is féligegyszerű, és mint azt az 5. állítás előtt beláttuk, felírható $R_n = S_{n+1} \oplus R_{n+1}$ alakban, ahol S_{n+1} egyszerű és izomorf egy test feletti teljes mátrixgyűrűvel. Ebből azonnal következik, hogy R_{n+1} is direkt összeadandó R-ben és nyilván része R_n-nek. A minimumfeltétel következtében tehát egyszer elérünk egy olyan indexhez, amikor a nullideált kapjuk. Ez azt jelenti, hogy $R = S_1 \oplus \ldots \oplus S_k$, vagyis R felírható a kívánt módon.

Most belátjuk, hogy 4.-ből következik 5. Ha tekintünk egy test feletti teljes mátrixgyűrűt, akkor azok a mátrixok, amelyeknek egy rögzített oszlopán kívül csupa 0-k állnak, nyilvánvalóan egy minimális balideált alkotnak. Az is világos, hogy ezeknek a balideáloknak a direkt összege létezik és kiadja a teljes mátrixgyűrűt. A 4. feltételből tehát következik, hogy a gyűrű egységelemes és véges sok minimális balideáljának a direkt összege.

Végezetül azt mutatjuk meg, hogy 5.-ből következik 1. Azt sem kell feltenni, hogy a fellépő balideálok száma véges, ez következik az egységelemességből. Valóban, legyen R a B_i balideálok direkt összege, és legyen e_i az 1 egységelemnek B_i-be eső komponense. Az $a = a \cdot 1 = \sum_i a \cdot e_i$ felírásból következik, hogy $a \cdot e_i \in B_i$, mert B_i balideál; és $a \in$ $\in B_i$ esetén az is adódik, hogy e_i a B_i (jobb oldali) egységeleme. Mivel a fenti összegben csak véges sok tag különbözhet 0-tól, ezért a fellépő balideálok száma véges. (Persze, léteznek más minimális balideálok is, mint a mátrixgyűrűk szerkezetéből ismeretes.) Mivel minden e_i idempotens, ezért a fellépő balideálok nem nilpotensek. Tekintsük most az Ra balideált, ahol $a \in B_i$ és $a \neq 0$. Világos, hogy azok a B_i-beli elemek, amelyekre ez a balideál $\{0\}$, maguk is egy B_i' balideált alkotnak. $B_i' \neq B_i$, mert $e_i \neq 0$. A B_i minimalitása következtében tehát csak $B_i' = \{0\}$ lehet. Eszerint csak $Ra = B_i$ lehet; és érvényes az $R = B_1 \oplus \cdots \oplus B_r$ felírás.

Legyen most $\mathcal{M}$ unitér bal oldali R-modulus, és tekintsük ennek egy $\mathbf{o}$-tól különböző $\mathbf{a}$ elemét. Az $(r+s)\mathbf{a} = r\mathbf{a} + s\mathbf{a}$ és $t(r\mathbf{a}) = (tr)\mathbf{a}$ azonosságokból következik, hogy $B_i\mathbf{a} = \{r\mathbf{a} \mid r \in R\}$ az $\mathcal{M}$-nek részmodulusa. $1 \cdot \mathbf{a} = \mathbf{a}$ miatt $\mathbf{a}$ eleme a $B_1\mathbf{a}, \ldots, B_r\mathbf{a}$ részmodulusok generátumának. Legyen most $\mathbf{b} = r\mathbf{a}$ a $B_i\mathbf{a}$ tetszőleges eleme. Ebből $R\mathbf{b} = Rr\mathbf{a} = B_i\mathbf{a}$ következik, és itt $B_i\mathbf{a}$ minimális részmodulus. Eszerint $\mathcal{M}$ minden eleme benne van véges sok minimális részmodulus generátumában.

Tekintsük most az $\mathcal{M}$ egy tetszőleges $\mathcal{A}$ részmodulusát. A Zorn-lemma alapján létezik $\mathcal{M}$-ben olyan maximális $\mathcal{B}$ részmodulus, amelyre $\mathcal{A} \cap \mathcal{B} = \{0\}$. Ez azt is jelenti, hogy létezik az $\mathcal{A} \oplus \mathcal{B}$ direkt összeg. Azt fogjuk megmutatni, hogy ez a direkt összeg megegyezik $\mathcal{M}$-mel, amihez elég azt bizonyítani, hogy $\mathcal{A}$ és $\mathcal{B}$ együttesen generálják $\mathcal{M}$-et. Mint láttuk, minden elem benne van véges sok minimális részmodulus generátumában, ezért elég azt bizonyítani, hogy az $\mathcal{A} \oplus \mathcal{B}$ generátum tartalmaz minden minimális részmodulust.

Legyen $\mathcal{N} \leq \mathcal{M}$ minimális részmodulus. Ha $\mathcal{N} \subseteq \mathcal{B}$, akkor természetesen része a generátumnak. Egyébként $\mathcal{B}$ maximalitása miatt $\langle \mathcal{N}, \mathcal{B} \rangle \cap \mathcal{A}$ tartalmaz egy $\mathbf{a} \neq \mathbf{o}$ elemet. Mivel $\mathbf{a} \in \langle \mathcal{N}, \mathcal{B} \rangle$, ezért felírható (nem feltétlenül egyértelműen) $\mathbf{a} = \mathbf{n} + \mathbf{b}$ alakban ($\mathbf{n} \in \mathcal{N}$, $\mathbf{b} \in \mathcal{B}$), ahol persze $\mathbf{a} \in \mathcal{A}$. Mivel $\mathcal{A} \cap \mathcal{B} = \{\mathbf{o}\}$ és $\mathbf{a} \neq \mathbf{o}$, ezért $\mathbf{n} \neq \mathbf{o}$. Így $\mathbf{n} = \mathbf{a} - \mathbf{b} \in$ $\in \mathcal{A} \oplus \mathcal{B}$, amiből következik, hogy a direkt összeg tartalmazza az $\mathbf{n}$ generálta részmodulust. $\mathcal{N}$ minimalitása alapján az $\mathbf{n}$ generálta $R\mathbf{n}$ részmodulus – mint bizonyítottuk – megegyezik $\mathcal{N}$-nel; és ezért $\mathcal{N}$ valóban része a generátumnak. ■

Megjegyzések. 1. A 10.22. tételben szereplő 4. állítás szimmetrikus. Ez azt jelenti, hogy a feltételek bármelyikével ekvivalens minden olyan feltétel is, amely úgy adódik, hogy a „bal” és „jobb” szavakat felcseréljük.

2. A fenti tételt algebrákra (lásd a következő részt) J. H. Wedderburn bizonyította. Az itt közölt bizonyítás Szele Tibor gondolatán alapszik. □

10.5. Algebrák, csoportalgebra

Tetszőleges félcsoport (vagy csoport) esetén ennek elemeit tekinthetjük úgy, mintha egy adott test feletti vektortér báziselemei volnának. Ezáltal a félcsoport elemei e vektortér lineáris transzformációivá válnak. A transzformációkat viszont nem csak szorozni, de összeadni is lehet. Így egy sokkal gazdagabb struktúrafajtát kapunk, amely olyan össze-

függésekre is rámutat, amelyek eleve „rejtve voltak”. Az alaptulajdonságok leírásánál itt is célszerű egy olyan absztrakció, mint amivel a permutációcsoportokból az absztrakt csoportokat nyertük.

10.23. Definíció. Az R gyűrű algebra a K test felett, ha unitér modulus a K test felett, a modulus-összeadás és a gyűrűösszeadás megegyezik, és tetszőleges $a \in K$, $\mathbf{a}, \mathbf{b} \in R$ esetén teljesül az $a(\mathbf{ab}) = (a\mathbf{a})\mathbf{b} = \mathbf{a}(a\mathbf{b})$ összefüggés. □

Megjegyzések. 1. Mint a modulusoknál általában, az R elemeit lehetőleg vastagított betűkkel jelöljük. Ha célszerű, akkor az $a\mathbf{a}$ jelölés helyett az $a \cdot \mathbf{a}$ jelölést fogjuk használni.

2. A definícióban leírt azonosságból következik, hogy az $a, b \in K$ és $\mathbf{a}, \mathbf{b} \in R$ elemekre teljesül az $(ab - ba) \cdot (\mathbf{ab}) = \mathbf{o}$ egyenlőség. Ebből következik az is, hogy egységelemes algebrákban például $ab-ba$ minden elemet $\mathbf{o}$-ba visz. Ezek az elemek tehát egy ideálban vannak, amely testekről lévén szó vagy az egész, vagy 0. Ha minden elem 0-ba viszi a modulus elemeit, akkor teljesen érdektelen esetről van szó, ha nem, akkor ez a test kommutativitását jelenti. Ez indokolja, hogy csak kommutatív test feletti algebrákról beszélünk. Lehet test helyett tetszőleges gyűrűt tekinteni, de ekkor is érdemesebb csak kommutatív gyűrűket nézni.

3. Egy K (kommutatív) test feletti algebrák esetében minden további nélkül használni fogjuk a gyűrűelméleti és moduluselméleti fogalmakat, azzal a megkötéssel, hogy „rész-” esetében mindig olyan részt értünk, amely mindkét értelemben résznek tekinthető (részalgebra, ideál).

4. Az algebratulajdonságok olyan erősek, hogy már ezeknek egy része is igen sok gyakran előforduló struktúratípust ad. Nagyon fontos olyan algebrák ismeretesek, ahol a gyűrűaxiómák nem mind teljesülnek. Ezek közül is kiemelkednek a nem asszociatív algebrák, ahol R-ben a gyűrűtulajdonságok az asszociativitás kivételével teljesülnek.

5. Ha az algebrának mint vektortérnek egy bázisát tekintjük, akkor ezek szorzása a disztributivitás alapján már meghatározza az összes szorzatot. Éppen ezért megadható e szorzásokra egy – elég bonyolult – szükséges és elégséges feltétel, amely biztosítja az asszociativitást. □

10.24. Tétel. *Ha a K test feletti R algebra egységelemes, akkor tartalmaz egy K-val izomorf részalgebrát. A K egy elemével való szorzás ugyanazt adja, mint a megfelelő belső elemmel való szorzás.*

Bizonyítás. Legyen $\mathbf{e}$ az R egységeleme. Ha tetszőleges $a \in K$ elemnek megfeleltetjük az $a\mathbf{e}$ elemet, ezáltal nyilvánvalóan egy K-val izomorf részalgebrát kapunk; s a további állítás az $(a\mathbf{e})\mathbf{a} = a(\mathbf{ea}) = a\mathbf{a}$ következménye. ■

Megjegyzések. 1. A 10.24. tétel alapján egységelemes algebrák esetében mindig feltehetjük, hogy az adott test része a szóban forgó algebrának.

2. Egységelemes algebrára számos példát ismerünk. Egy test felett algebra annak minden algebrai vagy transzcendens bővítése. Algebra a felette vett akárhány határozatlanú polinomgyűrű vagy a felette vett $(n \times n)$-es teljes mátrixgyűrű. □

A továbbiakban egy igen fontos „algebrafajtát” konstruálunk.

10.25. Tétel. *Adott S félcsoport esetén tekintsük az S mint szabad generátorrendszer generálta szabad K modulust. E modulusban pontosan egy olyan szorzás értelmezhető, amelynek S-re való megszorítása megegyezik az S-beli szorzással, és amelyre ez K feletti algebra. A kapott K_S algebrát az S félcsoport K feletti félcsoportalgebrájának nevezzük.*

Bizonyítás. K_S elemei mint szabad modulus elemei, egyértelműen felírhatók $a_1\mathbf{s}_1 + \dots + a_n\mathbf{s}_n$ alakban, ahol $a_i \in K$ és $\mathbf{s}_i \in S$. Ezeknek az összeadása és K-beli elemmel

való szorzása már eleve értelmezett. Ha az előbbivel együtt még egy másik $b_1\mathbf{t}_1 + \cdots + b_k\mathbf{t}_k$ elem is adott ($b_j \in K$, $\mathbf{t}_j \in S$), akkor ezek szorzata az algebraazonosságok szerint éppen az összes $(a_i b_j)\mathbf{s}_i\mathbf{t}_j$ alakú elemek összege lesz. Egyszerű számolással belátható, hogy az így értelmezett szorzattal valóban K feletti algebrát kapunk, az asszociativitás az S-beli és K-beli szorzás asszociativitásából következik. ■

Megjegyzések. 1. Ha a félcsoport egységelemes, akkor ez az egységelem egyszersmind az algebrának is egységeleme.

2. Tanulságos példa az az eset, amikor a félcsoport bizonyos elemek által szabadon generált monoid. Ekkor a félcsoportalgebra nem más, mint a K test feletti polinomgyűrű; a határozatlanok éppen a félcsoport generátorelemei. □

Különösen fontos speciális eset a következő:

10.26. Definíció. Ha a félcsoport csoport, akkor a félcsoportalgebrát csoportalgebrának nevezzük. □

10.27. Tétel (Maschke)**.** *Ha G n-edrendű csoport, akkor a K_G csoportalgebra pontosan akkor féligegyszerű gyűrű, ha K karakterisztikája nem osztója a csoport rendjének.*

Bizonyítás. Tegyük fel először, hogy K karakterisztikája osztója a csoport rendjének. Ebből azonnal következik, hogy a karakterisztika egy p prímszám (tehát nem 0). Legyen most $\eta = \mathbf{g}_1 + \cdots + \mathbf{g}_n$, ahol a jobb oldalon a G csoport (mint K_G-modulus!) minden egyes eleme pontosan egyszer lép fel. Világos, hogy a G csoport bármely g elemére teljesül a $g\eta = \eta$ összefüggés. Így az η generálta egydimenziós altér ideál. Adódik továbbá az $\eta^2 = n\eta$ összefüggés, ami a karakterisztikafeltétel miatt éppen azt jelenti, hogy ez az ideál nilpotens.

Tegyük most fel, hogy n nem osztható K karakterisztikájával. A Wedderburn–Artin-struktúratétel alapján elég azt bebizonyítani, hogy ebben az esetben tetszőleges $\mathcal{M}$ bal oldali unitér K_G-modulusnak bármely $\mathcal{M}'$ részmodulusa direkt összeadandója is. Tekintettel arra, hogy $\mathcal{M}$ egyszersmind vektortér is a K test felett, ezért létezik az $\mathcal{M}$-nek olyan $\mathcal{M}''$ altere, amelyre $\mathcal{M} = \mathcal{M}' \oplus \mathcal{M}''$. Ez azt jelenti, hogy $\mathcal{M}$-nek tetszőleges $\mathbf{a}$ eleme egyértelműen felírható $\mathbf{a} = \mathbf{a}' + \mathbf{a}''$ alakban, ahol $\mathbf{a}' \in \mathcal{M}'$ és $\mathbf{a}'' \in \mathcal{M}''$. Ebből a $g\mathbf{a} = g\mathbf{a}' + g\mathbf{a}''$ összefüggéshez jutunk, ahol g tetszőleges eleme a G csoportnak. Mivel $\mathcal{M}'$ részmodulus, ezért $g\mathbf{a}' \in \mathcal{M}'$, és így $(g\mathbf{a}')'' = \mathbf{o}$. Ebből a $g\mathbf{a} = g\mathbf{a}' + g\mathbf{a}''$ felírásnál $g\mathbf{a}$-nak az $\mathcal{M}''$-be eső komponensét meghatározva a

$$(g\mathbf{a})'' = (g\mathbf{a}'')'' \tag{I}$$

összefüggéshez jutunk. Ezek után definiáljuk az $\mathcal{M}$ tetszőleges $\mathbf{a}$ eleméhez az

$$\overline{\mathbf{a}} = \frac{1}{n}\sum_{g\in G} g^{-1}(g\mathbf{a})'' \tag{II}$$

elemet, ahol tehát az összegzésben g végigfut a G csoport elemein. Mivel n nem osztható a K karakterisztikájával, ezért $1/n$ értelmes. Triviálisan belátható, hogy $\overline{(\mathbf{a}+\mathbf{b})} = \overline{\mathbf{a}} + \overline{\mathbf{b}}$ és $\overline{c\mathbf{a}} = c\overline{\mathbf{a}}$, ahol $\mathbf{a}, \mathbf{b} \in \mathcal{M}$ és $c \in K$. Ez azt jelenti, hogy a (II) alatt definiált elemek $\mathcal{M}$-nek egy $\overline{\mathcal{M}}$ alterét alkotják. Kimutatjuk, hogy $\overline{\mathcal{M}}$ részmodulus. Tekintettel arra, hogy G elemei K_G-nek bázisát alkotják, ezért elég azt belátni, hogy tetszőleges rögzített $h \in G$ esetén

$h\overline{\mathbf{a}} = \overline{h\mathbf{a}}$, és így $h\overline{\mathbf{a}} \in \overline{\mathcal{M}}$. Amennyiben az $\overline{\mathbf{a}}$ definíciójában szereplő g végigfut G elemein, akkor vele együtt $k = gh$ is végigfut G elemein. A $k = gh$ összefüggésből azt is kapjuk, hogy $g^{-1} = g^{-1}kk^{-1} = g^{-1}ghk^{-1} = hk^{-1}$. Mármost

$$\overline{h\mathbf{a}} = \frac{1}{n}\sum_{g\in G} g^{-1}(gh\mathbf{a})'' = \frac{1}{n}\sum_{k\in G} hk^{-1}(k\mathbf{a})'' = h\cdot\frac{1}{n}\sum_{k\in G} k^{-1}(k\mathbf{a})'' = h\cdot\overline{\mathbf{a}}.$$

Így valóban $h\overline{\mathbf{a}} \in \overline{\mathcal{M}}$. Az (I) alatti összefüggés felhasználásával a következőket nyerjük:

$$\text{(III)} \qquad (\overline{\mathbf{a}})'' = \frac{1}{n}\sum_{g\in G}(g^{-1}(g\mathbf{a})'')'' = \frac{1}{n}\sum_{g\in G}(g^{-1}g\mathbf{a})'' = \frac{1}{n}(n\mathbf{a}'') = \mathbf{a}'',$$

felhasználva, hogy a (II)-ben definiált összegnek n tagja van. A (III) alatti összefüggésből azonnal kapjuk, hogy $(\mathbf{a} - \overline{\mathbf{a}})'' = \mathbf{o}$; ami az eredeti felbontás szerint azt jelenti, hogy $\mathbf{a} - \overline{\mathbf{a}} \in \mathcal{M}'$. Eszerint az $\mathcal{M}'$ és $\overline{\mathcal{M}}$ részmodulusok generálják az $\mathcal{M}$ modulust. Ahhoz, hogy $\mathcal{M}$ e két modulus direkt összege (ami bizonyítja, hogy $\mathcal{M}'$ direkt összeadandó), azt kell még belátni, hogy e két modulusnak csak $\mathbf{o}$ a közös eleme. Ha $\overline{\mathbf{a}} \in \mathcal{M}'$, akkor $(\overline{\mathbf{a}})'' = \mathbf{o}$, ami (III) szerint az $\mathbf{a}'' = \mathbf{o}$ összefüggéshez vezet. Így $\mathbf{a} \in \mathcal{M}'$, tehát $g\mathbf{a} \in \mathcal{M}'$, mert $\mathcal{M}'$ részmodulus. Ekkor viszont $(g\mathbf{a})'' = \mathbf{o}$, a G tetszőleges g elemére, amiből természetesen $g^{-1}(ga)'' = \mathbf{o}$ is következik. A (II) alatti definíció szerint tehát $\overline{\mathbf{a}} = \mathbf{o}$, amit bizonyítanunk kellett. ■

Tegyük most fel, hogy a K karakterisztikája nem osztója G rendjének, amikor is Maschke tétele szerint a csoportalgebrának létezik egy teljes mátrixgyűrűk direkt összegére való

$$K_G = R_1 \oplus \cdots \oplus R_s$$

felbontása. E mátrixgyűrűkben a mátrixok elemei természetesen nem szükségképpen K-beliek, hanem egy-egy, nála bővebb $F_1, \ldots, F_s$ testből valók. Ezek a testek általában nem is kommutatívak, és nem is feltétlen megegyezőek. Tegyük fel, hogy például az első r darab test megegyezik (lehet, hogy ezeken felül is van olyan mátrix, amelynek az elemei ugyanebből a testből valók). Ekkor a mátrixfelírás úgy adható meg, hogy ezeket egy nagyobb mátrixba foglaljuk. Ha e mátrixoknak rendre $i_1, \ldots, i_r$ sora és oszlopa van (persze $r \le s$), akkor egy olyan mátrixot készíthetünk, amelyben a sorok és oszlopok száma $i_1 + \cdots + i_r$, és a mátrix r számú blokkból áll, amelyekben a sorok (és oszlopok) száma rendre $i_1, \ldots, i_r$. Ilyen módon a csoport elemeinek megfeleltettünk egy-egy mátrixot, amelyekre nyilvánvalóan igaz, hogy a szorzatnak megfeleltetett mátrix a megfelelő mátrixok szorzata; azaz a megfeleltetés homomorfizmus.

10.28. Definíció. Egy G (véges) csoportnak egy F (nem feltétlen kommutatív) test feletti $(n \times n)$-es mátrixok multiplikatív félcsoportjába képező homomorfizmusát n-edfokú reprezentációnak nevezik. Ha a homomorfizmus injektív, akkor hű reprezentációról beszélünk. Ha a homomorfizmust a csoportalgebrára kiterjesztve e homomorfizmus magja egy maximális ideál, akkor azt mondjuk, hogy a reprezentáció irreducibilis. □

Megjegyzések. 1. Könnyen látható, hogy pontosan akkor kapunk irreducibilis reprezentációt, ha a csoportalgebra felbontásában egyetlen egyszerű komponenst veszünk figyelembe.

2. Minden csoportnak van egy triviális reprezentációja, nevezetesen az, amikor minden elemet az egységelemre képezünk le. Azt is könnyű belátni, hogy minden (véges) csoportnak van hű reprezentációja. Tekintsük ugyanis a vizsgált test feletti csoportalgebrát. A csoportelemek ennek egy

bázisát alkotják. Ha e bázist balról megszorozzuk egy-egy csoportelemmel, akkor ez lineáris transzformációt hoz létre, amelynek mátrixában minden sorban pontosan egy egyes áll, s a többi elem 0. Könnyen ellenőrizhető, hogy ez a megfeleltetés hű reprezentáció.

3. Egyszerű csoportok nemtriviális reprezentációja nyilván csak hű lehet. Mivel egy mátrixnak megfeleltetve a determinánsát, ugyancsak szorzathomomorfizmust kapunk, ezért a most tárgyalt reprezentációban minden csoportelemnek egy ± 1-determinánsú mátrix felel meg. Ez indokolja, hogy a véges egyszerű csoportok keresésekor olyan fontos szerepet játszanak a ± 1-determinánsú mátrixok csoportjai. □

A következő tételre a későbbiekben is szükségünk lesz:

10.29. Tétel. *Egy test feletti véges dimenziós algebra minden eleme algebrai e test felett.*

Bizonyítás. Legyen $\mathbf{a}$ a K test feletti véges dimenziós $\mathcal{A}$ algebra egy eleme. A dimenzió végessége miatt az $\mathbf{a}, \mathbf{a}^2, \ldots$ elemek nem lehetnek mind lineárisan függetlenek; amiből triviálisan adódik, hogy $\mathbf{a}$ gyöke egy K-beli együtthatós (nem-0) polinomnak. ■

Igen fontos speciális esetet tárgyal a következő:

10.30. Tétel. *Ha K algebrailag zárt, akkor a K_G felbontásában szereplő minden egyes teljes mátrixgyűrű elemei K-ból valók.*

Bizonyítás. Tekintsük a K_G felbontásában szereplő bármelyik R_i teljes mátrixgyűrűt. Mivel ez részalgebra, ezért algebra a K test felett. Az az F_i test, amely felett R_i teljes mátrixgyűrű, izomorf a skalármátrixok gyűrűjével. Tekintettel arra, hogy a skalármátrixok ugyancsak algebrát alkotnak K felett, ezért úgy tekinthetjük, hogy F_i is algebra K felett. Mivel F_i egységelemes, ezért a 10.24. tétel szerint feltehető, hogy $K \leq F_i$, és az algebratulajdonságok következtében benne van F_i centrumában (azaz elemei az F_i minden elemével felcserélhetők). Legyen $\mathbf{a} \in F_i$. Tekintettel arra, hogy G véges, $K(\mathbf{a})$ a K-nak véges algebrai bővítése. Amennyiben K algebrailag zárt, akkor ez csak az $\mathbf{a} \in K$ esetben lehet, azaz $F_i = K$. ■

Most ismét egy általános tételt bizonyítunk be gyűrűk centrumáról, amely a későbbiekben is fontos szerepet játszik.

10.31. Tétel. *Direkt összeg centruma megegyezik a centrumok direkt összegével.*

Bizonyítás. A kényelem kedvéért kéttagú direkt összegre végezzük a bizonyítást. Ebből teljes indukcióval bizonyíthatunk véges sok tagú direkt összegre. (Ennek alapján a tétel triviálisan következik végtelen sok tagúra is, de erre nem lesz szükségünk.)

Legyen $R = A \oplus B$. Az $a + b$ elem ($a \in A$, $b \in B$) akkor és csak akkor eleme R centrumának, ha minden $x + y$ alakú elemmel felcserélhető ($x \in A$, $y \in B$). Mivel a direkt összeg tulajdonság szerint $ay, ya, bx, xb \in A \cap B = \{0\}$, ezért a felcserélhetőség az $ax + by = xa + yb$ egyenlőség teljesülésével ekvivalens. Az összegként való felírás egyértelműsége miatt a fenti egyenlőség pontosan akkor teljesül, ha $ax = xa$ és $by = yb$. ■

10.32. Definíció. Legyen K algebrailag zárt test, és legyen $K_G = R_1 \oplus \cdots \oplus R_s$ a csoportalgebrának teljes mátrixgyűrűkre való direkt felbontása. A csoport elemeinek megfeleltetve az elem i-edik komponensre való vetületének a nyomát (azaz a főátlóban

álló elemeinek az összegét), egy $\chi : G \to K$ függvényt kapunk, amelyet az i-edik csoportkarakternek nevezünk. □

Megjegyzés. Noha a fellépő mátrixok nem egyértelműek, az bizonyítható, hogy a csoportkarakterek igen. Erre csupán bizonyos esetekben lesz szükségünk, amikor ezt majd külön belátjuk. □

10.33. Tétel. *Egydimenziós komponensekhez tartozó karakterek multiplikatívak (tehát homomorfizmusok). Az egydimenziós komponensek és a multiplikatív karakterek (azaz a $\chi : G \to K$ homomorfizmusok) egyértelműen meghatározzák egymást.*

Bizonyítás. Legyen R_i egydimenziós, és legyen $\mathbf{e}$ az egységeleme. Ekkor van olyan $\varphi : G \to K$ függvény, hogy tetszőleges $\mathbf{g} \in G$ esetén feltétel szerint $\mathbf{ge} = \varphi(\mathbf{g})\mathbf{e}$. A $\mathbf{g} \mapsto \varphi(\mathbf{g})$ megfeleltetés (amely éppen az i-edik karakter) nyilvánvalóan multiplikatív. Ha valamelyik $\varphi(\mathbf{g}) = 0$ volna, akkor multiplikativitás alapján nyilván tetszőleges $\mathbf{h} \in G$ esetén $\varphi(\mathbf{h}) = \varphi(\mathbf{g})\varphi(\mathbf{g}^{-1}\mathbf{h})$ is 0 volna, azaz $\mathbf{e}$ a csoportalgebrát annullálná – ellentétben a radikálmentességgel. Írjuk fel $\mathbf{e}$-t

$$\mathbf{e} = \sum_{\mathbf{g}\in G} c_{\mathbf{g}}\mathbf{g} \qquad (c_{\mathbf{g}} \in K)$$

alakban, ahol tehát $\mathbf{g}$ végigfut G elemein. Ebből tetszőleges $\mathbf{h} \in G$ esetén $\mathbf{he} = \varphi(\mathbf{h}) \cdot \mathbf{e}$ alapján $\sum_{\mathbf{g}\in G} c_{\mathbf{g}} \cdot \mathbf{hg} = \sum_{\mathbf{g}\in G} \varphi(\mathbf{h})c_{\mathbf{g}} \cdot \mathbf{g}$ adódik. Mivel $\mathbf{g}$-vel együtt – rögzített $\mathbf{h}$ esetén – $\mathbf{hg}$ is végigfut a csoport elemein, amelyek a csoportalgebra egy bázisát alkotják, ezért a kapott egyenlőségből – komponensekre térve – a $c_{\mathbf{g}} = \varphi(\mathbf{h})c_{\mathbf{hg}}$ összefüggést kapjuk. A $\mathbf{g} = 1$ esetben a $\varphi(\mathbf{h}) = c_1/c_{\mathbf{h}}$ eredmény adódik (figyelembe véve, hogy $\varphi(\mathbf{h}) \neq 0$ és $\mathbf{e} \neq \mathbf{o}$). Így minden egydimenziós komponens a fenti módon meghatároz egy multiplikatív karaktert.

Legyen most $\varphi : G \to K$ egy multiplikatív karakter (azaz csoporthomomorfizmus), amely nem azonosan 0. Az

$$\mathbf{x} = \sum_{\mathbf{g}\in G} \varphi(\mathbf{g}^{-1}) \cdot \mathbf{g}$$

elemre

$$\mathbf{hx} = \sum_{\mathbf{g}} \varphi(\mathbf{g}^{-1}\mathbf{h}^{-1}\mathbf{h}) \cdot \mathbf{hg} = \varphi(\mathbf{h}) \cdot \sum_{\mathbf{hg}} \varphi((\mathbf{hg})^{-1}) \cdot \mathbf{hg} = \varphi(\mathbf{h}) \cdot \mathbf{x},$$

$$\mathbf{xh} = \sum_{\mathbf{g}} \varphi(\mathbf{hh}^{-1}\mathbf{g}^{-1}) \cdot \mathbf{gh} = \varphi(\mathbf{h}) \cdot \sum_{\mathbf{gh}} \varphi((\mathbf{gh})^{-1}) \cdot \mathbf{gh} = \varphi(\mathbf{h}) \cdot \mathbf{x}$$

teljesülnek. Így $\mathbf{x}$ egy egydimenziós ideált generál, amely a féligegyszerűség miatt előfordul a komponensek között. Ezért alkalmas c-vel $c\mathbf{x}$ ennek a komponensnek az egységeleme: $\mathbf{e} = \sum_{\mathbf{g}} c\varphi(\mathbf{g}^{-1}) \cdot \mathbf{g}$. A két eljárást egymás után elvégezve (bármelyikkel kezdve), triviálisan visszajutunk az eredetihez, ami azt jelenti, hogy e leképezések és e komponensek egyértelműen meghatározzák egymást. ■

10.34. Tétel. *Egy csoport multiplikatív karakterei a $\varphi\psi : \mathbf{g} \mapsto \varphi(\mathbf{g})\psi(\mathbf{g})$ szorzásra csoportot alkotnak. A $\sum_{\mathbf{g}} \varphi(\mathbf{g})\psi^{-1}(\mathbf{g})$ szorzatösszeg értéke rögzített φ és ψ esetén vagy 0, vagy $|G|$ attól függően, hogy φ és ψ különbözőek vagy megegyeznek.*

Bizonyítás. A tételben definiált szorzat nyilván ismét multiplikatív karakter. Az is világos, hogy a szorzás asszociatív. Az a karakter, amelyik minden csoportelemnek az 1-et felelteti meg, e félcsoport egységeleme; és egy karakter inverze az a karakter, amely minden egyes csoportelemhez az eredeti kép inverzét rendeli hozzá. Tekintsük most az $\mathbf{e} = \sum_{\mathbf{g}} a\varphi(\mathbf{g}^{-1})\mathbf{g}$ és $\mathbf{f} = \sum_{\mathbf{h}} b\varphi(\mathbf{h}^{-1})\mathbf{h}$ idempotens elemeket, amelyek mindegyike egydimenziós részalgebrát generál. Ezek szorzatában írjunk $\mathbf{g}$ helyébe $\mathbf{th}^{-1}$-et:

$$\mathbf{ef} = \sum_{\mathbf{h},\mathbf{t}} ab\varphi(\mathbf{h})\psi(\mathbf{h}^{-1})\varphi(\mathbf{t}^{-1})\mathbf{t} = \left(\sum_{\mathbf{h}} b\varphi(\mathbf{h})\psi(\mathbf{h}^{-1})\right)\cdot \mathbf{e}.$$

Az $\mathbf{e} \neq \mathbf{f}$ esetben a szorzat $\mathbf{o}$, míg egyenlőség esetén $\mathbf{e}$. A jobb oldalon $\mathbf{e}$ együtthatóját a következőképpen határozhatjuk meg: A karakter szorzattartásából és az inverzének a definíciójából $\psi(\mathbf{h}^{-1}) = (\psi(\mathbf{h}))^{-1} = \psi^{-1}(\mathbf{h})$. Azt kell csupán még belátni, hogy $b = 1/|G|$. Ezt úgy kapjuk, hogy az $\mathbf{e} = \mathbf{f}$ esetet nézzük, amikor az $1 = \sum_{\mathbf{g}} b$, ami $n \cdot |G|$, mert a jobb oldalon a tagok száma megegyezik G rendjével. ■

10.35. Tétel. *A multiplikatív karakterek száma akkor és csak akkor egyezik meg a csoport elemeinek a számával, ha a csoport kommutatív. Ekkor rögzített csoportelemekkel az összes karakterre elkészítve a* $\sum_{\varphi} \varphi(\mathbf{g}) \cdot \varphi(\mathbf{h}^{-1})$ *összeget, ez vagy* 0*, vagy* $|G|$*, attól függően, hogy a két csoportelem különbözik-e vagy sem.*

Bizonyítás. A multiplikatív karakterek száma akkor és csak akkor egyenlő a csoport elemszámával, ha minden egyes direkt összeadandó egydimenziós. Mivel egy teljes mátrixgyűrű pontosan akkor kommutatív, ha egydimenziós, ezért a feltétel a csoportalgebra kommutativitásával ekvivalens. Ez pedig nyilvánvalóan ugyanazt jelenti, mint a csoport kommutativitása.

A fenti összeget $\sum_{\varphi} \varphi(\mathbf{gh}^{-1})$ alakba írhatjuk, amikor is az állítás a következőkkel válik ekvivalenssé: $\sum_{\varphi} \varphi(\mathbf{g})$ rögzített csoportelemre vagy 0, vagy a csoport elemszámát adja, annak megfelelően, hogy a szereplő csoportelem különbözik-e az egységelemtől vagy sem. Mint a 10.34. tételben láttuk, az egyes komponensek egységeleme $(1/|G|) \cdot \sum_{\mathbf{g}} \varphi(\mathbf{g})\mathbf{g}^{-1}$ alakú. Mivel ezek éppen a csoportalgebra egységelemének a komponensei, ezért összegük az egységelem, ami egyszersmind a csoport egységeleme is. Ezt az összeget az eredeti bázisban felírva minden egyes komponens együtthatója 0 lesz, kivéve az egységelemét, ami 1. Más szóval, ha egy rögzített $\mathbf{g}$ elemre az összes $\varphi(g^{-1})/|G|$ elemet összeadjuk, ez 1, ha $\mathbf{g}$ az egységelem és 0 egyébként. ■

Megjegyzés. A multiplikatív karakterek nullkarakterisztikájú test és egy kommutatív G csoport esetében pontosan a Hom $(G, \mathbf{C})$ csoport elemei, ahol $\mathbf{C}$ a komplex egységgyökök csoportja. Kimutatható, hogy véges Abel-csoportokra a karaktercsoport az eredeti csoporttal izomorf. □

Ha egy csoportalgebra szerkezetét meg akarjuk adni, vagy más szóval, meg szeretnénk határozni egy csoport reprezentációit, akkor eleve bizonyos támpontot adnak a következők:

algebrailag zárt test felett a komponensek dimenziója négyzetszám. A dimenziók összege éppen a csoport elemszáma. Csak az okoz gondot, hogy hány komponens lép fel. Erre válasz a következő:

10.36. Tétel. *Ha az algebrailag zárt K test feletti csoportalgebrának teljes mátrixgyűrűk direkt összegére való felbontása $K = R_1 \oplus \cdots \oplus R_s$, akkor s megegyezik a csoport konjugált elemosztályainak a számával.*

Bizonyítás. Világos, hogy egy teljes mátrixgyűrű centruma éppen azokból a mátrixokból áll, amelyek az egységelem skalárszorosai. Így tehát a centrum egydimenziós. A 10.31. tétel szerint tehát K_G centruma s-dimenziós. Nézzük most meg, hogy egy $\mathbf{u} = \sum_{\mathbf{g}} c_{\mathbf{g}}\mathbf{g}$ elem mikor tartozik a centrumhoz. Ha $\mathbf{u}$ eleme a centrumnak, akkor természetesen G minden $\mathbf{h}$ elemével is felcserélhető. Ez viszont fordítva is igaz, mert G elemei az algebrának egy bázisát alkotják. Mivel G elemeinek van inverze, ezért a felcserélhetőséget $\sum_{\mathbf{g}} c_{\mathbf{g}}\mathbf{g} = \sum_{\mathbf{g}} c_{\mathbf{g}}\mathbf{h}^{-1}\mathbf{g}\mathbf{h}$ alakban írhatjuk fel. Tekintettel arra, hogy a csoportelemek az algebra egy bázisát alkotják, a fenti egyenlőség komponensenkénti egyenlőséggel ekvivalens: $c_{\mathbf{hgh}^{-1}} = c_{\mathbf{g}}$. Ennek tetszőleges $\mathbf{h}$ esetén teljesülnie kell, ami azt jelenti, hogy egy csoportelemnek ugyanaz az együtthatója, mint bármelyik konjugáltjának. Tegyük fel, hogy a konjugált elemosztályok száma r, és jelölje $\mathbf{v}_1, \ldots, \mathbf{v}_r$ az egyes osztályok elemeinek az összegét. A megállapítottak szerint a centrumelemek pontosan ezeknek a $\mathbf{v}_1, \ldots, \mathbf{v}_r$ elemeknek a lineáris kombinációi; tehát a centrum r-dimenziós, következésképpen $s = r$. ■

Az eljárás megvilágítására célszerű példaképpen néhány kis elemszámú permutációcsoport reprezentációinak az alakját meghatározni. Maguknak a reprezentációknak a meghatározása sokkal bonyolultabb.

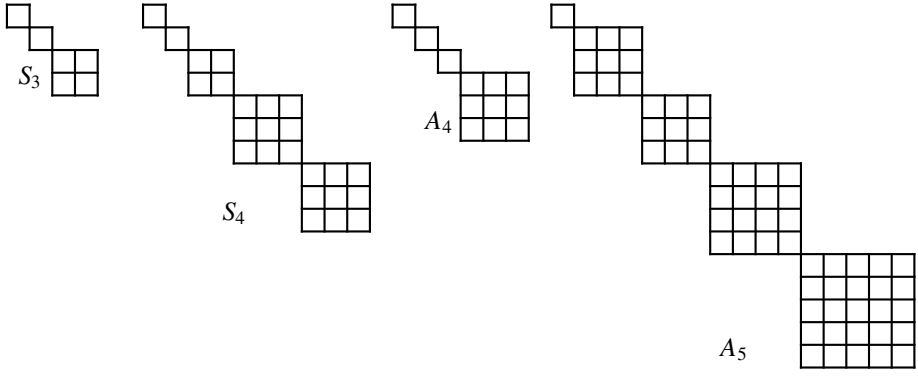
1) S_3 elemeinek a száma 6. Két permutálás pontosan akkor konjugált, ha ciklusfelbontásaik azonos típusúak. Így a konjugált elemosztályok: az egységelem, a kettes ciklusok és a hármas ciklusok. Ennek megfelelően olyan a, b, c természetes számokat kell találni, amelyekre $a^2+b^2+c^2 = 6$. A szimmetrikus csoportoknak mindig van két multiplikatív karaktere: az egyik, amikor minden elemet 1-re képezünk, a másik, amikor a párosokat 1-re, a páratlanokat (-1)-re. Így például $a = b = 1$; amiből triviálisan $c = 2$. (A fenti egyenletnek egyébként sincs más pozitív egész megoldása.)

2) S_4 elemeinek a száma 24. A konjugált elemosztályok száma 5, mert ennyi különböző típusú permutáció van S_5-ben. Itt is van két multiplikatív karakter, tehát az $1 + 1 + a^2 + b^2 + c^2 = 24$ egyenletet kell megoldani. Ennek triviálisan (lényegileg) egy megoldása van: $a = 2$, $b = c = 3$.

3) A_4 elemeinek a száma 12. Egy elem konjugáltjainak a száma – mint tudjuk – normalizátorának indexével egyezik meg. Egy hármas ciklusról megállapítható, hogy csak önmaga hatványaival cserélhető fel, így négy konjugáltja van. Mivel összesen nyolc hármas ciklus található, ezért ezek két konjugált elemosztályt alkotnak. A transzpozíciópárok szorzatai (a V_4-beli nem-egységek) csak egymással cserélhetők fel; ez újabb elemosztály. Az egységelem ismét egy elemosztály. Így a komponensek száma 4. A négyelemű normálosztó szerinti faktor harmadrendű ciklikus csoport, amelynek legalább három különböző

homomorfizmusa van egy algebrailag zárt testbe. Így a négy komponens közül legalább három helyen egydimenziós altér szerepel, ezért a negyedik (3×3)-as mátrixokat jelent. (Itt sincs más pozitív egész megoldás.)

4) A_5 elemeinek a száma 60. Mivel ez nemkommutatív egyszerű csoport, ezért egyetlen multiplikatív karaktere létezik. Az előző példához hasonlóan megállapítható, hogy a konjugált elemosztályok száma 5. Így az $1 + a^2 + b^2 + c^2 + d^2 = 60$ egyenletet kell természetes számokban megoldani. Mivel 59-et 8-cal osztva 3-at kapunk maradékul, ezért a négy szám közül három páratlan, s a negyedik 4-gyel is osztható. Ez a negyedik így nyilván csak 4 lehet; s az $59 - 16 = 43$-nak három négyzetszám összegére való egyetlen felbontása: $9 + 9 + 25$. Természetesen nagyobb csoportok esetén az eljárás lényegesen bonyolultabb. Általában a reprezentációs blokkok nagyságára vonatkozó egyenletnek nem is egyértelmű a megoldása.



Megjegyzés. Amennyiben nem a komplex test feletti reprezentációkat vizsgáljuk, akkor már a centrum sem feltétlenül a test feletti skalármátrixokból áll, hiszen K-nak lehet algebrai bővítése. Ha a centrumot sikerül meghatározni, még akkor is gondot okoz, hogy a mátrixok elemei egy nem feltétlenül kommutatív úgynevezett *ferdetestből* valók. A szerkezet megállapításában nagy segítséget jelent az a tétel, amely kimondja, hogy egy ferdetestnek a centruma feletti dimenziója mindig négyzetszám. □

10.6. A Jacobson-radikál

A továbbiakban egy újabb radikálfogalmat vezetünk be, amely szorosan kapcsolódik a féligegyszerű gyűrűkhöz.

10.37. Definíció. Legyen R egységelemes gyűrű. Készítsük el minden egyes $\mathcal{M}$ minimális bal oldali unitér R-modulusra az $\mathcal{M}$-nek az $\ell(\mathcal{M}) \lhd R$ annullátorideáljainak a halmazát. Ezek metszetét a gyűrű $J(R)$ Jacobson-radikáljának nevezzük.

Tekintettel arra, hogy a szóban forgó annullátorok mind ideálok, ezért a Jacobson-radikál is ideálja a gyűrűnek.

Valójában a fenti ideált bal oldali Jacobson-radikálnak kellene nevezni, hiszen bal oldali R-modulusok segítségével értelmeztük. A következő tételből viszont ki fog derülni, hogy ez megegyezik a „jobb oldali Jacobson-radikállal”.

10.38. Tétel. *Tetszőleges egységelemes R gyűrű $J(R)$ Jacobson-radikáljára az alábbiak teljesülnek:*

(1) *$J(R)$ az R maximális balideáljainak a metszete.*

(2) *$J(R)$ az R azon a elemeiből áll, amelyekre tetszőleges $r \in R$ esetén az $1-ra$ elemnek létezik inverze.*

(3) *$J(R)$ az R azon a elemeiből áll, amelyekre tetszőleges $r, s \in R$ esetén az $1 - ars$ elemnek létezik inverze.*

(4) *$J(R)$ az R azon a elemeiből áll, amelyekre tetszőleges $r \in R$ esetén az $1-ar$ elemnek létezik inverze.*

(5) *$J(R)$ az R maximális jobbideáljainak a metszete.*

Ha az R valamely B balideáljához van olyan n pozitív egész, amelyre $B^n \subseteq J(R)$, akkor $B \subseteq J(R)$.

Bizonyítás. (1) Legyen B az R-től különböző maximális balideál. A maximalitás alapján R/B minimális (unitér) bal oldali R-modulus, amelyre $\ell(R/B) \leq B$. Így – $J(R) \leq$ $\leq \ell(R/B)$ miatt – $J(R)$ része a maximális balideálok metszetének.

Fordítva, tekintsünk egy tetszőleges $\mathcal{M}$ minimális unitér bal oldali R-modulust és legyen $\mathbf{u} \in \mathcal{M}$ ($\mathbf{u} \neq \mathbf{o}$). Ha $r\mathbf{u} \neq \mathbf{o}$ ($r \in R$), akkor $\mathcal{M}$ minimalitása miatt van olyan $s \in R$, amelyre $s(r\mathbf{u}) = \mathbf{u}$, azaz $1 - sr \in \ell(\mathbf{u})$. Eszerint 1 eleme az r és $\ell(\mathbf{u})$ generálta balideálnak, vagyis $\ell(\mathbf{u})$ maximális. Tekintettel arra, hogy az összes $\{\ell(\mathbf{u}) \mid \mathbf{u} \in \mathcal{M}\}$ alakú balideál metszete éppen $\ell(\mathcal{M})$, és az összes $\ell(\mathcal{M})$ alakú ideál metszete a Jacobson-radikál, ezért $J(R)$ előáll (bizonyos) maximális balideálok metszeteként. Ezért az összes maximális balideál metszete nem lehet nagyobb, mint $J(R)$; következésképpen megegyezik vele.

(2) bizonyításához tegyük fel először, hogy az $1 - ra$ elemnek nincs balinverze. Ez azt jelenti, hogy az általa generált $R(1 - ra)$ balideál nem tartalmazza 1-et. A Zorn-lemma alapján az ilyen tulajdonságú balideálok között van maximális, ami nyilván maximális balideál R-ben. Ha B egy ilyen balideál, akkor természetesen $a \notin I$, mert ellenkező esetben $1 = (1 - ra) + ra \in I$ volna.

Ha viszont van olyan maximális I balideál, amelyre $a \notin I$, akkor az a és I által együttesen generált $Ra + I$ balideál megegyezik R-rel, és így van olyan $r \in R$ és $b \in I$, amire $1 = ra + b$, és így a $b = 1 - ra$ elemnek nincs balinverze.

Legyen most $a \in J(R)$ és írjuk $1 - ra$ balinverzét $1 - s$ alakba. Az $1 = 1 - s - ra +$ $+ sra$ összefüggésből azt kapjuk, hogy $s = (sr + r)a \in J(R)$. Ezért az $1 - s$ elemnek is létezik balinverze, amely a szorzás asszociativitása miatt pontosan $1 - ra$, vagyis az $1 - ra$ elemnek létezik (kétoldali) inverze.

Legyen $a \in J(R)$ és alkalmazzuk (2)-t a helyett az as elemre ($s \in R$), amely ugyancsak $J(R)$-beli, hiszen a Jacobson-radikál (kétoldali) ideál. Eszerint tetszőleges $r \in R$ esetén létezik inverze az $1 - sar$ elemnek. Ha viszont tetszőleges $s, r \in R$ elemekre létezik inverze az $1 - sar$ elemnek, akkor a speciális $s = 1$ választással pontosan (2) adódik. Így (3) is igaz.

A (3) alatti feltétel viszont bal-jobb szimmetrikus, ami azt jelenti, hogy a Jacobson-radikált jobb oldali R-modulusokkal definiálva ez (5)-tel, (4)-gyel és (3)-mal ekvivalens.

A tétel utolsó állításának a bizonyításához mindenekelőtt megjegyezzük, hogy definíció szerint a Jacobson-radikál pontosan azokból az elemekből áll, amelyek minden minimá-

lis bal oldali R-modulust annullálnak. Ebből természetesen következik, hogy tetszőleges B balideál pontosan akkor annullál minden minimális bal oldali R-modulust, ha $B \subseteq J(R)$.

Tekintsük most az R egy tetszőleges B balideálját és egy $\mathcal{M}$ bal oldali R-modulust. Világos, hogy a $B\mathcal{M} = \left\{ \sum_i b_i \mathbf{u}_i \mid b_i \in B, \mathbf{u}_i \in \mathcal{M} \right\}$ elemek $\mathcal{M}$ egy részmodulusát alkotják; továbbá, ha B_1 és B_2 az R balideáljai, akkor $(B_1 B_2)\mathcal{M} = B_1(B_2\mathcal{M})$.

Tegyük fel, hogy a B balideálhoz létezik olyan n pozitív egész szám, amelyre $B^n \subseteq \subseteq J(R)$, azaz tetszőleges $\mathcal{M}$ minimális bal oldali R-modulusra $B^n\mathcal{M} = \{0\}$. Legyen n minimális erre a tulajdonságra nézve. Ez azt jelenti, hogy $\mathcal{N} = B^{n-1}\mathcal{M} \neq \{0\}$ – de itt $n-1$ nem feltétlenül pozitív. Mivel $\mathcal{M}$ minimális és $\mathcal{N} \neq \{0\}$, ezért csak $\mathcal{N} = \mathcal{M}$ lehet, amiből $B\mathcal{M} = \{0\}$, vagyis $B \subseteq J(R)$ következik. ■

10.39. Tétel. *Legyen R egységelemes (bal oldali) Artin-gyűrű. Ekkor:*
R pontosan akkor féligegyszerű, ha $J(R) = \{0\}$.
$R/J(R)$ féligegyszerű.

Bizonyítás. Ha $J(R) = \{0\}$ és B az R-nek nilpotens balideálja, akkor alkalmas pozitív egész számra $B^n = \{0\} \subseteq J(R)$ miatt – az előző tétel utolsó állítása alapján – $B = \{0\}$, azaz R radikálmentes. Így féligegyszerű, hiszen Artin-gyűrű. Amennyiben R féligegyszerű és $R_1 + \cdots + R_n$ minimális ideáljaira való felbontása, akkor az R_i-ben levő bármely B balideált az összes többi R_j annullál, s a direkt összeg tulajdonság alapján ezek metszete $\{0\}$ (az $n = 1$ esetben is). Így valóban $J(R) = \{0\}$.

Alkalmazzuk az előző tétel utolsó állítását az $R/J(R)$ gyűrűre. Ennek balideáljai $B/J(R)$ alakúak, ahol $J(R) \subseteq B$. ■

Feladatok

1. Az R kommutatív féligegyszerű gyűrű e és f idempotens elemeire legyen $e \leq f$, ha $e \cdot f = e$. Bizonyítsuk be, hogy ez a reláció részbenrendezés. Mit tükröz ez a részbenrendezés? Bizonyítsuk be, hogy az idempotensek egy félhálót alkotnak erre a rendezésre. Mikor lesz egy idempotens minimális? Definiáljuk idempotensek ortogonalitását. Hogyan általánosíthatjuk ezt a rendezést nemkommutatív esetre? (Több lehetőség is van.)

2. Legyen K egy kommutatív test és $f(x) \in K[x]$. Bizonyítsuk be, hogy az $R = K[x]/(f(x))$ maradékosztály-gyűrű algebra K felett; ez az algebra Artin-gyűrű. Mikor lesz féligegyszerű? Mikor lesz egyszerű? Határozzuk meg ideáljait és idempotens elemeit.

3. Legyen G egy n-edrendű ciklikus csoport és K egy test. Határozzuk meg a K_G csoportalgebrát.

4. Bizonyítsuk be, hogy nullkarakterisztikájú test esetén bármely kommutatív véges G csoport karaktercsoportja izomorf a Hom $(G, \mathbf{C})$ csoporttal, ahol $\mathbf{C}$ a komplex egységgyökök csoportja.

5. Legyen $\Gamma = \mathrm{Char}(G)$ a véges kommutatív G csoport karaktercsoportja. Definiálja az R relációt $\{\chi R g \mid \chi \in \Gamma, g \in G\}$ a $\chi(g) = 1$ összefüggés. Vizsgáljuk az ezáltal meghatározott Galois-kapcsolatot. Bizonyítsuk be, hogy $\Gamma \cong G$.

6. Legyen N a K test n-edfokú normális (szeparábilis) bővítése és G e bővítés Galois-csoportja. Legyen az ${}_N R$ bal oldali N-modulus egy bázisa a G csoport elemeinek a halmaza. N bal oldali ${}_N R$-algebrává tehető úgy, hogy $\left(\sum \alpha_i \sigma_i\right)(\xi) = \sum \alpha_i \cdot (\sigma_i(\xi))$. Ezáltal az ${}_N R$ modulust algebrává tettük, mert a fenti reláció egy szorzást indukál rajta. Határozzuk meg ezt a szorzást és írjuk le ezt az algebrát!

7. Határozzuk meg a D_n diédercsoport reprezentációját a komplex számtest felett.

8. Mi történik az irreducibilis reprezentációk számával, ha nem algebrailag zárt test felett nézzük?

9. Határozzuk meg a Q kvaterniócsoport reprezentációját $\mathbb{Q}$, $\mathbb{V}$, $\mathbb{K}$ felett.

10. Legyen G véges kommutatív csoport, és Γ a karaktercsoportja a komplex számtest felett. Bizonyítsuk be, hogy $\chi \in \Gamma$ és $g \in G$ esetén $\chi^{-1}(g) = (\chi(g))^{-1} = \overline{(\chi(g))}$. Milyen mátrix az, amelyben a „χ-edik” sor „g-edik” eleme $\chi(g)$?

11. Az S_n komplex test feletti reprezentációjában van két multiplikatív karakter. Írjuk fel a megfelelő idempotenseket. Bizonyítsuk be, hogy több multiplikatív karaktere nem létezik. Hány multiplikatív karaktere lehet (van) egy nemkommutatív egyszerű csoportnak?

12. Legyen $S = \{x^r \mid r \in \mathbb{Q}\}$, és vezessük be S-en az $x^r \cdot x^s = x^{r+s}$ szorzást és tekintsük a $R = \mathbb{Q}_S$ félcsoportalgebrát. Bizonyítsuk be, hogy ebben x többszörösei egy I ideált alkotnak; az R/I gyűrű idempotens és előáll nilpotens ideáljai növő láncainak az egyesítéseként.

13. Tekintsük azokat a végtelen mátrixokból álló gyűrűket, amelyekben

(a) véges sok elem van;

(b) minden sorban és oszlopban véges sok elem van;

(c) minden sorban véges sok elem van.

Ezek közül melyek idempotensek, egységelemesek, radikálmentesek, bal oldali Artin-gyűrűk, féligegyszerűek?

14. Igaz-e, hogy egy R féligegyszerű gyűrű minden homomorf képe, ideálja, balideálja is féligegyszerű? Igaz-e, hogy ha egy R gyűrű egy ideálja és a szerinte vett faktor féligegyszerű, akkor R is az?

15. Adjunk meg olyan gyűrűt, amelynek balideáljaira teljesül, de jobbideáljaira nem teljesül a minimumfeltétel.

16. Legyen $\mathcal{V}$ az (α, β) párok összessége, ahol α, β elemei egy F nemkommutatív testnek. Bizonyítsuk be, hogy $\mathcal{V}$ mindkét oldali kétdimenziós F-vektortér, de a lineáris bal- és jobbfüggés nem ugyanaz.

17. Legyen $S = \{x^r \mid r \in \mathbb{Q}\}$, és vezessük be S-en az $x^r \cdot x^s = x^{r+s}$ szorzást. Mutassuk meg, hogy így egy $\mathcal{S}$ kommutatív félcsoportot kapunk. Bizonyítsuk be, hogy a $\mathbb{Q}_{\mathcal{S}}$ félcsoportalgebrában minden végesen generált ideál főideál; de nem létezik egyértelmű faktorizáció!

18. Határozzuk meg a kommutatív féligegyszerű gyűrűket.

19. Az R egyszerű gyűrűnek nincs nilpotens balideálja. Igaz-e, hogy féligegyszerű? Egyáltalában lehet-e egy egyszerű gyűrűnek nilpotens balideálja?

20. Legyen R féligegyszerű gyűrű és ${}_R\mathcal{M}$ minimális nemtriviális bal oldali R-modulus. Mi a kapcsolat R és $End_R({}_R\mathcal{M})$ között?

21. Legyen $K = \mathbb{Q}_p$ a p elemű prímtest, $q \neq p$ prímszám és A a p elemű ciklikus csoport.

(1) Mutassuk meg, hogy K_A testek direkt összege.

(2) Milyen kapcsolatnak kell fennállnia p és q között ahhoz, hogy e testek mindegyike K legyen?

(3) A p és q között fennálló kapcsolattól függően K-nak hányadfokú bővítései lépnek fel K_G-ben?

(4) Mi a feltétele annak, hogy K_G két test direkt összege legyen?

22. Legyen $K = \mathbb{Q}_p$ és G a p elemű ciklikus csoport ($p = 2, 3, 5, 7$). Határozzuk meg K_G összes nilpotens elemét és radikálját.

23. a) Legyen E a K test feletti n-dimenziós $\mathcal{V}$ vektortér lineáris transzformációiból álló K-algebra. Legyen $\mathbf{e}_1, \ldots, \mathbf{e}_n$ a $\mathcal{V}$ egy bázisa, és definiálja a $\mathbf{Q}_i$ ($1 \leq i \leq n$) elemeket $\mathbf{Q}_i\mathbf{e}_i = \delta_{i,j}\mathbf{e}_{i+1}$. Bizonyítsuk be, hogy (az indexeket mod (n) véve):

(1) A $\mathbf{Q}_i$ elemek generálják E-t.

(2) $\mathbf{Q}_i\mathbf{Q}_j = 0$, ha $j \neq i + 1$.

(3) $\mathbf{Q}_i \cdot \mathbf{Q}_{i+1} \cdot \ldots \cdot \mathbf{Q}_n \cdot \mathbf{Q}_1 \cdot \ldots \mathbf{Q}_{i-1} \cdot \mathbf{Q}_i = \mathbf{Q}_1$.

b) Bizonyítsuk be, hogy ha a $\mathbf{Q}_1, \ldots, \mathbf{Q}_n$ elemek a fenti három feltételnek eleget tesznek, akkor létezik $\mathcal{V}$-nek olyan $\mathbf{f}_1, \ldots, \mathbf{f}_n$ bázisa, amelyre $\mathbf{Q}_i\mathbf{f}_i = \delta_{i,j}\mathbf{f}_{i+1}$.

c) Bizonyítsuk be, hogy E minden $\varphi : \mathbf{X} \mapsto \varphi(\mathbf{X})$ automorfizmusa belső; azaz egy invertálható $\mathbf{T} \in E$ elemmel $\mathbf{X} \mapsto \mathbf{T}^{-1}\mathbf{X}\mathbf{T}$ alakú.

10.7. Algebrák valósan zárt testek felett

A vektorterek esetében két fontos test szerepelt, a komplex számok és a valós számok teste. Mint ahogy az algebrailag zárt testeket a komplex számok általánosításának tekinthetjük, ugyanúgy tekinthetjük a valósan zárt testeket a valós számtest általánosításának:

10.40. Definíció. Egy nullkarakterisztikájú K testet valósan zártnak nevezünk, ha $x^2 + 1$ irreducibilis felette, és a testet e polinom i gyökével bővítve algebrailag zárt testet kapunk. □

10.41. Tétel. *Ha $a \neq 0$ eleme egy K valósan zárt testnek, akkor a és $-a$ közül pontosan az egyik négyzete egy K-beli elemnek.*

Bizonyítás. Mindkettő nem lehet K-beli elem négyzete, mert különben ezek hányadosa, -1 is K-beli elem négyzete volna, ami ellentmond $x^2 + 1$ irreducibilitásának.

Tegyük fel, hogy a nem négyzete K-beli elemnek, vagyis az $x^2 - a$ polinom K felett irreducibilis. A bővítés algebrai zártsága alapján e polinomnak van egy $b + ci$ alakú gyöke ($b, c \in K$), ahol $c \neq 0$, feltétel szerint. A kapott $b^2 - 2bci - c^2 = a$ összefüggésből $i \notin K$ miatt $2bc = 0$ következik. Mivel $c \neq 0$, ezért $b = 0$, azaz $a = -c^2$, illetve $c^2 = -a$. ■

10.42. Tétel. *Valósan zárt testben elemek négyzetösszege felírható egyetlen elem négyzeteként.*

Bizonyítás. Legyenek a, b elemei a K valósan zárt testnek. Mivel $K(i)$ algebrailag zárt, ezért léteznek olyan $c, d \in K$, hogy $(c+di)^2 = a+bi$. Világos, hogy ekkor konjugáltjaikra hasonlóképpen fennáll $(c-di)^2 = a-bi$. Ezekből szorzással a $(c^2+d^2)^2 = a^2+b^2$ összefüggéshez jutunk, ami a tétel állítását bizonyítja. ■

10.43. Következmény. *Valósan zárt testben elemek négyzetösszege nem lehet* -1. ■

A most kapott feltétel kevesebb, mint a valós zártság, hiszen a racionális számtest nyilván nem valósan zárt, de racionális számok négyzetösszege nem lehet -1.

10.44. Definíció. Egy testet formálisan valósnak nevezünk, ha elemeinek négyzetösszege nem lehet -1. □

Megjegyzés. Egy $p \neq 0$ karakterisztikájú testben $\overbrace{1^2+\cdots+1^2}^{(p-1)\text{-szer}} = -1$, így a test nem lehet formálisan valós. □

Mielőtt a formálisan valós és a valósan zárt testek feletti algebrák vizsgálatára térnénk, részletesebben megvilágítjuk ezeknek az algebrailag zárt testekhez való kapcsolatát.

Tekintsünk egy formálisan valós testet. Ennek algebrai lezártjában a Zorn-lemma értelmében létezik maximális formálisan valós test. Ki fogjuk mutatni, hogy ez mindig valósan zárt.

10.45. Tétel. *Ha K az algebrai lezártjában maximális formálisan valós test, akkor teljesülnek rá a következők:*

(1) *Ha $a \in K$ és $a \neq 0$, akkor a és $-a$ közül pontosan az egyik állítható elő K-beli elem négyzeteként.*

(2) *Minden K-beli együtthatós páratlan fokú polinomnak van K-ban gyöke.*

Bizonyítás. Mivel K formálisan valós, ezért 0-tól különböző a elemre nem lehet mind a, mind $-a$ négyzet. Tegyük most fel, hogy a nem állítható elő K-beli elem négyzeteként. Először azt mutatjuk meg, hogy a nem lehet K-beli elemek négyzetösszege sem.

Feltételünk szerint az x^2-a polinomnak nincs K-ban gyöke, ezért, ha e polinom egy α gyökével bővítjük K-t, akkor olyan testet kapunk, amely már nem formálisan valós. Ez az állítás egy

$$-1 = \sum_i (c_i\alpha + d_i)^2 = a\left(\sum_i c_i^2\right) + \sum_i d_i^2 + 2\alpha \sum_i c_i d_i$$

alakú összefüggéshez vezet, ahol $c_i, d_i \in K$. Mivel $\alpha \notin K$, ezért a jobb oldalon levő harmadik tag 0. Ha mármost a négyzetösszeg volna, akkor a megadott összefüggésből az adódna, hogy -1 előállítható K-beli elemek négyzetösszegeként, ami lehetetlen.

A kapott feltétel azt is jelenti, hogy ami előáll K-beli elemek négyzetösszegeként, annak K-ban létezik négyzetgyöke is. Ezt fogjuk felhasználni annak a bizonyítására, hogy $-a$ előáll K-beli elem négyzeteként. A -1 kapott előállításából átrendezéssel a $(-a)\cdot\sum_i c_i^2 = 1 + \sum_i d_i^2$ összefüggéshez jutunk. Itt $\sum_i c_i^2 = 0$ lehetetlen, mert ekkor

$-1 = \sum_i d_i^2$ volna. Így $-a$ kifejezhető két négyzetösszeg hányadosaként. Tekintettel arra, hogy minden négyzetösszeg egy K-beli elem négyzete, és két négyzetelem hányadosa is négyzetelem (mint láttuk, a nevező nem 0), ezért $-a$ valóban előállítható egy K-beli elem négyzeteként.

A második állítást a szóban forgó polinom fokára vonatkozó teljes indukcióval bizonyítjuk. Ha a polinom elsőfokú, akkor az állítás triviálisan igaz.

Legyen $f(x)$ egy K-beli együtthatós n-edfokú polinom (n páratlan), és tegyük fel, hogy minden, az n-nél alacsonyabb páratlan fokú K-beli együtthatós polinomnak van K-ban gyöke. Ha $f(x)$ reducibilis, akkor valamelyik tényezője páratlan fokú (különben a szorzatuk, azaz $f(x)$ is páros fokú volna), és így az indukciós feltevés miatt van K-ban gyöke. Kimutatjuk, hogy $f(x)$ irreducibilitása ($n \neq 1$ esetén) lehetetlen.

Legyen tehát $f(x)$ irreducibilis, és legyen α az $f(x)$ egy gyöke a K algebrai lezártjában. E gyökkel bővítve K-t, a maximalitás miatt olyan testet kapunk, amely nem formálisan valós. Mivel e test elemei felírhatók α-nak n-nél alacsonyabb fokú polinomjaként, ezért léteznek olyan $h_i(x)$ K-beli együtthatós, n-nél alacsonyabb fokú polinomok, amelyekre

$$-1 = \sum_i h_i(\alpha)^2.$$

Ez azt jelenti, hogy létezik olyan $g(x)$ ugyancsak K-beli együtthatós polinom, amelyre

$$-1 = \sum_i h_i(x)^2 + f(x)g(x)$$

teljesül. A jobb oldalon az első tag foka legfeljebb $2n-2$. Emellett azt is tudjuk, hogy e tag páros fokú: ha a $h_i(x)$-ek fokának a maximuma k, akkor az összeg legfeljebb $2k$-adfokú, s a $2k$-adfokú tag együtthatója K-beli elemek négyzetösszegeként áll elő; ez pedig nem lehet 0, mert K formálisan valós. A fokok összehasonlításából azt kapjuk, hogy $g(x)$ foka kisebb n-nél, és ha e fokot n-nel növeljük, akkor páros számot kapunk. Mivel n páratlan szám, ezért $g(x)$ foka is csak páratlan lehet. Így $g(x)$-nek van K-ban egy b gyöke, ami a $-1 = \sum_i h_i(b)^2$ összefüggéshez vezet, ellentmondva a K-ra kirótt feltételnek. ■

10.46. Tétel. *Ha a K formálisan valós testre teljesül a* 10.45. *tételben található* (1) *és* (2) *feltétel, akkor K valósan zárt.*

Bizonyítás. Az (1) feltétel miatt x^2+1 irreducibilis K felett, így $K(i)$ a K-nak valódi algebrai bővítése. Azt kell még belátni, hogy $K(i)$ algebrailag zárt. A 8.9. tétel (a felbontási test létezése) szerint elég azt belátni, hogy $K(i)$ a K-nak algebrai lezártja, azaz, hogy minden K-beli együtthatós polinomnak van K-ban gyöke.

A bizonyítás közben szükségünk lesz azonban arra, hogy a $K(i)$ feletti másodfokú polinomoknak van $K(i)$-ben gyökük. Ez nyilván ekvivalens azzal, hogy $K(i)$-ben minden elem négyzet. Tekintsük az $a+bi$ elemet ($a, b \in K$). Azt fogjuk bebizonyítani, hogy ez egy alkalmas elem négyzete. Mivel -1 négyzetelem $K(i)$-ben, ezért elég az állítást $a+bi$ és $-a-bi$ valamelyikére bizonyítani. Tegyük fel, hogy a-t úgy választottuk, hogy a négyzetelem K-ban (ez az (1) feltétel miatt feltehető). Mivel a test formálisan valós, ezért $-a^2-b^2$ nem lehet négyzetelem. Az (1) feltétel szerint tehát létezik olyan $u \in K$, amelyre

$u^2 = a^2 + b^2$. Ugyancsak az (1) feltétel alapján feltehető, hogy u is négyzetelem. Ekkor viszont – ugyanúgy, mint $a^2 + b^2$ esetében láttuk – feltehető, hogy $a + u$ is négyzetelem: $a+u = c^2$. Ebből következik, hogy $u-a = b^2/(u+a)$ felírható d^2 alakban, mert két négyzetelem hányadosa is négyzetelem. Mármost, egyszerű számítás adja, hogy $a + bi = (c + di)^2$. (A fenti bizonyítás technikai részletei pontosan ennek az egyenlőségnek a feltételezéséből adódtak.)

Térjünk most rá annak a bizonyítására, hogy minden K-beli együtthatós polinomnak van $K(i)$-ben gyöke. Minden egyes polinom foka egyértelműen $2^n k$ alakban írható fel, ahol k páratlan szám és $n \geq 0$ egész. A bizonyítást n-re vonatkozó teljes indukcióval végezzük. Az $n = 0$ esetben éppen a (2) feltétel miatt igaz az állítás. Tegyük fel, hogy az állítás igaz minden olyan esetben, amikor a polinom fokában 2 kitevője kisebb, mint n, és tekintsünk egy olyan $f(x)$ r-edfokú K-beli együtthatós polinomot, amelynek fokában 2 kitevője éppen n. A 8.9. tétel szerint K-nak van olyan L bővítése, amelyben az $f(x)$ polinom lineáris faktorokra esik szét. Feltehető, hogy $f(x)$ irreducibilis, amiből következik, hogy $f(x)$ minden gyöke különböző, hiszen K karakterisztikája 0. Legyenek e gyökök $\alpha_1, \ldots, \alpha_r$. Tetszőleges $c \in K$ elemmel készítsük el az összes $\alpha_i\alpha_j + c(\alpha_i + \alpha_j)$ alakú elemet. Mivel ezek egymás konjugáltjai, és számuk $\binom{r}{2}$, ezért legalább egyikük gyöke egy olyan irreducibilis polinomnak, amelynek fokában 2 kitevője kisebb, mint n, hiszen $\binom{r}{2}$-ben 2 kitevője csak $(n-1)$.

Feltétel szerint tehát e polinom valamelyik gyöke eleme a $K(i)$ testnek. Mivel K végtelen és az indexpárok száma véges, ezért valamelyik indexpárhoz végtelen sok olyan K-beli c található, hogy ugyanaz az indexpár – például $\alpha_1\alpha_2 + c(\alpha_1 + \alpha_2)$ – lép fel. Mint a 7.16. tétel bizonyításában láttuk – felhasználva, hogy végtelen sok c jön szóba – választhatjuk a c elemet úgy, hogy az indexektől függetlenül az $\alpha_1\alpha_2 + c(\alpha_1 + \alpha_2)$ elemmel bővítve K-t, a bővítés az $\alpha_1\alpha_2$ és $\alpha_1 + \alpha_2$ elemek mindegyikét tartalmazza. Ezek benne vannak tehát $K(i)$-ben; ami azt jelenti, hogy α_1 és α_2 egy $K(i)$ feletti másodfokú polinom gyökei. Az előzetesen bizonyított állítás szerint tehát elemei $K(i)$-nek, és így $f(x)$-nek van $K(i)$-ben gyöke. ■

Most a komplex számok konstrukciójához hasonlatos eljárással fogunk algebrákat konstruálni formálisan valós testek felett. Az előállított algebrákban azonban nem tesszük fel a szorzás asszociativitását.

10.47. Tétel. *Legyen R a K formálisan valós test felett egységelemes (nem feltétlenül asszociatív) algebra, amelyben teljesülnek a következő tulajdonságok:*

1. *Minden nemnulla elemének van inverze.*

2. *Létezik egy olyan $x \mapsto \overline{x}$ megfeleltetés, amely az alábbiaknak tesz eleget ($\overline{x}$-et az x konjugáltjának nevezzük):*

(1) *$x \mapsto \overline{x}$ involúció (azaz $\overline{(\overline{x})} = x$) és $\overline{1} = 1$.*

(2) *$x \mapsto \overline{x}$ antihomomorfizmus, azaz $\overline{x+y} = \overline{x} + \overline{y}$ és $\overline{x \cdot y} = \overline{y} \cdot \overline{x}$.*

(3) *$x + \overline{x} \in K$ és $x \cdot \overline{x}$ a K-ban négyzetösszeg.*

Ekkor az (a, b) párok ($a, b \in R$) egy R' algebrát alkotnak a K felett a következő műveletekkel:

$$(a, b) + (c, d) = (a + c, b + d), \qquad (a, b) \cdot (c, d) = (ac - \overline{d}b, da + b\overline{c}), \qquad \overline{(a, b)} = (\overline{a}, -b).$$

A kapott R' algebra is rendelkezik a tételben kirótt tulajdonságokkal, és R'-nek a K feletti dimenziója kétszer akkora, mint R-é.

Bizonyítás. A definícióból világos, hogy R' vektortér a K test felett. A szorzás disztributivitása abból következik, hogy a konjugálás összegtartó, és a szorzat így rögzített a és b esetén (c, d)-ben, rögzített c és d esetén (a, b)-ben lineáris – felhasználva az R-beli disztributivitást.

$(1, 0)$ az R'-nek nyilván egységeleme. $(a, b) + (\overline{a}, -b) = (a + \overline{a}, 0)$ és $(a, b) \cdot (\overline{a}, -b) = (a\overline{a} + \overline{b}b, 0)$ miatt mindegyikük egy R-beli elemszerese $(1, 0)$-nak, így R-beli. Azt kell még belátni, hogy $a\overline{a}+\overline{b}b$ az R-ben négyzetösszeg. Ez abból következik, hogy a konjugálás involúció, és egy R-beli elemnek és konjugáltjának a szorzata négyzetösszeg.

Még két bizonyítani való van: a konjugálás R'-ben is involúció (ez triviális); a másik az inverzelem létezése. Mivel egy elemet a konjugáltjával szorozva az eredmény az egységelemnek egy R-beli elemszerese, ezért az inverz létezéséhez azt kell bizonyítani, hogy ez az elem nem 0; ami viszont azonnal következik abból, hogy a szóban forgó elem négyzetösszeg és a test formálisan valós. (Ha a négyzetösszeg 0 volna, akkor $a = b = 0$ lenne.) ■

Nem kell azt gondolni, hogy az inverzelem létezése maga után vonja az osztás elvégezhetőségét. Ezt lényegében csak az asszociativitás (vagy annak gyengébb formája) tudja biztosítani. Sőt, az is belátható, hogy a fenti típusú algebrák között olyanok is vannak, amelyekben nullosztókat találhatunk.

10.48. Tétel. *A 10.47. tételben konstruált R' algebra természetes módon tartalmazza az R-et. R' akkor és csak akkor kommutatív, ha R-ben a konjugálás az identitás; akkor és csak akkor asszociatív, ha R-ben érvényes a kommutativitás.*

Bizonyítás. Világos, hogy az $a \mapsto (a, 0)$ megfeleltetés beágyazás. Ha R' kommutatív, akkor természetesen R is az. A $(0, 1)$ és $(0, a)$ szorzatának kétféle kiszámításából $\overline{a} = a$ adódik. Fordítva, ha R kommutatív és a konjugálás az identitás, akkor egyszerű számolás adja, hogy R' kommutatív.

Ha R' asszociatív, akkor R is az. Az $((l, 0)\cdot(b, 0))\cdot(0, \overline{c}) = (1, 0)\cdot((b, 0)\cdot(0, \overline{c}))$ azonosságból $cb = bc$ következik. Fordítva, R kommutativitásából R' asszociativitása számolással igazolható. ■

A fenti módon egy formálisan valós testből lépésenként konstruálhatunk egyre újabb algebrákat. Az első lépésnél az $i = (0, 1)$ jelöléssel az $a + bi$ alakú elemekhez jutunk. Ez kommutatív algebra. A következő lépésben az úgynevezett *kvaterniókat* kapjuk. A $j = (0, 1)$ és $k = (0, i)$ jelöléssel ennek az algebrának a K feletti bázisa: $1, i, j, k$. Ez a négydimenziós algebra asszociatív, de nem kommutatív. A báziselemek szorzatát a következőképpen határozhatjuk meg: Az 1 egységelem, $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, és ha e párokat fordított sorrendben szorozzuk össze, akkor a szorzat a fentieknek a negatívja.

A kvaterniók szorosan kapcsolódnak a térvektorokhoz. Az (a, b, c) térvektoroknak megfeleltetjük az $ai+bj+ck$ úgynevezett *tiszta kvaterniót*. Két tiszta kvaternió szorzatában az 1 együtthatója a megfelelő vektorok skalárszorzatának a negatívja; a tiszta kvaternió rész pedig a megfelelő vektorok vektoriális szorzatához tartozó tiszta kvaternió.

Ha még egy lépéssel tovább megyünk, akkor nyolcdimenziós algebrát kapunk, amit a test feletti Cayley–Dickson-algebrának neveznek. Ez az algebra már nem is asszociatív, csupán alternatív; amit úgy is definiálhatunk, hogy minden olyan háromtényezős szorzat asszociatív, amelyben a három tényező közül valamelyik kettő megegyezik. Kimutatható (elég bonyolult számolással), hogy az alternativitás feltétele az „előző" algebra asszociativitása. Azt is be lehet látni, hogy az alternativitás következményeként a kapott algebrában az elsőfokú egyenletek megoldhatók és az algebrában nincsenek nullosztók. A következő lépésben már olyan algebra adódik, amelyben nullosztók is vannak.

A továbbiakban a célunk annak a bizonyítása lesz, hogy valósan zárt testek esetében bizonyos értelemben nincs is más asszociatív algebra, mint amiket az előzőekben konstruáltunk.

10.49. Tétel (Frobenius)**.** *Valósan zárt test feletti véges dimenziós, nullosztómentes, asszociatív algebra három van:*

(1) *saját maga (*1*-dimenziós);*

(2) *algebrai lezártja (*2*-dimenziós);*

(3) *a felette vett kvaterniók (*4*-dimenziós).*

Bizonyítás. Tekintsük a K valósan zárt test feletti A véges dimenziós, nullosztómentes asszociatív algebrát. Tetszőleges $a \in A$ $(a \neq 0)$ esetén az $\{ax \mid x \in A\}$ halmaz az asszociativitás alapján A-nak részalgebrája. A nullosztómentesség miatt az a-val való szorzás K felett független elemeket ismét független elemekbe visz, és így a konstruált algebra az eredetivel megegyező dimenziós. Ezért A minden eleme benne van a konstruált algebrában, tehát minden $b \in A$ felírható $b = ax$ alakban. Ugyanígy látható be az is, hogy olyan A-beli y elem is található, amelyre $b = ya$. Eszerint A ferdetest, amelynek K részteste. A 10.29. tétel szerint A minden eleme gyöke egy K-beli együtthatós (nemnulla) polinomnak. Ebből a nullosztómentesség miatt következik, hogy gyöke egy K-beli együtthatós K felett irreducibilis polinomnak is. A 10.40. definícióból következik, hogy K feletti irreducibilis polinom legfeljebb másodfokú lehet. Így bármely $a \in A$ gyöke egy $x^2 + bx + c \in K[x]$ polinomnak. Ez azt jelenti, hogy az $a + b/2$ elem négyzete K-ban van. Más szóval A minden eleme felírható két olyan elem összegeként, amelyek egyike K-ban van, másikának négyzete van K-ban.

Mivel A egységelemes, ezért $K \subseteq A$. Most a bizonyítást több különböző állításra bontjuk.

1. Állítás. *Ha egy A-beli elem négyzete K-beli négyzetelem, akkor a szóban forgó elem is K-beli.*

Bizonyítás. Az $a \in A$ és $b \in K$ elemekre teljesüljön az $a^2 = b^2$ egyenlőség. Tekintettel arra, hogy K elemei A minden elemével felcserélhetők, ezért a fenti egyenlőségből $(a + b) \cdot (a - b) = 0$ következik, ami a nullosztómentesség miatt csak úgy lehetséges, hogy $a \in \{b, -b\}$, azaz $a \in K$.

2. Állítás. *Jelölje N azoknak az A-beli elemeknek a halmazát, amelyeknek a négyzete K-ban van, de nem K-beli (0-tól különböző) négyzetelemek. Ekkor $A = K + N$ (az összeadás komplexusösszeg).*

Bizonyítás. Mint láttuk, tetszőleges $a \in A$ elem felírható $a = k + n$ alakban ($k \in K$ és $n \in N$), csupán az nem világos, hogy nem lehet-e $n^2 = k_1^2$, ahol $k_1 \in K$ (K valósan zárt!). Ebben az esetben azonban az első állítás szerint a szóban forgó összeg mindkét tagja K-beli, tehát az összeg is K-beli. Márpedig K-beli és N-beli elemek is felírhatók a kívánt alakban, mert 0 mindkét halmaznak eleme.

Legközelebbi célunk annak a bizonyítása, hogy a fenti összeg alterek direkt összege. Az eleve triviális, hogy K altér, ezért ezt most N-ről kell belátni.

3. Állítás. *N egy elemét K-beli elemmel szorozva ismét N-beli elemet kapunk.*

Bizonyítás. Valóban, ha $a \in K$ és $u \in N$, akkor $(au)^2 = a^2u^2 \in K$. Ha e szorzat 0-tól különböző K-beli négyzetelem volna, akkor u^2 is 0-tól különböző K-beli elem négyzete lenne, ami csak az $u = 0$ esetben lehet. Így valóban $au \in N$.

Mielőtt bebizonyítanánk, hogy N zárt az összeadásra, be kell látnunk egy másik állítást is.

4. Állítás. *Ha u és v az N-nek (K felett) lineárisan független elemei, akkor 1, u, v is lineárisan függetlenek.*

Bizonyítás. Tegyük fel, hogy 1, u, v lineárisan összefüggnek. Mivel u és v lineárisan függetlenek, ezért egyikük sem 0. Így az $a \cdot 1 + b \cdot u + c \cdot v = 0$ felírásban ($a, b, c \in K$) a, b, c egyike sem lehet 0. Ekkor feltehető, hogy például $c = -1$, amiből a $v = a + bu$ összefüggéshez jutunk. Négyzetre emelés után azt kapjuk, hogy $2abu = v^2 - a^2 - b^2u^2 \in K$, ami a 3. állítás és a nullosztómentesség miatt csak úgy lehet, hogy a, b, u valamelyike 0, ami szintén lehetetlen.

5. Állítás. *N zárt az összeadásra.*

Bizonyítás. Legyenek $u, v \in N$. Ha ezek az elemek lineárisan összefüggnek, akkor összegük is nyilván N-beli. Tegyük most fel, hogy függetlenek. Mivel $u + v$ és $u - v$ is elemei A-nak, ezért mindketten gyökei egy-egy másodfokú K-beli együtthatós polinomnak:

$$(u + v)^2 = a(u + v) + b \qquad \text{és} \qquad (u - v)^2 = c(u - v) + d,$$

K-beli a, b, c, d elemekkel. A négyzetre emelést elvégezve, majd rendezve, a következő összefüggéseket kapjuk:

$$uv + vu = au + av + (b - u^2 - v^2) = (-1) \cdot \big(cu - cv + (d - u^2 - v^2)\big).$$

A középen és a jobb oldalon álló kifejezést összehasonlítva az $(a+c)u+(a-c)v+(b-d-$ $- 2u^2 - 2v^2) = 0$ összefüggéshez jutunk; amiből a 4. állítás alapján az következik, hogy $a - c = a + c = 0$, következésképpen $a = c = 0$. Így $u + v$ és $u - v$ négyzete is K-beli.

Ha e négyzetek bármelyike K-beli elem négyzete lenne, akkor az első állítás szerint ez az elem K-beli elem volna, ami ellentmond annak, hogy 1, u, v lineárisan függetlenek. Vagyis $u+v, u-v \in N$, amint állítottuk.

Az 5. állítás bizonyítása során az is kiderült, hogy $uv+vu = b-u^2-v^2 \in K$. Ha u és v bármelyikét is rögzítjük, akkor az $uv+vu$ a másiknak lineáris függvénye. Vegyük figyelembe azt is, hogy $uu+uu$ egy K-beli elem négyzetének negatívja. Ezekből kapjuk:

6. Állítás. *$S(u,v) = -(uv+vu)/2$ pozitív definit lineáris függvény az N vektortéren. (A pozitív definitség úgy értendő, hogy pozitívnak nevezzük a 0-tól különböző elemek négyzeteit. A valósan zártság következtében ez a tulajdonság biztosítja, hogy mindazok az eredmények igazak legyenek, amelyek a valós számtest feletti vektorterekre teljesültek.)*

A 6. állítás szerint $S(u,v)$ skalárszorzat az N vektortéren. E skalárszorzathoz mindig található egy ortonormált bázis. Vizsgáljuk most meg, hogy milyen esetek lehetségesek.

Ha N nulldimenziós, akkor A egydimenziós.

Ha N legalább egydimenziós, akkor létezik ortonormált bázisa. Legyen e bázis egyik eleme i. Erre $S(i,i) = 1$ miatt $i^2 = -1$ adódik. (Egyébként az ortonormált bázis bármely elemének a négyzete -1.) Lehet, hogy N egydimenziós; ekkor A nyilvánvalóan éppen K algebrai lezártja lesz.

Ha N legalább kétdimenziós, akkor legyenek i és j egy ortonormált bázis elemei. Az ortogonalitás éppen azt jelenti, hogy $ij+ji = 0$. Kimutatjuk, hogy i, j és $k = ij$ ortonormált rendszert alkotnak. $k^2 = ijij = i(-ij)j = -1$ következtében $k \in N$ és k normált. $ik+ki = iij+iji = -j+j = 0$ miatt i és k ortogonálisak. j és k ortogonalitása hasonlóképpen mutatható ki. Ha e három elem N egy bázisa, akkor A éppen a K feletti kvaterniótesttel izomorf.

Végül azt bizonyítjuk be, hogy N nem lehet háromnál több dimenziós. Tekintsünk egy $u \in N$ elemet, amely i, j, k mindegyikére ortogonális. Ez azt jelenti, hogy $iu+ui = ju+uj = ku+uk = 0$. Így $ku = -uk = -uij = iuj = -iju = -ku$, amiből $2ku = 0$ következik. A nullosztómentességet felhasználva azt kapjuk, hogy $u = 0$, ami azt jelenti, hogy az N térben nincs újabb, mindhárom vektorra merőleges vektor, a tér háromdimenziós. ■

10.50. Tétel. *A 10.49. tételben szereplő három feltétel egyike sem hagyható el.*

Bizonyítás. Tegyük fel először, hogy K nem valósan zárt. Ha K algebrailag zárt, akkor – mint láttuk – a három lehetőség közül csak az első léphet fel. Egyéb testek esetében viszont van a testnek olyan véges algebrai bővítése, amely nem másodfokú i-vel való bővítés. Ez olyan véges dimenziós, nullosztómentes, asszociatív algebra, amely a felsoroltaktól különbözik.

Az asszociativitás szükségességét láttuk, mert a Cayley–Dickson-algebráról említettük, hogy nullosztómentes és nyilván véges dimenziós.

A másik két ellenpéldában nem lényeges, hogy milyen K testről van szó. A K feletti teljes mátrixgyűrűkben csak a nullosztómentesség, a K feletti polinomgyűrűk esetében pedig csak a dimenzió végessége nem teljesül. ■

A gyűrűk és az algebrák esetében a szorzásnak a legfontosabb tulajdonsága az összeadásra vonatkozó kétféle disztributivitás. Ez teszi lehetővé azt, hogy az elemeket az additív csoport lineáris transzformációiként foghassuk fel. Ennek megfelelően egy asszociatív

nemkommutatív algebrából kétféleképpen is képezhetünk nemasszociatív algebrát, szorzás helyett az $ab - ba$ vagy az $ab + ba$ műveletet választva. A két lehetőség közül az előbbi a fontosabb:

10.51. Definíció. Egy K test feletti véges dimenziós vektorteret Lie-algebrának nevezünk az $[a, b]$ szorzásra, ha $[a, b]$ bilineáris függvény, és a következők teljesülnek:

$$[a, a] = 0 \qquad \text{és} \qquad [[a, b], c] + [[b, c], a] + [[c, a], b] = 0,$$

az algebra tetszőleges a, b, c elemeire. □

A második azonosságot *Jacobi-azonosságnak* nevezik. Kimutatható, hogy a Jacobi-azonosságban csak az lényeges, hogy a szereplő három elemet ciklikusan permutáljuk, és az, hogy a belső zárójel mindig ugyanazon az oldalon legyen.

A definícióban szereplő első azonosságból nyilvánvalóan következik az $[a, b] = -[b, a]$, úgynevezett antikommutativitás. Az antikommutativitás miatt Lie-algebrák készítésekor elegendő csak az egyik oldali szorzást definiálni.

A Lie-algebrák esetében is beszélhetünk ideálokról. Az L Lie-algebra I alterét ideálnak nevezzük ($I \lhd L$), ha egy I-beli és egy L-beli elem szorzata mindig I-beli elem. Itt is definiálhatnánk az ideálokat a homomorfizmusok magjaként. Az antikommutativitás következtében Lie-algebrák minden egyoldali ideálja eleve kétoldali.

Az L Lie-algebra A és B részalgebráinak az $[A, B]$ szorzatát – az asszociatív esethez hasonlóan – a következőképpen definiáljuk: $\left\{\sum [a, b] \mid a \in A, b \in B\right\}$.

A Lie-algebrák előállítására kétféle tétel létezik. Ezeknek a bizonyítását nem közöljük. Az első tétel tulajdonképpen nem sokat árul el a Lie-algebra szerkezetéről. Ez csupán azt az eljárást általánosítja, amellyel a térvektorok a kvaterniókból előállíthatók.

10.52. Tétel (Ado–Iwasawa)**.** *Egy (véges dimenziós) A asszociatív algebra Lie-algebrává válik az* $[a, b] = ab - ba$ *szorzással. Minden Lie-algebra beágyazható egy fenti módon nyert Lie-algebrába.*

(Az első állítás természetesen triviálisan bizonyítható.)

A Lie-algebrák szerkezete jelentős a véges csoportok elméletében is és az algebrai geometriában is. E szerkezet megállapításához néhány fogalomra van szükség.

Definiáljuk egy Lie-algebra hatványait. Tekintettel arra, hogy a szorzás nem asszociatív, a definícióban figyelemmel kell lenni a zárójelezésre.

Az L Lie-algebra első hatványa: $L^1 = L$*; a továbbiakat az* $L^n = [L^{n-1}, L]$ *rekurzió definiálja.*

Igen fontos a Lie-algebrák egy másik konstrukciója, amely a csoportelméleti kommutátorképzéssel analóg.

Legyen $L^{(0)} = L$. Ha $L^{(i)}$ definiált, akkor legyen $L^{(i+1)} = [L^{(i)}, L^{(i)}]$.

Azokat a Lie-algebrákat fogjuk mindenekelőtt nézni, amelyeknél a fenti sorozat valamikor 0-t ad. Ezek között vannak nagyon egyszerű szerkezetűek, s ezek között vannak triviálisak.

Egy Lie-algebrát Abel-félének nevezünk, ha minden elempárjára $[a, b] = 0$ *teljesül.*

Az egydimenziós Lie-algebrák triviálisan Abel-félék.

Az L Lie-algebrát feloldhatónak, illetve nilpotensnek nevezzük, ha létezik olyan n természetes szám, amelyre $L^{(n)} = 0$, illetve $L^n = 0$.

Be lehet bizonyítani, hogy minden nilpotens Lie-algebra feloldható (pl. kimutatható, hogy $L^{(n)} \leq L^{2^n}$). Ezzel szemben nem minden feloldható Lie-algebra nilpotens. Tekintsük az a, b elemek generálta vektorteret az $[a, b] = a$ összefüggés definiálta Lie-szorzattal. Erre az L Lie-algebrára L^n az a generálta altér, míg $L^{(2)} = 0$.

10.53. Tétel. *Minden L Lie-algebrában létezik egy N legnagyobb nilpotens és egy S legnagyobb feloldható nemtriviális ideál. Ezekre $[L, S] \leq N \leq S$ teljesül.*

Az L legnagyobb feloldható ideálját az L *radikáljának* nevezzük. Ha L radikálja $\{0\}$, akkor azt mondjuk, hogy L *féligegyszerű*.

A továbbiakban feltesszük, hogy az alaptest nullkarakterisztikájú és algebrailag zárt.

Tekintsük most az L Lie-algebrát mint vektorteret. Legyen R e vektortér lineáris transzformációinak az algebrája, és A az R-ből elkészített Lie-algebra (10.52. tétel). Ekkor *létezik egy $L \to A$ homomorfizmus, amelynél x-nek azt az $Ad(x)$ transzformációt feleltetjük meg, amelyre $Ad(x) : y \mapsto yx$.*

A most definiált reprezentációban fontos szerepet játszik egy bilineáris függvény, az úgynevezett *Killing-féle forma*. Ezt $B(x, y) = \mathrm{tr}(Ad(x) \cdot Ad(y))$ definiálja, ahol $\mathrm{tr}(M)$ az M mátrix nyomát (a fődiagonális elemeinek összegét) jelöli. (Minthogy a nyom független attól, hogy a lineáris transzformációt melyik bázisban írjuk fel, ezért a fenti függvény jóldefiniált.)

$B(x, y)$ szimmetrikus, és bizonyítható a következő értelemben vett asszociativitás: $B(x, [y, z]) = B([x, y], z)$. A Killing-formára érvényes az alábbi, Élie Cartantól származó

10.54. Tétel. *$B(x, y)$ akkor és csak akkor nem elfajuló, ha a megfelelő Lie-algebra féligegyszerű.*

(Egy $A(x, y)$ bilineáris forma elfajuló, ha van a o-tól különböző olyan x vektor, hogy tetszőleges y vektorra fennáll az $A(x, y) = 0$ összefüggés.)

Féligegyszerű Lie-algebrákra hasonló tétel érvényes, mint a féligegyszerű asszociatív algebrákra: *Féligegyszerű Lie-algebra egyszerűek direkt összege.* Itt is meghatározható az egyszerű radikálmentesek szerkezete. E szerkezet meghatározása geometriai vizsgálatoknál is fontos szerepet játszik.

Az L egyszerű Lie-algebrának létezik egy H, úgynevezett *Cartan-részalgebrája*, amelyet az alábbi kritérium definiál: *H nilpotens és saját normalizátora* (a normalizátor az a maximális részalgebra, amelyben ő normális – azaz ideál). Bizonyítható, hogy minden Lie-algebrának van Cartan-részalgebrája, amely nem egyértelmű ugyan, de bármely kettő egy alkalmas automorfizmussal egymásba vihető.

10.55. Tétel. *Az L egyszerű radikálmentes Lie-algebra mint vektortér felbontható az*

$$L = H + L_1 + \cdots + L_r$$

direkt összeg alakba, ahol H az L Cartan-részalgebrája, és minden egyes L_i egy e_i vektor generálta egydimenziós altér.

H Abel-féle Lie-algebra; és a Killing-forma H-n sem elfajuló.

Bármely H-beli h elemre és bármely i indexre $[h, e_i] = f_i(h)e_i$, ahol f_i a H algebrát a K alaptestbe vivő lineáris függvény. Minden i indexhez található olyan egyértelműen meghatározott H-beli h_i elem, amelyre $B(h, h_i) = f_i(h)$. Ezek a h_i elemek generálják a H részalgebrát.

10.56. Tétel (a 10.55. tétel kiegészítése)**.** *Ha a h_i elemek közül kiválasztjuk H-nak egy bázisát, akkor az összes többi h_i-k előállíthatók a kiválasztottak racionális együtthatós lineáris kombinációjaként.*

A h_i elemek valós együtthatós lineáris kombinációiból álló valós vektortéren a $B(x, y)$ Killing-forma pozitív definit.

A 10.55. tétel és annak 10.56. kiegészítése segítségével az egyszerű, radikálmentes Lie-algebrák szerkezetének a meghatározása visszavezethető egy geometriai feladatra, nevezetesen egy valós euklideszi térben a h_i-k meghatározására. A 10.55. tételben szereplő h_i elemeket *az L Lie-algebra csillagának nevezzük.*

Egy L Lie-algebra csillaga egyértelműen leírható az alábbi három tulajdonsággal:

(I) A csillagban h_i-vel rajta kívül csak a $-h_i$ párhuzamos.

(II) A csillag szimmetrikus bármely rögzített h_i-re merőleges hipersíkra (a merőlegesség a $B(x, y)$ skalárszorzatban értendő, hipersíkon a vektortérnél eggyel kevesebb dimenziós alteret értünk).

(III) A csillag bármely különböző x és y elemeire a $2 \cdot \dfrac{B(x, y)}{B(x, x)}$ hányados egész szám.

Már egyedül a harmadik feltételből is megállapítható, hogy a csillag elemeire az $|2 \cdot B(x, y)/B(x, x)|$ értéke legfeljebb 3. Egyszerű geometriai megfontolásokból megállapíthatók az alábbiak:

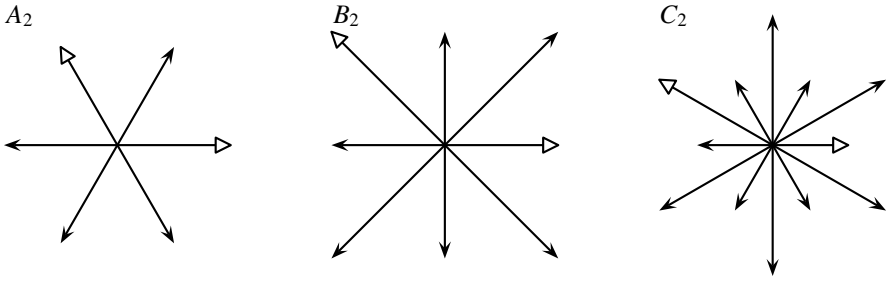
A csillag két vektorának a hajlásszöge csak; $0°$, $30°$, $45°$, $60°$, $90°$, illetve ezek kiegészítő szögei lehetnek. A párhuzamos vektorok esetében a hosszarány 1, merőlegeseknél eleve semmi nem mondható. A másik három esetben – a szögek növekedésének megfelelően – ez az arány $\sqrt{3}$, $\sqrt{2}$, illetve 1.

A csillagból egyértelműen azonnal meghatározható a keresett egyszerű Lie-algebra dimenziója. Ha ugyanis a csillag az n-dimenziós térben van, akkor a Cartan-részalgebra n-dimenziós; míg a 10.55. tételben szereplő összeadandók r száma megegyezik a csillag elemszámával. Így a keresett dimenzió éppen e két szám összege.

Megjegyezzük, hogy ha két, egymásra merőleges térben felveszünk egy-egy csillagot, akkor ezek egyesítési halmaza nyilvánvalóan ismét csillag lesz. Ekkor az új csillag felbontható. Éppen ezért csak felbonthatatlan csillagokkal érdemes foglalkozni.

Egydimenziós térben egyetlen csillag adható meg, amely két ellentétes irányú vektorból áll. Csillagelemszám + dimenzió = 2 + 1 = 3. A megfelelő Lie-algebra 3-dimenziós. A szóban forgó csillagot A_1 jelöli.

Kétdimenziós térben a következő három csillag adható meg:

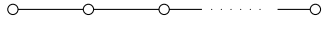


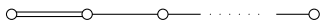
A megfelelő Lie-algebrák dimenziója: $6 + 2 = 8$, $8 + 2 = 10$, $12 + 2 = 14$.

A csillag szerkezete leírható egy gráf, az úgynevezett *Dynkin-diagram* segítségével. A gráfban nem lesznek hurokélek, de egy-egy szögpont esetenként két vagy három éllel is összekötött. Megjegyezzük, hogy a Dynkin-diagram elkészíthető féligegyszerű Lie-algebrák esetében is; s a szerkezete elárulja az egyszerűséget. Nevezetesen, a Lie-algebra pontosan akkor lesz egyszerű, ha az adott Dynkin-diagram összefüggő gráf.

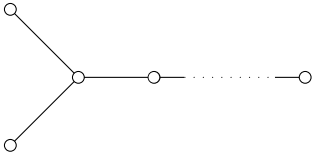
A Dynkin-diagram elkészítéséhez tekintsünk a csillagban egy olyan bázist, amelyeknek a szöge a „lehető legnagyobb". Ilyen mindig létezik. (A megadott kétdimenziós csillagok esetében például a külön megjelölt vektorpárok.) A Dynkin-diagram csúcspontjainak száma a kiválasztott vektorok száma (tehát a tér dimenziója). A Dynkin-diagram két csúcspontját nem kötjük össze, ha a két vektor egymásra merőleges. Egy éllel kötjük össze, ha a két vektor szöge 120°, kettővel, ha a szög 135°, hárommal, ha 150°.

Ennek megfelelően a következő típusú Dynkin-diagramok készíthetők el (az index a dimenziószámot jelenti).

A_n  (ha $n \geq 1$);

B_n  (ha $n \geq 1$);

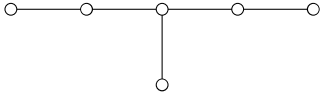
C_n Azonos B_n-nel ($n \geq 3$). (A megkülönböztetést azért kell tenni, mert az első két pontnak megfelelő vektorok különböző hosszúságúak, és más-más csillag adódik annak megfelelően, hogy az egyenlő hosszúságú vektorok hossza a nagyobb vagy a kisebb.)

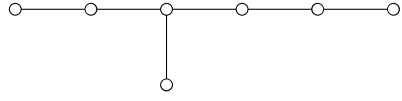
D_n  (ha $n \geq 4$);

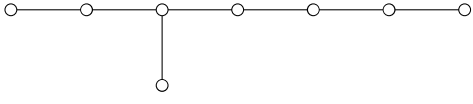
A fenti sorozatokon kívül még öt diagram van:

G_2 ;

F_4 ;

E_6  ;

E_7  ;

E_8  .

A másik – bár kevésbé fontos – nemasszociatív algebra az asszociatív algebrákból az $a \times b = ab + ba$ szorzással nyerhető úgynevezett *Jordan-algebra*. Ezt a szorzásra vonatkozó $a \times b = b \times a$ és $((a \times a) \times b) \times a = (a \times a) \times (b \times a)$ azonosságokkal szokták definiálni.

Feladatok

1. Bizonyítsuk be, hogy van olyan K test, amelynek minden algebrai bővítésében van az x^2+1 polinomnak gyöke, és K nem algebrailag és nem valósan zárt.

2. Lehet-e véges karakterisztikájú test formálisan valós, valósan zárt?

3. A K test feletti A nem feltétlen asszociatív algebra egy bázisa legyen $\{a_1, \dots, a_n\}$. Bizonyítsuk be, hogy ha a báziselemek szorzata asszociatív, akkor az algebra is az.

Tegyük fel, hogy az $f : \mathbb{N} \times \mathbb{N} \to \mathbb{K}$ és $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ függvényekre $a_i \cdot a_j = f(i, j) \cdot a_{g(i,j)}$. Mi a feltétele annak, hogy ez a szorzás asszociatív legyen? (A feltétel csúnya.)

4. Legyen K tetszőleges (kommutatív) test, $u \in K$. Legyen $1, a, b, a \cdot b$ a K feletti A algebra egy bázisa; legyen továbbá a „hiányzó” szorzatokra $a^2 = b^2 = u$, valamint $b \cdot a = -a \cdot b$. Milyen feltétel mellett lesz A (ferde)test (azaz nemkommutatív test)? (Adott K mellett milyen u-k jönnek szóba és milyen K esetén van ilyen A?)

Miért nem működik ez az eljárás véges K testekre?

Konstruáljunk p karakterisztikájú ($p \neq 0$) ferdetestet.

Különböző u-k esetén kaphatunk-e izomorf ferdetesteket?

5. Legyen $\{a_1, \dots, a_n\}$ illetve $\{b_1, \dots, b_k\}$ a ${}_K A$, illetve a ${}_K B$ algebra egy-egy bázisa. Definiáljuk ezeknek az algebráknak a szorzatát úgy, hogy a báziselemeket jelölje $a_i b_j$, s ha $a_i \cdot a_r = \sum \lambda_{i,r}^{(p)} a_p$ és $b_j \cdot b_s = \sum \mu_{j,s}^{(q)} b_q$, akkor legyen $(a_i b_j) \cdot (a_r b_s) = \sum\sum \lambda_{i,r}^{(p)} \mu_{j,s}^{(q)} (a_p b_q)$. Bizonyítsuk be, hogy ez is algebra K felett; amelyet a fenti algebrák szorzatának nevezünk.

6. Legyenek $H \leq G$ véges csoportok. Bizonyítsuk be, hogy K_H részalgebrája K_G-nek. Mit mondhatunk akkor, ha H normálosztó?

7. Legyen $G = A \times B$ véges csoport. Bizonyítsuk be, hogy K_G izomorf a K_A és K_B algebrák szorzatával.

8. A $\mathbb{Q}$ test feletti kvaterniók konjugáltját definiáljuk a 10.47. tétel szerint, azaz $\alpha = a + bi + cj + dk$ konjugáltja $\overline{\alpha} = a - bi - cj - dk$. A α kvaternió normája $N(\alpha) = \alpha \cdot \overline{\alpha}$. Mutassuk meg, hogy $N(\alpha) = a^2 + b^2 + c^2 + d^2$, és a norma multiplikatív.

Egy kvaterniót *egésznek* nevezünk, ha normája egész. Bizonyítsuk be, hogy az egész kvaterniók az összes kvaterniók Q testének egy E részgyűrűjét alkotják. Határozzuk meg azokat az egész kvaterniókat, amelyekben nem minden együttható (az a, b, c, d számok) egész. Bizonyítsuk be, hogy ezek E-beli egységek; ami azzal ekvivalens, hogy normájuk 1.

9. Bizonyítsuk be, hogy a K formálisan valós test feletti kvaternióalgebra minden automorfizmusa belső, azaz $x \mapsto a^{-1} x a$ alakú.

10. Bizonyítsuk be, hogy ha a K formálisan valós test feletti kvaternióalgebra két elemének megegyezik a minimálpolinomja, akkor van olyan algebra-automorfizmus, amelyik az egyiket a másikba viszi.

11. Bizonyítsuk be, hogy ha K formálisan valós test, akkor $K(i)$-nek egyetlen belső automorfizmusa triviális, de ha az algebra két elemének megegyezik a minimálpolinomja, akkor van olyan automorfizmus, amelyik az egyiket a másikba viszi.

12. Bizonyítsuk be, hogy egy ε egységgyök csak akkor lehet eleme egy formálisan valós testnek, ha $\varepsilon^2 = 1$.

ÖTÖDIK RÉSZ
EGYÉB ALGEBRAI STRUKTÚRÁK

Az eddigi algebrai struktúrákban a műveletek mindig az összeadásnak vagy a szorzásnak megfelelő műveletek voltak. A bevezetésben szerepeltek ugyan a műveletekre vonatkozó általános megállapítások, de ezek mind csak a két fontos műveletet „segítették". (Itt elsősorban az egyváltozós és nullváltozós műveletekre gondolunk.) Szerepeltek relációk is, de ezek is csak az „igazi" műveletek jobb leírását tették lehetővé. (Mint például a Galois-kapcsolatnál fellépő hálók az egyenletek megoldását segítették elő.) Valójában viszont „mindenfajta művelet az algebrához tartozik". Ilyenek például a logikai műveletek is. Ezeken a határterületeken nem dönthető el, hogy mi melyik ághoz tartozik; de ez nem is célszerű. A továbbiakban olyan algebrai (vagy „algebrai is") struktúrákat vizsgálunk, amelyekben a műveletek értelmezésében a relációk (is) fontos szerepet játszanak. Mindenekelőtt az általános (univerzális) algebrai fogalmakat célszerű megvizsgálni, a bevezetésnél kissé mélyebb módon.

11. Általános algebrák

11.1. A kifejezések algebrája

A továbbiakban olyan eredményeket ismertetünk, amelyek nem valamilyen rögzített tulajdonságú algebrákra, hanem teljesen általánosan érvényesek. Ennek megfelelően a vizsgált algebraosztály típusáról sem teszünk fel semmit. Nem célunk azonban olyan kérdésekkel foglalkozni, amelyek különböző típusú algebrák kapcsolatáról szólnak. A fentieknek megfelelően rögzítünk egy τ típust. Legyen $\mathbf{F}$ a műveleti nevek halmaza. Egy-egy rögzített τ típusú algebra esetében az $\mathbf{f} \in \mathbf{F}$ műveleti névnek megfelelő műveletet $\varphi_{\mathbf{f}}$ fogja jelölni. (Valójában itt azt is ki kellene jelölni, hogy a művelet melyik algebrának a művelete. Ha ez nem egyértelmű, akkor ezt meg is fogjuk tenni.)

Az első kérdés, amivel foglalkozunk, a következő. Ha egy adott algebra elemeivel egymás után műveleteket végzünk, akkor eleve megmondhatjuk, hogy miképpen, milyen sorrendben végezzük a műveleteket. Kissé pontosabban megfogalmazva, előre megadhatunk egy kifejezést, és utána behelyettesítjük az elemeket. Először tehát azt kellene megmondani, hogy milyen alakúak lesznek ezek a kifejezések. A kifejezéseket éppen úgy, mint a testbeli együtthatós polinomokat, formálisan fogjuk megkonstruálni. Bizonyos technikai követelmények miatt eltérünk a kifejezések „zárójeles" előállításától, és a műveleti jelet nem az elemek közé, hanem eléjük írjuk. Ez az úgynevezett „lengyel írásmód" szokatlan

először, de számos előnye van és bizonyos értelemben sokkal természetesebb. (Megjegyezzük, hogy igen sok kézi számítógép követi ezt az írásmódot, ami lehetővé teszi a regiszterek gazdaságosabb kihasználását és a programok rövidebb előállítását is.)

A jobb megértés végett előrebocsátunk egy példát. (A félreértések elkerülésére a műveleteket most nagybetűkkel jelöljük.) Tekintsük például a valós számok körében a következő műveleteket: Az összeadást, vagyis azt az S kétváltozós műveletet, amely az (a, b) párhoz az $a + b$ elemet rendeli hozzá. A szorzást, azaz a $P : (a, b) \mapsto ab$ műveletet. Legyen továbbá $H(a, b) = a^b$ (tekintsünk el attól, hogy ez esetenként értelmetlen), $N(a) = -a$ és $E = 1$. Ezeknek a műveleteknek a változószáma rendre $2, 2, 2, 1, 0$.

A műveleteket úgy írjuk fel, hogy előreírjuk a műveleti jelet, és utána – zárójelek nélkül! – azt az elemrendszert, amire a műveletet alkalmazni akarjuk. Így például $Sab = a+b$, $Pxy = xy$ stb. Ez az írásmód akkor is alkalmazható, hogy ha több műveletet kell végeznünk egymás után. Írjuk fel így először az $(a+b)c$ kifejezést. Ez szorzat, tehát a P betűvel kell kezdeni. A szorzat első tényezője Sab, a második c; így a kifejezés $PSabc$ lesz. Ha a fenti betűsorozatot leírjuk, abból vissza is olvasható, hogy melyik (számunkra „érthető” formában megadott) kifejezésről van szó. Hasonlóképpen például $ac + bc$ nem más, mint „összege a és c, valamint b és c szorzatának”: $SPacPbc$. Még összetettebb mondjuk az $(1 - u)^{x+y}$ felírása: $HSENuSxy$. Vigyázni kell azonban arra, hogy nem minden betűsorozat értelmes. Például az aSb betűsorozatnak nincs értelme, mert az S betű után két másik betűnek (vagy két értelmes betűsorozatnak) kell állnia. Ugyancsak nem ad formulát az $Sabc$ sorozat sem, mert itt fennmarad egy felesleges c betű. Látható, hogy a sorozat végén mindig olyan betűnek kell állnia, amelyikkel műveletet végzünk. Állhat ezért műveleti jel is a sorozat végén; nevezetesen az E, mert az nullváltozós – nem kell tehát, hogy valamire „vonatkozzon” (aNE nem más, mint $a - 1$). A kifejezések algebráját hasonlóképpen lehetne megkonstruálni, mint azt a szabad félcsoportoknál tettük. A fentiek alapján viszont a kifejezéseket (zárójelek nélküli!) betűsorozatoknak tekinthetjük, amelyek éppen a szereplő jelek generálta szabad félcsoport elemeinek tekinthetők. Ezt az elképzelést fogjuk követni, ügyelve arra, hogy a kifejezések pontosan az „értelmes” sorozatok legyenek.

11.1. Tétel. *Legyen $\tau : \mathbf{F} \to \mathbb{N}$ tetszőleges típus és $\mathbf{X}$ az $\mathbf{F}$-től idegen halmaz. Legyen $\mathfrak{S} = \mathfrak{S}(\mathbf{X}, \mathbf{F})$ az $\mathbf{X} \cup \mathbf{F}$ halmaz generálta szabad félcsoport az $S(\mathbf{X}, \mathbf{F})$ tartóhalmazzal és az egymás mellé írással mint művelettel. Az $\mathfrak{S}(\mathbf{X}, \mathbf{F})$ félcsoport egy τ típusú $\langle S(\mathbf{X}, \mathbf{F}), F\rangle$ algebrává tehető a következő módon:*

Az $\mathbf{F}$ minden egyes $\mathbf{f}$ eleméhez hozzárendelünk egy $n = \tau(\mathbf{f})$ változós $\varphi_{\mathbf{f}}$ függvényt, amelyet

$$\varphi_{\mathbf{f}}(\mathbf{w}_1, \ldots, \mathbf{w}_n) = \mathbf{f}\mathbf{w}_1 \ldots \mathbf{w}_n$$

definiál a félcsoport tetszőlegesen adott $\mathbf{w}_1, \ldots, \mathbf{w}_n$ szavaira.

Bizonyítás. Mivel a szabad félcsoportban a szavak felírása egyértelmű, ezért a kérdéses $\varphi_{\mathbf{f}}$ függvények jól definiáltak. Az pedig, hogy a definiált algebra τ típusú, azonnal adódik a definícióból – hiszen éppen így definiáltuk. ■

A következőkben kiválasztjuk az „értelmes” kifejezéseket. Ebben az elképzelésben segítségünkre lehet bizonyos számítógépes rendszer, ahol „zsákautomaták” szerepelnek. Itt az adatokat és műveleteket egymás után „bedobáljuk” egy zsákba. Az adatok „súlya” egyre nyújtja a zsákot; mindig a legutóbb bedobott adat van felül. Amikor egy n-változós műveletet „dobunk be”, akkor ez a „legfelül levő” n adaton végzi el a műveletet, ezeket az

adatokat „törli” és helyükbe a művelet eredményét írja. A zsák „megnyúlása” $(n-1)$-gyel rövidebb lesz. Az automata akkor működik eredményesen, ha végezetül egy adat marad meg (a végeredmény) és közben mindig marad adat a zsákban. Ezt definiáljuk most „precízen”:

11.2. Definíció. Definiáljuk a 11.1. tételben megadott $\mathfrak{S}$ félcsoport elemeinek a μ súlyát a következőképpen:

(1) Legyen $\mu(\mathbf{x}) = 1$, ha $\mathbf{x} \in \mathbf{X}$ és $\mu(\mathbf{f}) = 1 - \tau(\mathbf{f})$, ha $\mathbf{f} \in \mathbf{F}$.

(2) Tetszőleges $\mathbf{w}$ szó $\mu(\mathbf{w})$ súlya legyen egyenlő a szóban szereplő betűk súlyának – multiplicitással vett – összegével.

Egy $\mathbf{w}$ szót τ típusú kifejezésnek nevezünk, ha kielégíti az alábbi két feltételt:

a) Bármely $\mathbf{w} = \mathbf{uv}$ felbontás esetén $\mathbf{v}$ súlya pozitív.

b) $\mu(\mathbf{w}) = 1$. □

11.3. Tétel. *Az $\langle S(\mathbf{X}, \mathbf{F}), F\rangle$ algebrában a τ típusú kifejezések egy $\mathfrak{F}(\tau, \mathbf{X})$ részalgebrát, az úgynevezett $\mathbf{X}$ feletti τ típusú kifejezésalgebrát alkotnak. Ennek az algebrának $\mathbf{X}$ generátorrendszere. Az algebra bármely, legalább 2 hosszúságú $\mathbf{w}$ eleméhez létezik egy egyértelműen meghatározott n-változós $\varphi_{\mathbf{f}}$ művelet (n pozitív) és léteznek ugyancsak egyértelműen meghatározott, $\mathbf{w}$-nél rövidebb $\mathbf{w}_1, \ldots, \mathbf{w}_n$ szavak, amelyekre $\mathbf{w} = \varphi_{\mathbf{f}}(\mathbf{w}_1, \ldots, \mathbf{w}_n)$ teljesül.*

Bizonyítás. Mindenekelőtt megjegyezzük, hogy a vizsgált szabad félcsoportban a súly – definíció szerint – additív, azaz a szorzat súlya megegyezik a tényezők súlyának az összegével. Ebből az is adódik, hogy az 1 súlyú szavak részalgebrát alkotnak. Ha ugyanis $\varphi_{\mathbf{f}}$ egy n-változós művelet és $\mathbf{w}_1, \ldots, \mathbf{w}_n$ 1 súlyú szavak, akkor $\mathbf{w} = \varphi\mathbf{f}(\mathbf{w}_1, \ldots, \mathbf{w}_n)$ súlya: $\mu(\mathbf{f}) +$

$+ \mu(\mathbf{w}_1) + \cdots + \mu(\mathbf{w}_n) = (1-n) + \overbrace{1 + \cdots + 1}^{n \text{ darab}} = 1.$

Tegyük most fel, hogy minden egyes $\mathbf{w}$ eleget tesz az a) feltételnek is. Ekkor $\mathbf{w}$ bármely felbontása $(\mathbf{f}\mathbf{w}_1 \ldots \mathbf{w}_{i-1}\mathbf{u}_i)\cdot(\mathbf{v}_i\mathbf{w}_{i+1} \ldots \mathbf{w}_n)$ alakú. Itt $\mathbf{u}_i\mathbf{v}_i$ a $\mathbf{w}_i$ egy felbontása, amiből feltétel szerint az is következik, hogy $\mathbf{v}_i$ súlya pozitív. A súlyra vonatkozó megjegyzés szerint ebből következik, hogy $\mu(\mathbf{v}_i\mathbf{w}_{i+1} \ldots \mathbf{w}_n) \geq 1 - (n-i)$. Ez nemcsak azt jelenti, hogy a kapott súly pozitív, hanem azt is, hogy a súly nagyobb, mint $n-i$. Tekintettel arra, hogy $\mathbf{w}_{i+1} \ldots \mathbf{w}_n$ súlya (az additivitás következtében) pontosan $n-i$, ezért az a leghosszabb $\mathbf{v}$ szó, amelyre $\mathbf{w} = \mathbf{uv}$, $\mu(\mathbf{v}) = n-i$ és $\mathbf{v} \neq \mathbf{w}$ teljesül, pontosan $\mathbf{w}_{i+1} \ldots \mathbf{w}_n$.

Ezzel természetesen azt már beláttuk, hogy a kifejezések valóban egy τ típusú (rész)algebrát alkotnak. Azt, hogy $\mathbf{X}$ generátorrendszer, és hogy felépítését minden elem egyértelműen meghatározza, egyszerre bizonyítjuk a szó hosszára vonatkozó teljes indukcióval. Ha a szó 1 hosszúságú, akkor ez egy 1 súlyú betű, tehát vagy generátorelem, vagy nullváltozós művelet. Ezek benne vannak a generátumban, s a második állítás nem vonatkozik rájuk.

Tegyük most fel, hogy a két állítás igaz minden, k-nál rövidebb szóra, és legyen $\mathbf{w}$ egy k hosszúságú szó. Bontsuk fel e szót $\mathbf{uv}$ alakba úgy, hogy $\mathbf{u}$ hossza 1 legyen. Mivel $\mathbf{v}$ súlya pozitív és $\mathbf{w}$ súlya 1, ezért $\mathbf{u}$ súlya vagy 0, vagy negatív; $\mathbf{u}$ tehát mindenképpen egy $\mathbf{f}$ n-változós műveleti jel (n pozitív); továbbá $\mathbf{v}$ súlya pontosan n. A feltételből az is következik, hogy $\mathbf{w}$-ben – és így $\mathbf{v}$-ben is – az utolsó betű súlya pozitív, tehát csak 1 lehet. Az is nyilvánvaló, hogy ha egy 1 betűvel hosszabb szót veszünk és annak a súlya az eredetinél nagyobb, akkor csak 1-gyel lehet nagyobb annál. Ezért $\mathbf{v}$ felírható $\mathbf{v} = \mathbf{w}_1 \ldots \mathbf{w}_n$ alakban,

ahol $\mathbf{w}_{i+1} \dots \mathbf{w}_n$ a leghosszabb olyan szelete a $\mathbf{v}$-nek, amelynek a súlya $n - i$. Ilyen szavak tehát léteznek, s mint láttuk, $\mathbf{w}$ e szavakat $\mathbf{f}$ ismeretében egyértelműen meghatározza. $\mathbf{f}$ viszont nem más, mint $\mathbf{w}$ első betűje, tehát ez is egyértelműen meghatározott. Azt kell még belátni, hogy minden egyes kapott szó kielégíti a tétel a) és b) feltételeit, és hogy eleme az $\mathbf{X}$ generálta részalgebrának. Ez utóbbi triviálisan fog következni az előbbiből a teljes indukciós feltétel miatt – hiszen e szavak mindegyike legfeljebb olyan hosszú, mint $\mathbf{v}$, ami $\mathbf{w}$-nél határozottan rövidebb.

Azonnal kapjuk a b) feltételt a következőkből:

$$\mu(\mathbf{w}_i) = \mu(\mathbf{w}_i \dots \mathbf{w}_n) - \mu(\mathbf{w}_{i+1} \dots \mathbf{w}_n) = (n - i + 1) - (n - i) = 1.$$

Az a) feltétel bizonyításához legyen $\mathbf{w}_i = \mathbf{u}_i \mathbf{v}_i$. Feltétel szerint $\mu(\mathbf{v}_i \mathbf{w}_{i+1} \dots \mathbf{w}_n) \geq n - i + 1 = \mu(\mathbf{w}_{i+1} \dots \mathbf{w}_n) + 1$, amiből a súly additivitása miatt $\mu(\mathbf{v}_i)$ pozitivitása következik. ■

Érdemes a 11.3. tétel utolsó állítását kissé jobban szemügyre venni. Ez a tulajdonság igen fontos, és azt fejezi ki, hogy két kifejezés csak akkor egyezik meg, ha pontosan ugyanúgy van felépítve a határozatlanokból. Másképpen ezt úgy is fogalmazhatjuk, hogy ha megadunk egy kifejezést, akkor ez *egyértelműen* elárulja azt is, hogy ezt a kifejezést miképpen építettük fel. Ennek a tulajdonságnak van egy fontos következménye, amelyet a következőkben vizsgálunk majd meg.

11.2. Szabad algebrák

A kifejezésalgebrák egy fontos tulajdonságát fogalmazzuk meg. Azt, hogy a kifejezésalgebrák valóban ilyen tulajdonságúak, csak később fogjuk belátni. A tulajdonság, amiről beszélünk, az, hogy az algebra szabad. Szabad algebrákról speciális esetekben már volt szó, ezeket most általában definiáljuk.

11.4. Definíció. Legyen $\mathcal{K}$ adott τ típusú algebrák egy osztálya. Egy τ típusú $\mathfrak{F}(\mathcal{K}, \mathbf{X})$ algebrát az $\mathbf{X}$ halmaz generálta $\mathcal{K}$ fölött szabad vagy $\mathcal{K}$-szabad algebrának nevezünk, ha a következők teljesülnek:

Válasszunk ki $\mathcal{K}$-ból egy tetszőleges $\mathfrak{A}$ algebrát, és tekintsünk egy tetszőleges φ függvényt, amely az $\mathbf{X}$ halmazt a kiszemelt algebra A tartóhalmazába képezi. Ekkor mindig létezik olyan $\psi : \mathfrak{F}(\mathcal{K}, \mathbf{X}) \to \mathfrak{A}$ homomorfizmus (tehát művelettartó leképezés), amelynek az $\mathbf{X}$-re való megszorítása megegyezik φ-vel. □

Megjegyzések. 1. Algebraosztályon mindig *absztrakt osztályt* értünk; ami azt jelenti, hogy az osztály minden elemével együtt annak minden izomorf képét is odaszámítjuk. Így például az összes permutációcsoport nem absztrakt osztály, de az összes kételemű csoport már az.

2. Algebraosztályról beszélünk és nem algebrahalmazról. Absztrakt algebraosztály esetén nem is lehet másképpen (kivéve, ha az osztály üres). Ugyanis bármely elemmel együtt hozzátartoznak azok az elemek is, amelyek úgy állnak elő, hogy az eredeti algebrát a rendszámokkal indexezzük. Ezek mind különbözőek, „annyian vannak, mint a rendszámok”; amelyek nem alkotnak halmazt.

3. A műveletartást természetesen a következőképpen értjük: Ha $\mathbf{f}$ egy n-változós műveleti név és $\mathfrak{A}$-ben $f_{\mathfrak{A}}$, $\mathfrak{B}$-ben $f_{\mathfrak{B}}$ realizálja, továbbá a_i-nek b_i a képe, akkor $f_{\mathfrak{A}}(a_1, \dots, a_n)$ képe $f_{\mathfrak{B}}(b_1, \dots, b_n)$. □

Abból a feltételből, hogy $\mathbf{X}$ generátorrendszer, következik, hogy a φ függvényt legfeljebb egyféleképpen terjeszthetjük ki homomorfizmussá. A fenti definícióból tehát kiolvasható a

11.5. Tétel. *A 11.4. definícióban szereplő φ függvény a ψ homomorfizmust egyértelműen meghatározza.* ■

Megjegyezzük, hogy a definícióban nem állítottuk, hogy egy szabad algebra maga is feltétlenül eleme a vizsgált algebraosztálynak. Ez általában nem is igaz. Az sem igaz, hogy egy algebraosztályhoz és egy generátorhalmazhoz pontosan egy szabad algebra tartozna. Az összes szóba jövő szabad algebrák között létezik egy legnagyobb – ami az osztálytól nem függ, és létezik egy legkisebb – ami már függ az osztálytól.

11.6. Tétel. *Bármely kifejezésalgebra a τ típusú algebrák bármely osztálya fölött szabad.*

Bizonyítás. Tekintsük az $\mathfrak{F}(\tau, \mathbf{X})$ algebrát és az adott algebraosztály egy $\mathfrak{A}$ elemét. Legyen $\mathbf{f}_{\mathfrak{A}}$ a $\mathbf{f}$ műveleti névnek az $\mathfrak{A}$-ban megfelelő művelet. A ψ leképezést rekurzívan definiáljuk. Vegyük először az 1 hosszúságú szavakat. Ha $\mathbf{w} \in \mathbf{X}$, akkor legyen $\psi(\mathbf{w}) = \varphi(\mathbf{w})$. Ha $\mathbf{w} \in \mathbf{F}$, akkor $\mathbf{w}$ egy $\mathbf{f}$ nullváltozós műveleti név. Legyen $\mathfrak{A}$-ban a megfelelő nullváltozós művelet értéke $a_{\mathbf{f}}$, és legyen $\psi\mathbf{f} = a_{\mathbf{f}}$. Ez a megfeleltetés művelettartó abban az értelemben, hogy ha egy $\mathfrak{F}(\tau, \mathbf{X})$-beli művelet eredménye 1 hosszúságú szó, akkor teljesül a művelettartás. Az is világos, hogy ψ-t az $\mathbf{X}$-re megszorítva pontosan a φ-t kapjuk.

Tegyük most fel, hogy a k-nál rövidebb szavakra már definiáltuk ψ-t úgy, hogy az $\mathbf{X}$-re való megszorítása megegyezik φ-vel; továbbá, ha $\varphi_{\mathbf{f}}(\mathbf{w}_1, \ldots, \mathbf{w}_n)$ k-nál rövidebb szó, akkor $\psi(\varphi_{\mathbf{f}}(\mathbf{w}_1, \ldots, \mathbf{w}_n)) = \mathbf{f}_{\mathfrak{A}}(\psi(\mathbf{w}_1), \ldots, \psi(\mathbf{w}_n))$. Legyen most $\mathbf{w}$ tetszőleges k hosszúságú szó. A 11.3. tétel szerint ez a szó egyértelműen felírható $\mathbf{w} = \mathbf{f}\mathbf{w}_1 \ldots \mathbf{w}_n = \varphi_{\mathbf{f}}(\mathbf{w}_1, \ldots$ $\ldots, \mathbf{w}_n)$ alakban, ahol $\mathbf{w}_1, \ldots, \mathbf{w}_n$ mind k-nál rövidebb szavak. Mivel e szavak k-nál rövidebbek, ezért a képük már egyértelműen meghatározott. Eszerint $\mathbf{w}$ képe is egyértelműen meghatározható a $\psi(\mathbf{w}) = \mathbf{f}_{\mathfrak{A}}(\psi(\mathbf{w}_1), \ldots, \psi(\mathbf{w}_n))$ összefüggéssel. A művelettartást figyelembe véve csak ez lehet $\mathbf{w}$ képe, és a definíció egyben biztosítja, hogy a művelettartás teljesül minden olyan esetben, amikor a művelet értéke k hosszúságú szó. Tekintettel arra, hogy csak k hosszúságú szavak képét definiáltuk ebben a lépésben, ezért ψ-nek $\mathbf{X}$-re való megszorítása φ marad.

Ezzel a φ kiterjeszthetőségét bizonyítottuk. Az pedig, hogy $\mathbf{X}$ generálja a kifejezésalgebrát, már a 11.3. tételben szerepelt. ■

A 11.4. definíció lényegében azt mondja ki, hogy a $\mathcal{K}$ fölötti szabad algebrákban a generátorrendszer elemei között semmi más összefüggés nincs, mint aminek az osztály minden algebrájában bárhogyan felvett elemek között teljesülnie kell. A 11.6. tétel pedig azt jelenti, hogy a kifejezésalgebra ilyen. Ez nyilvánvalóan teljesül, hiszen a kifejezésalgebrában a generátorelemek között egyáltalán nincs semmiféle összefüggés. (Természetesen ezt pontosan be kell bizonyítani – amint ezt az idézett tételben tettük.) Elképzelhető azonban, hogy a vizsgált algebraosztályban bizonyos összefüggések mindig teljesülnek (pl. a félcsoportok körében az asszociativitás). Egy-egy szabad algebra tehát annál jobban jellemző az algebraosztályra, minél „közelebb” van hozzá, minél több olyan összefüggés teljesül benne, ami az osztály minden elemére igaz. Tulajdonképpen ez valószínűsíti azt, hogy létezik egy legközelebbi szabad algebra is, amelyben pontosan azok az összefüggések teljesülnek, amelyek az osztályban minden lehetséges esetben fennállnak. Mindenekelőtt a közelséget fogalmazzuk meg pontosan.

11.7. Definíció. Azt mondjuk, hogy az $\mathfrak{F}_2(\mathcal{K}, \mathbf{X})$ szabad algebra közelebb fekszik a $\mathcal{K}$ osztályhoz, mint az $\mathfrak{F}_1(\mathcal{K}, \mathbf{X})$, ha létezik olyan $\sigma : \mathfrak{F}_1 \to \mathfrak{F}_2$ homomorfizmus, amelynek az $\mathbf{X}$ generátorrendszerre való megszorítása az identitás.

(Könnyen belátható, hogy a „közelebb fekvés" ekvivalenciától eltekintve valóban rendezés.)

A továbbiakban fel fogjuk használni a „második izomorfizmustételt", amelyet most pontosan idézünk:

2.24. Tétel. *Legyen adva a $\psi : \mathfrak{A} \to \mathfrak{C}$ és a szürjektív $\varphi : \mathfrak{A} \to \mathfrak{B}$ homomorfizmus úgy, hogy* $\mathrm{Ker}\,(\varphi) \leq \mathrm{Ker}\,(\psi)$. *Ekkor létezik pontosan egy olyan $\sigma : \mathfrak{B} \to \mathfrak{C}$ homomorfizmus, amelyre $\psi = \sigma \circ \varphi$.*

Ez a tétel megfordítható:

11.8. Tétel. *Ha a 2.24. tételben a szürjektív ψ homomorfizmusra $\psi = \sigma\varphi$, akkor* $\mathrm{Ker}\ \varphi \leq \mathrm{Ker}\ \psi$.

Bizonyítás. Ha $(a, b) \in \mathrm{Ker}\ \varphi$, azaz $\varphi a = \varphi b$, akkor $\psi a = \sigma\varphi a = \sigma\varphi b = \psi b$, azaz $(a, b) \in \mathrm{Ker}\ \psi$. ■

11.9. Tétel. *Legyen $\mathcal{C}$ az $\mathfrak{F} = \mathfrak{F}(\tau, \mathbf{X})$ kongruenciáinak hálója és jelölje $\mathcal{C}(\mathcal{K})$ a $\mathcal{C}$ azon Θ elemeinek a halmazát, amelyre $\mathfrak{F}/\Theta$ izomorf egy $\mathcal{K}$-beli algebra valamelyik részalgebrájával. $\mathfrak{F}/\Theta$ pontosan akkor lesz az $\mathbf{X}$ generálta, $\mathcal{K}$ feletti szabad algebra, ha ez a Θ alsó korlátja $\mathcal{C}(\mathcal{K})$ minden elemének. $\mathfrak{F}/\Theta_2$ pontosan akkor fekszik közelebb a $\mathcal{K}$ osztályhoz, mint $\mathfrak{F}/\Theta_1$, ha $\Theta_1 \leq \Theta_2$. Ennek megfelelően, ha Θ_0 jelöli a $\mathcal{C}(\mathcal{K})$ elemeinek a legnagyobb alsó korlátját, akkor $\mathfrak{F}/\Theta_0$ a $\mathcal{K}$-hoz legközelebbi szabad algebra.*

Bizonyítás. Mindegyik állítás triviális abban az esetben, amikor $\mathcal{K}$-nak minden eleme egyelemű algebra. Ezzel az esettel a továbbiakban nem foglalkozunk.

Legyen Θ tetszőleges alsó korlátja a $\mathcal{C}(\mathcal{K})$ összes Θ_i elemének. Válasszuk ki az $\mathbf{X}$ generátorhalmaz két tetszőleges ($\mathbf{x}$ és $\mathbf{y}$) elemét. Képezze le φ a generátorhalmazt a $\mathcal{K}$ egy legalább kételemű algebrájába úgy, hogy a két kiválasztott elem képe különbözzék ($\mathcal{K}$-ban van legalább kételemű algebra). Ekkor a 11.6. tétel szerint e leképezés kiterjeszthető $\mathfrak{F}$ egy ψ homomorfizmusává. E homomorfizmusra tehát $\mathrm{Im}\ \psi$ egy $\mathcal{K}$-beli algebra részalgebrája; vagyis $\mathrm{Ker}\,\psi \in \mathcal{C}(\mathcal{K})$. A Θ választása szerint $\Theta \leq \mathrm{Ker}\,\psi$; és így az $(\mathbf{x}, \mathbf{y}) \notin \mathrm{Ker}\,\psi$ feltételből $(\mathbf{x}, \mathbf{y}) \notin \Theta$ is következik. Ez azt jelenti, hogy a $\varrho : \mathfrak{F} \to \mathfrak{F}/\Theta$ természetes homomorfizmusnak a generátorrendszerre való megszorítása az identitás. Más szóval $\mathfrak{F}/\Theta$ is az $\mathbf{X}$ generálta algebra, mert $\varrho : \mathbf{X} \to \varrho\mathbf{X}$ bijekció. Képezzük most le φ-vel $\varrho\mathbf{X}$-et $\mathcal{K}$ egy tetszőleges $\mathfrak{A}$ elemébe. A 11.6. tétel alapján létezik olyan $\psi : \mathfrak{F} \to \mathfrak{A}$ homomorfizmus, amelynek a generátorrendszerre való megszorítása megegyezik $\varphi\varrho$-val. Most is nyilvánvalóan teljesül a $\mathrm{Ker}\,\psi \in \mathcal{C}(\mathcal{K})$ feltétel, amiből $\Theta \leq \mathrm{Ker}\,\psi$ következik. Ez azt jelenti, hogy $\varrho a = \varrho b$ esetén $(a, b) \in \Theta$, tehát $(a, b) \in \mathrm{Ker}\,\psi$, és így $\psi a = \psi b$. Eszerint az a ψ' megfeleltetés, amely a ϱa elemet ψa-ba képezi, egyértelmű megfeleltetés. Ebből triviális számolással – amelyet az olvasóra bízunk – adódik, hogy ψ' az $\mathfrak{F}/\Theta$-t műveletartó módon képezi $\mathfrak{A}$-ba. Mivel $\psi'\varrho$ és ψ az $\mathbf{X}$ generátorrendszeren ugyanúgy hatnak, ezért e két homomorfizmus megegyezik (11.5. tétel). Továbbá, ψ' a $\varrho\mathbf{x}$ generátorelemet $\psi\mathbf{x}$-be

viszi, ami ψ definíciója szerint éppen $\varphi\varrho\mathbf{x}$. Így ψ' a generátorelemekre megszorítva a φ-t adja, vagyis $\mathfrak{F}/\Theta$ szabad.

Legyen most $\mathfrak{F}_i = \mathfrak{F}/\Theta_i$; és legyen $\sigma_i : \mathfrak{F} \to \mathfrak{F}_i$ a természetes homomorfizmus ($i = 1, 2$). A 11.8. tétel szerint a $\sigma : \mathfrak{F}_1 \to \mathfrak{F}_2$ tulajdonságú σ pontosan a $\Theta_1 \leq \Theta_2$ esetben létezik.

A harmadik állítás bizonyításához elég annyit figyelembe venni, hogy a kongruenciák hálója teljes. Így létezik a kívánt legnagyobb alsó korlát. Az előző állítás szerint a legnagyobb alsó korláthoz tartozó faktoralgebra éppen a $\mathcal{K}$-hoz legközelebbi szabad algebra. ■

11.10. Tétel (a 10.9. tétel kiegészítése)**.** *A $\mathcal{K}$-hoz legközelebbi szabad algebrák előállíthatók $\mathcal{K}$-beli algebrák részalgebrái direkt szorzatának részalgebráiként.*

Bizonyítás. Legyen $\sigma_0 : \mathfrak{F} \to \mathfrak{F}_0 = \mathfrak{F}/\Theta_0$ a $\mathcal{K}$-hoz legközelebbi szabad algebrára való természetes leképezés. Legyenek továbbá a $\mathcal{C}(\mathcal{K})$-beli Θ_i-kre $\psi_i : \mathfrak{F} \to \mathfrak{F}/\Theta_i$ természetes homomorfizmusok. $\Theta_i \geq \Theta_0$ következtében a 11.8. tétel alapján a $\sigma_0 a \mapsto \psi_i a$ megfeleltetés homomorfizmus. Ebből következik, hogy a fenti algebrák direkt szorzatába való $\sigma_0 a \mapsto (\ldots, \psi_i a, \ldots)$ megfeleltetés is homomorfizmus. Ez a homomorfizmus azonban injektív. Valóban, ha $\sigma_0 a$ és $\sigma_0 b$ képe megegyezik, akkor a képvektorok minden koordinátája megegyezik, azaz minden szóba jövő i-re $\psi_i a = \psi_i b$ teljesül. Ez azt jelenti, hogy (a, b) minden egyes Θ_i-nek eleme. Ezért eleme ezek metszetének is, ami éppen Θ_0. Így $\sigma_0 a = \sigma_0 b$, ami valóban az injektivitást jelenti. Az $\mathfrak{F}/\Theta_i$-k $\mathcal{K}$-beli algebrák részalgebráival izomorfak. Ezeknek képeztük a direkt szorzatát, és $\mathfrak{F}_0$ e direkt szorzat egy részalgebrájával volt izomorf. Az állítás most már következik abból, hogy absztrakt algebraosztályt vizsgálunk. ■

11.11. Következmény. *Ha egy adott számosságú halmaz generálta szabad algebra benne van egy algebraosztályban, akkor ez – izomorfizmustól eltekintve – az osztályban levő egyetlen ezen számosságú halmazzal generált $\mathcal{K}$-szabad algebra.*

Bizonyítás. Ha az $\mathfrak{F}/\Theta_1$ szabad algebra eleme az osztálynak, akkor $\Theta_1 \in \mathcal{C}(\mathcal{K})$ miatt $\Theta_0 \leq \Theta_1$. Mivel a fordított irányú kapcsolatot már beláttuk, ezért valóban következik az egyértelműség. ■

11.12. Következmény. *Ha egy $\mathcal{K}$ (absztrakt) algebraosztály minden elemével együtt annak minden részalgebráját és elemeivel együtt azoknak direkt szorzatait is tartalmazza, akkor benne van minden $\mathcal{K}$-szabad algebra is.*

Bizonyítás. A 11.10. tételből következik, hogy a hozzá legközelebbi szabad algebrák benne vannak az osztályban. A 11.11. következmény szerint pedig ezek egyértelműen meghatározottak. ■

Megjegyzés. Természetesen elég sok szabad algebra lehet egy osztályban anélkül, hogy ez az osztály részalgebraképzésre vagy direktszorzat-képzésre zárt volna. Ha tekintjük például az adott típusú kifejezésalgebrák osztályát, akkor ez nyilvánvalóan tartalmazza az összes, hozzá legközelebbi szabad algebrát. Ennek ellenére általában sem részt, sem direkt szorzatot nem tartalmaz. □

11.13. Tétel. *Ha egy absztrakt algebraosztály bármely számosságú halmaz generálta szabad algebrát tartalmaz, akkor minden eleme előállítható egy osztálybeli szabad algebra homomorf képeként.*

Bizonyítás. Legyen $\mathfrak{A}$ a szóban forgó $\mathcal{K}$ osztály egy eleme. Tekintsünk egy szabad generátorhalmazt, amelynek elemszáma megegyezik az $\mathfrak{A}$ tartóhalmazának a számosságával. Ez azt jelenti, hogy a generátorhalmazt szürjektíven leképezhetjük $\mathfrak{A}$-ba. A szabad algebra definíciója szerint ennek létezik egy homomorf kiterjesztése a szabad algebrára, amely természetesen ugyancsak szürjektív. ■

11.3. Azonosságokkal definiálható osztály

A szabad algebrák tárgyalásakor négy „eljárást” találtunk, amelyekkel újabb algebrákat képezhettünk. Ezek: izomorfizmus, részalgebra, homomorfizmus és direkt szorzat. Ez a négy eljárás a következőkben is igen fontos lesz. Mindenekelőtt néhány ezekre vonatkozó eredményt fogalmazunk meg.

11.14. Definíció. Legyen $\mathcal{K}$ tetszőleges (nem feltétlenül absztrakt) algebraosztály.

$I(\mathcal{K})$ jelöli a $\mathcal{K}$-beli algebrákkal izomorf algebrák osztályát.

$S(\mathcal{K})$ jelöli a $\mathcal{K}$-beli algebrák részalgebráinak az osztályát.

$H(\mathcal{K})$ jelöli a $\mathcal{K}$-beli algebrák homomorf képeinek az osztályát.

$P(\mathcal{K})$ jelöli a $\mathcal{K}$-beli algebrákból képezett direkt szorzatok osztályát.

Egy $\mathcal{K}$ algebraosztályt varietásnak nevezünk, ha $S(\mathcal{K})$, $H(\mathcal{K})$ és $P(\mathcal{K})$ részei $\mathcal{K}$-nak. □

Megjegyzések. 1. Egy varietás mindig absztrakt algebraosztály. Mivel minden izomorf kép egyúttal homomorf kép is, ezért bármely $\mathcal{K}$ varietás tartalmazza $I(\mathcal{K})$-t is.

2. Általában, ha absztrakt osztályt akarunk képezni, akkor $S(\mathcal{K})$, illetve $P(\mathcal{K})$ nem vezet ilyenhez, mert egy részalgebra izomorf képe nem részalgebrája az adott algebrának, és hasonló a helyzet direkt szorzat esetében is.

3. A fordított irányú tartalmazások: $\mathcal{K} \subseteq S(\mathcal{K})$, $\mathcal{K} \subseteq H(\mathcal{K})$, $\mathcal{K} \subseteq P(\mathcal{K})$ mindig teljesülnek. Ennek belátását az olvasóra bízzuk. □

11.15. Tétel. *Tetszőleges $\mathcal{K}$ algebraosztályra érvényesek az alábbi összefüggések:*

$$PH(\mathcal{K}) \subseteq HP(\mathcal{K}), \qquad PS(\mathcal{K}) \subseteq SP(\mathcal{K}), \qquad SH(\mathcal{K}) \subseteq HS(\mathcal{K}),$$

$$PP(\mathcal{K}) \subseteq P(\mathcal{K}), \qquad SS(\mathcal{K}) \subseteq S(\mathcal{K}), \qquad HH(\mathcal{K}) \subseteq H(\mathcal{K}).$$

Bizonyítás.

1. Legyen $\mathfrak{A}$ az $\mathfrak{A}_i$ algebráknak, $\mathfrak{B}$ a $\mathfrak{B}_i$ algebráknak a direkt szorzata, és legyenek $\varphi_i : \mathfrak{A}_i \to \mathfrak{B}_i$ szürjektív homomorfizmusok. Az $(\ldots, a_i, \ldots)$ vektornak megfeleltetve a $(\ldots, b_i, \ldots)$ vektort, nyilvánvalóan az $\mathfrak{A}$-nak egy $\mathfrak{B}$-re való szürjektív homomorfizmusát kapjuk. Ez azt jelenti, hogy $\mathcal{K}$-beli algebrák homomorf képeinek a direkt szorzata előállítható ezen algebrák direkt szorzatának egy homomorf képeként.

2. Legyenek most a $\mathfrak{B}_i$-k az $\mathfrak{A}_i$ algebrák részalgebrái. A $\mathfrak{B}_i$-k direkt szorzatában levő vektorok természetesen az $\mathfrak{A}_i$-k direkt szorzatának is elemei, s mivel a $\mathfrak{B}_i$-k a műveletekre zártak, ezért direkt szorzatuk részalgebrája az $\mathfrak{A}_i$-k direkt szorzatának.

3. Legyen $\mathfrak{C}$ az $\mathfrak{A}$ algebra $\mathfrak{B}$ homomorf képének egy részalgebrája. Azok az $\mathfrak{A}$-beli elemek, amelyeknek a képe a fenti homomorfizmusnál $\mathfrak{C}$-be esik, $\mathfrak{A}$-nak egy részalgebráját alkotják. E részalgebrára megszorítva az eredeti homomorfizmust, a kép nyilvánvalóan $\mathfrak{C}$ lesz.

A másik három triviálisan igaz: direkt szorzatok direkt szorzata az eredetinek direkt szorzatával izomorf, részalgebrának a részalgebrája az eredetinek is részalgebrája, homomorf kép homomorf képe az eredetinek is homomorf képe. ■

11.16. Következmény. *A $\mathcal{K}$ algebraosztály akkor és csak akkor varietás, ha $HSP(\mathcal{K}) \subseteq \mathcal{K}$.*

Egy $\mathcal{K}$ algebraosztályt tartalmazó legszűkebb varietás $HSP(\mathcal{K})$.

Bizonyítás. Tetszőleges $\mathcal{K}$ algebraosztályra érvényesek az alábbiak:

1. $HHSP(\mathcal{K}) \subseteq HSP(\mathcal{K})$.

2. $SHSP(\mathcal{K}) \subseteq HSSP(\mathcal{K}) \subseteq HSP(\mathcal{K})$.

3. Felhasználva az izomorfizmus és a részalgebraképzés felcserélhetőségét is:

$PHSP(\mathcal{K}) \subseteq HPSP(\mathcal{K}) \subseteq HSPP(\mathcal{K}) \subseteq HSIP(\mathcal{K}) \subseteq HISP(\mathcal{K}) \subseteq HSP(\mathcal{K})$.

Ezzel beláttuk, hogy $HSP(\mathcal{K})$ mindig varietás.

Tekintsünk most egy tetszőleges algebrát. Vegyük az ebből álló egytényezős direkt szorzatot, továbbá ennek azt a részalgebráját, amelyik a direkt szorzat minden elemét tartalmazza, s végül vegyük azt a homomorfizmust, amely a kapott algebrát – triviális módon – bijektíven leképezi az eredetibe. Amit az eljárás során kaptunk, az direkt szorzat részalgebrájának homomorf képe; ami nyilvánvalóan azt jelenti, hogy $\mathcal{K}$ mindig része $HSP(\mathcal{K})$-nak.

Ha mármost $\mathcal{K}$ benne van egy $\mathcal{V}$ varietásban, akkor teljesül a $HSP(\mathcal{K}) \subseteq HSP(\mathcal{V})$ összefüggés. A varietás definíciójából következik, hogy $P(\mathcal{V}) \subseteq \mathcal{V}$, így $SP(\mathcal{V}) \subseteq S(\mathcal{V}) \subseteq \mathcal{V}$, végül $HSP(\mathcal{V}) \subseteq H(\mathcal{V}) \subseteq \mathcal{V}$. Ez pedig éppen a következmény második állítását bizonyítja.

Ebből következik, hogy ha $\mathcal{K} = HSP(\mathcal{K})$, akkor ez a legkisebb olyan varietás, amely $\mathcal{K}$-t tartalmazza; mindenesetre $\mathcal{K}$ varietás. Ha viszont $\mathcal{K}$ varietás, akkor megegyezik a legkisebb, őt tartalmazó varietással, azaz $HSP(\mathcal{K})$-val. ■

A következőkben azt szeretnénk definiálni, hogy egy algebrában valamilyen azonosság teljesül. Egy egyenlőségen azt értjük, hogy bizonyos elemekből a műveletek segítségével kétféle módon újabb elemeket nyerünk, amelyek megegyeznek. Például az egész számok körében $7 + 7 + 7 = 2 \cdot 10 + 1$. Ez nem azonosság, mert a szereplő négy szám helyébe más értéket írva az egyenlőség nem áll fenn. Ezzel szemben a $3 \cdot (4 + 2) = 3 \cdot 4 + 3 \cdot 2$ esetében bármit írunk a szereplő $2, 3, 4$ számok helyébe, mindig igaz marad az egyenlőség. Egy azonosság tehát azt jelenti, hogy két kifejezésünk van, amelyekben a határozatlanok helyébe akármit is írunk az algebrából, a kapott két elem mindig megegyezik. Világos tehát, hogy valamely algebrának egy azonossága a kifejezésalgebra két eleme közötti kapcsolatot jelent. Kérdés azonban, hogy melyik kifejezésalgebrát tekintsük. Mivel

az azonosságokban akármennyi határozatlan előfordulhat, ezért nem elegendő véges sok elem generálta kifejezésalgebrát venni. Tekintettel azonban arra, hogy egy azonosságban mindig csak véges számú határozatlan léphet fel, ezért elegendő olyan kifejezésalgebrával foglalkozni, amelyet megszámlálható sok elem generál (azaz a generátorelemeket indexezhetjük a természetes számokkal).

11.17. Definíció. Legyen $\mathfrak{F}(\tau, \omega)$ a megszámlálható sok elemmel definiált kifejezésalgebra. Ennek szabad generátorait a továbbiakban $\mathbf{x}_1, \ldots, \mathbf{x}_n, \ldots$ jelöli.

Azt mondjuk, hogy az $\mathfrak{F}(\tau, \omega)$ algebra elemeiből alkotott $(\mathbf{p}, \mathbf{q})$ pár azonosság a τ típusú $\mathfrak{A}$ algebrában, ha a szabad generátoroknak az $\mathfrak{A}$-ba való bármely leképezésekor a leképezésnek a kifejezésalgebrára való homomorf kiterjesztése $\mathbf{p}$-t és $\mathbf{q}$-t az $\mathfrak{A}$ algebrának ugyanarra az elemére képezi le. (E kép természetesen függ a leképezéstől.)

A $(\mathbf{p}, \mathbf{q})$ elempárt azonosságnak nevezzük algebrák egy osztályában, ha az osztály minden elemében azonosság. □

11.18. Tétel. *Ha* $(\mathbf{p}, \mathbf{q})$ *azonosság egy algebraosztályban, akkor azonosság az osztályt tartalmazó legkisebb varietásban is.*

Bizonyítás. Legyen $\mathfrak{A}$ az $\mathfrak{A}_i$ algebrák direkt szorzata, az egyes komponensekre való π_i vetítésekkel. Tekintsünk egy tetszőleges $\varphi : \mathfrak{F}(\tau, \omega) \to \mathfrak{A}$ homomorfizmust. Ha $\pi_i\varphi\mathbf{p} = \pi_i\varphi\mathbf{q}$ teljesül minden i indexre, akkor a $\varphi\mathbf{p}$ és $\varphi\mathbf{q}$ vektorok minden koordinátája megegyezik; így a két vektor is egyenlő. Tehát a $\mathcal{K}$-ban teljesülő tetszőleges azonosság igaz $P(\mathcal{K})$-ban is.

Legyen $\mathfrak{B} \leq \mathfrak{A}$ és $\varphi : \mathfrak{F}(\tau, \omega) \to \mathfrak{B}$ tetszőleges homomorfizmus. Mivel φ egyúttal $\mathfrak{A}$-ba is képez, ezért, ha $(\mathbf{p}, \mathbf{q})$ azonosság $\mathfrak{A}$-ban, akkor azonosság $\mathfrak{B}$-ben is. Ez azt jelenti, hogy minden $\mathcal{K}$-beli azonosság azonosság $SP(\mathcal{K})$-ban is.

Legyen most $\alpha : \mathfrak{A} \to \mathfrak{B}$ szürjektív homomorfizmus, és φ a szabad generátoroknak $\mathfrak{B}$-be való leképezése. Az α szürjektivitása miatt minden egyes i indexhez található olyan $a_i \in \mathfrak{A}$, hogy $\alpha a_i = \varphi\mathbf{x}_i$. Egy-egy ilyen a_i-t kiválasztva, a szabad algebra definíciója szerint létezik olyan $\psi : \mathfrak{F}(\mathcal{K}, \omega) \to \mathfrak{B}$ homomorfizmus, amelyre $a_i = \psi\mathbf{x}_i$. Az $\alpha\psi$ homomorfizmus ψ definíciója szerint éppen a φ (egyik) kiterjesztése. Ha mármost $\psi\mathbf{p} = \psi\mathbf{q}$, akkor ebből nyilvánvalóan következik $\alpha\psi\mathbf{p} = \alpha\psi\mathbf{q}$. Végeredményben azt kaptuk, hogy a $\mathcal{K}$-beli azonosságok $HSP(\mathcal{K})$-ban is teljesülnek. ■

A varietások és az azonosságok kapcsolatának a leírásához szükségünk lesz a szabad algebrák két egyszerű tulajdonságára.

11.19. Tétel. *Legyen* $\mathcal{K}$ *egy rögzített* τ *típusú algebraosztály, és* $\alpha : \mathbf{X} \to \mathbf{Y}$ *a szabad generátorhalmazok egy leképezése. Ha* α *injektív (szürjektív) leképezés, akkor* α*-nak a szabad algebrákra való kiterjesztése is az.*

Bizonyítás. A két állítást egyszerre bizonyítjuk. Egy leképezés injektivitása ugyanis azt jelenti, hogy létezik bal oldali inverze, szürjektivitása pedig a jobb oldali inverz létezésével ekvivalens. Eszerint feltételeink úgy foglalhatók egybe, hogy van olyan $\alpha : \mathbf{X} \to \mathbf{Y}$ és $\beta : \mathbf{Y} \to \mathbf{X}$ leképezés, hogy $\beta\alpha$ az $\mathbf{X}$ halmaz identitása. (Ekkor α injektív és β szürjektív.) A szabad algebra definíciója szerint a megfelelő $\alpha' : \mathfrak{F}(\mathcal{K}, \mathbf{X}) \to \mathfrak{F}(\mathcal{K}, \mathbf{Y})$ és

$\beta' : \mathfrak{F}(\mathcal{K}, \mathbf{Y}) \to \mathfrak{F}(\mathcal{K}, \mathbf{X})$ homomorfizmusok léteznek és $\beta'\alpha'$-nek az $\mathbf{X}$-re való megszorítása az identitás. A kiterjesztés egyértelműsége szerint ekkor $\beta\alpha$ is csak az identitás lehet, amiből azonnal következik, hogy α' injektív és β' szürjektív. ■

11.20. Tétel. *Legyen az adott típusú $\mathcal{K}$ varietás része az ugyanilyen típusú $\mathcal{K}^*$ varietásnak. Ekkor bármely $\mathbf{X}$ generátorhalmazra létezik olyan szürjektív $\psi : \mathfrak{F}(\mathcal{K}^*, \mathbf{X}) \to \mathfrak{F}(\mathcal{K}, \mathbf{X})$ homomorfizmus, amelynek az $\mathbf{X}$-re való megszorítása az identitás.*

Bizonyítás. Mivel mindkét osztály varietás, ezért léteznek a megfelelő szabad algebrák. Tekintettel arra, hogy $\mathcal{K}^*$ nagyobb, ezért tartalmazza az $\mathfrak{F}(\mathcal{K}, \mathbf{X})$ algebrát. Mivel ebben a varietásban $\mathfrak{F}(\mathcal{K}^*, \mathbf{X})$ szabad, ezért a $\iota : \mathbf{X} \to \mathbf{X}$ identikus leképezésnek létezik egy $\psi : \mathfrak{F}(\mathcal{K}^*, \mathbf{X}) \to \mathfrak{F}(\mathcal{K}, \mathbf{X})$ kiterjesztése, amely szürjektív, hiszen a kép tartalmaz egy generátorrendszert. ■

11.21. Definíció. Legyen Σ az $\mathfrak{F}(\tau, \omega)$ elemeiből alkotott elempárok halmaza. Az $\mathfrak{A}$ algebrát Σ modelljének nevezzük, ha Σ minden eleme azonosság $\mathfrak{A}$-ban. Ha a $\mathcal{K}$ algebraosztály minden eleme modellje Σ-nak, akkor azt mondjuk, hogy $\mathcal{K}$ is modellje Σ-nak. Ha $\mathcal{K}$ még tartalmazza is a Σ összes modelljét, akkor $\mathcal{K}$-t a Σ-val definiált osztálynak nevezzük. Ha $\mathcal{K}$-hoz létezik olyan Σ halmaz, hogy $\mathcal{K}$ éppen a Σ-val definiált osztály, akkor azt mondjuk, hogy $\mathcal{K}$ azonosságokkal definiálható. □

Megjegyzés. A definícióból világos, hogy „azonosságokkal definiálható osztály” a következőket jelenti: Felírunk egy azonosságokból álló halmazt; s az osztály éppen azokból az algebrákból áll, amelyekben a felsorolt azonosságok igazak. □

11.22. Tétel (Birkhoff)**.** *Egy algebraosztály akkor és csak akkor definiálható azonosságokkal, ha varietás.*

Bizonyítás. Ha az osztály azonosságokkal definiálható, akkor a 11.18. tétel szerint az osztály varietás.

Tekintsünk most egy $\mathcal{K}$ varietást. Mindenekelőtt felírjuk azokat az elempárokat, amelyek $\mathcal{K}$ elemeire azonosságok. Legyen $\varphi : \mathfrak{F}(\tau, \omega) \to \mathfrak{F}(\mathcal{K}, \omega)$ az a homomorfizmus, amelynek a generátorokra való megszorítása az identitás. Definiáljuk most Σ-t mint azoknak a $(\mathbf{p}, \mathbf{q})$ pároknak a halmazát, amelyekre $\varphi\mathbf{p} = \varphi\mathbf{q}$ teljesül.

Legyen most $\alpha : \mathfrak{F}(\mathcal{K}, \omega) \to \mathfrak{A}$ tetszőleges homomorfizmus egy $\mathcal{K}$-beli algebrába. Mivel $\mathfrak{F}(\mathcal{K}, \omega)$ szabad, ezért a $\varphi\mathbf{x}_i \mapsto \alpha\mathbf{x}_i$ megfeleltetés kiterjeszthető egy β homomorfizmussá. Az egyértelmű kiterjeszthetőség alapján kapjuk, hogy $\alpha = \beta\varphi$, és így $\alpha\mathbf{p} = \beta\varphi\mathbf{p} = \varphi\beta\mathbf{q} = \alpha\mathbf{q}$. Ez pedig azt jelenti, hogy Σ minden eleme azonosság $\mathcal{K}$-ban.

Tekintsük most a Σ összes modelljéből álló $\mathcal{K}^*$ osztályt. Legyen $a_i \in \mathfrak{A} \in \mathcal{K}^*$, és tekintsük a $\varphi\mathbf{x}_i \mapsto a_i$ megfeleltetést. Mivel $\mathfrak{F}(\tau, \omega)$ szabad, ezért létezik olyan $\alpha : \mathfrak{F}(\tau, \omega) \to \mathfrak{A}$ homomorfizmus, amelynél $\alpha\mathbf{x}_i = a_i$. Ha mármost $(\mathbf{p}, \mathbf{q})$ azonosság $\mathfrak{F}(\mathcal{K}, \omega)$-ban, akkor $\mathcal{K}^*$ definíciója szerint azonosság $\mathfrak{A}$-ban is. Ez pontosan azt jelenti, hogy $\operatorname{Ker}\varphi \leq \operatorname{Ker}\alpha$. Mivel φ szürjektív, ezért van olyan $\beta : \mathfrak{F}(\mathcal{K}, \omega) \to \mathfrak{A}$ homomorfizmus, amelyre $\alpha = \beta\varphi$ teljesül (11.8. tétel). Ebből $a_i = \alpha\mathbf{x}_i = \beta\varphi\mathbf{x}_i$ miatt következik, hogy β a $\varphi\mathbf{x}_i \mapsto a_i$ megfeleltetés homomorf kiterjesztése. Így $\mathfrak{F}(\mathcal{K}, \omega)$ szabad $\mathcal{K}^*$-ban is.

A tétel már bebizonyított első állítása szerint $\mathcal{K}^*$ varietás. A 11.13. tétel szerint a $\mathcal{K}^*$ minden eleme előállítható egy $\mathcal{K}^*$-beli szabad algebra homomorf képeként. A két varietás egyenlőségéhez ezért elég azt bebizonyítani, hogy minden $\mathcal{K}^*$-beli szabad algebra eleme $\mathcal{K}$-nak, hiszen $\mathcal{K}$ zárt a homomorfizmusképzésre. Legyen $\mathbf{X}$ egy megszámlálható generátorhalmaz, amelyre tehát tudjuk, hogy $\mathfrak{F}(\mathcal{K}^*, \mathbf{X}) \in \mathcal{K}$. Tekintsünk most egy tetszőleges $\mathbf{Y}$ generátorhalmazt. Ha $\mathbf{Y}$ véges, akkor feltehető, hogy $\mathbf{Y} \subseteq \mathbf{X}$, és így $\mathfrak{F}(\mathcal{K}^*, \mathbf{Y}) \leq \mathfrak{F}(\mathcal{K}^*, \mathbf{Y})$. Ezért $\mathfrak{F}(\mathcal{K}^*, \mathbf{Y}) \in \mathcal{K}$, mert $\mathcal{K}$ zárt a részalgebraképzésre.

Legyen most $\mathbf{Y}$ végtelen. Ha megszámlálható, akkor a megfelelő $\mathcal{K}^*$-beli szabad algebra $\mathcal{K}$-ban van, hiszen izomorf az $\mathfrak{F}(\mathcal{K}^*, \mathbf{X})$ algebrával. Egyébként tekintsük $\mathbf{Y}$-nak az összes megszámlálható $\mathbf{X}_\lambda$ részhalmazát, ahol λ végigfut egy Λ indexhalmazon; és minden $\mathbf{X}_\lambda$ részhalmazhoz egy olyan $\varphi_\lambda : \mathbf{Y} \to, \mathbf{X}_\lambda$ leképezést, amelynek az $\mathbf{X}_\lambda$-ra való megszorítása az identitás. A 11.19. tétel szerint ezeknek létezik $\psi_\lambda : \mathfrak{F}(\mathcal{K}^*, \mathbf{Y}) \to \mathfrak{F}(\mathcal{K}^*, \mathbf{X}_\lambda)$ homomorfizmus kiterjesztése. Tekintsük most a $\mathfrak{G}(\mathcal{K}^*, \mathbf{Y}, \Lambda) = \prod_\lambda \mathfrak{F}(\mathcal{K}^*, \mathbf{X}_\lambda)$ direkt szorzatot. Mivel $\mathcal{K}$ varietás és minden komponens $\mathcal{K}$-beli (hiszen $\mathbf{X}_\lambda$ megszámlálható), ezért a direkt szorzat is $\mathcal{K}$-beli. Legyen most $\psi : \mathfrak{F}(\mathcal{K}^*, \mathbf{Y}) \to \mathfrak{G}(\mathcal{K}^*, \mathbf{Y}, \Lambda)$ az a homomorfizmus, amelyik minden $\mathbf{p} \in \mathfrak{F}(\mathcal{K}^*, \mathbf{Y})$ elemhez a $(\ldots, \psi_\lambda(\mathbf{p}), \ldots)$ vektort rendeli hozzá. Tegyük fel, hogy $\mathbf{p}, \mathbf{q} \in \mathfrak{F}(\mathcal{K}^*, \mathbf{Y})$ különböző elemek. Mivel a műveletek véges változósak, ezért ezek mindegyike benne van egy véges generátorhalmaz generátumában, és így valamelyik $\mathbf{X}_\lambda$ generátumában; és már ott is különbözők. Eszerint – erre a λ-ra – $\psi_\lambda \mathbf{p} \neq \psi_\lambda \mathbf{q}$, vagyis ψ injektív, vagyis $\mathfrak{F}(\mathcal{K}^*, \mathbf{Y}) \leq \mathfrak{G}(\mathcal{K}^*, \mathbf{Y}, \Lambda)$. Mivel $\mathcal{K}$ varietás, ezért $\mathfrak{F}(\mathcal{K}^*, \mathbf{Y}) \in \mathcal{K}$. ■

Megjegyzés. A most bizonyított tétel leírást ad ugyan az azonosságokkal definiálható algebraosztályokra, de a konstrukciós eljárás (direkt szorzat részének faktora) általában teljesen áttekinthetetlen algebrákat ad. Bizonyos speciális esetekben lehetséges egyszerűbb konstrukciót megadni. Ennek ellenére igen hasznos a tétel olyan állítás bizonyítására, hogy valamely algebraosztály nem definiálható azonosságokkal. □

Erre adunk három példát. Mindhárom esetben Abel-csoportokat tekintünk.

1. Könnyen látható, hogy egy torziócsoportnak bármely részcsoportja és bármely faktorcsoportja is torziócsoport. Ezzel szemben a direkt szorzatuk nem mindig torziócsoport: Ha az i-edik csoport éppen i-edrendű ciklikus csoport és tekintjük azt a vektort, amelyben mindegyik komponensben generátorelem áll, ez az elem nem véges rendű. A torziócsoportok osztályát tehát nem definiálhatjuk azonosságokkal.

2. A másik példa az osztható csoportok osztálya. Könnyen látható, hogy osztható csoportok faktora is, és direkt szorzata is osztható csoport. Nem lesz azonban mindig osztható a részcsoportja. Pl. a racionális számok additív csoportja osztható, de ennek részcsoportja az egész számok additív csoportja, ami nem az. Így az osztható csoportok osztályát sem lehet azonosságokkal definiálni.

3. Tekintsük végül az ún. torziómentes Abel-csoportokat; így nevezzük azokat az Abel-csoportokat, amelyekben az egységelem az egyetlen véges rendű elem. Itt is teljesül két „zártsági feltétel": torziómentes csoportok részcsoportja is és direkt szorzata is torziómentes. Ezzel szemben nem torziómentes a faktora, hiszen minden szabad Abel-csoport nyilvánvalóan torziómentes és minden Abel-csoport előáll szabadnak a faktoraként. Eszerint a torziómentes Abel-csoportok osztálya sem definiálható azonosságokkal.

A tétel „másik irányát” akkor szoktuk alkalmazni, amikor olyan algebrákat akarunk előállítani, amelyek pontosan ugyanazokat az azonosságokat elégítik ki, mint bizonyos előre megadott algebrák.

A 11.17. definíció relációt létesít azonosságok és algebrák között. Ez a reláció egy Galois-kapcsolatot hoz létre – bár az algebrák nem alkotnak halmazt, csak osztályt (az algebrák „száma” minden számosságnál nagyobb). Ennek ellenére lehet beszélni a létrejött Galois-kapcsolatról. A 11.22. tétel éppen azt írja le, hogy miképpen állíthatók elő azok az algebraosztályok, amelyek a Galois-kapcsolatban zártak; míg a 11.18. tétel lényegében megadja a lezárási operációt.

Természetesen vetődik fel a kérdés, hogy melyek lesznek a zárt azonossághalmazok. A 11.22. tétel bizonyítása során láttuk, hogy ezek megkonstruálhatók; nevezetesen éppen a szabad algebrákra való homomorfizmusok magjai. A kérdés tehát először is az, hogy miképpen ismerhető fel, hogy egy algebra valamely algebraosztályban levő szabad algebra-e. Ha $\mathfrak{F}$ az $\mathbf{X}$ halmaz generálta szabad algebra egy $\mathcal{K}$ osztályban, akkor természetesen minden $\mathbf{X} \to \mathfrak{F}$ leképezés egyértelműen kiterjeszthető homomorfizmussá. Ez a feltétel viszont már elegendő is, hiszen ez azt jelenti, hogy $\mathfrak{F}$ szabad abban az osztályban, amelynek egyetlen eleme önmaga. Így tehát azokat a kongruenciákat kell csupán leírni, amelynél $\mathfrak{F}(\tau, \omega)$ képe önmaga felett szabad.

Tekintsük tehát az $\mathfrak{F}(\tau, \omega)$-nak egy Σ azonossághalmazát, és nézzük meg, mikor lesz Σ olyan kongruencia, amely szerinti faktor egy kívánt tulajdonságú szabad algebrát állít elő.

Ez akkor és csak akkor teljesül, ha Σ egy olyan $\varphi : \mathfrak{F}(\tau, \omega) \to \mathfrak{F}(\tau, \omega)/\Sigma$ szürjektív homomorfizmus magja, hogy a $\varphi(\mathbf{x}_i)$ elemeket bárhogyan képezzük is le a faktor elemeire, ez a leképezés kiterjeszthető a faktor egy endomorfizmusává.

Először is azt fogalmazzuk meg, hogy Σ kongruencia. Σ reflexivitása a következőt jelenti:

(I) $(\mathbf{p}, \mathbf{p}) \in \Sigma$ *tetszőleges* $\mathbf{p} \in \mathfrak{F}(\tau, \omega)$ *esetén.*

A szimmetria, illetve a tranzitivitás a következőképpen fogalmazható:

(II) *Ha* $(\mathbf{p}, \mathbf{q}) \in \Sigma$, *akkor* $(\mathbf{q}, \mathbf{p}) \in \Sigma$ *is igaz.*

(III) *Ha* $(\mathbf{p}, \mathbf{q}), (\mathbf{q}, \mathbf{r}) \in \Sigma$, *akkor* $(\mathbf{p}, \mathbf{r}) \in \Sigma$ *is teljesül.*

A művelettartás nyilvánvalóan ekvivalens az alábbi megfogalmazással:

(IV) *Ha* $\mathbf{f}$ *egy* n*-változós műveleti név és* $(\mathbf{p}_i, \mathbf{q}_i), \ldots, (\mathbf{p}_n, \mathbf{q}_n) \in \Sigma$, *akkor fennáll* $(\mathbf{fp}_1 \ldots \mathbf{p}_n, \mathbf{fq}_1 \ldots \mathbf{q}_n) \in \Sigma$ *is.*

A (IV) feltételt figyelembe véve, az (I) feltétel nyilvánvalóan gyengíthető:

(I′) $(\mathbf{x}_i, \mathbf{x}_i) \in \Sigma$ *minden* $\mathbf{x}_i \in \mathbf{X}$ *esetén.*

Tekintsük most a faktoralgebrában a $\varphi(\mathbf{x}_i)$ generátoroknak egy $\varphi(\mathbf{x}_i) \mapsto \varphi(\mathbf{r}_i)$ megfeleltetését. Feltétel szerint ez kiterjeszthető egy α homomorfizmussá. Mivel a kifejezések algebrája szabad, ezért létezik olyan β homomorfizmus, amelyre $\beta\mathbf{x}_i = \mathbf{r}_i$ teljesül. Mármost az $\alpha\varphi$ és $\varphi\beta$ homomorfizmusok a szabad generátorokon megegyeznek, így a két homomorfizmus is egyenlő. (Az α homomorfizmus β-t nem egyértelműen határozza meg, hiszen φ nem injektív – kivéve, ha Σ csupán az (I) alatti elemeket tartalmazza.) A most leírt konstrukció fordítva is elvégezhető. Ha a β homomorfizmusra $\beta\mathbf{x}_i = \mathbf{r}_i$ teljesül, akkor a $\varphi(\mathbf{x}_i) \mapsto \varphi\beta(\mathbf{x}_i)$ megfeleltetést egy α homomorfizmussá kiterjesztve, teljesül az $\alpha\varphi = \varphi\beta$ egyenlőség, mert a két homomorfizmus megegyezik a szabad generátorokon. Ezért

a faktorokon vizsgált leképezések helyett mindig tekinthetünk az $\mathfrak{F}(\tau, \omega)$ szabad generátorain adott leképezéseket. Így a $\varphi(\mathbf{x}_i) \mapsto \varphi(\mathbf{r}_i)$ homomorfizmussá való kiterjeszthetőségének szükséges és elégséges feltétele – a 11.8. tétel figyelembevételével – az, hogy a kifejezésalgebra tetszőleges β endomorfizmusa esetén $\operatorname{Ker}\varphi \leq \operatorname{Ker}\varphi\beta$ teljesüljön. Ez más szóval azt jelenti, hogy valahányszor $(\mathbf{p}, \mathbf{q}) \in \Sigma$, mindannyiszor teljesülnie kell annak is, hogy $(\beta\mathbf{p}, \beta\mathbf{q}) \in \Sigma$.

Az alábbiakban ezt a tulajdonságot fogalmazzuk meg szemléletesebben.

11.23. Definíció. Az $\mathfrak{F}(\tau, \omega)$ kifejezésalgebra tetszőleges β endomorfizmusát behelyettesítésnek nevezzük. □

A behelyettesítés szemléletesen megfogalmazva a következőket jelenti:

Minden egyes i természetes számhoz hozzárendelünk egy $\mathbf{r}_i$ kifejezést. Ezután minden egyes $\mathbf{p}$ kifejezésben minden előforduló $\mathbf{x}_i$ helyébe a megfelelő $\mathbf{r}_i$ kifejezést írjuk.

Ennek segítségével a következőképpen fogalmazhatjuk meg annak a feltételét, hogy a vizsgált faktor szabad algebrát adjon:

(V) *Ha $(\mathbf{p}, \mathbf{q}) \in \Sigma$, s a β behelyettesítéskor ezeknek $\mathbf{p}'$ és $\mathbf{q}'$ felel meg, akkor $(\mathbf{p}', \mathbf{q}') \in \Sigma$ is teljesül.*

Érdemes megjegyezni a következőket: Ha Σ tartalmaz egy $(\mathbf{x}_i, \mathbf{x}_j)$ alakú párt, ahol $i \neq j$, akkor az (V) tulajdonságból azonnal adódik, hogy minden egyes $(\mathbf{p}, \mathbf{q})$ párt tartalmaz. Ebben az esetben a kapott szabad algebra egyetlen elemű. Minden más esetben a szabad generátorok képei különbözőek. A triviális esetet zárja ki tehát az alábbi feltétel:

(VI) *Ha i és j különböző természetes számok, akkor $(\mathbf{x}_i, \mathbf{x}_j) \notin \Sigma$.*

Ezzel a következő tételt bizonyítottuk:

11.24. Tétel. *Azonosságok egy Σ halmaza akkor és csak akkor áll elő valamely $\mathcal{K}$ algebraosztályban teljesülő azonosságok halmazaként, ha kielégíti az* (I′), (II), (III), (IV) *és* (V) *feltételeket. A szóban forgó algebraosztály akkor és csak akkor tartalmaz nemtriviális algebrát, ha Σ-ra* (VI) *is igaz.* ■

Megjegyzések. 1. A fenti Galois-kapcsolatnak két haszna is van. Világos, hogy a varietások úgy viselkednek, mintha egy háló elemei volnának. Ez a felfogás azonban ellentétben van az axiomatikus halmazelmélettel, mert egy-egy varietás elemeinek száma „túl nagy”, a varietások nem halmazok (hanem csak osztályok). Ezzel szemben a megfelelő azonossághalmazok könnyen kezelhetők. Ezek ugyanis mind a kifejezésalgebra direkt négyzetéből képezett hatványhalmaz elemei. Így számukra adható egy számossági korlát. Ez az eljárás lehetővé teszi, hogy mégis beszélhessünk bizonyos értelemben a varietások hálójáról.

2. A másik haszon abban áll, hogy egyszerűen meg tudjuk adni a varietások számát, illetve erre korlátot tudunk adni. Ha például a műveleteknek a száma is véges, akkor a kapott hálónak legfeljebb kontinuumnyi eleme van. Ez azt jelenti, hogy ilyen típusú algebrák esetén nem lehet „iszonyatosan sok” varietást konstruálni.

3. Egyébként a fentiek a „varietásháló” szerkezetét is bizonyos fokig meghatározzák. Kimutatható ugyanis, hogy a fellépő azonosságok hálója algebrai háló, és a kérdéses háló ezzel duálisan izomorf. Azt is viszonylag könnyen meg lehet mutatni, hogy e hálóban a kompakt elemek pontosan azok a varietások, amelyek véges sok azonossággal is definiálhatók. □

11.4. Szubdirekt előállítás

A 11.22. tétel következménye, hogy ha a bizonyos algebrákat tartalmazó legkisebb, azonosságokkal definiált osztályt akarjuk előállítani, akkor ennek az elemei a képezhető szorzatok részalgebráinak a homomorf képei lesznek. Ez az előállítás igen bonyolult még akkor is, ha a kiinduló algebrák száma esetleg egészen kevés. Éppen ezért célszerű olyan előállítást keresni, ahol a kapott algebrák sokkal jobban látható módon épülnek fel az adottakból, bár látszólag ez ellen szól, hogy az adottak többen vannak és bonyolultabbak most, mint az előző meggondolás során. Az eredeti konstrukcióban a legkevésbé áttekinthető rész a homomorf kép képzése. Ezért a legkellemesebb az lenne, ha direkt szorzatok részeként lehetne az algebrákat előállítani. Annál is inkább hasznos egy ilyen előállítás, mert a szabad algebrák létezését (illetve az osztályhoz legközelebbinek az osztályhoz tartozását) is ezekkel az operációkkal tudtuk biztosítani. Ilyen előállítás valóban mindig létezik, sőt, a részalgebrát is bizonyos fokig meg lehet szorítani. Elöljáróban szükség van a kérdéses eljárás, az úgynevezett szubdirekt szorzat definíciójára.

A szubdirekt szorzatot értelemszerűen úgy definiáljuk, mint *egy direkt szorzat olyan részalgebráját, amelyben minden komponensnek minden eleme előfordul e részalgebra egy alkalmas elemének a megfelelő komponensében.* Ebből azonnal következik, hogy a szubdirekt szorzat még a direkt szorzat rögzítése esetében sem lesz egyértelmű.

Példaként megemlítjük az adott $\mathcal{K}$ algebraosztályhoz legközelebb eső szabad algebrák konstrukcióját. Ez úgy állt elő mint $\mathcal{K}$-beli algebrák bizonyos részalgebráinak a szubdirekt szorzata.

Az eredeti definíciót célszerű úgy módosítani, hogy a szubdirekt szorzatokkal izomorf algebrákat is szubdirekt szorzatnak tekinthessük. Ez azt jelenti, hogy azokat az algebrákat tekintsük szubdirekt szorzatnak, amelyek egy direkt szorzatba szubdirekt szorzatként ágyazhatók be. Ha φ a direkt szorzatba való injektív homomorfizmus és π_i a direkt szorzatnak az i-edik komponensre való vetítése, akkor a következőket állapíthatjuk meg:

Az a feltétel, hogy „minden komponensben minden elemet felhasználunk”, úgy fogalmazható, hogy $\pi_i\varphi$ mindig szürjektív. A φ injektivitása a következőképpen fogalmazható: $\varphi a = \varphi b$ azt jelenti, hogy e két vektor minden komponense megegyezik, azaz $\pi_i\varphi a = \pi_i\varphi b$; e feltételből kell tehát annak következnie, hogy $a = b$. A fenti két feltétel nyilvánvalóan átírható úgy, hogy bennük csak a $\varphi_i = \pi_i\varphi$ homomorfizmusok szerepeljenek. E két feltételből viszont azonnal megadható egy direkt szorzatba való beágyazás; nevezetesen, ha minden a elemnek megfeleltetjük a $(\ldots, \varphi_i a, \ldots)$ vektort. Ezek figyelembevételével értelmezhetjük a szubdirekt szorzatot az alábbi módon:

11.25. Definíció. Az $\mathfrak{A}$ algebra az $\mathfrak{A}_i$ algebrák egy szubdirekt szorzata, ha léteznek olyan $\varphi_i : \mathfrak{A} \to \mathfrak{A}_i$ szürjektív homomorfizmusok, amelyek összességükben injektívek abban az értelemben, hogy ha minden i indexre teljesül a $\varphi_i a = \varphi_i b$ egyenlőség, akkor $a = b$ is fennáll.

A fenti esetben $\mathfrak{A}$ egy szubdirekt felbontásáról beszélünk és az egyes algebrákat $\mathfrak{A}$ szubdirekt komponenseinek, s a φ_i homomorfizmusokat kísérő projekcióknak nevezzük.

Ha egy szubdirekt felbontásnál valamelyik kísérő projekció bijektív, akkor azt mondjuk, hogy a szubdirekt felbontás triviális. Ha egy algebra minden szubdirekt felbontása triviális, akkor az algebrát szubdirekt irreducibilisnek nevezzük. □

Megjegyzések. 1. A szubdirekt felbontás és a szubdirekt irreducibilitás nyilvánvalóan függ attól, hogy algebrák milyen osztályában vizsgáljuk. Világos, hogy minden szubdirekt felbontás előfordul

akkor, ha az algebraosztály homomorf zárt. Az is világos, hogy bizonyos algebrák minden szubdirekt szorzata benne van az osztályában, ha az osztály direkt szorzatra is és részalgebrára is zárt. Ennek megfelelően *a továbbiakban mindig feltesszük, hogy a szubdirekt felbontást egy varietásban vizsgáljuk.*

2. Érdemes megfigyelni, hogy a szubdirekt felbontás trivialitásának a feltétele erősebb annál, mint hogy valamelyik komponens az eredetivel izomorf legyen. Azt kívánjuk meg, hogy az izomorfizmust a megfelelő kísérő projekció hozza létre. □

Könnyen belátható, hogy ha egy algebra szubdirekt felbontásában egyes komponenseket a megfelelő projekciókkal együtt akárhányszor ismételünk, mindig egy-egy újabb szubdirekt felbontást nyerünk. Az alábbiakban a szubdirekt szorzat egy olyan leírását adjuk, amely kiküszöböli a feleslegesen ismételt komponenseket.

11.26. Tétel. *Ha a* $\varphi : \mathfrak{A} \to \mathfrak{A}_i$ *homomorfizmusok az* $\mathfrak{A}$*-nak egy szubdirekt felbontását adják, akkor a* $\operatorname{Ker}\varphi_i$ *kongruenciák metszete* 0 *(a legkisebb kongruencia).*

Ha az $\mathfrak{A}$ *algebra* Θ_i *kongruenciáinak a metszete* 0*, akkor a* $\varphi_i : \mathfrak{A} \to \mathfrak{A}/\Theta_i$ *természetes homomorfizmusok az* $\mathfrak{A}$ *egy szubdirekt felbontását hozzák létre.*

A fenti szubdirekt felbontás akkor és csak akkor triviális, ha a szereplő kongruenciák valamelyike 0*.*

Bizonyítás. Mivel a szubdirekt felbontás kísérő projekciói összességükben injektívek, ezért ha az (a, b) minden egyes homomorfizmusmagnak eleme, akkor $a = b$. Így a megfelelő magok metszete valóban 0.

Tegyük most fel, hogy adottak a megfelelő Θ_i kongruenciák. A megfelelő homomorfizmusok szürjektivitása triviális. Ha $\varphi_i a = \varphi_i b$ minden i indexre teljesül, akkor (a, b) minden egyes Θ_i-nek eleme, és így – feltétel szerint – teljesül $a = b$.

A tétel utolsó állítása azonnal következik abból, hogy egy homomorfizmus pontosan akkor injektív, ha magja 0. ■

11.27. Következmény. *Egy algebra akkor és csak akkor szubdirekt irreducibilis, ha* 0*-tól különböző kongruenciái között van legkisebb.*

Bizonyítás. A 11.26. tétel szerint a szubdirekt irreducibilitásnak az a feltétele, hogy ha bizonyos kongruenciák metszete 0, akkor ezek között mindig szerepel a 0 is.

Tegyük fel először, hogy létezik a 0-tól különböző kongruenciák közt egy legkisebb Θ_0 kongruencia. Ha mármost bizonyos kongruenciák metszete 0, akkor nem lehet ezek mindegyike Θ_0-nál nagyobb vagy egyenlő. Tekintettel arra, hogy a 0-tól különböző kongruenciák mindegyike legalább akkora, mint Θ_0, ezért kell szerepelnie közöttük a Θ_0-nak is.

A megfordítás bizonyításához tekintsük az összes, 0-tól különböző kongruencia metszetét. Mivel ezek között 0 nem szerepel, így metszetük egy, a 0-tól különböző Θ_0 kongruencia. Ez a kongruencia a konstrukció alapján minden 0-tól különbözőnek alsó korlátja, tehát valóban legkisebb ezek közt. ■

Nemcsak a szubdirekt irreducibilis algebrák jellemezhetők, hanem az is leírható, hogy mikor lesz egy faktoralgebra szubdirekt irreducibilis:

11.28. Tétel. *Legyen* Φ *az* $\mathfrak{A}$ *algebra egy kongruenciája. Az* $\mathfrak{A}/\Phi$ *algebra akkor és csak akkor szubdirekt irreducibilis, ha léteznek az algebrának olyan* a *és* b *elemei, hogy az algebra egy* $\Theta \geq \Phi$ *kongruenciájára* $\Theta > \Phi$ *pontosan akkor teljesül, ha* $(a, b) \in \Theta$*.*

Bizonyítás. A 11.8. tétel alapján a $\operatorname{Ker}\psi \leftrightarrow \operatorname{Ker}\psi\gamma$ megfeleltetés rendezéstartó bijekció az $\mathfrak{A}/\operatorname{Ker}\gamma$ összes kongruenciái és az $\mathfrak{A}$-nak $\operatorname{Ker}\gamma$-t tartalmazó kongruenciái között. Így $\mathfrak{A}/\Phi$ pontosan akkor szubdirekt irreducibilis, ha a Φ-nél nagyobb kongruenciák közt van egy legkisebb – tekintettel a 11.27. következményre. Ha most az a és b elemeket úgy választjuk, hogy (a, b) benne legyen ebben a legkisebb kongruenciában, de ne legyen benne Φ-ben, akkor ezek triviálisan rendelkeznek a kívánt tulajdonsággal. Márpedig ilyen elempár a két kongruencia különbözősége miatt biztosan van. ■

Megjegyzés. Azt a legkisebb kongruenciát, amelynél a és b egy osztályban vannak, $\Theta(a, b)$-vel jelöljük, és *főkongruenciának* nevezzük. A fenti tétel szerint a szóban forgó a és b elemek $\mathfrak{A}/\Phi$-beli a' és b' képére $\Theta(a', b')$ éppen a faktor minimális kongruenciájával egyezik meg. Általában egy szubdirekt irreducibilis algebra legkisebb nemtriviális kongruenciája főkongruencia. Ugyanis a Θ_0 minimális kongruenciára és bármely a, b elempárra $\Theta_0 \leq \Theta(a, b)$. Egyenlőség pontosan akkor áll fenn, ha $a \equiv b(\Theta_0)$. □

A 11.28. tétel alapján egy varietás minden elemét előállíthatjuk szubdirekt szorzat segítségével:

11.29. Tétel (Birkhoff)**.** *Egy varietásban minden algebra előállítható a varietás szubdirekt irreducibilis elemeinek szubdirekt szorzataként.*

Bizonyítás. Tekintsük az $\mathfrak{A}$ algebra tetszőleges különböző a és b elemeit. Nézzük $\mathfrak{A}$-nak azokat a kongruenciáit, amelyek nem tartalmazzák az (a, b) párt. Ez a kongruenciahalmaz a tartalmazásra mint részbenrendezésre nézve nyilvánvalóan induktív. A Zorn-lemma szerint tehát létezik közöttük maximális. Az $\mathfrak{A}$-nak egy ilyen maximális kongruencia szerinti faktora a 11.28. tétel szerint szubdirekt irreducibilis. Tekintsük $\mathfrak{A}$-nak e faktorokra való természetes homomorfizmusát. Megmutatjuk, hogy e homomorfizmusok szubdirekt szorzatot hoznak létre. Ezzel készen is lesz a bizonyítás, mert e faktorok szubdirekt irreducibilisek. E homomorfizmusok – definíció szerint – szürjektívek. Ha tekintjük az algebra a és b különböző elemeit, akkor a konstruált kongruenciák definíciója szerint van olyan homomorfizmus, amelynél ezek képe is különböző. Ha tehát a képek mindig megegyeznek, akkor a két elem is egyenlő. ■

A most konstruált felbontásban vannak olyan faktorok, amelyek elhagyhatók. Sőt, az is előfordulhat, hogy bármely faktort el lehet hagyni. Ez azt mutatja, hogy a megadott felbontás egyáltalában nem egyértelmű.

Tulajdonképpen a fenti felbontás nagyon keveset árul el az algebrák szerkezetéről. De ez nem is várható, hiszen ez a tétel tetszőleges varietásban igaz. Könnyen belátható, hogy az itt megfogalmazott tétel igaz egy varietás véges vagy „véges-szerű” algebráira. (Ez utóbbin olyan osztályt értünk, amely részre, homomorf képre és véges direkt szorzatra zárt.) Így speciális esetben alkalmazható véges Abel-csoportokra vagy féligegyszerű gyűrűkre. Ebben az esetben az eredmények a megfelelő alaptételnek egy-egy gyengébb formái.

Mindenesetre nagyon fontos ismerni egy varietás összes szubdirekt irreducibilis elemét, mert ezek segítségével mégis szemléletesebben előállíthatók az algebrák, mint ha homomorfizmust is kellene használni. Az összes szubdirekt irreducibilis algebra meghatározása is igen nehéz. Ha ugyanis bizonyos szubdirekt irreducibiliseket meg is adunk, még nagyon sok szubdirekt irreducibilis állhat elő, amikor a „HSP”-nél a homomorfizmust képezzük.

Egy varietás leírásában igen fontos az, hogy a szabad algebrákat ismerjük. Amennyiben a szubdirekt irreducibilis algebrákat ismerjük, akkor ezek segítségével viszonylag egyszerűen leírhatjuk a szabad algebrákat is. Sőt, általában nincs is szükség az összes szubdirekt irreducibilis algebra ismeretére.

11.30. Tétel. *Egy $\mathcal{K}$ varietásban az n elem generálta szabad algebra a következőképpen írható le:*

Tekintjük az összes olyan φ függvényt, amely az $1, \dots, n$ természetes számokat a varietás valamely – legfeljebb n elemmel generálható – szubdirekt irreducibilis algebrája generátorelemeire képezi le. Tekintjük az ezeknél kapott képek generátumainak a direkt szorzatát az összes szóba jövő φ függvényre, és vesszük az

$$x_i = (\dots, \varphi(i), \dots)$$

alakú elemek generálta részalgebrát. Ez a keresett szabad algebrával izomorf.

Bizonyítás. A szóban forgó szabad algebra felírható szubdirekt irreducibilis algebrák szubdirekt szorzataként, amelyek generálhatók n elemmel – mert az eredeti algebra is generálható –, és azt is feltehetjük, hogy a generátorelemek képei a képek generátorelemei. Ezzel éppen a tételben előírt szubdirekt felbontást adtuk meg. ■

Megjegyzések. 1. A 11.30. tételben szereplő szubdirekt felbontásban általában túl sok szubdirekt irreducibilis algebrát adtunk meg. Ha ugyanis egy-egy szubdirekt irreducibilis algebrának van egy automorfizmusa, amely a generátorelemeket permutálja, akkor ehhez az algebrához ugyanaz a kongruencia tartozik. Így csak azokat az elhelyezéseket kell figyelembe venni, amelyek automorfizmussal nem vihetők egymásba. Különösen vigyázni kell arra, amikor a szubdirekt irreducibilis algebra kevesebb elemmel generált. Ebben az esetben nem tekinthetjük a fenti eseteket azonosnak, mert bizonyos szabad generátorok képei egybeesnek, és nem mindegy, hogy melyeké.

2. A szabad algebrák és a szubdirekt felbontások fontos szerepet játszanak a hálók – mint algebrai struktúrák – leírásában. □

Feladatok

1. Bizonyítsuk be, hogy a testek nem alkotnak variretást – következésképpen nincsenek „szabad testek”.

2. Bizonyítsuk be, hogy a nullosztómentes gyűrűk sem alkotnak varietást.

3. Határozzuk meg a p elemű csoportot tartalmazó legkisebb varietást. (Műveletek az összeadás, inverzképzés és a nullelem.)

4. Határozzuk meg a p elemű testet tartalmazó legkisebb varietást. (Műveletek az összeadás, inverzképzés, szorzás és a nullelem.)

5. Határozzuk meg a véges testeket tartalmazó legkisebb varietást. (Műveletek az összeadás, inverzképzés, szorzás és a nullelem.)

6. Határozzuk meg a szubdirekt irreducibilis véges Abel-csoportokat. Ebben az esetben minek a gyengébb változata a 11.29. tétel?

7. Határozzuk meg a szubdirekt irreducibilis féligegyszerű gyűrűket. Ebben az esetben minek a gyengébb változata a 11.29. tétel?

8. Bizonyítsuk be, hogy a p-hatványrendű egységgyökök csoportja szubdirekt irreducibilis.

9. Bizonyítsuk be, hogy a racionális számok additív csoportja nem szubdirekt irreducibilis.

10. Bizonyítsuk be, hogy minden egyszerű algebra szubdirekt irreducibilis.

11. Melyek a féligegyszerű gyűrűk feletti modulusok varietásában a szubdirekt irreducibilisek?

12. Hálók

12.1. Hálók mint algebrai struktúrák

A harmadik fejezetben már definiáltuk a hálókat. Hálón olyan részbenrendezett halmazt értettünk, amelyen bármely nemüres véges részhalmaznak van legkisebb felső és legnagyobb alsó korlátja. A részbenrendezés tranzitivitása miatt ez ekvivalens azzal, hogy bármely kételemű halmaznak van legkisebb felső és legnagyobb alsó korlátja. Láttuk, hogy mindkét korlát egyértelműen meghatározott. Ez lehetőséget ad arra, hogy e korlátok képzését műveletnek tekintsük. A következőkben e két művelet jellemző tulajdonságait soroljuk fel.

12.1. Tétel. *Jelölje az $\langle L; \leq \rangle$ hálóban $a \vee b$, illetve $a \wedge b$ az a és b elemek legkisebb felső, illetve legnagyobb alsó korlátját. Ezekre mint műveletekre teljesülnek az alábbiak:*

(1) *Mindkét művelet idempotens:*
$(1')\ a \vee a = a;$ $(1'')\ a \wedge a = a.$

(2) *Mindkét művelet kommutatív:*
$(2')\ a \vee b = b \vee a;$ $(2'')\ a \wedge b = b \wedge a.$

(3) *Mindkét művelet asszociatív:*
$(3')\ (a \vee b) \vee c = a \vee (b \vee c);$
$(3'')\ (a \wedge b) \wedge c = a \wedge (b \wedge c).$

(4) *Érvényes a két elnyelési tulajdonság:*
$(4')\ (a \vee b) \wedge a = a;$ $(4'')\ (a \wedge b) \vee a = a.$

Bizonyítás. Az (1) tulajdonság abból következik, hogy ha egy halmaznak egyetlen eleme van, akkor ez az elem mind a legkisebb felső, mind a legnagyobb alsó korlátja a halmaz elemeinek. A (2) tulajdonság abból adódik, hogy a legkisebb felső korlát és a legnagyobb alsó korlát nem függ mástól, mint a halmaz elemeitől – azaz nem függ attól, hogy milyen sorrendben tekintjük ezeket az elemeket.

A részbenrendezett halmazok dualitási elve alapján a (3) tulajdonságból elég például az egyesítésre vonatkozó állítást megmutatni. Legyen $u = (a \vee b) \vee c$ és $v = a \vee (b \vee c)$. A definíció alapján $c \leq u$ és $a \vee b \leq u$. Ez utóbbiból az is következik, hogy $a \leq u$ és $b \leq u$.

A legkisebb felső korlát definíciója szerint az $a \leq u$ feltétel mellett $b \vee c \leq u$ is igaz. Ismét a legkisebb felső korlát definícióját felhasználva kapjuk, hogy $v = a \vee (b \vee c) \leq u$. Mivel a kapott eredmény nem függ attól, hogy az egyes elemek konkrétan a háló mely elemei, ezért ugyanígy érvényes a $c \vee (b \vee a) \leq (c \vee b) \vee a$ összefüggés is. A már bebizonyított kommutativitás szerint viszont a kapott egyenlőtlenség bal oldalán u áll, a jobb oldalán pedig v. Így $u \leq v$ is igaz, amiből az antiszimmetriát használva $u = v$ következik.

Az $u \leq v$ esetben nyilvánvalóan igaz az $u = u \wedge v$ és $v = u \vee v$ összefüggés (l. a 12.2. kiegészítést). Az $a \wedge b \leq a \leq a \vee b$ kapcsolatból azonnal következik tehát a két elnyelési tulajdonság. ■

12.2. Tétel (a 12.1. tétel kiegészítése)**.** *Az $\langle L; \leq \rangle$ hálóban az $a \leq b$, $a \wedge b = a$ és $a \vee b = b$ feltételek ekvivalensek.*

Bizonyítás. Ha $a \leq b$, akkor b eleve felső korlátja mindkét elemnek. Tekintettel arra, hogy minden közös felső korlát eleve felső korlátja b-nek, így b a két elem legkisebb felső korlátja. Az $a \wedge b = a$ feltétel most már a dualitásból adódik. A felső korlát definíciója szerint az $a \vee b = b$ esetben b felső korlátja a-nak; míg az alsó korlát definíciója szerint $a \wedge b = a$ esetén a alsó korlátja b-nek. Mindkét esetben igaz tehát az $a \leq b$ reláció. ■

A kapott eredmény megfordítható a következőképpen:

12.3. Tétel. *Legyen $\langle L; \{+, \cdot\} \rangle$ egy olyan $\langle 2, 2 \rangle$ típusú algebrai struktúra, amelyben az alábbi azonosságok teljesülnek:*

(1) $a + a = a \cdot a = a$.

(2) $a + b = b + a$ *és* $a \cdot b = b \cdot a$.

(3) $(a + b) + c = a + (b + c)$ *és* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(4) $(a + b) \cdot a = (a \cdot b) + a = a$.

Ekkor az algebrában az $a + b = b$ és az $a \cdot b = a$ feltételek ekvivalensek. E feltétel fennállását az $a \leq b$ relációval jelölve, az L halmaz egy részbenrendezését kapjuk. L e részbenrendezésre háló, amelyben $a + b$, illetve $a \cdot b$ szolgáltatja az a és b elemek legkisebb felső, illetve legnagyobb alsó korlátját.

Bizonyítás. Az $a + b = b$ esetben $a \cdot b = a \cdot (a + b) = (a + b) \cdot a = a$; míg $a \cdot b = a$ esetén $a + b = (a \cdot b) + b = (b \cdot a) + b = b$.

$a + a = a$ biztosítja a reláció reflexivitását. Az $a \leq b$ és $b \leq a$ esetben a feltételeket $a + b = b \cdot a = b$ alakban írva kapjuk, hogy $a = (a + b) \cdot a = b \cdot a = b$; azaz a reláció antiszimmetrikus. Legyen most $a \leq b \leq c$, azaz $a + b = b$ és $b + c = c$. Ebből következik, hogy $a + c = a + (b + c) = (a + b) + c = b + c = c$. Ezzel a tranzitivitást is bizonyítottuk; és így valóban részbenrendezett halmazt kaptunk.

A kommutativitást is figyelembe véve az $(a + b) \cdot a = (a \cdot b) + a = a$ feltételből azt kapjuk, hogy $a + b$ mind a-nak, mind b-nek felső, míg $a \cdot b$ mindkettőjüknek alsó korlátja. Ha $a + u = b + u = u$, akkor $(a + b) + u = a + (b + u) = a + u = u$ és hasonlóképpen $a \cdot v = b \cdot v = v$ esetén $(a \cdot b) \cdot v = a \cdot (b \cdot v) = a \cdot v = v$. Ez pedig éppen azt jelenti, hogy $a + b$ a legkisebb felső és $a \cdot b$ a legnagyobb alsó korlát. ■

A 12.1. tételben az $\langle L; \leq \rangle$ relációval adott hálóból elkészítettük az $\langle L; \{\vee, \wedge\} \rangle$ hálót. Jelölje ezt az eljárást $\langle L; \leq \rangle \Rightarrow \langle L; \{\vee, \wedge\} \rangle$. A 12.3. tételben a $\langle L; \{\vee, \wedge\} \rangle$ hálóból (ott

a műveleteket megfelelően + és · jelölték) készítettünk egy $\langle L; \leq \rangle$ hálót. Ezt az eljárást jelölje $\langle L; \leq \rangle \Leftarrow \langle L; \{\vee, \wedge\} \rangle$.

12.4. Tétel. *Ha $\mathcal{L}$ egy relációval megadott háló, akkor $\Leftarrow (\mathcal{L} \Rightarrow) = \mathcal{L}$; ha $\mathcal{L}$ egy műveletekkel megadott háló, akkor $(\Leftarrow \mathcal{L}) \Rightarrow = \mathcal{L}$.*

Bizonyítás. A 12.1. tételben felsorolt tulajdonságok alapján a relációval definiált hálóból kapott algebra kielégíti a 12.3. tételben megkívánt feltételeket. Így a két konstrukció valóban elvégezhető egymás után. A 12.2. kiegészítést figyelembe véve azonnal adódik, hogy a 12.3. tételben definiált reláció megegyezik az eredeti részbenrendezési relációval.

Induljunk most ki egy megfelelő algebrai struktúrából. A 12.3. tétel szerint a konstrukció után egy hálót kapunk, és így ezután elvégezhető a másik konstrukció. A 12.3. tétel állítása szerint $a+b$, illetve $a \cdot b$ az a és b elemeknek a legkisebb felső, illetve a legnagyobb alsó korlátja. Ez pedig azt jelenti, hogy $a \vee b$ definíció szerint $(a+b)$-vel és $a \wedge b$ definíció szerint $(a \cdot b)$-vel egyezik meg. ■

Megjegyzés. Ha a 12.3. tételben a szereplő algebrától egyáltalában nem kívánnánk meg az asszociativitást, akkor is kapnánk egy „relációstruktúrát". Itt a reláció nem lenne tranzitív, és $a + b$ *valamelyik* közös felső korlát, $a \cdot b$ pedig *valamelyik* közös alsó korlát lenne. Itt is elvégezhető a struktúrakonstrukció, mégpedig úgy, hogy összehasonlíthatatlan elemekre a korlátok valamelyikét nevezzük ki „összegnek", illetve „szorzatnak". Az $\Rightarrow$ algebra $\Leftarrow$ reláció konstrukciópár ekkor is visszaadná az eredeti relációt, és a $\Leftarrow$ reláció $\Rightarrow$ algebra az eredeti algebrát. Csupán a relációt figyelembe véve viszont az algebra nem egyértelműen meghatározott, mert nem tudjuk egyértelműen kiválasztani a figyelembe veendő alsó és felső korlátot. □

A hálóműveletek jelölésére a továbbiakban a szokottabb $\vee$ és $\wedge$ jeleket fogjuk használni.

12.5. Definíció. Egy $\langle L; \{\vee, \wedge\} \rangle$ algebrai struktúrát hálónak nevezünk, ha a felsorolt két műveletre érvényesek a 12.1. tételben megadott azonosságok. Más szóval a két művelet kommutatív, asszociatív, idempotens, és eleget tesznek az elnyelési azonosságoknak.

Ha a hálóban van olyan u, illetve v elem, amelyre tetszőleges $x \in L$ esetén $u \wedge x = u$, illetve $v \vee x = v$, akkor ezeket az elemeket korlátelemeknek nevezzük; u-ra a 0 és v-re az 1 jelet használjuk. □

Annak, hogy a hálókban többé-kevésbé egyenrangúan szerepelnek a műveletek, illetve egy reláció, az az előnye, hogy műveleti kapcsolatokat sok esetben relációval rövidíthetünk. Megjegyezzük, hogy az elemekre felírt bármely egyenlőség mindig felírható relációkkal, de egy relációkkal felírt kapcsolat nem mindig írható egyenlőség alakban. (Például $a \leq$ $\leq u$, $b \leq u$ együttesen $u = (a \vee b) \vee x$ alakba írható, alkalmas x elemmel. Ha azonban az előbbihez még az $a \leq b$ és $b \leq v$ relációkat is hozzávesszük, akkor ezt a kapcsolatot egyetlen egyenlőséggel már nem fejezhetjük ki.)

A hálóknál mint algebrai struktúráknál a részbenrendezéssel való definícióhoz hasonlóan ugyancsak elkerülhető a tételek „kétszeres bizonyítása", a dualitási elv segítségével:

Hálók dualitási elve. *Ha egy tétel minden hálóban igaz, akkor igaz tételt nyerhetünk belőle úgy, hogy a két műveleti jelet mindenütt a másikkal pótoljuk, továbbá felcseréljük a kisebb-egyenlő, nagyobb-egyenlő jeleket, a kisebb és nagyobb jeleket, valamint* 0*-t és* 1*-et is.* □

A dualitási elv nyilvánvalóan következik abból, hogy a hálóazonosságok között mindegyikkel együtt szerepel a duálisa is, és ezek felcserélése egyúttal a részbenrendezés „irányát" is megváltoztatja.

Megjegyzések. 1. A továbbiakban valamely 2-nél több elemű H részhalmaz esetén a H elemeinek az egyesítését, illetve metszetét $\bigvee H$ vagy $\bigvee\{h \mid h \in H\}$, illetve $\bigwedge H$ vagy $\bigwedge\{h \mid h \in H\}$ is fogja jelölni. Amennyiben ismerjük a halmaz elemeit, akkor a műveleteknél (ha csak az egyik művelet szerepel) az asszociativitást felhasználva nem írjuk ki a zárójeleket: $a \vee b \vee c$, vagy $x \wedge y \wedge z$. A kommutativitás miatt az elemek sorrendje sem számít.

2. Némely esetben az eredményeket úgy is kimondjuk, hogy azok akkor is érvényesek legyenek, ha végtelen halmaz legkisebb felső, illetve legnagyobb alsó korlátjára vonatkoznak. □

A reláció és a műveletek imént említett kapcsolatai közül igen alapvetőket fogalmazunk most meg:

12.6. Tétel. *Legyen x az L háló X részhalmazának legkisebb felső, y pedig az Y részhalmaz elemeinek a legnagyobb alsó korlátja. Ha minden $x_i \in X$ és minden $y_j \in Y$ esetén teljesül az $x_i \leq y_j$ összefüggés, akkor $x \leq y$ is igaz.*

A hálóműveletre teljesül a monotonitás, azaz $a \leq b$ esetén tetszőleges c mellett igaz az $a \vee c \leq b \vee c$ és $a \wedge c \leq b \wedge c$ összefüggés.

Minden $x \in L$ elemre $0 \leq x \leq 1$, és $x = 0 \vee x = 1 \wedge x$.

Bizonyítás. Mivel Y elemei az X elemeinek felső korlátai és x az X elemeinek legkisebb felső korlátja, ezért x az Y minden elemének alsó korlátja. Ebből következik, hogy x alsó korlátja az Y elemei legnagyobb alsó korlátjának is.

A második állítás bizonyítása végett legyen $a \leq b$, azaz $a = a \wedge b$ és $b = a \vee b$. Ekkor $(a \wedge c) \wedge (b \wedge c) = (a \wedge b) \wedge c = a \wedge c$; és hasonlóan $(a \vee c) \vee (b \vee c) = (b \vee c)$. ■

Az utolsó állítás triviálisan következik a korlátelemek definíciójából.

A hálók elképzelésénél igen hasznos, hogy a hálókat vagy egy részletüket le lehet rajzolni úgy, hogy a kisebb elem „lejjebb" helyezkedjen el. Ez azért még sok okot ad a félreérthetőségre, aminek eloszlatásához hasznos az alábbi fogalom:

12.7. Definíció. Azt mondjuk, hogy az L háló a elemét követi a háló b eleme (jelben $a \prec b$), ha $a < b$, és bármely $a \leq c \leq b$ esetben $c \in \{a, b\}$. □

12.8. Tétel. *Véges háló a és b elemeire akkor és csak akkor teljesül $a < b$, ha létezik közöttük egy $a \prec a_1 \prec \ldots \prec a_r \prec b$ elemlánc.*

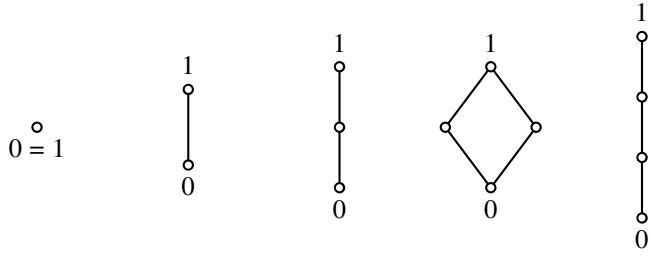
Bizonyítás. Ha egy adott típusú elemlánc létezik, akkor a részbenrendezés tranzitivitása miatt $a < b$. Fordítva, tegyük fel, hogy $a < b$, és tekintsünk egy olyan $a = a_0 < a_1 < \ldots < a_r < a_{r+1} = b$ elemláncot, amely a lehető legtöbb elemet tartalmazza. A végesség miatt ilyen elemlánc létezik; és a maximalitásból nyilvánvalóan következik minden i indexre az, hogy $a_i \prec a_{i+1}$. ■

Ez a tétel lehetőséget ad a hálók pontosabb szemléltetésére a következőképpen. Ha a-t követi b, akkor nemcsak „alatta van" a b-nek, hanem vonallal össze is kötjük őket. Világos, hogy a fenti mód tetszőleges véges részbenrendezett halmaz ábrázolására is alkalmas.

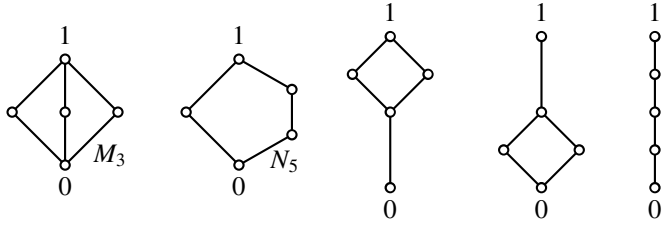
Éppen ezért ellenőrizni kell azt is, hogy bármely két elemnek pontosan egy legkisebb felső és pontosan egy legnagyobb alsó korlátja legyen.

Mielőtt lerajzoljuk a kis elemszámú véges hálókat, megjegyezzük, hogy véges hálóban mindig létezik 0-elem és 1-elem (az összes elem metszete, illetve egyesítése), ezért csak a további elemek elhelyezkedését kell megvizsgálni.

Ha a hálónak egyetlen eleme van, akkor természetesen ez a 0-elem is és az 1-elem is. Ha a háló kételemű, akkor további elem még mindig nincsen. Háromelemű háló esetén egyetlen további elem létezik, erre semmi más összehasonlítási lehetőség nincs. Négyelemű hálóban a két nem korlátelem vagy összehasonlítható, vagy nem. Ennek megfelelően a legfeljebb négyelemű hálók a következők:



Nézzük most az ötelemű hálókat. Itt három nem korlátelem van. Osztályozzuk a lehetőségeket aszerint, hogy hány összehasonlítási reláció lehetséges közöttük. Lehet, hogy egy sincs, lehet, hogy egy van. Ez a két eset nyilván egyértelmű. Ha két reláció van, ez csak úgy lehet, hogy valamelyikük a másik kettőnél kisebb, illetve nagyobb. Közöttük nem lehet, mert ekkor a tranzitivitás miatt már három reláció van. Ez is lehetséges; több reláció már viszont nem. Így az ötelemű hálók az alábbiak:



Az általános algebrai eredményeket, illetve elnevezéseket a hálók esetén is minden további nélkül használni fogjuk. Vannak azonban bizonyos speciális fogalmak, amelyek csak hálóelméleti úton (tehát a relációt felhasználva) közelíthetők meg.

12.9. Definíció. Az L háló egy K részhálója konvex, ha K-beli $a \leq b$ és tetszőleges $x \in L$ esetén az $a \leq x \leq b$ feltételből $x \in K$ következik.

Az I részháló ideál, ha $x \leq y \in I$ esetén $x \in I$ teljesül.

A D részháló duális ideál (vagy filter – magyarul szűrő), ha $x \geq y \in D$ esetén $x \in D$ következik.

Ha $u \leq v$ a háló elemei, akkor az $[u, v] = \{x \mid u \leq x \leq v\}$ halmazt intervallumnak nevezzük; $[0, v]$ neve főideál, $[u, 1]$ neve főfilter. □

Megjegyzések. 1. A filter fogalma alapvető a logikában és a topológiában.

2. Tulajdonképpen az intervallumhoz hozzá kell tenni, hogy zárt intervallum (általában csak ilyenekkel fogunk foglalkozni). Hasonlóképpen lehet definiálni a nyílt, illetve (kétféle) félig nyílt intervallumot, ezek – jelöléssel együtt – $(u, v) = \{x \mid u < x < v\}$, $(u, v] = \{x \mid u < x \leq v\}$, $[u, v) = \{x \mid u \leq x < v\}$. Ennek a jelölésnek a haszna, hogy akkor is jelölhető a főideál, illetve főfilter, amikor a hálónak nincsenek korlátelemei: $(0, v] = \{x \mid x \leq v\}$, illetve $[v, 1) = \{x \mid v \leq x\}$. □

12.10. Tétel. *Egy háló bármely ideálja és duális ideálja konvex részháló; bármely konvex részháló egy ideálnak és egy duális ideálnak a metszete. Minden intervallum konvex részháló; s ha egy konvex részhálónak van legkisebb és legnagyobb eleme, akkor ez intervallum. Főideál, illetve főfilter mindig ideál, illetve filter.*

Háló kompatibilis osztályozásában minden osztály konvex részháló. Ha egy φ hálóhomomorfizmusnál az Im *φ-nek létezik legkisebb (legnagyobb) eleme, akkor az erre képeződő elemek ideált (duális ideált) alkotnak.*

Bizonyítás. Ha $a \leq b \leq c$ és a, c elemei az ideálnak vagy a duális ideálnak, akkor a két reláció egyikéből már következik, hogy b is eleme. Ha K tetszőleges konvex részháló, akkor tekintsük azoknak az elemeknek az I halmazát, amelyek valamely K-beli elemnek alsó korlátai, illetve azt a D halmazt, amelynek elemei valamely K-beli elemnek felső korlátai. Ha $x, y \in I$, akkor van olyan $a, b \in K$, amelyekre $x \leq a$ és $y \leq b$. Ekkor $x \vee y \leq a \vee b$. Tetszőleges $z \leq x$ esetén $z \leq a$. Így $x \wedge y \leq x$ miatt $x \wedge y \in I$; amiből következik, hogy I ideál. D-re a dualitásból következik a megfelelő eredmény. Ha $a \in K$, akkor $a \leq a$ miatt $a \in I \cap D$. Ha $x \in I \cap D$, akkor van olyan $a, b \in K$, amelyekre $a \leq x \leq b$, tehát $x \in K$, mert K konvex.

$[u, v]$ definíció szerint konvex. Ha $x, y \in [u, v]$, akkor az egyesítés és metszet definíciója alapján $u \leq x \wedge y \leq v$ és $u \leq x \vee y \leq v$, tehát minden intervallum konvex részháló. Ebből az is azonnal adódik, hogy főideál az valóban ideál és főfilter az valóban filter.

Tegyük most fel, hogy K egy kompatibilis osztályozás egy osztálya, $a, b \in K$ és $a \leq x \leq b$. A kompatibilitás miatt $a = (a \vee x) \wedge a$ és $x = (a \vee x) \wedge b$ egy kongruenciaosztályba esnek, így $x \in K$.

Tegyük fel, hogy $a' = \varphi a$ az Im φ-nek a legkisebb eleme. Azt már láttuk, hogy az a'-re képeződő elemek konvex részhálót alkotnak. Azt kell még belátni, hogy ha $\varphi b = a'$ és $c \leq b$, akkor $\varphi c = a'$ is teljesül. Mivel a' az Im φ-nek a legkisebb eleme, ezért $a' \wedge \varphi c = a'$. Ebből

$$\varphi c = \varphi(c \wedge b) = \varphi c \wedge \varphi b = \varphi c \wedge a' = a',$$

amint állítottuk.

A duális ideálokra vonatkozó állítás azonnal következik a dualitásból. ■

Megjegyzések. 1. Nem minden részháló konvex. Véges hálók esetén például $\{0, 1\}$ mindig részháló, de csak akkor konvex, ha a hálónak legfeljebb két eleme van.

2. Nem minden konvex részháló áll elő kompatibilis osztályozás osztályaként. Például az M_3-mal jelzett ötelemű hálóban a 0 elem bármely, 1-től különböző elemmel együtt ideált alkot, de mint később látni fogjuk, nem osztály egyetlen kompatibilis osztályozásánál sem. □

Tekintettel arra, hogy a hálókat kétféleképpen definiáltuk, ezért – elvileg – kétféle lehetőség van a részháló definíciójára is. Az egyikben a részhálót mint részalgebrát tekintjük – és ezt a definíciót már el is fogadtuk. Lehetne azonban azt mondani, hogy a részháló

a hálónak olyan része, mely az eredeti részbenrendezésre (illetve ennek a részre való megszorítására) hálót alkot. E két fogalom nem ugyanazt jelenti! Nézzük például a negyediknek felrajzolt ötelemű hálóban a két korlátelemen kívül a két összehasonlíthatatlan elemet. Ezek a részbenrendezésre nézve nyilvánvalóan négyelemű hálót alkotnak. De ez mégsem részháló, mert a két összehasonlíthatatlan elem egyesítése a részben és az egész hálóban különbözik. Éppen ezért fontos jól megjegyezni, hogy *ha egy részhálót rajzban adunk meg, ellenőrizni kell, hogy a műveletek a részben és az egészben megegyeznek-e.*

A kétféle lehetőség a homomorfizmusnál is megjelenik. Itt is lehet beszélni olyan leképezésről, amely művelettartó, és olyanról, amely relációtartó. Az előbbi példa mutatja, hogy relációtartó leképezés nem feltétlenül művelettartó. Sőt, a két négyelemű háló egyikét leképezhetjük bijektíven a másikba egy relációtartó leképezéssel, amely nyilvánvalóan nem művelettartó.

A kétféle leképezés között „egyirányú" kapcsolat létezik:

12.11. Tétel. *Minden hálóhomomorfizmus részbenrendezés-tartó.*

Bizonyítás. Legyen φ egy hálóhomomorfizmus, amely az L hálót képezi le. Tekintsük az L háló $a \leq b$ elemeit. Ekkor $\varphi a = \varphi(a \wedge b) = \varphi a \wedge \varphi b$ biztosítja, hogy $\varphi a \leq \varphi b$. ■

A későbbiekben szükségünk lesz néhány további fogalomra.

12.12. Definíció. Ha az L hálónak vannak korlátelemei – azaz 0-eleme és 1-eleme –, akkor a hálót korlátosnak nevezzük. Ha egy korlátos háló valamely a és b elemére $a \vee b = 1$ és $a \wedge b = 0$ teljesül, akkor ezeket egymás komplementereinek nevezzük. Ha a háló bármely elemének van komplementere, akkor komplementumos hálóról beszélünk. Ha a háló bármely két eleme összehasonlítható, akkor azt mondjuk, hogy a háló lánc.

Ha az $[u, v]$ intervallum x, y elemeire $x \vee y = v$ és $x \wedge y = u$, akkor ezeket (az adott intervallumra nézve) egymás relatív komplementumainak nevezzük. Ha egy intervallum minden elemének van relatív komplementuma, akkor ezt relatív komplementumos intervallumnak hívjuk. Egy háló relatív komplementumos, ha minden intervalluma relatív komplementumos. □

Természetesen egy hálóhomomorfizmus nem feltétlenül viszi a korlátelemeket korlátelembe, s így a komplementer képe sem lesz biztosan a kép komplementere. Ha ezt biztosítani szeretnénk, akkor a korlátelemeket nullváltozós művelettel kell rögzíteni. Ez már biztosítja, hogy komplementerek is komplementerpárba képeződjenek. Ebből az is triviális, hogy relatív komplementumos intervallum képe is az. Ha azonban egy elemnek több komplementere van, akkor viszont már nem biztos, hogy a kép a kívánalomnak megfelelő komplementer lesz. Ilyen esetben a komplementerképzést is művelettel lehet biztosítani.

Az ideálokat most tovább vizsgáljuk. A definícióban két különböző típusú fogalom szerepelt. Ha a műveleti zártságot elhagyjuk, akkor is egy fontos fogalmat kapunk.

12.13. Definíció. Egy részbenrendezett halmaz nemüres részhalmazát (duálisan) öröklődőnek nevezzük, ha minden elemmel együtt a nála (nagyobbakat) kisebbeket is tartalmazza. □

Az öröklődés megfogalmazható úgy is, hogy ha $a \in I$, akkor tetszőleges b mellett $a \wedge b \in I$ is fennáll. Ha az egyesítést +, a metszetet $\cdot$ jelöli, akkor ez a feltétel – a művelettartással együtt – lényegében valóban az ideál gyűrűelméleti definíciójának analogonja.

Ennek az analógiának megfelelően definiáljuk a prímideált is, amely a hálóelméletben is igen jelentős szerepet játszik.

12.14. Definíció. Az L háló egy ideálját (duális ideálját) valódinak nevezzük, ha L-től különbözik.

Az L háló egy P (Q) valódi ideálja (duális ideálja) prímideál (duális prímideál), ha $a \wedge b \in P$ ($a \vee b \in Q$) esetén a és b valamelyike eleme P-nek (Q-nak).

A duális prímideálokat ultrafilternek (ultraszűrőnek) is nevezik. □

12.15. Tétel. *Legyenek P és Q az L hálóban egymás komplementer részhalmazai. P akkor és csak akkor öröklődő, ha Q duálisan öröklődő. Ebben az esetben az alábbi feltételek ekvivalensek:*

(1) *P prímideál.*

(2) *Q duális prímideál.*

(3) *P ideál és Q duális ideál.*

(4) *P és Q részháló.*

(5) *Ha $a \vee b \in Q$ és $a \wedge b \in P$, akkor a és b egyike P-nek, másikuk Q-nak eleme.*

(6) *Létezik az L-nek a kételemű hálóra való olyan szürjektív homomorfizmusa, amelynél a P elemei a 0-elemre és Q elemei az 1-elemre képeződnek le.*

Bizonyítás. Tegyük fel, hogy P öröklődő, és legyen $a \in Q$. Ha $a \leq b$, akkor b nem lehet a P eleme, mert különben – a feltétel szerint – a is eleme volna P-nek. A dualitás miatt a megfordítás is igaz.

Most a további állítások ekvivalenciájának a bizonyítására térünk rá.

Az ideál és a duális ideál definíciója szerint a (3) és (4) állítások ekvivalensek, mert P eleve öröklődő és Q duálisan öröklődő.

Ha P prímideál, akkor ideál, és ezenkívül az is teljesül, hogy ha $a, b \notin P$, akkor $a \wedge b \notin P$. Mivel P és Q egymás komplementerei, ezért ez utóbbi feltétel azzal ekvivalens, hogy $a, b \in Q$ esetén $a \wedge b \in Q$ is teljesül. Ez pedig – a duális öröklődést figyelembe véve – pontosan azt jelenti, hogy Q duális ideál. Így (1) és (3) valóban ekvivalensek, és a dualitás alapján (2) és (3) ekvivalenciája is következik.

Ha (4) teljesül, és a, b mindegyike P-ben vagy mindegyike Q-ban van, akkor ugyanide esik mind $a \vee b$, mind $a \wedge b$ a műveleti zártság miatt. Így (5) is igaz. Ha (5) teljesül, akkor tekintsünk két elemet P-ből. Az öröklődés miatt ezek metszete is P-hez tartozik, és a feltétel szerint egyesítésük is csak P-nek egy eleme lehet. Ez éppen azt jelenti, hogy P részháló. A dualitás szerint Q is részháló; tehát (4) is fennáll.

Ha (6) igaz, akkor a 12.10. tétel szerint teljesül (3) – figyelembe véve, hogy minden elem vagy 0-ra, vagy 1-re képeződik. Tegyük most fel, hogy (3) fennáll, és feleltessük meg P elemeinek a 0-t és Q elemeinek az 1-et. Mivel P és Q egyike sem üres, ezért a megfeleltetés szürjektív. Ha e φ megfeleltetésnél $\varphi a = \varphi b$, akkor a részháló-tulajdonság szerint igaz a művelettartás. Ha a képek különbözőek, akkor az öröklődés és a duális öröklődés következtében $\varphi(a \wedge b) = 0$ és $\varphi(a \vee b) = 1$, ami a képek különbözősége folytán biztosítja a művelettartást. ■

A hálók szemléletes elképzeléséhez segítséget nyújt a hálók reprezentációja. Tudjuk, hogy egy halmaz részhalmazai a halmazelméleti egyesítés és metszet műveletekre hálót

alkotnak. Majd látni fogjuk, hogy e háló részhálójaként csak nagyon speciális hálók állnak elő. Ezzel szemben kimutatható, hogy minden háló beágyazható egy alkalmas halmaz részhalmazhálójába rendezéstartó módon. A leképezés tehát itt sem művelettartó. Megadható viszont egy konkrét hálótípusba való művelettartó leképezés. Ez a konkrét típus egy halmaz összes partícióinak (vagy ekvivalenciarelációinak) a halmaza. Az itt létrehozható homomorfizmus azonban elég bonyolult, és tulajdonképpen azt mutatja, hogy a „partíciók" szinte áttekinthetetlenek. Partícióhálóba való metszettartó beágyazást ezzel szemben viszonylag könnyen lehet konstruálni.

Feladatok

1. A relációval definiált hálók esetében ne tegyük fel a $\leq$ tranzitivitását, csak annyit, hogy minden a, b párra létezik egy $a \vee b$ felső és egy $a \wedge b$ alsó korlát, azzal a megkötéssel, hogy $a \leq b$ esetén b a kijelölt felső és a a kijelölt alsó korlát. Bizonyítsuk be, hogy e két műveletre a 12.3. tétel axiómái mind teljesülnek – kivéve a két asszociativitást.

2. A műveletekkel megadott hálók esetében hagyjuk el a két asszociativitást. Bizonyítsuk be, hogy $a \wedge b = a$ és $a \vee b = b$ ekvivalensek. Bizonyítsuk be, hogy az ezzel a kapcsolattal definiált $\leq$ relációra a rendezéssel definiált hálótulajdonságok mind teljesülnek, kivéve a reláció tranzitivitását.

3. Bizonyítsuk be, hogy bármelyik asszociativitásból következik a rendezés tranzitivitása; következésképpen a két asszociativitás ekvivalens.

4. Bizonyítsuk be, hogy az előző feladatokban vizsgált struktúrára $x \vee [(x \wedge y) \vee (x \wedge z)] = x$, illetve $x \wedge [(x \vee y) \wedge (x \vee z)] = x$ jelenti azt, hogy az egyesítés minden közös felső korlátnál kisebb-egyenlő, illetve a metszet minden közös alsó korlátnál nagyobb-egyenlő. Adjunk példát arra, hogy ez a két azonosság nem ekvivalens.

5. Legyen a hatelemű $0, a, b, c, d, 1$ halmazban $0 \prec a \prec c \prec 1$, $0 \prec b \prec d \prec 1$, $a \prec d$ és $b \prec c$ az összes követési reláció. Bizonyítsuk be, hogy ez nem háló.

6. Legyen $\mathcal{P}$ az L háló részhalmazainak a halmaza. Mint tudjuk, $\mathcal{P}$ háló a halmazok metszetére és egyesítésére mint műveletekre nézve. Bizonyítsuk be, hogy L beágyazható $\mathcal{P}$-be akár metszettartó, akár egyesítéstartó leképezéssel.

7. Bizonyítsuk be, hogy M_3 nem ágyazható be művelettartó módon egy halmaz részhalmazhálójába; ha egy halmaz A, B, C részhalmazainak páronként vett metszete mindig ugyanaz, akkor az $A \cup B$, $B \cup C$ és $C \cup A$ mind különböznek.

8. Bizonyítsuk be, hogy egy háló minden ideálja pontosan akkor lesz prímideál, ha minden filtere ultrafilter. Jellemezzük ezeket a hálókat.

12.2. Disztributív hálók

Látni fogjuk majd, hogy a gyűrűelméleti disztributivitás analogonja a hálók esetében nem mindig teljesül. A disztributivitást a hálók esetében a dualitás miatt valójában kétféle módon is megfogalmazhatjuk. Ezek és egyéb vizsgálatok előkészítésére előrebocsátunk néhány alapvető összefüggést.

12.16. Tétel. *Legyenek a, b, c az L háló elemei. Ekkor fennállnak az alábbi összefüggések:*

(1) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$.

(2) $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$.

(3) $m(a, b, c) \leq M(a, b, c)$, *ahol* $m(a, b, c) = (a \wedge b) \vee (b \wedge c) \vee (c \wedge a)$ *a három elem úgynevezett alsó mediánsa és* $M(a, b, c) = (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$ *a felső mediáns.*

(4) *Ha* $a \leq c$, *akkor* $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.

Bizonyítás. Mind a négy esetben a bal oldalon bizonyos elemek egyesítése, a jobb oldalon pedig bizonyos elemek metszete szerepel. Az olvasóra bízzuk annak az ellenőrzését, hogy a bal oldalon figyelembe veendő elemek minden esetben alsó korlátjai a jobb oldalon fellépő elemeknek. Ebből viszont már a 12.6. tétel alapján következik mindegyik egyenlőtlenség. ■

Megjegyzés. Az $m(x, y, z) = (x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$ és $M(x, y, z) = (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$ kifejezéseket *többségi kifejezéseknek* nevezik. Ha ugyanis az x, y, z elemek közül legalább kettőnek a helyébe ugyanazt helyettesítjük, akkor a kifejezés értéke ez a „többségi érték” lesz. □

12.17. Definíció. Az L hálót rendre egyesítés-disztributívnak, metszet-disztributívnak, illetve disztributívnak fogjuk nevezni, ha tetszőleges a, b, c elemeire teljesül:

(1) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

(2) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

(3) $m(a, b, c) = M(a, b, c)$.

Amennyiben az L háló bármely a, b, c elemeire $a \leq c$ esetén teljesül az $a \vee (b \wedge c) = (a \vee b) \wedge c$ egyenlőség, akkor a hálót modulárisnak nevezzük. □

Megjegyzések. 1. A 12.16. tétel alapján a most megadott egyenlőségekben az egyik tartalmazási irány minden hálóban igaz; csupán a másikat kell ellenőrizni.

2. Egyébként a modularitás is tekinthető egyenlőségnek, mert a feltételt úgy írhatjuk át, hogy c helyébe egyszerűen $(a \vee c)$-t írunk. Azért adjuk meg ezt az egyenlőséget mégis a fenti alakban, mert így sokkal szemléletesebb.

3. Mindenesetre látható, hogy a fent definiált négy hálóosztály (amelyek közül az első háromról a következő tételben ki fogjuk mutatni, hogy megegyeznek) egy-egy hálóvarietást alkot; hiszen azonosságokkal definiáltuk. □

12.18. Tétel. *Tetszőleges L hálóra ekvivalensek az alábbi állítások:*

(1) *L disztributív.*

(2*a*) *L egyesítés-disztributív.*

(2*b*) *L metszet-disztributív.*

(3*a*) *Az L tetszőleges I ideáljára* $(I,u)\cap(I,v)=(I,u\wedge v)$, *ahol* (I,x) *az I és x generálta (azaz az I-t és x-et tartalmazó legkisebb) ideált jelöli.*

(3*b*) *Az L tetszőleges D duális ideáljára* $(D,u)\cap(D,v)=(D,u\vee v)$, *ahol* (D,x) *a D és x generálta (azaz a D-t és x-et tartalmazó legkisebb) duális ideált jelöli.*

(4) *Ha I az L hálónak ideálja, D duális ideálja, és D diszjunkt az I-hez, akkor létezik az I-t tartalmazó, D-hez diszjunkt prímideál.*

(5) *Ha* $a,b\in L$ *és* $b\not\leq a$, *akkor van olyan a elemet tartalmazó prímideál, amelynek b nem eleme.*

(6) *Ha* $a,b\in L$ *és* $b\not\leq a$, *akkor létezik az L-nek a kételemű hálóba való olyan homomorfizmusa, amely az a elemet* 0*-ba és a b elemet* 1*-be képezi.*

(7) *L kételemű hálók szubdirekt szorzata.*

(8) *L izomorf egy halmaz részhalmazhálójának valamely részhálójával (M. H. Stone).*

Bizonyítás. Tegyük fel, hogy L disztributív. Ebből bebizonyítunk egy egyenlőtlenséget:

$$\begin{aligned}a\vee(b\wedge c)&=(a\vee(a\wedge b)\vee(a\wedge c))\vee(b\wedge c)=\\&=a\vee m\geq m=M\geq M\wedge c=\\&=(a\vee b)\wedge(a\vee c)\wedge(b\vee c)\wedge c=\\&=(a\vee b)\wedge c.\end{aligned}$$

c helyébe $(a\vee c)$-t írva kapjuk, hogy:

$$\begin{aligned}(a\vee b)\wedge(a\vee c)\leq a\vee(b\wedge(a\vee c))&=a\vee[b\wedge(a\vee b)\wedge(b\vee c)\wedge(a\vee c)]=\\&=a\vee(b\wedge M)\leq a\vee M=a\vee m=\\&=a\vee(a\wedge b)\vee(a\wedge c)\vee(b\wedge c)=a\vee(b\wedge c).\end{aligned}$$

(A számolás során többször felhasználtuk az elnyelési azonosságot, valamint a monotonitást.)

A kapott egyenlőtlenséget a 12.16. tétellel összevetve kapjuk, hogy teljesül (2a) A dualitás következtében (2b) is következik (1)-ből.

Tegyük most fel, hogy az L hálóra (2a) teljesül, és tekintsük L-nek egy I ideálját. Mindenekelőtt megadjuk az (I,x) ideál elemeit. Mivel az ideál az egyesítésre zárt és öröklődő, ezért ennek az ideálnak eleme minden olyan y, amelyhez található olyan I-beli a elem, hogy $y\leq a\vee x$. Az ilyen tulajdonságú elemek viszont már ideált alkotnak: Az öröklődés nyilvánvaló; s ha $y\leq a\vee x$ mellett $z\leq b\vee x$, alkalmas I-beli b-re, akkor mindegyiknek felső korlátja az $(a\vee b)\vee x$, ami így felső korlátja $(y\vee z)$-nek, s $a\vee b\in I$ miatt $y\vee z$ is eleget tesz az adott feltételnek. $a\leq a\vee x$ és $x\leq a\vee x$ biztosítja, hogy a fenti ideálnak része I, és tartalmazza x-et.

Az $u\wedge v\leq u$ és $u\wedge v\leq v$ alapján azonnal következik, hogy $(I,u\wedge v)\subseteq(I,u)\cap(I,v)$. Most megmutatjuk a fordított irányú tartalmazást. Legyen evégett w eleme a jobb oldali metszetnek. Ez azt jelenti, hogy létezik olyan $a,b\in I$, hogy $w\leq a\vee u$ és $w\leq b\vee v$. A $c=a\vee b$ elemre a monotonitás miatt teljesül $w\leq c\vee u$ és $w\leq c\vee v$. Így az I ideál c elemére $w\leq(c\vee u)\wedge(c\vee v)$ is fennáll. A (2a) feltétel szerint a jobb oldalon álló kifejezés

$c \vee (u \wedge v)$; ami azt jelenti, hogy $w \in (I, a \wedge v)$. A dualitás alapján (2b)-ből következik, hogy (3b) is igaz.

Tegyük most fel, hogy (3a) igaz az L háló minden ideáljára. Tegyük fel, hogy az L háló I ideálja és D duális ideálja diszjunktak. Tekintsük az I ideált tartalmazó és D-hez diszjunkt ideálok egy láncát. Ezek egyesítési halmaza nyilvánvalóan az I-t tartalmazó és D-hez diszjunkt ideál. Ez azt jelenti, hogy az I-t tartalmazó és D-hez diszjunkt ideálok a tartalmazásra nézve induktív halmazt alkotnak. A Zorn-lemma szerint tehát létezik ezek között egy P ideál, amely a fenti tulajdonságra maximális. Megmutatjuk, hogy bármely ilyen P ideál prím. Ehhez azt kell belátni, hogy ha $u, v \notin P$, akkor $u \wedge v$ sem eleme P-nek.

Ha $u, v \notin P$, akkor P maximalitása szerint léteznek olyan u_1 és v_1 elemek, hogy $u_1 \in (P, u) \cap D$ és $v_1 \in (P, v) \cap D$. Ebből egyrészt az következik, hogy $w = u_1 \wedge v_1$ is eleme D-nek. Másrészt w eleme a (P, u) és (P, v) ideálok mindegyikének, tehát a (3a) feltétel miatt $w \in (P, u \wedge v)$. Így a $(P, u \wedge v)$ ideálnak és a D duális ideálnak megtaláltuk egy közös elemét; ami csak úgy lehet, hogy $u \wedge v \notin P$, mert $P \cap D$ üres. Ezzel bebizonyítottuk a (4) tulajdonságot. A dualitást figyelembe véve, (3b)-ből következik a (4) feltétel duálisa. Tekintettel arra, hogy duális prímideál komplementerhalmaza prímideál, ezért (4) duálisa önmaga. Ez azt jelenti, hogy (3b)-ből is következik (4)

Tegyük most fel, hogy az L háló rendelkezik a (4) alatti tulajdonsággal. Legyenek $a, b \in L$, és $b \not\leq a$. Definiáljuk az I és a D halmazt a következőképpen:

$$I = \{x \mid x \leq a\} \qquad \text{és} \qquad D = \{y \mid y \geq b\}.$$

I triviálisan ideál és D duális ideál. E két halmaz $b \not\leq a$ miatt diszjunkt; a (4) tulajdonság alapján tehát létezik olyan prímideál, amely I-t tartalmazza és D-hez diszjunkt. A nyilvánvaló $a \in I$ és $b \in D$ következtében $a \in P$ és $b \notin P$. Így L-re igaz az (5) tulajdonság.

Tegyük most fel, hogy L rendelkezik az (5) alatti tulajdonsággal. A 12.15. tétel szerint ekkor rendelkezik a (6) alatti tulajdonsággal is.

Tegyük most fel azt, hogy az L háló (6) alatti tulajdonságú. Tekintsük L-nek a kételemű hálóba való összes olyan homomorfizmusát, amelynél a magok különbözőek. (Tehát minden prímideál – duális prímideál felbontáshoz csak egyetlen homomorfizmust tekintünk.) E homomorfizmusok mind szürjektívek. Tegyük fel, hogy az $a, b \in L$ képei a fenti homomorfizmusok mindegyikére megegyeznek. A (6) tulajdonság szerint ekkor sem $b \not\leq a$, sem $a \not\leq b$ nem teljesülhet, azaz $a \leq b$ és $b \leq a$, amiből $a = b$ következik. Így a definiált homomorfizmusok összességükben injektívek, ami bizonyítja a kívánt szubdirekt felbontást.

Tegyük most fel, hogy az L hálóra teljesül a (7) tulajdonság. Jelöljük a_λ-val a λ-adik komponens 1-elemét, és legyen H az összes szereplő a_λ-k halmaza. Legyen φ_λ az a homomorfizmus, amelyik az L hálót a λ-adik komponensre képezi. Definiáljuk L-nek a H hatványhalmazára való φ leképezését úgy, hogy $\varphi a = \{a_\lambda \mid \varphi_\lambda(a) = a_\lambda\}$.

Mármost $a_\lambda \in \varphi(a \vee b)$ akkor és csak akkor áll fenn, ha $a_\lambda = \varphi_\lambda(a \vee b) = \varphi_\lambda a \vee \varphi_\lambda b$, ami pontosan akkor teljesül, ha a jobb oldalon levő elemek valamelyike a_λ. Ez azzal ekvivalens, hogy $a_\lambda \in \varphi a \cup \varphi b$. Az $a_\lambda \in \varphi(a \wedge b)$ feltétel azt jelenti, hogy $a_\lambda = \varphi_\lambda(a \wedge b) = \varphi_\lambda a \wedge \varphi_\lambda b$, vagyis $\varphi_\lambda a = \varphi_\lambda b = a_\lambda$. Ez viszont az $a_\lambda \in \varphi a \cap \varphi b$ feltétellel ekvivalens. A definiált φ leképezés tehát homomorfizmus. Mivel a szubdirekt felbontásnál megadott homomorfiz-

musok összességükben injektívek, ezért az itt definiált homomorfizmus is injektív. Ezzel beláttuk, hogy L kielégíti a (8) feltételt.

Tegyük fel végül, hogy L kielégíti a (8) feltételt. Az izomorfizmus miatt feltehetjük, hogy L megegyezik egy H halmaz részhalmazai halmazának bizonyos részhálójával. Tekintettel arra, hogy egy algebrában teljesülő minden azonosság igaz az algebra részalgebráiban is, ezért elég azt kimutatni, hogy a H halmaz részhalmazainak a hálója disztributív. Tekintsük a H halmaz A, B és C részhalmazait. Azt kell bizonyítanunk, hogy ezek alsó és felső mediánsa megegyezik. A 12.16. tétel miatt elegendő annak a kimutatása, hogy a felső mediáns minden eleme eleme az alsó mediánsnak is. Az alsó mediáns definíció szerint azokból az elemekből áll, amelyek a három halmaz közül legalább kettőben benne vannak. Legyen most x a felső mediáns eleme, azaz $x \in (A \cup B) \cap (A \cup C) \cap (B \cup C)$. Ez azt jelenti, hogy x minden egyes, páronként vett egyesítésben benne van. Benne van például az $A \cup B$ halmazban is. Ha x e két halmaz mindegyikének eleme, akkor – mint láttuk – eleme az alsó mediánsnak. Mivel x a két halmaz valamelyikében biztosan benne van, feltehető, hogy $x \in A$ és $x \notin B$. Mivel x benne van minden, páronkénti egyesítésben, ezért benne van $(B \cup C)$-ben is. Ez viszont csak úgy lehet, hogy $x \in C$, hiszen $x \notin B$. Így $x \in A \cap C$, tehát valóban eleme az alsó mediánsnak. ■

12.19. Tétel (a 12.18. tétel kiegészítése)**.** *Minden disztributív háló moduláris.*

A (8) *alatti megfeleltetésnél relatív komplementumok képe relatív komplementum.* 0*-elemes hálónál ennek a képe az üres halmaz,* 1*-elemesnél ennek képe az egész halmaz. Ekkor a megfeleltetés során komplementer elemek képe komplementer halmaz.*

Bizonyítás. A 12.18. tétel bizonyításában szereplő $a \vee (b \wedge c) \geq (a \vee b) \wedge c$ egyenlőtlenségből és a 12.16. tételből azonnal következik az első állítás.

A második állítás első része azonnal következik a művelettartásból. A második rész bizonyításához elég annyit megjegyezni, hogy a konstruált szubdirekt felbontásban a 0-elemnek minden komponense 0, és az 1-elemnek minden komponense 1. Az utolsó állítás azonnal következik a második állítás első részéből. ■

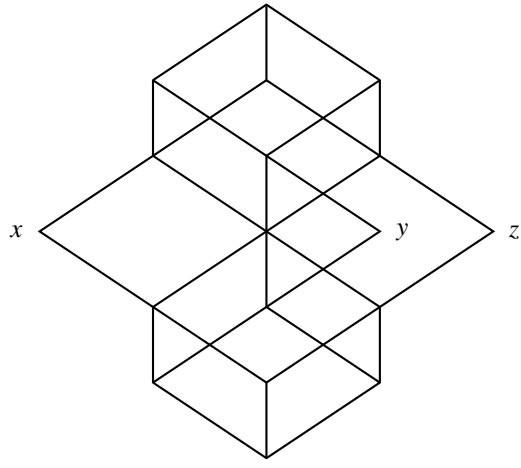
12.20. Következmény. *Disztributív háló akkor és csak akkor szubdirekt irreducibilis, ha kételemű.*

Bizonyítás. Mivel kételemű algebra mindig szubdirekt irreducibilis, ezért csak azt kell bizonyítani, hogy más szubdirekt irreducibilis disztributív háló nincs. Ez pedig azonnal következik a (7) feltételből. ■

Megjegyzések. 1. A (3) feltételben minden I ideál esetén az ideálon kívüli elemeknek megfeleltettünk egy, az 1-t tartalmazó ideált. Láttuk, hogy ez a megfeleltetés általában „majdnem" metszettartó. Azt viszont könnyen meg lehet mutatni, hogy a megfeleltetés mindig egyesítéstartó (ideálok egyesítésén természetesen a generátumokat értjük).

2. A tételben szereplő eljárást bármely háló esetében elvégezhetjük, megfeleltetve neki kételemű hálók szubdirekt szorzatát. Az így kapott háló természetesen disztributív lesz, és az eredetinek homomorf képe. Belátható, hogy ez a legnagyobb disztributív homomorf kép. □

12.21. Tétel. *Az alábbi ábra az x, y, z elemek generálta szabad disztributív hálót mutatja.*



Bizonyítás. A 11.30. tétel szerint a három generátorelemet minden lehetséges különböző módon le kell képezni a kételemű háló generátorrendszerére. Ez eleve szürjektív leképezést jelent, mert egyetlen elem nem generálja a kételemű hálót. Így az összes ilyen leképezések száma $2^3 - 2 = 6$. Ez azt jelenti, hogy a generátorelemeket hatkomponensű vektoroknak tekinthetjük. Minden egyes komponensben két generátorelemnek ugyanaz a képe, a harmadiké ettől különböző. Attól függően, hogy a 0 lép fel kétszer vagy az 1, a következő lehetőségeket kapjuk:

$$x = (001110), \qquad y = (010101), \qquad z = (100011).$$

Ezekből kell egyesítéssel és metszettel minden lehetséges elemet előállítani. Egyetlen olyan elem van, amelyben minden komponensben 1 áll: $x \vee y \vee z$. Három olyan elem van, amelyben egyetlen 0 áll. Ezek: $x \vee y = (011111)$, $x \vee z$ és $y \vee z$. Ezeknek páronként alkotott metszetei azok, amelyekben két 0 szerepel. A generátorelemeken kívül három 0-t tartalmaz a (000111) elem, amely éppen a generátorelemek mediánsa (ez a rajzon levő két „kocka" közös csúcsa). A számolások elvégzését az olvasóra bízzuk. ■

A disztributív hálókat fel lehet ismerni a rajzukról. Ez a rajz, mint ahogy a három elemmel generált szabad disztributív háló is mutatja, nem „síkbeli" rajz; olyan metszéspontok is keletkeznek, amelyek nem tartoznak a hálóhoz. Mielőtt a disztributív hálók „rajzról való felismerését" megadnánk, szükség van arra, hogy a moduláris hálókra is hasonló eredményt mutassunk meg. Ehhez a disztributív esethez hasonlóan megadjuk a moduláris hálók mediánsokkal való jellemzését.

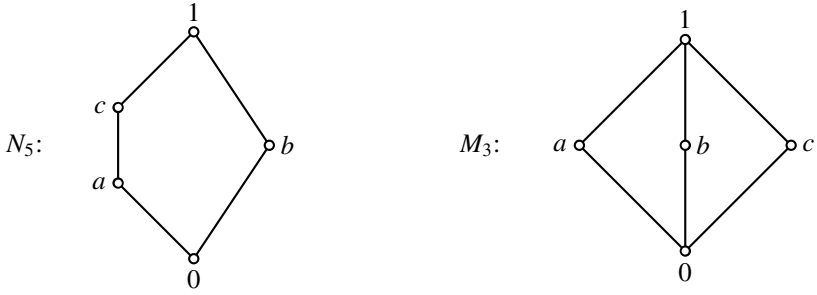
12.22. Tétel. *Ha egy tetszőleges L háló a, b, c elemei között legalább két összehasonlítható pár van, akkor $m(a, b, c) = M(a, b, c)$. Az L háló akkor és csak akkor moduláris (vagy disztributív), ha valahányszor L-nek a, b, c elemei között van összehasonlítható, mindannyiszor ezek alsó és felső mediánsa megegyezik.*

Bizonyítás. Mint a kis elemszámú hálók vizsgálatakor láttuk, ha három elem közt két összehasonlítható pár van, akkor vagy van az elemek között legnagyobb, vagy van legkisebb, vagy mindkettő van. A dualitás és az elemeknek a mediánsban való szimmetrikus elhelyezkedése miatt feltehető, hogy c a legnagyobb közülük. Ekkor triviális számolással mindkét mediánsra $a \vee b$ adódik.

Tegyük most fel, hogy $a \leq c$. Ekkor a két mediánst kiszámolva, az alsó mediánsra $a \vee (b \wedge c)$, a felsőre $(a \vee b) \wedge c$ adódik. Ezek egyenlősége pedig éppen a modularitással azonos.

Az összehasonlíthatatlan elemhármasra a két mediáns megegyezése – a 11.17. definíció szerint – éppen a disztributivitást adja. ■

12.23. Tétel. *Az ábrán látható N_5 háló szubdirekt irreducibilis és nem moduláris. Az ábrán látható M_3 háló egyszerű – így eleve szubdirekt irreducibilis – moduláris, de nem disztributív.*



Bizonyítás. Az N_5 hálóban $m(a, b, c) = a \neq c = M(a, b, c)$. A 12.22. tétel szerint tehát N_5 nem moduláris. Az M_3 hálóban $m(a, b, c) = 0 \neq 1 = M(a, b, c)$, így ez nem disztributív. Ha e hálóban veszünk két összehasonlítható elemet, akkor valamelyikük 0 vagy 1. Így, ha három elem közt van összehasonlítható pár, akkor van két összehasonlítható pár, ezért a 12.22. tétel következtében a három elem két mediánsa megegyezik. Ez pedig ugyancsak a 12.22. tétel miatt azt jelenti, hogy a háló moduláris.

A másik két állítás bizonyításához elöljáróban megjegyezzük, hogy véges háló tetszőleges nem-0 kongruenciájában vannak olyan kongruens elemek, amelyek egyike a másikat követi, feltéve, hogy van két különböző elem, amelyek kongruensek. Ugyanis e feltétel mellett a két elemet tartalmazó osztály konvex részháló, amiből következik az állításunk.

Nézzük először N_5-nek Θ nem-0 kongruenciáit. A dualitás alapján három lényegesen különböző eset van: $(a, c) \in \Theta$, $(0, a) \in \Theta$ és $(0, b) \in \Theta$ (és ezek duálisai). Azt bizonyítjuk be, hogy az első eset mindig fennáll. Ha $(0, b) \in \Theta$, akkor $a = a \vee 0 \equiv a \vee b = 1(\Theta)$, és a konvexitás bizonyítja állításunkat. A második esetben azt kapjuk, hogy $b = b \vee 0 \equiv$ $\equiv b \vee a = 1(\Theta)$. Most a dualitás alapján úgy tekinthetjük, hogy ezt az esetet visszavezettük az előbbire; így $\Theta \neq 0$ miatt $(a, c) \in \Theta$ mindig igaz. Könnyen belátható hogy az az osztályozás, amelynél egyetlen nemtriviális osztály – nevezetesen az (a, c) osztály – két elemet tartalmaz, valóban kongruencia, s a szerinte vett faktor az a négyelemű háló, amelyik nem lánc. Így van legkisebb kongruencia, ami biztosítja a szubdirekt irreducibilitást.

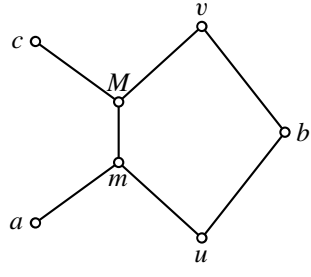
Az M_3 kongruenciáinak a vizsgálatakor a három nem-korlátelem szimmetrikus helyzete és a dualitás alapján elegendő egy olyan Θ kongruenciát nézni, amelynek eleme a $(0, a)$ pár. Az alábbi meggondolás egyszerűbb számolással is megmutatható volna, mégis

inkább a hosszabb – de a lényegre rámutató – utat választjuk. Nevezzük a $(0, x)$ alakú párokat alsó pároknak és az $(x, 1)$ alakúakat felső pároknak, ha $x \in \{a, b, c\}$. A $(0, x)$ és $(x, 1)$ összetartozó párok, a $(0, x)$ és $(y, 1)$ idegen párok, ha $x \neq y$. Mármost, ha $(0, a) \in \Theta$, és $b \neq a$, akkor $b = b \vee 0 \equiv b \vee a = 1(\Theta)$. Ez azt jelenti, hogy ha egy alsó pár kongruens, akkor minden, nem hozzá tartozó felső pár is kongruens. A dualitás szerint tehát minden olyan alsó pár kongruens, amelyik nem tartozik a kapott felső párokhoz. Tekintettel arra, hogy két felső párt kaptunk, azért egy alsó pár nem tartozhat ezek mindegyikéhez, amiből következik, hogy minden alsó pár – így minden felső pár is – kongruens. Ez pedig biztosítja az egyszerűséget. (Ugyanígy látható be az olyan hálók egyszerűsége is, ahol „középen" nem három, hanem akármennyi elem van. A fenti módszerrel ezekről is belátható, hogy modulárisak és egyszerűek.) ■

12.24. Tétel. (Dedekind). *Egy L háló akkor és csak akkor moduláris, ha nincs N_5-tel izomorf részhálója.*

Bizonyítás. A feltétel szükséges: Ha ugyanis L moduláris, akkor ez egy azonosság teljesülését jelenti. Így az azonosság L minden részhálójában is teljesül – márpedig N_5-ben nem teljesül a modularitás.

Most az elégségességet bizonyítjuk. Legyen $a \leq c$ esetén $m = m(a, b, c) < M(a, b, c) = M$. Az $a \leq c$ feltételből kiszámolva $m = a \vee (b \wedge c)$ és $M = c \wedge (b \vee a)$ adódik. Az $u = b \wedge c$ és $v = b \vee a$ jelöléssel a következőket kapjuk: $m = a \vee u$ és $M = c \wedge v$.



Az ábrán láthatjuk, hogy $\{m, M, u, v, b\}$ olyan részt alkotnak, amely N_5-re „hasonlít". Először is be kell látni, hogy ez részháló; azaz, ahol legkisebb felső, illetve legnagyobb alsó korlátot látunk, ott egyesítés és metszet van.

$m \vee b = a \vee u \vee b = a \vee ((b \wedge c) \vee b) = a \vee b = v$; s a monotonitás miatt $v = m \vee b \leq M \vee b \leq v$, azaz $M \vee b = v$. A dualitást felhasználva kapjuk, hogy ezek az elemek tényleg részhálót alkotnak. Azt kell még megmutatni, hogy ez a részháló valóban ötelemű, és nem az N_5 egy homomorf képe. A 12.23. tételben láttuk azonban, hogy minden, a 0-tól különböző homomorfizmus egybeejti a két összehasonlítható nem-korlátelemet; ami itt $m < M$ miatt nem lehetséges. ■

12.25. Tétel (Birkhoff). *Egy L háló akkor és csak akkor disztributív, ha sem N_5-tel, sem M_3-mal nincs izomorf részhálója.*

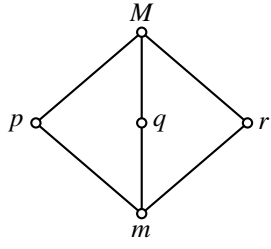
Bizonyítás. Tekintettel arra, hogy a disztributivitás is azonossággal definiálható, ezért a szükségesség bizonyítása analóg a moduláris esettel.

Az elégségesség bizonyításánál két esetet különböztetünk meg. Ha L nem moduláris, akkor a 12.24. tétel következtében van N_5-tel izomorf részhálója, s ekkor készen vagyunk. Azt az esetet kell még megnézni, amikor L nem disztributív ugyan, de moduláris. Azt mutatjuk meg, hogy ekkor L tartalmaz az M_3-mal izomorf részhálót.

Feltétel szerint léteznek olyan összehasonlíthatatlan a, b, c elemek az L-ben, amelyekre $m = m(a, b, c) < M(a, b, c) = M$. Legyenek $p = (m \vee a) \wedge M$, $q = (m \vee b) \wedge M$, $r = (m \vee c) \wedge M$. A modularitás következtében:

$$p = m \vee (a \wedge M), \qquad q = m \vee (b \wedge M), \qquad r = m \vee (c \wedge M).$$

Mivel $m \leq p, q, r \leq M$, ezért ez az öt elem az M_3-hoz hasonló elhelyezkedésű. Ahhoz, hogy részhálót kaptunk, be kell látni, hogy a látott egyesítések és metszetek valóban azok.



Az elemeknek a mediánsban való szimmetrikus elhelyezkedése, valamint a dualitás miatt elegendő a hat lehetséges esetből csupán egyet vizsgálni. Legyen ez például $p \vee q$.

Ezeket az elemeket mindenekelőtt úgy fejezzük ki, hogy jobban láthassuk, miképpen kaphatók az eredeti három elemből. Az elnyelési tulajdonság miatt $m \vee a = a \vee (b \wedge c)$. Felhasználva a nyilvánvaló $b \wedge c \leq M$ összefüggést, azt kapjuk, hogy $p = ((b \wedge c) \vee a) \wedge M = (b \wedge c) \vee (a \wedge M) = (b \wedge c) \vee (a \wedge (b \vee c))$. (Itt a modularitást és ismét az elnyelési tulajdonságot használtuk.) Hasonlóképpen adódik a $q = (a \wedge c) \vee (b \wedge (a \vee c))$ összefüggés is. Most tehát:

$$p \vee q = [(b \wedge c) \vee (a \wedge (b \vee c))] \vee [(a \wedge c) \vee (b \wedge (a \vee c))].$$

A kommutativitás és az asszociativitás következtében:

$$p \vee q = [(b \wedge c) \vee (b \wedge (a \vee c))] \vee [(a \wedge c) \vee (a \wedge (b \vee c))].$$

A $b \wedge c \leq b$ reláció, valamint a modularitás alapján:

$$(b \wedge c) \vee ((a \vee c) \wedge b) = ((b \wedge c) \vee (a \vee c)) \wedge b;$$

ami viszont megegyezik $[(a \vee c) \wedge b]$-vel. Hasonlóképpen kapjuk, hogy $(a \wedge c) \vee (a \wedge (b \vee c)) = (b \vee c) \wedge a$; végeredményben tehát $p \vee q = [(a \vee c) \wedge b] \vee [(b \vee c) \wedge a]$. Ismét alkalmazható a modularitás, az $(a \vee c) \wedge b \leq b \vee c$ feltétel miatt, amiből $p \vee q = [((a \vee c) \wedge b) \vee a] \wedge (b \vee c)$ következik. Ismét használjuk a modularitást: $a \vee c \geq a$ miatt $a \vee (b \wedge (a \vee c)) = (a \vee b) \wedge (a \vee c)$; és így

$$p \vee q = [(a \vee b) \wedge (a \vee c)] \wedge (b \vee c) = M.$$

Még azt kell megmutatni, hogy valóban M_3 szerepel, és nem annak egy homomorf képe. De M_3 egyszerűsége következtében, ha egy homomorf kép szerepelne, akkor $m = M$ volna – ellentétben a feltevésünkkel. ■

Feladatok

1. Bizonyítsuk be, hogy egy hálóban $\Theta(a, b) = \Theta(a \wedge b, a \vee b)$. ($\Theta(u, v)$ az a legkisebb kongruencia, amelynél u és v egy osztályba esik.)

2. Bizonyítsuk be, hogy egy disztributív hálóban $c \equiv d(\Theta(a, b))$ akkor és csak akkor igaz, ha $c = m(c, d, m(a, b, c))$ és $d = m(c, d, m(a, b, d))$.

3. Tetszőleges $\mathfrak{A}$ algebra $\mathfrak{B}$ részalgebrájának bármely Θ kongruenciája kiterjeszthető az $\mathfrak{A}$ egy $\overline{\Theta}$ kongruenciájává; ez a legkisebb olyan kongruencia, amelynél minden egyes Θ-beli osztály egyetlen osztályban marad. Az $\mathfrak{A}$ tetszőleges Φ kongruenciája megszorítható $\mathfrak{B}$ egy Φ^* kongruenciájává, amelynél $\mathfrak{B}$ két eleme pontosan akkor kongruens, ha Φ-nél az. Világos, hogy $\left(\overline{\Theta}\right)^* \geq \Theta$. Ha itt mindig egyenlőség van, akkor azt mondjuk, hogy érvényes a kongruencia-kiterjeszthetőség.

Bizonyítsuk be, hogy egy hálóban pontosan akkor érvényes a kongruencia-kiterjeszthetőség, ha a háló disztributív.

4. Bizonyítsuk be, hogy egy háló pontosan akkor disztributív, ha bármely intervallumban legfeljebb egy relatív komplementum van.

5. Bizonyítsuk be, hogy minden lánc disztributív háló.

6. Határozzuk meg az $a_0 \prec a_1 \prec \ldots \prec a_n$ lánc különböző kongruenciáinak a számát.

7. Adjunk felső korlátot az n elemmel generált szabad disztributív háló elemszámára. (A pontos elemszám nem ismeretes.)

8. Bizonyítsuk be, hogy a három elemmel generált szabad hálónak végtelen sok eleme van.

9. Adjunk meg az alsó és felső mediánson kívüli további többségi kifejezéseket (végtelen sok van).

10. Bizonyítsuk be, hogy ha $t(x, y, z)$ többségi kifejezés, akkor $m(x, y, z) \leq t(x, y, z) \leq M(x, y, z)$. (Ezért „alsó” mediáns az m és „felső” mediáns az M.)

11. Bizonyítsuk be, hogy egy disztributív hálóban minden konvex rész egy alkalmas kongruenciának az osztálya.

12. Bizonyítsuk be, hogy a három elemmel generált szabad hálóban nincs sem legkisebb, sem legnagyobb elem.

13. Mutassuk meg, hogy egy hálóban prímideálok tartalmazhatják egymást. Adjunk meg olyan példát, amelyben láncot alkotnak.

14. Bizonyítsuk be, hogy egy háló pontosan akkor disztributív, ha $c \leq a \vee b$ esetén van olyan $a' \leq a$ és $b' \leq b$, amelyekre $c = a' \vee b'$.

15. Egy egyesítés-félhálót nevezzünk disztributívnak, ha $c \leq a \vee b$ esetén van olyan $a' \leq a$ és $b' \leq b$, amelyekre $c = a' \vee b'$. Bizonyítsuk be, hogy egy véges disztributív egyesítés-félháló mindig (disztributív) háló.

16. Legyen L a 0-elemes S egyesítés-félháló ideálhálója. Bizonyítsuk be, hogy L akkor és csak akkor disztributív, ha S az.

12.3. Moduláris hálók

A következő tétel is mutatja a moduláris hálók jelentőségét:

12.26. Tétel. *Az alábbi hálók modulárisak:*

(1) *Csoport normálosztóhálója.*

(2) *Abel-csoport részcsoporthálója.*

(3) *Modulus részmodulushálója.*

(4) *Gyűrű egyoldali ideáljainak hálója.*

(5) *Gyűrű kétoldali ideáljainak hálója.*

Bizonyítás. Az első állítást tulajdonképpen már beláttuk, amikor bizonyítottuk, hogy egy csoport normálosztói rendelkeznek a modularitási tulajdonsággal (6.4. tétel). Tulajdonképpen ott azt a – formálisan erősebb – eredményt bizonyítottuk, hogy a normálosztóhálókban érvényes az „intervallumok izomorfizmusa". (Ezt a következő tételben tárgyaljuk majd.) Most mégis adunk egy közvetlen egyszerű bizonyítást (1)-re.

A modularitáshoz a következő tartalmazást kell belátni: ha $A \leq C$ és B a G csoport három normálosztója, akkor $A(B \cap C) \geq AB \cap C$. Legyen c eleme a jobb oldali részcsoportnak, ami a $c \in C$ tulajdonságon kívül azt is jelenti, hogy $c = ab$ alakú ($a \in A$, $b \in B$), hiszen A és B normálosztók. Mivel $a \in A \leq C$, ezért a $b = a^{-1}c$ elem is C-ben van. Így $b \in B \cap C$; ami pontosan azt jelenti, hogy a megadott felírás már egy kívánt típusú felbontást ad.

A többi állítás mindegyike speciális esetként adódik az előzőből.

Mivel Abel-csoport minden részcsoportja normálosztó, ezért (2) valóban (1) speciális esete.

Tekintsük egy modulus részmodulusainak a hálóját. Két részmodulus halmazelméleti metszete a metszetük. Egyesítésük pedig megegyezik az általuk generált (additív) részcsoporttal. Ez azt jelenti, hogy a részmodulushálóa tartó Abel-csoport részcsoporthálójának részhálója. (2) szerint a részcsoportháló moduláris, így ennek minden részhálója is moduláris. Tehát (3) is igaz.

Egy R gyűrű bal oldali (jobb oldali) ideáljainak a hálója a gyűrűnek mint önmaga feletti bal oldali (jobb oldali) R-modulusnak a részmodulushálója. Így (3) szerint valóban moduláris.

(5) bizonyításához csak azt kell figyelembe venni, hogy két ideálnak a metszete, illetve egyesítése nem változik meg, ha ezeket például balideáloknak tekintjük. Így az ideálháló a balideálok hálójának részhálója – tehát moduláris. ■

12.27. Definíció. Mint a 12.9. definícióban szerepelt, az L-beli $u \leq v$ elemek esetén az $[u, v] = \{x \mid u \leq x \leq v\}$ halmazt (az u, v elemek generálta) intervallumnak nevezzük.

Azt mondjuk, hogy az L hálóban érvényes az intervallumok izomorfizmustétele, ha tetszőleges $a, b \in L$ esetén a $\varphi : x \mapsto x \wedge b$, illetve a $\psi : x \mapsto x \vee a$ leképezéseket az $[a, a \vee b]$, illetve $[a \wedge b, b]$ intervallumokra megszorítva az $[a \wedge b, b]$, illetve az $[a, a \vee b]$ intervallumokra való izomorfizmust kapunk (amelyek egymás inverzei). □

12.28. Tétel. *Egy hálóban akkor és csak akkor érvényes az intervallumok izomorfizmustétele, ha a háló moduláris.*

Bizonyítás. Tegyük fel, hogy a hálóban érvényes az intervallumok izomorfizmustétele; és tekintsük a háló $a \leq c$ és b elemeit. Készítsük el a 12.24. tételben leírt módon az u, m, M, v elemeket. Az ott belátottak szerint alkalmazhatjuk az intervallumok izomorfizmustételét az $[u, b]$ és $[m, v]$ intervallumokra. Tekintettel arra, hogy $m \wedge b = M \wedge b = u$, ezért a $\varphi : [m, v] \to [u, b]$ izomorfizmusnál m és M képe megegyezik; tehát az injektivitás alapján $m = M$; tehát a háló moduláris.

Tekintsük most egy tetszőleges moduláris háló a és b elemeit; és nézzük a tételben megadott φ és ψ leképezéseket. Ezek definíciója alapján nyilvánvaló, hogy φ az $[a, a \vee b]$ intervallumot képezi az $[a \wedge b]$ intervallumba; és ψ fordítva.

Ha $x \in [a, a \vee b]$, akkor $\psi\varphi x = (x \wedge b) \vee a = x \wedge (b \vee a)$ – a modularitás miatt, mert $a \leq x$. Az $x \leq a \vee b$ feltételből most már következik az is, hogy $\psi\varphi x = x$. A dualitás miatt a $\varphi\psi$ leképezés is identikus, ami mindkét leképezés bijektivitását adja. Mármost $\varphi(x \wedge y) = (x \wedge y) \wedge b$ triviálisan megegyezik $(x \wedge b) \wedge (y \wedge b) = (\varphi x \wedge \varphi y)$-nal; vagyis φ metszettartó. A dualitás alapján ψ egyesítéstartó. Tekintettel arra, hogy e két leképezés egymás inverze, így mindkettő tartja az egyesítést is és a metszetet is; tehát valóban izomorfizmusok. ■

A következőkben a csoportokra vonatkozó Jordan–Hölder-tétel hálóelméleti részének az általánosításával foglalkozunk.

12.29. Definíció. Az L háló elemeinek egy $a = a_0 < a_1 < \ldots < a_{n-1} < a_n = b$ sorozatát az a és b elem közti n hosszúságú láncnak nevezzük. Ha emellett még $a_i \prec a_{i+1}$ is teljesül minden szóba jövő i-re, akkor maximális láncról beszélünk.

Az $a = b_0 < \ldots < b_k = b$ lánc az előzőnek finomítása, ha minden a_i valamelyik b_j-vel egyezik meg. Jelölje $\delta(a, b)$ az $a < b$ elemek közötti maximális láncok hosszának a minimumát (ha ilyen lánc egyáltalán létezik).

Amennyiben bármely $b, c \geq a$ esetén $\delta(a, b) + \delta(a, c) = \delta(a, b \wedge c) + \delta(a, b \vee c)$, akkor azt mondjuk, hogy δ dimenziófüggvény az a felett. Ha a fenti összefüggés minden $a \in L$ esetén teljesül, akkor δ-t dimenziófüggvénynek nevezzük.

12.30. Tétel (Jordan–Dedekind)**.** *Ha az L moduláris hálóban bármely $a < b$ elempárra létezik $\delta(a, b)$, akkor bármely, az a és b közti lánc hossza legfeljebb $\delta(a, b)$, bármely köztük levő maximális lánc hossza pontosan $\delta(a, b)$, és bármely köztük levő lánc maximális lánccá finomítható.*

Bizonyítás. Az állítást $\delta(a, b)$-re vonatkozó teljes indukcióval bizonyítjuk. Ha $\delta(a, b) = 1$, akkor $a \prec b$, és így nincs köztük egyetlen más lánc sem.

Tegyük most fel, hogy $\delta(a, b) = n$, és minden $c < d$ hálóbeli elempárra következik az állítás, ha $\delta(c, d) < n$. Tekintsük az $a = a_0 \prec a_1 \prec \ldots \prec a_{n-1} \prec a_n = b$ lánc mellett az $a = b_0 < b_1 < \ldots < b_{k-1} < b_k = b$ láncot is. Azt kell belátnunk, hogy $k \leq n$. Ha $b_{k-1} \leq a_{n-1}$, akkor $\delta(a, a_{n-1}) \leq n - 1 < n$ miatt $k - 1 \leq n - 1$, és így $k \leq n$. Ha $b_{k-1} \leq a_{n-1}$ nem teljesül, akkor $a_{n-1} \prec b$ következtében $a_{n-1} \vee b_{k-1} = b$. Tekintsük most a $c = a_{n-1} \wedge b_{k-1}$ elemet. Az intervallumok izomorfizmustétele miatt a $[c, b_{k-1}]$ és az $[a_{n-1}, a]$ intervallumok izomorfak; és így $c \prec b_{k-1}$. A $[c, a_{n-1}]$ és $[b_{k-1}, a]$ intervallumok izomorfizmusából pedig az következik, hogy $c < a_{n-1}$.

Mármost $\delta(a, a_{n-1}) < n$ miatt az $a \leq c < a_{n-1}$ lánc maximális lánccá finomítható, amelynek hossza $\delta(a, a_{n-1})$. E finomítás során mind $a \leq c$, mind $c < a_{n-1}$ maximális lánccá lett finomítva (az első lánc esetleg üres). Ebből következik, hogy $\delta(a, c) + \delta(c, a_{n-1}) = \delta(a, a_{n-1})$. Tekintettel arra, hogy $c \prec b_{k-1}$, ezért a és b_{k-1} között létezik egy maximális lánc, amelynek a hossza $1 + \delta(a, c)$. A $\delta(c, a_{n-1})$ pozitivitása miatt ez a szám legfeljebb $\delta(a, c) + \delta(c, a_{n-1}) = \delta(a, a_{n-1} < n$.

A teljes indukciós feltétel szerint tehát az a és a b_{k-1} között felírt lánc hossza kisebb, mint n. Így $k - 1 < n$; ami bizonyítja az első állítást.

Mivel az eredmény bármely a és b közti láncra igaz, ezért bármely lánc legfeljebb n hosszúságú lánccá finomítható; ami azt jelenti, hogy maximális lánccá finomítható. Ebből az is következik, hogy bármely más maximális lánc hossza is legfeljebb n. A $\delta(a, b)$ definíciója szerint viszont rövidebb sem lehet. ■

12.31. Tétel. *Ha az L háló bármely $a < b$ elemére létezik $\delta(a, b)$, akkor a modularitás ekvivalens azzal, hogy δ dimenziófüggvény.*

Bizonyítás. A 12.30. tételből következik, hogy moduláris hálóban $a \leq b \leq c$ esetén $\delta(a, b) + \delta(b, c) = \delta(a, c)$; amiből azonnal következik, hogy $a \leq b, c$ esetén $\delta(a, b) + \delta(a, c) = 2\delta(a, b \wedge c) + \delta(b \wedge c, b) + \delta(b \wedge c, c)$. Másrészt viszont $\delta(a, b \wedge c) + \delta(a, b \vee c) = 2\delta(a, b \wedge c) + \delta(b \wedge c, b) + \delta(b, b \vee c)$. Így e két szám egyenlőségéhez elég azt kimutatni, hogy $\delta(b \wedge c, c) = \delta(b, b \vee c)$; ami triviálisan következik az intervallumok izomorfizmustételéből.

Tegyük most fel, hogy δ dimenziófüggvény, és tekintsük a 12.24. tételben konstruált részhálót, amelynek elemei u, v, b, m, M. A megfelelő összefüggések alapján $\delta(u, m) + \delta(u, b) = \delta(u, u) + \delta(u, v) = \delta(u, M) + \delta(u, b)$ következik. Így $\delta(u, m) = \delta(u, M) = \delta(u, m) + \delta(m, M)$; amiből azonnal következik, hogy $m = M$, tehát a háló moduláris. ■

Ezután a moduláris hálókra vonatkozó másik fontos tételt bizonyítunk be, amelyet a Noether-gyűrűk ideáljainak a felbontásánál használtunk. Ehhez szükség van néhány fogalomra.

12.32. Definíció. Az L háló a elemét (metszet-) irreducibilisnek nevezzük, ha $a = b \wedge c$ csak akkor teljesül, ha b és c valamelyike megegyezik a-val.

Az $a = p_1 \wedge \ldots \wedge p_n$ előállítást irredundáns metszet-előállításnak nevezzük, ha bármely szóba jövő i index esetén a p_i elhagyásával kapott $p_i^* = p_1 \wedge \ldots \wedge p_{i-1} \wedge p_{i+l} \wedge \ldots \wedge p_n$ elemek mind különböznek a-tól. □

12.33. Tétel. *Ha az L hálóban érvényes a maximumfeltétel, akkor minden eleme előáll irreducibilis elemek metszeteként.*

Bizonyítás. Tekintsük L-nek azokat az elemeit, amelyeknek létezik irreducibilis elemek metszeteként való előállítása. Tegyük fel, hogy minden, a-nál nagyobb elem ilyen. Ha a irreducibilis, akkor a is ilyen. Ha a nem irreducibilis, akkor felírható $a = b \wedge c$ alakban, ahol $a < b$ és $a < c$. A feltétel szerint b és c mindegyike felírható a kívánt metszet alakban, ami azonnal adja, hogy a is előállítható így. A szóban forgó elemek halmaza tehát lefelé induktív; s a maximumfeltétel szerint ebből következik, hogy minden elem ilyen. ■

12.34. Tétel (Kuros–Ore). *Legyen az L moduláris háló a elemének irreducibilis elemek metszeteként való két előállítása*

$$a = p_1 \wedge \ldots \wedge p_n = q_1 \wedge \ldots \wedge q_k.$$

Ekkor minden szóba jövő i indexhez található olyan j index, hogy a 12.32. tételben megadott p^*-gal $a = p_i^* \wedge q_j$.

Amennyiben az eredeti felbontás irredundáns, akkor az új felbontás is az.

Bizonyítás. Tekintsük adott i mellett az $r_j = p_i^* \wedge q_j$ elemeket ($1 \leq j \leq k$). Ezekre az elemekre nyilvánvalóan teljesül, hogy $a = r_1 \wedge \ldots \wedge r_k$. Mivel $r_j \leq p_i^*$, ezért a fenti felbontás egyszersmind az $[a, p_i^*]$ intervallumban is felbontás. Ez az intervallum a 12.28. tétel szerint izomorf a $[p_i, p_i \vee p_i^*]$ intervallummal, és az izomorfizmusnál a-nak p_i felel meg. A p_i elem azonban irreducibilis a szóban forgó intervallumban, hiszen az egész hálóban is irreducibilis. Ezért a is irreducibilis a vizsgált intervallumban, ami azt jelenti, hogy a fenti felbontásban valamelyik r_j megegyezik a-val. Ez pedig éppen az első állítást adja.

Ha az eredeti előállítás irredundáns, akkor a kapott felbontásban q_j nem hagyható el, mert különben az eredeti felbontás nem volna irredundáns. Ha valamelyik p_m volna elhagyható, akkor e tétel szerint – p_m elhagyása után – q_j-t helyettesíthetnénk az eredeti $p_1, \ldots, p_n$ elemek valamelyikével. Mivel nem helyettesíthetjük egyszerre p_i-vel is és p_m-mel is, ezért itt is ellentmondást kapunk. ■

12.35. Tétel. *A 12.34. tétel feltételei mellett, ha mindkét felbontás irredundáns, akkor $n = k$.*

Bizonyítás. Kimutatjuk, hogy a q-k indexeit át lehet úgy számozni, hogy minden i indexre fennálljon az $a = q_1 \wedge \ldots \wedge q_i \wedge p_{i+1} \wedge p_n$ felbontás.

A 12.34. tétel szerint ez igaz $i = 1$ esetén. Bizonyítjuk, hogy ha i-re igaz, úgy igaz $(i + 1)$-re is. Valóban, a kapott $a = q_1 \wedge \ldots \wedge q_i \wedge p_{i+1} \wedge p_n$ felbontásban p_{i+1} kicserélhető az $a = q_1 \wedge \ldots \wedge q_n$ felbontás jobb oldalán levő valamelyik elemmel. Ennek az elemnek az indexe nagyobb, mint i, mert különben az i-edik lépésben kapott felbontás nem volna irredundáns. Így az index választható $(i + 1)$-nek, ami bizonyítja az állítást.

Ebből azonnal következik, hogy $n \leq k$; s ha a másik felbontás irredundanciáját is figyelembe vesszük, akkor $k = n$ adódik. ■

Megjegyzés. A 12.26. tétel alapján a 12.34. és a 12.35. tételek igazak bármely gyűrű ideáljaira. A 12.33. tétel miatt az előállítás mindig létezik, ha a gyűrű Noether-féle. Ezzel a 7.73. tételt bebizonyítottuk. □

Feladatok

1. Mutassuk meg, hogy van olyan L végtelen háló, amelyben nincs „követő pár”, azaz ha $a < b$ elemei L-nek, akkor van olyan $c \in L$, amelyre $a < c < b$.

2. Mutassuk meg, hogy bármely L véges háló tartalmaz követő párt, azaz $a \prec b$ elemeket.

3. Legyen L egy véges moduláris háló, amely tartalmaz M_3-mal izomorf részhálót. Mutassuk meg, hogy akkor tartalmaz „követő M_3-at", azaz olyan u, a_1, a_2, a_3, v elemeket, amelyekre $u \prec a_i \prec v$ minden $i \in \{1, 2, 3\}$ esetén.

4. A (véges) test feletti (véges dimenziós) vektortér altereit projektív geometriáknak nevezzük (l.: I. kötet 169. és 224. oldal). Ennek pontjai az egydimenziós alterek, egyenesei a kétdimenziós alterek, stb. Háromdimenziós tér alterei a projektív síkok. Bizonyítsuk be, hogy ha egy véges háló tartalmaz egy projektív síkot, akkor követéstartó módon is tartalmazza (azaz, ha φ a beágyazás, akkor $a \prec b$ esetén $\varphi a \prec \varphi b$ is teljesül).

5. Legyen M_n a következő módon definiálva: elemei $0, 1, a_1, \ldots, a_n$ és bármely i indexre $0 \prec a_i \prec 1$. Bizonyítsuk be, hogy van olyan véges moduláris háló (konkrétan projektív tér is), amelyik tartalmazza M_4-et, de nincs követéstartó beágyazás. (M_n-re is igaz, ha $n > 3$.)

6. Jelölje $S(p)$ a $\mathbb{Q}_p$ feletti projektív síkot. Adott $q_1, \ldots, q_r$ prímszámokra tekintsük az $S(q_1), \ldots, S(q_r)$ hálók tetszőleges L szubdirekt szorzatát. Mutassuk meg, hogy ha $S(p) \leq L$, akkor $p \in \{q_1, \ldots, q_r\}$. Mutassuk meg, hogy a moduláris hálók részvarietásainak a száma kontinuum (használjuk fel, hogy ha egy projektív sík része egy szubdirekt szorzatnak, akkor egy véges „részszorzatnak" is része).

7. Definiáljuk az $M_3 + M_3$ hálót a következőképpen: Elemei u, v, w, a_i, b_i, ahol $i \in \{1, 2, 3\}$, és $a \prec a_i \prec v \prec b_j \prec w$ ($i, j \in \{1, 2, 3\}$). Mutassuk meg, hogy $M_3 + M_3$ moduláris, és nem lehet egy (véges) Abel-csoport részcsoporthálója.

8. Definiáljuk az $M_{3,3}$ hálót a következőképpen: elemei $0, a, b, c, d, e, f, 1$, az a, b, c elemek követik 0-t, 1 követi a d, e, f elemeket, d követi az a, b, c elemeket és c-t követi d, e, f. Mutassuk meg, hogy $M_{3,3}$ sem lehet egy (véges) Abel-csoport részcsoporthálója, de ugyancsak moduláris.

9. Mutassuk meg, hogy $M_3 + M_3$ két darab M_3 szubdirekt szorzata.

10. Mutassuk meg, hogy $M_{3,3}$ egyszerű.

11. Adjunk meg olyan egyszerű moduláris hálót, amelynek végtelen sok eleme van.

12. Mutassuk meg, hogy végtelen sok olyan (nemizomorf) moduláris háló létezik, amelynek végtelen sok eleme van.

12.4. Atomos hálók és Boole-hálók

A csoportokkal, gyűrűkkel ellentétben a hálók esetén a kongruenciák egy-egy osztálya nem határozza meg egyértelműen a többit. Ez még disztributív hálók esetében sem teljesül. Például egy láncban diszjunkt intervallumok bármely rendszere kompatibilis osztályozást hoz létre. Az idézett struktúrákban a fenti jelenséget az inverzelem létezése biztosítja. (Emlékeztetünk rá, hogy a félcsoportok esetében sem határozta meg feltétlenül egy kongruenciaosztály a többit.) Az inverzelemnek a szerepét a hálók esetében – bizonyos fokig – a komplementer elem tölti be.

Amennyiben a hálónak nincs 0-eleme és 1-eleme, akkor természetesen komplementer elemről sem lehet beszélni. Lehetőség van azonban a komplementer elem „lokális" pótlására, ahogy ezt a 12.12. definícióban tettük:

Az L háló adott $u \leq a \leq v$ elemei esetén a b elemet az a elem $[u, v]$ intervallumbeli relatív komplementerének nevezzük, ha $a \wedge b = u$ és $a \vee b = v$.

Az L hálót relatív komplementumosnak nevezzük, ha bármely intervallumban bármely elemnek létezik relatív komplementere.

12.36. Tétel. *Relatív komplementumos háló adott kongruenciájában bármely kongruenciaosztály egyértelműen meghatározza a többit.*

Bizonyítás. Tekintsünk először két olyan kongruenciaosztályt, amelyeknek van összehasonlítható elemük. Legyenek ezek az A osztálybeli a és a B osztálybeli b elemek, amelyekre tehát $a \leq b$. Azt mutatjuk meg, hogy egy tetszőleges c elemről az A kongruenciaosztály ismeretében el tudjuk dönteni, hogy eleme-e B-nek. A konvexitás és az idempotencia miatt $c \equiv b$ azzal ekvivalens, hogy $c \wedge b \equiv b$ és $c \vee b \equiv b$. Ezért elegendő a kérdést a b-vel összehasonlítható elemekre megnézni. A dualitás következtében azt is feltehetjük, hogy a vizsgált elemre $c < b$ teljesül. A kompatibilitás következtében ekkor $u = a \wedge c \equiv a \wedge b = a$, ha fennáll a kongruencia. A kérdéses kongruenciának tehát egyik feltétele, hogy $u \equiv a$. Ha ez teljesül, akkor tekintsük c-nek az $[u, b]$ intervallumban levő v relatív komplementumát. A $c \equiv b$ kongruenciából adódó $v = u \vee (v \wedge b) \equiv u \vee (v \wedge c) = u \vee u = u$ összefüggésből azt a feltételt kapjuk, hogy v is eleme A-nak. Amennyiben viszont $u, v \in A$, akkor $c = c \vee u \equiv c \vee v = b$. Eszerint $c \in B$ pontosan akkor, ha $u, v \in A$; vagyis az A osztály meghatározza a B elemeit. A dualitás alapján ugyanez igaz, ha a $b \in B$ és $a \in A$ elemekre $a \geq b$ igaz. Az általános esetben tekintsünk egy tetszőleges $a \in A$ és egy $b \in B$ elemet. Legyen X (egy) az $a \vee b$ elemet tartalmazó kongruenciaosztály. A bizonyítás első lépése szerint A meghatározza X elemeit; és a dualitás alapján X meghatározza B elemeit; ezért az állítás bármely két kongruenciaosztályra igaz. ■

Tekintsük azt a hálót, amelynek elemei $0 \prec a \prec u \prec c \prec 1$ és $0 \prec b \prec 1$ (az N_5-ben a és c közé betettünk egy u elemet). Látható, hogy ez egy komplementumos háló. Viszont nem relatív komplementumos, mert az $[a, c]$ intervallumban u-nak nincs relatív komplementuma. Moduláris hálók esetében ez nem fordulhat elő.

12.37. Tétel. *Moduláris komplementumos háló relatív komplementumos.*

Bizonyítás. Tekintsük az $[u, v]$ intervallum egy a elemét és ennek egy a' komplementumát. A modularitás miatt $u \vee (a' \wedge v)$ és $(u \vee a') \wedge v$ az $[u, v]$ intervallumnak ugyanazt az a^+ elemét adja. A modularitás miatt $(u \vee a') \wedge a = u \vee (a' \wedge a) = u \vee 0 = u$; így $a \wedge a^+ = a \wedge v \wedge (a' \vee u) = v \wedge u = u$. A dualitás alapján kapjuk, hogy $a \vee a^+ = v$. ■

Különösen fontos a disztributív hálók esete.

12.38. Definíció. A komplementumos disztributív hálót Boole-hálónak (vagy Boole-algebrának) nevezzük.

12.39. Tétel. *Boole-hálóban a komplementum és a relatív komplementum egyértelmű; a Boole-háló tekinthető* $(0, 0, 1, 2, 2)$ *típusú algebrának.*

Bizonyítás. Nyilván elegendő a relatív komplementum egyértelműségét bizonyítani. Legyen az $[u, v]$ intervallum egy a elemének b és c relatív komplementuma; azaz legyen $a \wedge b = a \wedge c = u$ és $a \vee b = a \vee c = v$. Ebből kapjuk, hogy $m(a, b, c) = u \vee u \vee (b \wedge c) = b \wedge c$ és $M(a, b, c) = v \wedge v \wedge (b \vee c) = b \vee c$. A két mediáns megegyezéséből $b \wedge c = b \vee c$ következik, amiből triviálisan adódik, hogy $b = c$.

Így egy Boole-hálóban a következő műveleteket tekinthetjük: Két nullváltozós (a 0-elem és az 1-elem kijelölése), egy egyváltozós (a komplementerképzés – hiszen a komplementer egyértelmű) és két kétváltozós (a két hálóművelet). ■

A továbbiakban célszerű a Boole-hálókat eleve $(0, 0, 1, 2, 2)$ típusú algebráknak tekinteni, egyszersmind a fennálló azonosságokkal definiálni.

12.40. Tétel. *Egy* $\langle B; \{0, 1, ', \vee, \wedge\}\rangle$ *algebra akkor és csak akkor Boole-háló, ha:*
(1) $\vee$ *és a* $\wedge$ *műveletekre disztributív háló.*
(2) *Minden* $x \in B$ *esetén* $0 \vee x = x \wedge 1 = x$.
(3) *Minden* $x, y \in B$ *esetén* $(x')' = x'' = x$; $x \wedge x' = 0$; $0' = 1$ *és* $(x \vee y)' = x' \wedge y'$.

Bizonyítás. Mindenekelőtt megjegyezzük, hogy a felírt összefüggésekből azonnal következik az egyes műveletek változószáma.

Tetszőleges Boole-hálóban a tételben felsorolt azonosságok az utolsót kivéve triviálisan igazak. Tudjuk, hogy $(x \vee y)'$ az $x \vee y$ komplementere. A disztributivitás alapján $(x \vee y) \vee (x' \wedge y') = (x \vee y \vee x') \wedge (x \vee y \vee y') = 1 \wedge 1 = 1$. $(x \vee y) \wedge (x' \wedge y') = 0$ a dualitás következménye.

Tegyük most fel, hogy a felírt azonosságok teljesülnek. Azt kell belátnunk, hogy a fenti definíció olyan komplementumos disztributív hálót ad, amelyben 0 a legkisebb, 1 a legnagyobb elem, és x' az x komplementuma. Az algebra, definíció szerint, disztributív háló; és a (2) feltétel alapján 0, illetve 1 a megfelelő korlátelemek. Azt kell csupán bizonyítani, hogy x' az x komplementuma. Az $x \wedge x' = 0$ teljesülését a tételben kimondtuk. A további feltételek figyelembevételével az alábbi módon bizonyítható az, hogy $x \vee x' = 1$:

$$x \vee x' = ((x \vee x')')' = (x' \wedge x'')' = (x' \wedge x)' = 0' = 1. \blacksquare$$

Megjegyzések. 1. A fentiekből a dualitás alapján könnyen levezethető az $(x \wedge y)' = x' \vee y'$ azonosság is.

2. Mivel minden Boole-háló egyben disztributív háló, ezért ezeknek is tekinthetjük egy halmaz részhalmazaiként való reprezentációját. A 12.19. kiegészítés alapján a következőket nyerjük:

Minden Boole-háló izomorf egy halmaz részhalmazhálójának egy részhálójával. Ennél az izomorfizmusnál a 0*-elem képe az üres halmaz, az* 1*-elem képe az egész halmaz; egy elem komplementerének a képe az elem képének a komplementerhalmaza.*

3. Első látásra úgy tűnik, hogy a fenti reprezentációban minden részhalmaznak fel kellene lépnie. Ez nem így van. Például egy végtelen halmazban azok a halmazok, amelyek vagy végesek, vagy véges halmaz komplementerei, Boole-hálót alkotnak. (Ennek kimutatását az olvasóra bízzuk.) □

A halmazok esetén fontos művelet a részhalmazok szimmetrikus differenciája, amely azokat az elemeket tartalmazza, amelyek a két részhalmaz közül pontosan az egyiknek elemei. A fenti reprezentáció alapján ezt a műveletet tetszőleges Boole-hálóban értelmezhetjük:

12.41. Tétel. *Tetszőleges* B *Boole-hálóban legyen* $a + b = (a \wedge b') \vee (b \wedge a')$ *és* $ab = a \cdot b = a \wedge b$ $(a, b \in B)$. *Ekkor* $\langle B; \{+, \cdot\}\rangle$ *egy* 2*-karakterisztikájú, egységelemes kommutatív gyűrű, amelynek minden eleme idempotens.*

Bizonyítás. Feladatunk bizonyos azonosságok teljesülésének a kimutatása. Tekintettel arra, hogy szubdirekt szorzatban egy azonosság bizonyosan teljesül, ha teljesül minden

egyes komponensen, ezért elég a kívánt azonosságokat a kételemű Boole-hálóban bizonyítani.

Ha $a = b$, akkor $a+b = 0$, míg $a \neq b$ esetén $a+b = 1$. Az így definiált művelet éppen a kételemű testben vett összeadás. Az is triviális, hogy a definiált szorzás pedig az e testen tekintett szokásos szorzás. Mivel az állításban szereplő minden azonosság igaz a kételemű testben, ezért valóban egy kívánt tulajdonságú gyűrűt kapunk. ■

12.42. Definíció. Egy egységelemes gyűrűt Boole-gyűrűnek nevezünk, ha minden eleme idempotens. □

12.43. Tétel. *Boole-gyűrű 2-karakterisztikájú és kommutatív. Boole-gyűrűből Boole-hálót kapunk, ha a műveleteket a következőképpen definiáljuk:*

$$a \vee b = a + b + a \cdot b, \qquad a \wedge b = a \cdot b,$$

$$a' = 1 + a, \qquad 0 = 0, \qquad 1 = 1.$$

Bizonyítás. $a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$ alapján következik $ba = -ab$. Most $b = a$ választással $a = a^2 = -a^2 = -a$, amiből kapjuk, hogy a gyűrű karakterisztikája 2, és adódik $ab = -ba = ba$ is, tehát a gyűrű kommutatív.

Itt is hasonló típusú állítást kell bizonyítani, mint a 12.41. tételben. Ezért ezt is elegendő szubdirekt irreducibilis gyűrűkre nézni. Legyen a az R szubdirekt irreducibilis Boole-gyűrű 0-tól különböző eleme. Ha $ax = (1 + a)y$, akkor $ax = aax = a(1 + a)y = 0$, tehát a megfelelő ideálokra $(a) \cap (1 + a) = (0)$. Mivel e két ideál generálja a gyűrűt (hiszen 1 eleme a generátumnak), ezért R ezeknek a direkt összege. A szubdirekt irreducibilitás miatt tehát $1 + a = 0$, azaz $a = a + (1 + a) = 1 + 0 = 1$. Így R-nek két eleme van.

Tekintsük a definiált műveleteket a kételemű testen. Ha $a = b$, akkor $a \vee a = a$, míg $a \neq b$ esetén $ab = 0$ és $a + b = 1$ miatt $a \vee b = 1$. Ez a művelet tehát a hálóelméleti egyesítés ($0 < 1$ értelmezéssel). Mivel $ab = 1$ pontosan akkor teljesül, ha $a = b = 1$, ezért $\wedge$ megegyezik a hálóelméleti metszettel. A másik három művelet triviálisan adja a komplementert, illetve a korlátelemeket. ■

Megjegyzés. A fenti konstrukciók alapján világos, de közvetlen számolással is igazolható, hogy a 12.41., illetve a 12.43. tételben megadott konstrukciókat egymás után végrehajtva, mindig az eredeti műveleteket kapjuk vissza, akár Boole-hálóból, akár Boole-gyűrűből indultunk ki. Ezt röviden úgy fogalmazhatjuk, hogy a Boole-gyűrűk és a Boole-hálók a fenti módon egyértelműen megfeleltethetők egymásnak. Ennek következménye, hogy a fenti konstrukcióval minden Boole-gyűrűt, illetve minden Boole-hálót előállíthatunk. Ennek részletes bizonyítását az olvasóra bízzuk. □

Hálóelméleti vizsgálatoknál fontos szerepet játszanak azok a hálók, amelyekben minden elem minimálisoknak az egyesítése.

12.44. Definíció. Egy L háló p elemét atomnak nevezzük, ha $0 \prec p$. Az L hálót atomosnak nevezzük, ha minden elem előáll (esetleg végtelen sok) atom egyesítéseként.

q duális atom (vagy koatom), ha $q \prec 1$. □

Megjegyzések. 1. Az atomos háló elnevezés nem minden szerzőnél fedi a fenti fogalmat.

2. Atomos hálóra példa egy halmaz összes véges részhalmazának a tartalmazásra nézve vett hálója. Ez a háló disztributív.

3. A legfontosabb példa a véges dimenziós projektív geometria. Itt az atomok a projektív tér pontjai.

4. Ugyancsak fontos példa egy véges halmaz partíciói a tartalmazásra nézve. Tetszőleges halmaz esetében a P_1 és P_2 partíciókra $P_1 \leq P_2$, ha a P_1-hez tartozó minden osztály teljes egészében benne van egy P_2-höz tartozó osztályban; a legkisebb partíciónál minden elem egyedül alkot egy osztályt, a legnagyobbnál minden elem ugyanabba az osztályba esik. Könnyen belátható, hogy akármennyi partíció közös része is partíció, ezért ezek egy teljes hálót alkotnak. Itt atomok azok a partíciók, amelyekben egyetlen kételemű osztály van, a többi mind egyelemű. □

Ha egy halmaz összes részhalmazát tekintjük, akkor ezek hálója Boole-háló, amelynek – mint említettük – a halmaz elemei az atomjai. Léteznek azonban olyan Boole-hálók, amelynek nincsenek atomjai.

12.45. Tétel. *A végtelen sok elemmel generált szabad Boole-hálónak nincsenek atomjai.*

Bizonyításvázlat. Legyenek $\mathbf{x}_1, \ldots, \mathbf{x}_n \ldots$ a szabad generátorok. Ezek mindegyikének van komplementere: $\mathbf{x}_1', \ldots, \mathbf{x}_n' \ldots$, amelyek egymástól is és az adott generátoroktól is különböznek. A komplementerekre vonatkozó azonosságoktól eltekintve a szabad Boole-háló az ezek által generált szabad disztributív háló. A disztributivitás következtében minden elem egyértelműen felírható a fenti elemek egyesítéseinek metszeteként. Ha mármost $\mathbf{f} = f(\mathbf{x}_1, \mathbf{x}_1', \ldots)$ egy tetszőleges kifejezés, és $\mathbf{y}$ egy olyan generátorelem, amelyik nem szerepel az argumentumok közt, akkor világos, hogy $0 < \mathbf{f} \wedge \mathbf{y} < \mathbf{f}$, tehát $\mathbf{f}$ nem lehet atom. ■

Feladatok

1. Bizonyítsuk be, hogy N_5 nem atomos.

2. Bizonyítsuk be, hogy egy halmaz részhalmazaiból álló Boole-hálóban értelmezett összeadás nem más, mint a szereplő halmazok szimmetrikus differenciája; azaz az a halmaz, amelynek elemei a két halmaz közül pontosan egyben vannak benne.

3. Legyenek $A_1, \ldots, A_k$ egy halmaz részhalmazai. Határozzuk meg, mely elemekből áll a megfelelő Boole-gyűrűbeli $A_1 + \cdots + A_k$ halmaz.

4. Definiáljunk a H halmaz részhalmazain egy relációt: $a \sim B$, ha $A + B$ véges. Bizonyítsuk be, hogy ez egy kongruenciareláció és a faktorhálóban nincsenek atomok.

5. Határozzuk meg azokat a véges Abel-csoportokat, amelyeknek a részcsoporthálója atomos.

6. Adjunk meg olyan csoportot, amelynek a részcsoporthálója nem moduláris.

7. Bizonyítsuk be, hogy a kételemű halmaz partícióhálója disztributív, a háromeleműé nem disztributív, de moduláris, a négyeleműé nem moduláris.

8. Bizonyítsuk be, hogy egy (véges) projektív geometriában bármely két 0-tól különböző elemhez van olyan atom, amely az egyiknél kisebb, és a másikkal összehasonlíthatatlan.

9. Adjunk meg olyan hálót, amelyben minden lánc véges, de a láncok hossza nem korlátos.

10. Nevezzük az L háló S részhálóját szuperkonvexnek, ha $a, b \in S$, $u, v \notin S$ elemeire az $u < a$ és $u < b$, illetve $a < v$ és $b < v$ feltételek ekvivalensek. Bizonyítsuk be, hogy szuperkonvex részháló kongruenciaosztály.

11. Bizonyítsuk be, hogy egy disztributív háló minden ideálja prímideálok metszete; M_3-nak viszont van olyan ideálja, amelyik nem áll így elő.

12.5. Kongruenciahálók

Egy varietás algebrái kongruenciáinak hálója sok mindent elárul a varietásról. Egy főkongruencia „szerkezetét” a Malcev-lemma írja le, amit bizonyítás nélkül közlünk:

Tétel. *Legyenek a, b, c, d az $\mathfrak{A}$ algebra elemei. $c \equiv d(\Theta(a, b))$ akkor és csak akkor igaz, ha található olyan $c = c_0, \ldots, c_n = d$ elemlánc, hogy minden i indexhez létezik olyan $f_i(x, y, z_1, \ldots, z_{n(i)})$ kifejezés, hogy alkalmas $u_1, \ldots, u_{n(i)} \in \mathfrak{A}$ elemekkel*

$$c_i = f_i(a, b, u_1, \ldots, u_{n(i)}) \quad \text{és} \quad c_{i+1} = f_i(b, a, u_1, \ldots, u_{n(i)}).$$ ■

A kongruenciaháló disztributivitása a később tárgyalásra kerülő ultraszorzat segítségével lehetővé teszi a szubdirekt irreducibilis algebrák jobb megismerését. Erre létezik egy szükséges és elégséges feltétel, amely elég bonyolult. Ennek a legegyszerűbb esete az, amikor a varietásban létezik egy többségi kifejezés.

Tétel. *Ha $m(x, y, z)$ a $\mathcal{V}$ varietásban többségi kifejezés, akkor a $\mathcal{V}$-beli algebrák kongruenciahálója disztributív.*

Bizonyítás. Legyen α, β, γ három kongruencia. Azt kell belátni, hogy $(\alpha \vee \beta) \wedge \gamma \leq$ $\leq (\alpha \wedge \gamma) \vee (\beta \wedge \gamma)$. Tegyük fel, hogy a és b kongruensek a bal oldali kongruenciánál. Ez azt jelenti, hogy a metszet mindkét komponensénél kongruensek, tehát mindenesetre kongruensek γ-nál. Az, hogy $(\alpha \vee \beta)$-nál kongruensek, azt jelenti, hogy van olyan $a = c_0, \ldots, c_n = b$ elemlánc, hogy (c_i, c_{i+1}) vagy α-nak, vagy β-nak eleme. Tekintsük most a $d_i = m(a, b, c_i)$ sorozatot. Azonnal látható, hogy $d_0 = a$ és $d_n = b$. Mivel $a \equiv b(\gamma)$, ezért $d_i = m(a, b, c_i) \equiv m(a, a, c_i) = a(\gamma)$. Másrészt $d_i = m(a, b, c_i) \equiv m(a, b, c_{i+1}) =$ $= d_{i+1}(\Theta(c_i, c_{i+1}))$ miatt e két elem – megfelelően – vagy α-nál, vagy β-nál kongruens; következésképpen a lánc minden „szeme” vagy $(\alpha \wedge \gamma)$-nál, vagy $(\beta \wedge \gamma)$-nál kongruens. Így a és b kongruensek ezek egyesítésénél. ■

Következmény. *A hálók kongruenciahálója disztributív.* ■

A másik fontos tulajdonság a *kongruencia-felcserélhetőség* Ez azt mondja ki, hogy ha $a \equiv b(\alpha)$ és $b \equiv c(\beta)$, akkor van olyan d, hogy $a \equiv d(\beta)$ és $d \equiv c(\alpha)$.

Egy $p(x, y, z)$ kifejezést *Malcev-kifejezésnek* nevezünk, ha a varietás bármely $\mathfrak{A}$ algebrájának bármely a, b elemére $p(a, a, b) = b$ és $p(a, b, b) = a$.

Tétel. *Ha egy varietásban van Malcev-kifejezés, akkor algebráinak kongruenciahálója felcserélhető.*

Bizonyítás. Tegyük fel, hogy $a \equiv b(\alpha)$ és $b \equiv c(\beta)$. Definiálja d-t $d = p(a, b, c)$. Triviális számolással adódik, hogy ez a d megfelelő. ■

Megjegyzés. Bizonyítható, hogy a kongruencia felcserélhetőségből következik a kongruenciaháló modularitása. □

Feladatok

1. Bizonyítsuk be, hogy disztributív háló kongruenciahálója Boole-háló.

2. Nevezzünk egy $f(x_1, \ldots, x_n)$ kifejezést (n-)majdnem egyöntetűnek, ha minden olyan behelyettesítésnél, amikor egy kivétellel mindenhova ugyanazt helyettesítjük, a kifejezés értéke ez a „majdnem egyöntetű" érték lesz. (A többségi kifejezés 3-majdnem egyöntetű.) Bizonyítsuk be, hogy ha létezik n-majdnem egyöntetű kifejezés, akkor létezik $(n+1)$-majdnem egyöntetű is (tehát a változószám növelése a kifejezés „erejét" gyengíti). Bizonyítsuk be, hogy a majdnem egyöntetű kifejezés létezéséből is következik a kongruencia-disztributivitás.

3. Bizonyítsuk be, hogy csoportok kongruenciahálója felcserélhető.

4. Bizonyítsuk be, hogy van olyan algebra, amelynek a kongruenciahálója M_n, ha $3 \leq n \leq 6$.

5. Bizonyítsuk be, hogy $n = p^k + 1$ esetén (p prímszám) van olyan algebra, amelynek kongruenciahálója M_n.

13. Rendezett csoportok és testek

13.1. Részbenrendezett csoportok

A hálók vizsgálatánál a műveleteket a részbenrendezés segítségével értelmeztük. Vannak viszont olyan esetek, amikor a részbenrendezést az adott „szokványos típusú" algebrában tekintjük mint egy „kiegészítő tulajdonságot". A további vizsgálatok fő célja az az eset, amikor testeket vizsgálunk. Ennek bevezetéséül egy rövid szemlét tartunk a részbenrendezett csoportok körében.

13.1. Definíció. Egy $\leq$ részbenrendezési relációt kompatibilisnek nevezünk a $G = \langle G; \cdot \rangle$ csoporton, ha $a \leq b$ és tetszőleges G-beli elemekre $a \cdot c \leq b \cdot c$ és $c \cdot a \leq c \cdot b$ teljesülnek.

Ha adott a G csoporton egy kompatibilis részbenrendezés, akkor azt mondjuk, hogy $\langle G; \cdot, \leq \rangle$ részbenrendezett csoport. □

13.2. Definíció. Egy G rendezett csoportban a $P = \{x \mid 1 \leq x\}$ halmazt (1 a G egységeleme) a részbenrendezés pozitív kúpjának nevezik. □

13.3. Tétel. *Egy $\langle G; \leq \rangle$ csoport pozitív kúpja egyértelműen meghatározza a részbenrendezést. A pozitív kúp olyan P invariáns félcsoport, amelyre $P \cap P^{-1} = \{1\}$. Bármely ilyen tulajdonságú részfélcsoport egy alkalmas részbenrendezés pozitív kúpja.*

Bizonyítás. A művelettel való kompatibilitás miatt $a \leq b$ és $1 \leq ab^{-1}$ ekvivalensek, tehát a pozitív kúp valóban egyértelműen meghatározza a részbenrendezést.

Legyen P a részbenrendezés pozitív kúpja. Ha $1 \leq a, b$, akkor a kompatibilitás miatt $a \leq ab$ és a tranzitivitásból $1 \leq a \leq ab$ következik; tehát P részfélcsoport. Ha $1 \leq a$ és $b \in G$, akkor a kompatibilitás alapján $1 = b^{-1}b \leq b^{-1}ab$, vagyis P invariáns. Ha $a \in P \cap P^{-1}$, akkor $1 \leq a, a^{-1}$, azaz $a = a1 \leq aa^{-1} = 1$; így $a \leq 1 \leq a$, amiből $a = 1$ következik az antiszimmetria alapján.

Legyen végül P a G-nek a felsorolt tulajdonságokkal rendelkező részhalmaza, és definiálja a részbenrendezést a következő: $a \leq b$ pontosan akkor, ha $ab^{-1} \in P$. Ez a relációt egyértelműen meghatározza. A második állítás szerint, ha ez egy részbenrendezés pozitív kúpja, akkor az eredeti részbenrendezést kapjuk vissza. Azt kell még belátni, hogy a reláció részbenrendezés. $aa^{-1} = 1 \in P$ miatt a reláció reflexív. Ha $a \leq b \leq c$, akkor $ab^{-1}, bc^{-1} \in P$, amiből a P szorzásra való zártsága alapján $ac^{-1} = ab^{-1}bc^{-1} \in P$ következik; tehát a reláció tranzitív. Ha $ab^{-1}, ba^{-1} \in P$, akkor $(ab^{-1})^{-1} \in P$, azaz $ab^{-1} \in P^{-1}$, amiből $ab^{-1} = 1$, vagyis $a = b$ következik, mert $P \cap P^{-1} = \{1\}$. Így a reláció részbenrendezés. Ha $a \leq b$ és c tetszőleges, akkor egyrészt $ac(bc)^{-1} = acc^{-1}b^{-1} = ab^{-1} \in P$ alapján $ac \leq bc$, másrészt $ca(cb)^{-1} = c(ab^{-1})c^{-1}$ következtében $ca \leq cb$, felhasználva, hogy P normális halmaz. Ezzel a kompatibilitást is bebizonyítottuk. ■

A részbenrendezett csoportoknak két fontos esete van:

Ha a részbenrendezésre egy hálót kapunk, akkor az axiómák átírhatók azonosságokká, így a *hálószerűen rendezett csoportok* egy varietást alkotnak. Bebizonyítható, hogy ebben az esetben a háló mindig disztributív. A hálószerűen rendezett csoportok fontosságát az adja, hogy a valós függvények a pontonkénti összeadásra egy (kommutatív) hálószerűen rendezett csoportot alkotnak. E csoportban az egyesítés a felső, a metszet az alsó burkoló. Ugyancsak fontos példa egy lineárisan rendezett halmaz rendezéstartó (úgynevezett monoton) permutációinak a csoportja. Ez nem kommutatív, és bizonyítható, hogy minden hálószerűen rendezett csoport beágyazható egy lineárisan rendezett halmaz monoton permutációinak a csoportjába.

A másik fontos eset az, amikor a részbenrendezés lineáris, azaz teljes rendezésről van szó. Ebben az esetben *elrendezett csoportról* beszélünk.

13.4. Tétel. *Egy részbenrendezett csoport rendezése pontosan akkor lineáris, ha pozitív kúpjára* $P \cup P^{-1} = G$ *teljesül.*

Bizonyítás. A linearitás feltétele az, hogy bármely $a, b \in G$ elemre vagy $a \leq b$, vagy $b \leq a$ teljesül. Más szóval vagy $ab^{-1} \in P$, vagy $ba^{-1} \in P$. Ez utóbbi úgy is írható, hogy $ab^{-1} \in P^{-1}$. Tekintettel arra, hogy a csoport minden eleme felírható ilyen alakban, ezért a feltétel valóban azzal ekvivalens, hogy $P \cup P^{-1} = G$. ■

Itt a lényeges kérdés az, hogy értelmezhető-e a csoporton lineáris rendezés:

13.5. Tétel. *Egy kommutatív csoport pontosan akkor elrendezhető, ha torziómentes.*

Bizonyításvázlat. Additív írásmódot fogunk használni. Ha egy $n > 1$ természetes számra és a G csoport egy a elemére $na = 0$, akkor $(n-1)a = -a$. Tekintettel arra, hogy $(n-1)a \in P$ és $-a \in -P$, ezért $a = 0$, hiszen e két halmaznak ez az egyetlen közös eleme.

Ha a csoport torziómentes, akkor meg lehet mutatni, hogy beágyazható a racionális számok additív csoportjának „sok” példányban vett direkt összegébe. Ezek a komponensek mind elrendezhetők (mintha a racionális számok természetes rendezését vennénk), és megmutatható, hogy ez kiterjeszthető a direkt összegre. Ezt az elrendezést az eredeti csoportra megszorítva annak egy lineáris rendezését nyerjük. ■

Részbenrendezett csoportok esetében is beszélhetünk izomorfizmusról. Ez egy olyan bijekció, amely nem csak művelettartó, hanem a relációt is megőrzi (mindkét irányban!).

Feladatok

1. Bizonyítsuk be, hogy az egy elem által generált szabad Abel-csoportnak pontosan kétféle elrendezése van (tehát két különböző pozitív kúp adható meg), amelyek izomorfak.

2. Bizonyítsuk be, hogy a két elemmel generált szabad Abel-csoportnak kontinuumnyi sok(!) különböző elrendezése van, amelyek közt kontinuumnyi sok nem izomorf.

3. „Írjuk le” a két elemmel generált szabad Abel-csoport elrendezéseit.

13.2. Rendezett testek

Sok olyan algebrai struktúra ismert, amelyben a műveleteken kívül bizonyos relációk – leggyakrabban a részbenrendezés – szerepelnek. Erre legismertebb példa a valós számtest vagy annak részgyűrűi. Ilyenek voltak az előző pontban tárgyalt részbenrendezett csoportok. Mint ott is láttuk, a relációk és a műveletek között kell valami kapcsolatnak lenni, hogy ezek egymás struktúráját befolyásolni tudják. Ezek a kapcsolatok a relációknak a műveletekkel való kompatibilitását fejezik ki. A továbbiakban részbenrendezett integritási tartományokkal fogunk foglalkozni. Mint láttuk, ha a struktúrán relációkat is tekintünk, akkor már nem egy halmaz-művelethalmaz párról, hanem egy halmaz-művelethalmaz-relációhalmaz hármasról kell beszélnünk.

Integritási tartományok esetén az alaphalmaz kommutatív csoport, amelyet részbenrendezett csoportnak tekinthetünk. Mindenesetre az összeadás és a szorzás kommutativitása miatt nem kell a „kétoldali” kompatibilitást kikötni. Ezzel szemben egy integritási tartomány a szorzásra nézve nem csoport, amit a „pozitív kúpnak” megfelelő halmaz értelmezésénél kell figyelembe venni.

13.6. Definíció. $\langle R; \{+, \cdot\}, \{\leq\}\rangle$ részbenrendezett integritási tartomány, ha $\langle R; \{+, \cdot\}\rangle$ integritási tartomány, $\langle R; \{\leq\}\rangle$ részbenrendezett halmaz, és érvényesek az alábbi összefüggések:

(1) Ha $a \leq b$, akkor $a + c \leq b + c$.

(2) Ha $a \leq b$ és $0 \leq c$, akkor $ac \leq bc$.

Részbenrendezett integritási tartományban a $P = \{c \mid c > 0\}$ halmazt pozitivitási tartománynak nevezzük. Ha $a \in P$, akkor azt mondjuk, hogy az a elem pozitív. □

Most bebizonyítjuk, hogy a csoportokhoz hasonlóan a részbenrendezés itt is jellemezhető a pozitivitási tartományával.

13.7. Tétel. *Integritási tartomány elemeinek egy P halmaza akkor és csak akkor lesz egy – ezen az integritási tartományon értelmezett – részbenrendezett integritási tartomány pozitivitási tartománya, ha az alábbi három feltétel teljesül:*

(1) $0 \notin P$,

(2) *P zárt az összeadásra,*

(3) *P zárt a szorzásra.*

A pozitivitási tartomány és a részbenrendezés egyértelműen meghatározzák egymást.

Bizonyítás. Tulajdonképpen ez a bizonyítás hasonló a csoport esetéhez, de a pozitivitás eltérő definíciója miatt célszerűbb itt is teljes bizonyítást adni.

A részbenrendezés a pozitivitási tartományt definíció szerint meghatározza. Másrészt, a 13.6. definícióban szereplő meghatározás szerint $a < b$ ekvivalens a $b - a \in P$ feltétellel; amiből következik, hogy a pozitivitási tartomány is egyértelműen meghatározza a részbenrendezést.

Tekintsük most egy részbenrendezett integritási tartomány P pozitivitási tartományát. Az (1) tulajdonság a $<$ reláció irreflexivitása miatt teljesül. A 13.6. definíció (1) pontjából következik, hogy $a, b \in P$ esetén vagy $a + b \in P$, vagy $a + b = 0$ teljesül; felhasználva a reláció tranzitivitását is. Az $a + b = 0$ esetben az $a + b \leq 0$ feltételből azt kapjuk, hogy

$$a = (a + b) - b \leq 0 - b \leq b - b \leq 0 \leq a.$$

A tranzitivitás következtében tehát $a = 0$, és így $a \notin P$.

A 13.6. definíció (2) tulajdonsága alapján $a, b \in P$ esetén vagy $ab \in P$, vagy $ab = 0$ teljesül, ez utóbbi viszont a nullosztómentesség miatt lehetetlen.

Tegyük most fel, hogy az integritási tartománynak egy P részhalmaza rendelkezik a felsorolt három tulajdonsággal. Ennek segítségével – mint láttuk – csak úgy definiálhatjuk a részbenrendezést, hogy $a \leq b$, ha vagy $a = b$, vagy $b - a \in P$. Azt kell tehát megmutatni, hogy így valóban részbenrendezést definiáltunk, ami a műveletekkel is kompatibilis.

A reláció reflexivitása definíció szerint teljesül. A továbbiakhoz tekintsük a $P' = P \cup \{0\}$ halmazt (ez a csoportoknál definiált pozitív kúp). A pozitivitási tartomány (2) és (3) tulajdonsága triviálisan teljesül P'-re is, és nyilvánvaló, hogy $a \leq b$ ekvivalens a $b - a \in P'$ feltétellel.

Ha $a \leq b$ és $b \leq a$, akkor $b - a, a - b \in P'$. Mivel e két elem összege 0, ezért nem lehet mindkettő eleme P-nek; tehát $a = b$. Ha $a \leq b$ és $b \leq c$, akkor $c - a = (c - b) + (b - a) \in P'$, azaz $a \leq c$.

Ha $a \leq b$, akkor $(b + c) - (a + c) = b - a \in P'$ biztosítja az (1) feltételt. Ha $a \leq b$ és $0 \leq c$, akkor $bc - ac = (b - a) \cdot c = (b - a) \cdot (c - 0) \in P'$ biztosítja a második feltételt. ■

Az integritási tartományok esetében is igen fontos speciális eset az, amikor a rendezés lineáris, vagyis bármely két elem összehasonlítható. Az alábbi definíció ezzel nyilvánvalóan ekvivalens.

13.8. Definíció. Egy részbenrendezett integritási tartományt elrendezettnek nevezünk, ha bármely, 0-tól különböző elemre vagy ő, vagy a negatívja benne van a pozitivitási tartományban.

Egy integritási tartományt rendezhetőnek nevezünk, ha van benne fenti tulajdonságú pozitivitási tartomány. □

13.9. Tétel. *Egy integritási tartomány akkor és csak akkor elrendezhető, ha az* $a_1^2 + \dots + a_r^2$ *($a_i \neq 0$) alakú elemeiből álló, úgynevezett pozitív magja nem tartalmazza a* 0*-t.*

Bizonyítás. Tegyük fel, hogy az R integritási tartomány elrendezhető, és legyen P egy megfelelő pozitivitási tartomány. Ha $a \neq 0$, akkor a és $-a$ valamelyike hozzátartozik P-hez, és a szorzásra való zártság miatt P-ben van $a^2 = (-a)^2$ is. Ebből következik, hogy P tartalmazza a pozitív magot – hiszen zárt az összeadásra –, és így 0 nem lehet eleme a pozitív magnak. Ez egyszersmind azt is jelenti, hogy van olyan részbenrendezés, amelynek a pozitivitási tartománya éppen a pozitív mag.

Tegyük most fel, hogy a pozitív mag eleget tesz a kirótt feltételeknek, és tekintsük a pozitív magot tartalmazó pozitivitási tartományokat. Mivel ezek halmaza induktív, ezért alkalmazhatjuk a Zorn-lemmát, tehát van maximális pozitivitási tartomány.

Legyen Q egy maximális pozitivitási tartomány. Tekintsük azt a Q^* halmazt, amely azokból az a elemekből áll, amelyekhez található olyan $p \in Q$, hogy $pa \in Q$. A $pp \in Q$ feltétel miatt $Q \subseteq Q^*$. Ha alkalmas $p, q \in Q$ elemekkel $pa, qb \in Q$, akkor a műveletekre való zártság miatt $pqab = (pa)(qb) \in Q$ és $pq(a+b) = (pa)q + p(qb) \in Q$. Mivel $pq \in Q$, ezért Q^* is zárt a műveletekre. A nullosztómentesség miatt $0 \notin Q^*$, tehát Q^* is pozitivitási tartomány. Q maximalitásából a két pozitivitási tartomány egyenlősége következik. Ez azt jelenti, hogy a felvett maximális pozitivitási tartomány a következő tulajdonságú: ha p, $pa \in Q$, akkor $a \in Q$. (Tehát Q zárt az „osztásra”.)

Azt kell még megmutatni, hogy Q-ra teljesül a 13.8. definícióban megkívánt tulajdonság. Tegyük fel ezért, hogy $a \neq 0$ és $a \notin Q$. Vizsgáljuk a $p+qa$ alakú elemek P halmazát, ahol $p, q \in Q$, de valamelyikük 0 is lehet (mindkettő nem). Világos, hogy ez a halmaz az összeadásra zárt.

Tekintsük most a szorzást: $(p_1+q_1a)\cdot(p_2+q_2a) = (p_1p_2+q_1q_2a^2)+(p_1q_2+q_1p_2)a$. E szorzat is a kívánt alakban van írva – felhasználva, hogy $a^2 \in Q$, hiszen eleve hozzátartozik a pozitív maghoz. Ha itt $p_1p_2 + q_1q_2a^2 = p_1q_2 + q_1p_2 = 0$ volna, akkor a pozitivitási tartomány tulajdonságaiból $p_1p_2 = q_1q_2 = p_1q_2 = q_1p_2 = 0$ következne. Ebből viszont $(p_1+q_1)\cdot(p_2+q_2) = 0$ adódik, ami – ismét a pozitivitási tartomány tulajdonságait figyelembe véve – csak a $p_1 = q_1 = 0$ vagy a $p_2 = q_2 = 0$ esetben volna lehetséges. Ezt az esetet viszont eleve kizártuk.

Tetszőleges $p \in Q$ esetén, ha $pa \in Q$ volna – mint láttuk – $a \in Q$ is teljesülne. Így P valódi módon tartalmazza Q-t. Mivel Q maximális pozitivitási tartomány volt, ezért P nem lehet pozitivitási tartomány.

Tekintettel arra, hogy P az összeadásra és a szorzásra zárt, ezért csak az lehet, hogy a harmadik feltétel nem teljesül rá: tartalmazza 0-t. Így létezik olyan $p, q \in Q$, hogy $p + qa = 0$, azaz $q(-a) = p \in Q$. Ez viszont a Q-ra bizonyított tulajdonság szerint azt jelenti, hogy $-a \in Q$. ■

Ha az integritási tartomány test, akkor a 0-tól különböző elemekre az $a_0^2 + a_1^2 + \dots + a_r^2 = 0$ feltétel ekvivalens az $(a_1/a_0)^2 + \dots + (a_r/a_0)^2 = -1$ feltétellel. Így adódik:

13.10. Következmény. *Kommutatív test akkor és csak akkor elrendezhető, ha formálisan valós.* ■

Megjegyzés. Mivel valósan zárt testben minden elem vagy négyzet, vagy négyzetelem negatívja, ezért valósan zárt testnek egyetlen elrendezése létezik. Ez a tulajdonsága természetesen nem csak a valósan zárt testeknek van meg. □

A továbbiakban az elrendezések bővebb integritási tartományra való kiterjeszthetőségét vizsgáljuk.

Ha $R \leq S$ integritási tartományok, akkor S-nek minden elrendezése természetes módon indukálja R egy elrendezését. Ebben az elrendezésben pontosan azok lesznek az R pozitivitási tartományának az elemei, amelyek S pozitivitási tartományába eső R-beli elemek. Ezt tükrözi a következő:

13.11. Definíció. Legyen R az S integritási tartomány részgyűrűje, P az R egy elrendezéséhez tartozó pozitivitási tartomány. Az S-nek egy elrendezését az R-ben adott elrendezés kiterjesztésének nevezzük, ha a hozzá tartozó Q pozitivitási tartományra $R \cap Q = P$ teljesül. □

13.12. Tétel. *Integritási tartomány bármely elrendezésének pontosan egy kiterjesztése van a hányadostestére.*

Bizonyítás. Tegyük fel, hogy K az R integritási tartomány hányadosteste. Legyen R egy adott elrendezésének pozitivitási tartománya P, és ezen elrendezés kiterjesztésének a pozitivitási tartománya Q. Ha $b \neq 0$, akkor $ab = (ab^{-1})b^2$ és $ab^{-1} = (ab) \cdot (b^{-1})^2$ miatt az $ab \in Q$ és $ab^{-1} \in Q$ feltételek ekvivalensek. Ha most a hányadostest elemeit az integritási tartomány elemeivel írjuk fel, akkor K minden eleme ab^{-1} alakban írható, ahol $a, b \in R$. A kiterjesztés definíciója szerint tehát $ab^{-1} \in Q$ akkor és csak akkor teljesül, ha $ab \in P$. Ez azt jelenti, hogy a kiterjesztés egyértelmű.

Ha tehát létezik az elrendezésnek kiterjesztése, akkor a megfelelő pozitivitási tartományt azzal definiálhatjuk csak, hogy $ab^{-1} \in Q$ pontosan akkor teljesüljön, ha $ab \in P$. Először is meg kell mutatni, hogy így valóban pozitivitási tartományt nyerünk. $ab^{-1} = 0$ csak akkor lehet, ha $a = 0$, és így $0 \notin P$. Ha $ab^{-1}, cd^{-1} \in Q$, akkor $ab, cd \in P$. A pozitivitási tartomány tulajdonságait felhasználva: $(ac) \cdot (bd) = (ab) \cdot (cd) \in P$ és $(ad + bc) \cdot (bd) = (ab) \cdot d^2 + (cd) \cdot b^2 \in P$; amiből adódik Q-nak a műveletekre való zártsága. Ha $ab^{-1} \in Q \cap R$, akkor $(ab^{-1}) \cdot b^2 = ab \in P$. Mivel $b^2 \in P$ és P maximális pozitivitási tartomány R-ben, ezért $ab^{-1} \in P$, mint ahogy azt a 13.9. tétel bizonyításánál láttuk. ■

Megjegyzés. Az egész számok közül éppen a pozitívak az elemei a pozitív magnak. Ebből következik, hogy az egész számokat csak egyféleképpen lehet elrendezni. A 13.12. tétel alapján így a racionális számoknak is csak egyetlen elrendezése van. □

Elrendezett testek esetében beszélhetünk egy elem abszolút értékéről: *elrendezett test a elemének abszolút értéke a, ha eleme a pozitivitási tartománynak, és $-a$, ha a nem eleme a pozitivitási tartománynak.*

Az abszolút értékre könnyen bizonyíthatók a valós számok esetében ismert egyenlőtlenségek és egyenlőségek. Ennek általánosítását adjuk:

13.13. Definíció. Egy K test értékelésének nevezünk egy $\varphi : K \to L$ leképezést az L rendezett testbe, ha φ az alábbi tulajdonságú:

(1) $\varphi(0) = 0$; és ha $a \neq 0$, akkor $\varphi(a) > 0$.

(2) $\varphi(a + b) \leq \varphi(a) + \varphi(b)$.

(3) $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

Az értékelésre az abszolút értékkel való értékelésen kívül igen fontos példa az alábbi:

Tekintsünk egy R integritási tartományt, és abban egy olyan, 0-tól különböző P prímideált, amelyre a P hatványainak a 0-n kívül nincs közös elemük. Az R integritási tartomány K hányadostestének egy elemét írjuk fel a/b alakban, ahol $a, b \in R$. A P-re vonatkozó feltétel szerint létezik olyan egyértelműen meghatározott n és k természetes szám, hogy $a \in P^n \setminus P^{n+1}$ és $b \in P^k \setminus P^{k+1}$. Ha R-ben érvényes az egyértelmű prímtényezős felbontás, akkor könnyen belátható, hogy a $t = k - n$ szám csak az a/b-től függ. Ezek után legyen $\varphi(a/b) = \alpha^t$, ahol α rögzített, 1-nél nagyobb valós szám. Az így definiált függvényről belátható, hogy értékelés.

A most megadott példának két fontos speciális esete van. Az egyik, amikor a racionális számtestet – vagy ennek egy véges algebrai bővítését – értékeljük a fenti módon. A kapott, úgynevezett p-adikus értékelés (illetve annak – később tárgyalandó – perfekt lezártja) igen fontos szerepet játszik az algebrai számelméletben.

A (komplex) testbeli egyhatározatlanú polinomok esete pedig az algebrai geometriában jelent komoly segédeszközt.

A továbbiakban olyan általános eljárást vázolunk, amely speciális esetként megadja, miképpen konstruálhatók meg a valós számok a racionális számtest ismeretében.

Tetszőleges K test esetében a testbeli sorozatok $\mathcal{S}$ halmaza tekinthető a K direkt hatványának (megszámlálható sok példányban véve a K testet, és az indexezést a természetes számokkal végezve). Így a direkt szorzaton értelmezett műveletekre $\mathcal{S}$ gyűrű. Az $\mathbf{a} = (a_1, \ldots, a_n, \ldots)$ sorozat n-edik elemének nevezzük az a_n elemet, és a sorozat n-edik szeletének az $\mathbf{a}_n = (a_n, a_{n+l}, \ldots)$ sorozatot.

Tegyük most fel, hogy a K test értékelt; és $\varphi : K \to L$ az értékelésben szereplő függvény (ha $K = L$ a valós számtest, akkor φ minden számhoz az abszolút értéket rendeli hozzá). Egy sorozatot korlátosnak nevezünk, ha elemei értékeinek halmaza L-ben felülről korlátos (azaz létezik olyan $\alpha \in L$, hogy a sorozat minden a_n elemére $\varphi(a_n) < \alpha$). Jelölje $\mathcal{K}$ a korlátos sorozatok halmazát. Egy sorozatot alapsorozatnak nevezünk, ha a következő teljesül rá: Az L bármely $\varepsilon > 0$ eleméhez van a sorozatnak olyan szelete, hogy a szelet bármely a_i, a_j elemeire $\varphi(a_i - a_j) < \varepsilon$. Jelölje $\mathcal{A}$ az alapsorozatok halmazát. Egy sorozatot konvergensnek nevezünk, ha található hozzá egy $a \in K$ úgy, hogy az L minden $\varepsilon > 0$ eleméhez van a sorozatnak olyan szelete, amelynek bármely a_i elemére $\varphi(a_i - a) < \varepsilon$. Ekkor azt mondjuk, hogy a e sorozat limesze. Jelöljük $\mathcal{C}$-vel a konvergens sorozatok halmazát. Azon sorozatok (a nullasorozatok) halmazát, amelyeknek a limesze 0, $\mathcal{N}$-nel fogjuk jelölni. Jelöljük végül $\mathcal{I}$-vel azoknak a sorozatoknak (zérussorozatok) a halmazát, amelyeknek van olyan szeletük, hogy a szelet minden eleme 0.

Bebizonyítható, hogy $\mathcal{I} \leq \mathcal{N} \leq \mathcal{C} \leq \mathcal{A} \leq \mathcal{K} \leq \mathcal{S}$ részgyűrűk, továbbá $\mathcal{I}$ ideálja $\mathcal{S}$-nek és $\mathcal{N}$ ideálja $\mathcal{K}$-nak. A továbbiakban a $\mathcal{I}$ szerinti maradékosztály-gyűrűre térünk rá – azaz nem teszünk különbséget két sorozat között, ha azok véges sok helytől eltekintve megegyeznek. A most definiált részgyűrűk képeire nem vezetünk be új jelölést: ez nem okoz zavart. Kimutatható, hogy az $\mathcal{A} \setminus \mathcal{N}$ elemeinek alsó korlátja is van, azaz bármely ilyen sorozathoz létezik olyan $\eta > 0$ L-beli elem, hogy a sorozat bármely (elég nagy indexű) a_n elemére $\varphi(a_n) > \eta$ is igaz. Ennek következménye az, hogy ilyen sorozatoknak van az $\mathcal{A}$-ban inverzük. Ezt felhasználva bebizonyítható, hogy az $\mathcal{A}/\mathcal{N}$ maradékosztálygyűrű mindig test. E testbe beágyazható az eredeti test a következőképpen: Minden K-beli a elemhez hozzárendeljük azt az $\mathbf{a}$ sorozatot, amelynek minden eleme a. A kapott testet az eredeti K test $\overline{K}$ perfekt lezártjának nevezzük. A $\varphi : K \to L$ értékelés egyértelműen kiterjeszthető egy $\overline{\varphi} : \overline{K} \to \overline{L}$ értékeléssé. Ebben az új értékelésben a $\mathcal{A}$-beli sorozatoknak

létezik limesze, és ezek az elemek éppen kiadják $\overline{K}$ összes elemét. Sőt, a K elemeire is elvégezhető az eredeti konstrukció, amelynek során azt kapjuk, hogy minden alapsorozat konvergens. Felhívjuk a figyelmet arra, hogy az értékelés az $\overline{L}$ testre képez le. Ez az L-nek perfekt lezártja az abszolút értékre mint értékelésre nézve. A konstrukció, illetve $\overline{\varphi}$ értelmezéséhez be kell tehát először látni, hogy az abszolút értékkel való értékeléskor a kapott test is elrendezett, és az elrendezés az eredetinek a folytatása. Ez könnyen belátható, annak a felhasználásával, hogy $\mathcal{A} \setminus \mathcal{N}$ elemei alulról korlátosak.

13.14. Definíció. Egy R integritási tartomány elrendezése archimedesi, ha bármely a és b pozitív elemeihez van olyan n természetes szám, hogy $n \cdot a > b$.

Ha ilyen n nincs, akkor azt mondjuk, hogy b végtelenszer nagyobb, mint a, illetve a végtelenszer kisebb, mint b. Ezt a relációt $a \ll b$, illetve $b \gg a$ jelöli. □

A racionális vagy a valós számtest szokásos elrendezése archimedesi. A valós számok racionális számok segítségével való egyik legfontosabb konstrukciója a Dedekind-szeletekkel történik. (A másik a fent vázolt teljessé tétel.) Erre az ad módot, hogy a racionális számok közötti „hézagokba" pontosan egy új szám fér bele. Ennek az az oka, hogy az adott elrendezés archimedesi. Egyébként a „szeletalkotási" módszer nem működik. Ugyanis az elrendezésben „túl nagy hézagok vannak". Ebben az esetben csak az itt közölt módszerrel tehető a test teljessé. Megjegyezzük viszont, hogy a nagy hézagokba a „konvergens" sorozatok egyáltalán nem tudnak „belépni". Tekintsük példaként a racionális együtthatós polinomokat (a határozatlan x) azzal az elrendezéssel, hogy a pozitivitási tartomány elemei a pozitív főegyütthatós polinomok. Ez az elrendezés nem archimedesi, mert $n \cdot 1 > x$ soha nem teljesül; x „végtelen nagy". Itt egy törtkifejezés akkor lesz végtelen nagy, ha a számláló foka nagyobb, mint a nevezőé. A természetes számok és a legalább elsőfokú kifejezések között egy nagy hézag van. Ha α ebbe a hézagba esik, akkor $\alpha - 1$ is és $\alpha + 1$ is ebbe a hézagba esik. De teljessé tett testbe nem kerül bele például a $\sqrt{2}$ sem! Ennek oka az, hogy $1/x$ „végtelen kicsi", de pozitív: ha az r racionális számra $r^2 < 2$, akkor $r^2 < 2 - 1/x$. Megmutatható, hogy archimedesien elrendezett test izomorf a valós számtest egy résztestével.

Az említett p-adikus értékelés az egész számok esetében a következőket adja. Bármely (nem-0) r racionális szám (lényegében) egyértelműen felírható $\frac{a}{b} \cdot p^i$ alakban, ahol p relatív prím a-hoz és b-hez, és i egész szám. Ekkor $\varphi(r) = \alpha^{-i}$. Itt az a szokás, hogy α-t p-nek választják. Ekkor az értékelés definíciójában szereplő (2) egyenlőtlenségnél erősebb $\varphi(a + b) \leq \max(\varphi(a), \varphi(b))$ teljesül.

13.15. Definíció. Egy integritási tartomány φ értékelése nemarchimedesi, ha a (2) egyenlőtlenségben $\varphi(a + b) \leq \max(\varphi(a), \varphi(b))$ teljesül. □

Ilyenkor a φ-nél kapott p^{-i} helyett szokásos az i-t tekinteni és *kitevőértékelésről* beszélni. Erre a w „értékfüggvényre" a következő „axiómák" írhatók fel:

$$w(a + b) \geq \min(w(a) + w(b)) \qquad \text{és} \qquad w(ab) = w(a) + w(b).$$

Ez lehetőséget ad arra, hogy az értékeket egy tetszőleges elrendezett Abel-csoportból vegyük. Ilyen módon lehet például olyan „polinomokat" konstruálni, amelyekben az x határozatlan kitevői tetszőleges valós számok.

Feladatok

1. Bizonyítsuk be, hogy ha egy test elrendezése nem archimedesi, akkor minden pozitív a-hoz van olyan pozitív b és c, amelyekre $b \ll a \ll c$.

2. Bizonyítsuk be, hogy ha egy test elrendezése nem archimedesi, akkor minden pozitív $a \ll \ll b$-hez van olyan c, amelyre $a \ll c \ll b$.

3. Bizonyítsuk be, hogy a $\mathbb{Q}[x_1, x_2, \ldots]$ polinomgyűrűnek van olyan elrendezése, amelyben $x_i \ll x_j$, ha $i < 2$. Mutassuk meg, hogy ez akkor is igaz, ha az indexek a rendszámokon futnak végig.

4. Egy elrendezett test $(a_1, \ldots, a_n \ldots)$ sorozatát stacionáriusnak nevezzük, ha létezik olyan $N \in \mathbb{N}$ szám, hogy $i, j > N$ esetén $a_i = a_j$. Mutassuk meg, hogy minden stacionárius sorozat konvergens (tehát eleve alapsorozat).

5. Adjunk meg olyan elrendezett testet, amelyben minden alapsorozat stacionárius.

6. A racionális számok $\mathbb{Q}$ testében p-adikus kitevőértékelésnek nevezzük a következőt: Ha $a = b \cdot p^i$, egy p-hez relatív prím számlálójú és nevezőjű b-vel, akkor legyen $w_p(a) = i$. Bizonyítsuk be, hogy az ezen értékelés mellett kapott $\mathcal{Q}_p$ perfekt lezárt minden eleme egyértelműen felírható:

$$\alpha = a_{-k} p^{-k} + \cdots + a_{-1} p^{-1} + a_0 + a_1 p + \cdots + a_n p^n + \cdots$$

alakban, ahol az a_i együtthatókra $0 \leq a_i < p$ teljesül.

7. Bizonyítsuk be, hogy $\mathcal{Q}_p$-ben a felírt α elemre $w(\alpha) = -p$. Mutassuk meg, hogy azok a β elemek, amelyekre $w(\beta) \geq 0$, egy $\mathcal{R}_p$ (értékelésgyűrűnek nevezett) gyűrűt alkotnak, amelynek $\mathcal{Q}_p$ a hányadosteste. (Itt az értékelésgyűrű elemeit szokás egészeknek nevezni.) Mutassuk meg, hogy azok a γ elemek, amelyekre $w(\gamma) > 0$ egy $\mathcal{P}_p$ prímideált alkotnak (értékelésideál). Mutassuk meg, hogy $\mathcal{R}_p$ lokális gyűrű, és benne az ideálok láncot alkotnak.

8. Rögzített p esetén „keressük meg” $\mathcal{Q}_p$-ben a negatív egész számokat és a p-hez relatív prím nevezőjű törteket. Mutassuk meg, hogy ezek „egészek” (elemei $\mathcal{R}_p$-nek).

9. Mutassuk meg, hogy $\mathcal{Q}_p$ nem algebrailag zárt és nem is valósan zárt.

10. Milyen p prímszámokra létezik $\mathcal{Q}_p$-ben az $x^2 + 1$ polinomnak gyöke?

11. Írjuk fel a $\mathbb{Q}(x)$ test elemeit $r(x) = \dfrac{p}{q} \times x^i$ alakban, ahol sem p, sem q konstans tagja nem 0. Mutassuk meg, hogy $w(r(x)) = i$ kitevőértékelés. Mi az értékelésgyűrű, mi az értékelésideál? Bizonyítsuk be, hogy ez a test „megegyezik” a hatványsorokéval (de itt nem lehet behelyettesíteni!). Bizonyítsuk be, hogy a „deriválási szabályok” átvihetők. (Ezért lehet ennek a gyűrűnek az elemeit „generátorfüggvényekként” használni; anélkül, hogy a konvergenciakérdéseket vizsgálnánk.)

14. Relációalgebrák, algebrai logika

14.1. Relációalgebrák

Az eddigiekben két módon is kapcsolódtak relációk egy-egy algebrai struktúrához. Az egyik esetben – a hálók esetében – a műveleteket definiáltuk a relációk segítségével; a másik esetben a műveleteken kívül még újabb reláció is szerepelt, amely a műveletekkel kompatibilis volt. Megemlítjük, hogy van még egy igen fontos harmadik lehetőség is: Egy algebrai struktúrában mind a műveletek, mind a teljesülő azonosságok kifejezhetők relációk segítségével. Például minden kétváltozós f művelethez hozzárendelhetünk egy háromváltozós F relációt, amelyre $F(a, b, c)$ pontosan akkor igaz, ha $f(a, b) = c$. A g kétváltozós művelet kommutativitását egy G kétváltozós reláció fejezheti ki, amelyre $G(a, b)$ igazsága a $g(a, b) = g(b, a)$ teljesülését jelenti. A továbbiakban olyan algebrákat – úgynevezett relációalgebrákat – vizsgálunk, amelyekben műveletek is és relációk is szerepelnek. Ezek fontos szerepet játszanak az algebrai logikában is.

Az *algebrai logika* tárgya a matematikai logikában fellépő műveletek vizsgálata. Ilyen műveletek például az „és”, a „vagy”, a „nem”, a „következik”, az „igaz”, stb. Ezekkel úgynevezett „ítéleteket” kötünk össze, s ezek igazságát vizsgáljuk. Az alapítéletek között relációk igazsága is szerepel; ezért foglalkozunk a relációalgebrákkal. Mindenekelőtt pontosan definiáljuk ezt a fogalmat.

14.1. Definíció. Relációalgebrán egy $\mathfrak{A} = \langle A; F; R\rangle$ hármast értünk, ahol $\langle A; F\rangle$ általános (univerzális) algebra (a relációalgebra tartó univerzális algebrája) és R minden egyes eleme egy $\varrho : A^n \to \{0, 1\}$, úgynevezett n-változós reláció, ahol n pozitív egész. Ha ϱ az A^n egy elemét 1-re képezi, akkor azt mondjuk, hogy erre az elemre a reláció teljesül (vagy igaz), ha 0-ra képezi, akkor a reláció nem teljesül (vagy hamis).

Relációalgebra típusát az algebra típusához hasonlóan értelmezzük. Itt azonban két függvény van: τ, ami a műveleti nevek halmazát képezi a természetes számok halmazába és σ, amely a relációnevekét. A műveleti nevek realizációjával analóg módon értelmezzük a relációnevek realizációját egy adott struktúrában. □

Az alapvető algebrai fogalmakat a relációalgebrák körében is értelmezhetjük.

14.2. Definíció. Legyenek $\mathfrak{A} = \langle A; F; G\rangle$ és $\mathfrak{A}' = \langle A'; F'; G'\rangle$ azonos típusú relációalgebrák. $\varphi : \mathfrak{A} \to \mathfrak{A}'$ homomorfizmus, ha $\varphi : \langle A; F\rangle \to \langle A'; F'\rangle$ algebrahomomorfizmus és $\varrho \in F$, $\varrho' \in F'$ azonos nevű, n-változós relációkra $\varrho(a_1, \ldots, a_n) = 1$ esetén $\varrho'(\varphi(a_1), \ldots$ $\ldots, \varphi(a_n)) = 1$ is teljesül. φ akkor és csak akkor injektív, szürjektív, illetve bijektív, ha az algebrára megszorítva is ilyen tulajdonságú. □

Megjegyzés. A homomorfizmusnál csak azt kívántuk meg, hogy a reláció teljesülését tartsa meg. A relációalgebrában a reláció nem teljesülését nem kell megtartani (ez algebrák esetében is így volt definiálva). Ennek következtében egy bijektív homomorfizmus nem feltétlenül izomorfizmus. Lehet ugyanis, hogy az $\mathfrak{A}$ algebrán egy kétváltozós reláció van értelmezve, s az $\mathfrak{A}'$ algebra is ugyanaz, csak több elemáron lesz a reláció értéke 1. Minden elemnek önmagát megfeleltetve homomorfizmust kapunk, amely nyilvánvalóan bijektív, de nem invertálható. □

Mivel a homomorfizmusnál új elemrendszerek is relációban lehetnek, ezért vigyázni kell a részalgebra és faktoralgebra (vagy homomorf kép) definíciójánál is. A részalgebránál

meg kell kívánni, hogy minden relációban legyen, ami relációban lehet, a faktornál pedig azt, hogy csak az legyen relációban, aminek relációban kell lennie:

14.3. Definíció. Egy relációalgebra részalgebráját olyan részalgebraként definiáljuk, amelyen minden reláció ugyanazt az értéket veszi fel, mint az eredeti algebrában. Az $\mathfrak{A}$ relációalgebrának a $\mathfrak{B}$ relációalgebra faktoralgebrája, ha mint algebra faktoralgebrája, és pontosan akkor van a $(b_1, \ldots, b_n) \in B^n$ elem ϱ' (faktor)relációban, ha van A^n-nek olyan ϱ relációban levő $(a_1, \ldots, a_n)$ eleme, amelyet a homomorfizmrus $(b_1, \ldots, b_n)$-re képez le.

Relációalgebrák direkt szorzatát algebrák direkt szorzataként értelmezzük; egy reláció akkor és csak akkor teljesül egy vektorrendszerre, ha a megfelelő reláció minden egyes faktorban teljesül a vektorrendszer megfelelő komponenseire. □

Itt is igen fontos szerepet töltenek be az „abszolút” szabadon megkonstruált algebrák. Ezeknek az elemei itt nem kifejezések, hanem formulák vagy állítások. Például egy ilyen formula a következő: „vagy $x < y$, vagy ($u = v+pq$ és $p = v-t$)”. Egy ilyen formuláról két dolgot szükséges megállapítani. Először is azt, hogy milyen az alakja: az algebra műveleteiből, relációiból, egyenlőségeiből és logikai műveletekből van-e előállítva. A másik dolog az, hogy a betűk bizonyos értékeire a felírt formula igaz is lehet, más értékeire viszont nem biztos, hogy igaz. Még pontosabban megfogalmazva, az is lehet, hogy bizonyos elemek értékét bárhogyan megadhatjuk, de ezután a formula csak akkor lesz igaz, ha a többi betűk helyébe valamilyen – a megadottaktól függő – elemet teszünk. Ezeket szemünk előtt tartva adjuk az alábbi definíciókat.

14.4. Definíció. Legyen $\tau : F \to \mathbb{N}$ egy művelettípus és $\sigma : G \to \mathbb{N}$ egy relációtípus; továbbá $\mathfrak{A}$ egy (τ, σ) típusú relációalgebra. Legyen adott ezen felül egy speciális **e** binér relációtípus.

Készítsük el ezután az alábbi formális (szabad félcsoportokkal precízen definiálható) kifejezéseket: $\mathbf{r}(a_1, \ldots, a_n)$, ahol **r** egy n-változós eleme G-nek és $\mathbf{e}(a, b)$; itt $a, b, a_1, \ldots$ $\ldots, a_n \in \mathfrak{A}$. Ezeket az elemeket $\mathfrak{A}$-beli elemi ítéleteknek nevezzük. Tekintsük az $\mathfrak{A}$-beli elemi ítéletek generálta szabad Boole-hálót; ezt az $\mathfrak{A}$-beli ítéletek halmazának nevezzük.

Az $\mathfrak{A}$-beli ítéletek kiértékelésének nevezzük az $\mathfrak{A}$-beli ítéleteknek a kételemű Boole-hálóba való homomorfizmusát, ha e homomorfizmusnál $\mathbf{r}(a_1, \ldots, a_n)$ képe $\varrho(a_1, \ldots, a_n)$, ahol ϱ az **r**-nek $\mathfrak{A}$-beli realizációja, továbbá $\mathbf{e}(a, b)$ realizációjának a képe pontosan akkor 1, ha $a = b$.

Egy konkrét ítélet kiértékelésén ezen ítéletnek az adott kiértékeléskor vett képét értjük. □

Megjegyzés. Ez a definíció lehetővé teszi, hogy az $\mathfrak{A}$-beli ítéleteket formálisan kezeljük. Világos, hogy az 1-nek az „azonosan igaz” állítás, a 0-nak az „azonosan hamis” állítás felel meg. Az egyesítésnek megfelelő művelet a logikai „vagy”, a metszetnek megfelelő művelet a logikai „és”, a komplementernek megfelelő művelet pedig a logikai „nem”. Végül az **e** relációnak megfelelő állítás az egyenlőség. □

A (logikai) formulák tárgyalása előtt célszerű végiggondolni az algebrai formulákat; például a test feletti polinomokat.

A legformálisabb az általános polinom: $x^2 + y_1 \cdot x + y_0$ általános másodfokú polinom, ha x, y_1, y_0 határozatlanok, és $^2, +, \cdot$ jelentés nélküli jelek. Itt még azt sem mondjuk meg, hogy milyen test feletti polinomokról beszélünk. A kifejezés csak akkor válik „értelmessé”, ha a határozatlanok helyébe egy konkrét test elemeit és a műveleti jelek helyébe az adott test megfelelő műveleteit írjuk.

A következő fokozatban már megadjuk a vizsgált testet: $x^2 + a_1 \cdot x + a_0$, ahol a_1, a_0 az adott test elemei, x határozatlan. $^2, +, \cdot$ most is jelentés nélküli jelek, hiszen a határozatlanokkal és a test elemeivel nem végezhetünk műveleteket. Itt is csak behelyettesítés után értelmezhető a kifejezés. Úgy tekinthetjük, mintha a_1 és a_0 is határozatlanok volnának; de a behelyettesítésnél csak az „előírt" értéket helyettesíthetjük be. Ezt célszerű annyira mereven követni, hogy a $(2 + 3) \cdot x$ és $5 \cdot x$ kifejezéseket se tekintsük egyenlőknek. Ebben az esetben a fellépő struktúrabeli elemeket (ez jelen esetben a_1 és a_0) *paramétereknek* vagy *konstansoknak* nevezik.

Végezetül lehet, hogy egyáltalán nem szerepel határozatlan, a kifejezés: $c^2 + a_1 \cdot c + a_0$, ahol c, a_1, a_0 a test elemei, és a műveleti jelek a testben értelmezett műveleteket jelentik. Persze ez a kifejezés – látszatra – nem különbözik az elsőtől, de itt a test konkrét elemeiről van szó; még akkor is, ha „nem árultuk el", hogy melyekről. Mindenesetre itt a műveletek értelemmel bírnak és elvégezhetők. Az előző két esethez képest ez a lényeges különbség. Azokban csak egy *kifejezés* szerepel.

14.5. Definíció. Legyen $\mathbf{X}$ határozatlanok egy halmaza, $\tau : F \to \mathbb{N}$ és $\sigma : G \to$ $\to \mathbb{N}$ adott művelet-, illetve relációtípus. Az $\mathbf{X}$ generálta τ, σ típusú $\mathfrak{F}$ kifejezésalgebrára vonatkozó (elemi) ítéleteket (elemi) formuláknak nevezzük.

Legyen $\mathfrak{A}$ egy ugyanilyen típusú A alaphalmazú relációalgebra és tekintsük határozatlanoknak az $A \cup \mathbf{X}$ halmazt. Az ezáltal generált $\mathfrak{F}_{\mathfrak{A}}$ kifejezésalgebrára vonatkozó (elemi) ítéleteket ugyancsak (elemi) formuláknak nevezzük, amelyekben A elemei konstansok. □

14.6. Tétel. *Az $\mathfrak{F}_{\mathfrak{A}}$-beli határozatlanoknak az $\mathfrak{A}$ algebrába való tetszőleges leképezése – amelynél a konstansoknak önmaguk felelnek meg – egyértelműen indukálja a formuláknak az algebrabeli ítéletekre való művelettartó leképezését. Ezt a leképezést a formulák algebrában való realizációjának nevezzük.*

Bizonyítás. Legyen $\varphi : X \to A$ az $\mathfrak{A}$ algebra tartóhalmazába való tetszőleges leképezés. Tekintettel arra, hogy a kifejezésalgebra szabad, ennek létezik a kifejezésalgebrára való egyértelmű homomorfizmus-kiterjesztése. Jelöljük ezt is φ-vel. A φ-t egyértelműen kiterjeszthetjük az elemi formulákra a következőképpen. Ha $\mathbf{r}(\mathbf{u}_1, \ldots, \mathbf{u}_n)$ elemi formula, akkor megfeleltetjük neki az $\mathbf{r}(\varphi(\mathbf{u}_1), \ldots, \varphi(\mathbf{u}_n))$ ítéletet. Mivel az elemi formulák a formuláknak mint Boole-hálónak a szabad generátorhalmazát alkotják, ezért ez a megfeleltetés egyértelműen kiterjeszthető. ■

14.7. Definíció. A 14.5.-ben definiált formulákat nyílt formuláknak nevezzük. Legyen $\Phi = \Phi(\mathbf{x}_1, \ldots, \mathbf{x}_n, a_1, \ldots, a_k)$ egy nyílt formula, amelyben $\mathbf{x}_1, \ldots, \mathbf{x}_n$ határozatlanok és $a_1, \ldots, a_k$ (esetleges) paraméterek egy $\mathfrak{A}$ algebrából. Ha a Φ nyílt formulában az $\mathbf{x}_1, \ldots$ $\ldots, \mathbf{x}_n$ határozatlanok ($\mathbf{X}$-beli elemek) szerepelnek, akkor azt mondjuk, hogy ezek szabad változók vagy kötetlenek. Rekurzívan definiáljuk a kötött változókat. Ha a Φ formulában az $\mathbf{x}_1, \ldots, \mathbf{x}_r$ szabad változók és $\mathbf{y}_1, \ldots, \mathbf{y}_s$ kötött változók, akkor a

$$(\forall \mathbf{x}_r)\Phi \qquad \text{és a} \qquad (\exists \mathbf{x}_r)\Phi$$

is formula, és e formulában $\mathbf{x}_1, \ldots, \mathbf{x}_{r-1}$ szabad vátozók és $\mathbf{x}_r, \mathbf{y}_1, \ldots, \mathbf{y}_s$ kötött változók. A $(\forall \mathbf{x})$ alakú esetben $\mathbf{x}$ univerzálisan kötött, a $\exists \mathbf{x}$ alakú esetben $\mathbf{x}$ egzisztenciálisan kötött változó.

Ha egy formulában nincsenek szabad változók, akkor zárt formuláról beszélünk.

Azt, hogy egy $\Phi = \Phi(\mathbf{x}_1, \ldots, \mathbf{x}_n, a_1, \ldots, a_k)$ zárt formula, ahol $\mathbf{x}_1, \ldots, \mathbf{x}_n$ (kötött vagy szabad) határozatlanok és $a_1, \ldots, a_k \in \mathfrak{A}$ mikor igaz $\mathfrak{A}$-ban, a változók számára való rekurzióval definiáljuk.

$n = 0$ esetén Φ igaz, ha az „identikus realizáció” esetén Φ kiértékelése 1.

Tegyük fel, hogy minden olyan formulára definiáltuk, hogy mikor igaz $\mathfrak{A}$-ban, amelyben a fellépő határozatlanok száma kevesebb, mint n.

A $\Phi = (\forall \mathbf{x})\Psi$ alakú formula akkor igaz $\mathfrak{A}$-ban, ha bármely $a \in \mathfrak{A}$ esetén az $\mathbf{x} \mapsto a \in \in \mathfrak{A}$ homomorfizmusnál a kapott $\Psi \mapsto \Psi_a$ formula (amelyben $\mathbf{x}$ már nem szerepel) igaz $\mathfrak{A}$-ban.

A $\Phi = (\exists \mathbf{x})\Psi$ alakú formula akkor igaz $\mathfrak{A}$-ban, ha van olyan $a \in \mathfrak{A}$, amelyre az $\mathbf{x} \mapsto a \in \mathfrak{A}$ homomorfizmusnál a kapott $\Psi \mapsto \Psi_a$ formula (amelyben $\mathbf{x}$ már nem szerepel) igaz $\mathfrak{A}$-ban. □

Megjegyzések. 1. A $(\forall \mathbf{x})$ úgy olvasandó, hogy minden $\mathbf{x}$-re, a $(\exists \mathbf{x})$ úgy, hogy van olyan $\mathbf{x}$, amire.

2. A $(\forall \mathbf{x})\Phi$ és $(\exists \mathbf{x})\Phi$ akkor is megengedett, ha $\mathbf{x}$ nem szerepel Φ-ben.

3. A zárt formulák „igazsága” nem őrződik meg a legfontosabb algebrai operációk esetében. Létezik olyan zárt formula, amely egy algebrában teljesül, de ennek alkalmas részalgebrájában nem, olyan zárt formula is, amely egy algebrában teljesül, de alkalmas faktorában nem, és olyan is, amely bizonyos algebrákban igaz, de nem igaz ezek direkt szorzatában. □

A következő részben egy olyan algebrai (vagy logikai) konstrukciót mutatunk be, amely a zárt formulák igazságtartalmát megőrzi. Ennek a konstrukciónak éppen ezért igen fontos szerepe van a matematikai logikában és a modellelméletben.

14.2. 0–1 mérték, ultraszorzat (prímszorzat)

Mértéken általában olyan függvényt szoktak érteni, hogy egy adott halmaz bizonyos részhalmazaihoz valamilyen mérőszámot rendelünk hozzá; amelyik halmazhoz nagyobb szám van hozzárendelve, az „bizonyos értelemben” nagyobb. A mértékre néhány természetes axiómát is fel kell tenni – például azt, hogy részhalmaznak nem lehet nagyobb a mértéke, mint az egész halmaznak. Olyan speciális mértéket vezetünk be, amely vagy 0-t, vagy 1-et vesz fel, és a vizsgált halmaz bármely részhalmazának van mértéke. Mint érdektelent, eleve kizárjuk azt az esetet, amikor minden részhalmaz mértéke megegyezik.

14.8. Definíció. Tetszőleges H nemüres halmaz esetén a $P(H)$ hatványhalmaznak mint a tartalmazásra vett disztributív hálónak a kételemű disztributív hálóba való szürjektív homomorfizmusát 0–1 mértéknek nevezzük. □

14.9. Tétel. *Egy H nemüres halmazon értelmezett mérték ekvivalens egy olyan $\mu : P(H) \to \{0, 1\}$ függvény megadásával, amely a következő tulajdonságú:*

(1) *Minden részhalmaz mértéke vagy* 0, *vagy* 1.

(2) *Az üres halmaz mértéke* 0, *az egész halmazé* 1.

(3) *Két halmaz metszetének a mértéke a mértékek minimuma, az egyesítésük mértéke a mértékeik maximuma.*

Bizonyítás. Azonnal következik a 12.15. tétel (4) és (6) állításának az ekvivalenciájából. ■

14.10. Tétel. *A H halmaz tetszőleges h eleméhez létezik egy $\mu : P(H) \to \{0, 1\}$ mérték, amely pontosan azokhoz a részhalmazokhoz rendeli az 1-et, amelyek a h elemet tartalmazzák. Az ilyen mértékeket triviális mértékeknek nevezzük.*

Bizonyítás. A 14.9. tételben megadott feltételek mindegyike triviálisan teljesül. ■

14.11. Tétel. *Ha $\mu : P(H) \to \{0, 1\}$ a H halmazon értelmezett nemtriviális mérték, akkor e mértéknél minden véges halmaz 0-ra képeződik. Ha H végtelen, létezik rajta nemtriviális mérték.*

Bizonyítás. Tegyük fel, hogy a μ mérték a H egy véges részhalmazát 1-be viszi. Ekkor nyilván van egy minimális elemszámú B részhalmaz, amelynek a mértéke ugyancsak 1. Legyen B a C és D diszjunkt részhalmazok egyesítése, és tegyük fel, hogy $C \neq B$. Ebből azt kapjuk, hogy $\mu(C) = 0$ és $\mu(D) = 1$. Így csak $D = B$ lehet, ami azt jelenti, hogy $B = \{b\}$. Ebből következik, hogy a b-t tartalmazó bármelyik halmaznak a mértéke 1, és így a b-t nem tartalmazó halmazok mértéke csak 0 lehet, mert minden ilyen halmaz komplementere egy b-t tartalmazónak, és komplementerek mértéke nyilván különböző.

Tegyük most fel, hogy H végtelen. $P(H)$-ban a H véges részhalmazai nyilvánvalóan ideált alkotnak. Ez az ideál nem tartalmazza H-t, amely egymagában a $P(H)$-nak duális ideálja. Így létezik olyan prímideál, amely elválasztja ezeket; és ez éppen egy alkalmas 0–1 mérték létezését bizonyítja. ■

Alapvető az alábbi tételben szereplő, Łos által bevezetett fogalom és az általa bizonyított 14.14. tétel.

14.12. Tétel. *Legyen $\{\mathfrak{A}_\lambda \mid \lambda \in \Lambda\}$ azonos típusú relációalgebrák halmaza és μ egy 0–1 mérték a Λ halmazon. Legyen $\mathfrak{A}$ a fenti algebrák direkt szorzata a $\pi_\lambda : \mathfrak{A} \to \mathfrak{A}_\lambda$ projekciókkal. Az $\widetilde{\mathbf{a}}, \widetilde{\mathbf{b}} \in \mathfrak{A}$ elemekhez rendeljük hozzá az $E(\widetilde{\mathbf{a}}, \widetilde{\mathbf{b}}) = \{\lambda \mid \pi_\lambda(\widetilde{\mathbf{a}}) = \pi_\lambda(\widetilde{\mathbf{b}})\}$ halmazt. Azt mondjuk, hogy $\widetilde{\mathbf{a}}$ és $\widetilde{\mathbf{b}}$ majdnem mindenütt egyenlő, ha $\mu(E(\widetilde{\mathbf{a}}, \widetilde{\mathbf{b}})) = 1$. Tekintsünk egy $\mathbf{r}$ relációszimbólumot, és a megfelelő ϱ_λ relációkat. A direkt szorzaton bevezetünk egy ϱ relációt úgy, hogy $\varrho(\widetilde{\mathbf{a}}_1, \ldots, \widetilde{\mathbf{a}}_n)$ akkor teljesül, ha azoknak az indexeknek a halmaza, amelyekre $\varrho_\lambda(\pi_\lambda(\widetilde{\mathbf{a}}_1), \ldots, \pi_\lambda(\widetilde{\mathbf{a}}_n))$ fennáll, 1 mértékű (a reláció majdnem mindenütt teljesül).*

Az a reláció, hogy két elem majdnem mindenütt egyenlő, ekvivalenciareláció. Az e szerinti faktort a μ-vel definiált ultraszorzatnak nevezzük. A ultraszorzat a nyilvánvaló műveletdefinícióra és a fenti relációdefinícióra nézve az eredetiekkel azonos típusú algebrát alkot.

Bizonyítás. Mindenekelőtt belátjuk, hogy ekvivalenciarelációt definiáltunk. A reflexivitás és a szimmetria triviálisan teljesül. A tranzitivitás bizonyításához először is megjegyezzük, hogy $E(\widetilde{\mathbf{a}}, \widetilde{\mathbf{b}}) \cap E(\widetilde{\mathbf{b}}, \widetilde{\mathbf{c}})$ nyilván része az $E(\widetilde{\mathbf{a}}, \widetilde{\mathbf{c}})$ halmaznak. Mivel 1 mértékűek, ezért metszetük is 1 mértékű, és 1 mértékűnél nagyobb halmaz is 1 mértékű, ezért a reláció valóban tranzitív.

A művelet definíciójának a jogosságához be kell bizonyítani, hogy a „majdnem mindenütt egyenlő”, mint reláció, kongruenciareláció. Legyen f egy n-változós művelet, $\widetilde{\mathbf{a}} = f\widetilde{\mathbf{a}}_1, \ldots, \widetilde{\mathbf{a}}_n$, $\widetilde{\mathbf{b}} = f\widetilde{\mathbf{b}}_1, \ldots, \widetilde{\mathbf{b}}_n$. Legyen továbbá $E_i = E(\widetilde{\mathbf{a}}, \widetilde{\mathbf{b}})$, minden szóba jövő i-re.

Világos, hogy $E(\tilde{\mathbf{a}}, \tilde{\mathbf{b}})$ tartalmazza az összes E_i metszetét; ha tehát ezek mind 1 mértékűek, akkor $E(\tilde{\mathbf{a}}, \tilde{\mathbf{b}})$ is 1 mértékű – ami bizonyítja, hogy valóban kongruenciarelációt kaptunk.

Mivel egy varietás a direkt szorzatra és a homomorf képre zárt, ezért a kapott algebra – a relációktól eltekintve – abban a varietásban van, amit a tényezők generálnak.

A relációtartásra vonatkozó állítás is triviális. Tekintsük a szóba jövő elemeknek azokat a komponenseit, amelyekre az adott reláció fennáll, és azokat, amelyekre a reláció nem áll fenn. A két halmaz közül pontosan az egyik lesz 1 mértékű; s ennek megfelelően áll fenn a reláció vagy sem. ■

Megjegyzés. A tétel bizonyítása során két igen fontos dolog derült ki. A műveletekre vonatkozóan az, hogy egy azonosság a ultraszorzatokban pontosan akkor igaz, ha majdnem minden komponensben igaz. A relációra vonatkozóan pedig azt láttuk, hogy nemcsak a reláció teljesülése „öröklődik", hanem az is, hogy a reláció nem áll fenn. □

A következőkhöz szükségünk van egy – a Boole-hálókra vonatkozó – egyszerű tulajdonságra:

14.13. Tétel. *Legyen A a B Boole-háló nemüres részhalmaza, és definiáljuk – megfelelően – az A', $A^{\wedge}$ és $A^{\vee}$ halmazokat mint azt a legszűkebb, A-t tartalmazó halmazt, amely zárt a komplementerképzésre, a metszetre, illetve az egyesítésre. Ekkor $A^* = ((A')^{\wedge})^{\vee}$ éppen az A generálta rész-Boole-háló.*

Bizonyítás. $A \subseteq A^*$ triviális, éppúgy, mint A^*-nak az egyesítésre való zártsága. Mivel A nem üres, ezért van egy x eleme, amelynek komplementere eleme A'-nek. Így ezek metszete benne van A^*-ban, s mivel ezek is benne vannak A^*-ban, így az egyesítésük is. Ez biztosítja, hogy $0, 1 \in A^*$. A disztributivitás miatt A^* a metszetre is zárt. Az $(a \vee b)' = a' \wedge b'$ és $(a \wedge b)' = a' \vee b'$ összefüggésekből következik, hogy A^* bármely elemének a komplementere felírható A'-beli elemek egyesítéseinek metszeteként. Az egyesítések – definíció szerint – hozzátartoznak A^*-hoz, és ezek metszetei, az előbb bizonyított állítás szerint, ugyancsak elemei A^*-nak. Így A^* az A-t tartalmazó Boole-háló; és triviálisan a legkisebb ilyen. ■

Az ultraszorzat kiemelkedő fontosságát mutatja az alábbi

14.14. Tétel. *Tekintsük adott típusú $\mathfrak{A}_i$ algebrák tetszőleges $\mathfrak{B}$ ultraszorzatát. Egy Φ zárt formula akkor és csak akkor igaz $\mathfrak{B}$-ben, ha majdnem minden $\mathfrak{A}_i$-ben igaz.*

Bizonyítás. A formulában fellépő határozatlanok számára vonatkozó teljes indukcióval bizonyítunk.

Ha nincs a formulában határozatlan, akkor a formula egy ítélet. Ha a formula egy elemi ítélet, akkor az állítás az ultraszorzatra vonatkozó 14.12. tétel szerint igaz. Mint ott láttuk, ugyanez teljesül a komplementerre (az ítélet tagadására) is.

Legyenek $\Phi_1, \ldots, \Phi_n$ elemi ítéletek vagy komplementereik, és legyen $\varphi = \Phi_1 \wedge \ldots \wedge \Phi_n$. Ennek a kiértékelése pontosan akkor 1, ha minden Φ_i kiértékelése 1. Az ultraszorzaton egy-egy Φ_i kiértékelése pontosan akkor 1, ha az indexhalmaznak van olyan 1 mértékű E_i részhalmaza, hogy az ebbe eső indexhalmazhoz tartozó algebrákon a formula kiértékelése 1. Eszerint a Φ ítélet az ultraszorzaton pontosan akkor „igaz", ha az E_i indexhalmazok E

közös részébe eső indexhalmazhoz tartozó algebrákon igaz. Tekintettel arra, hogy véges sok 1 mértékű halmaz közös része is 1 mértékű, ezért a tétel állítása igaz a most tekintett Φ ítéletre is.

A következő lépésben vegyünk eddig tekintett $\Phi_1, \ldots, \Phi_n$ ítéleteket, és legyen $\varphi = \Phi_1 \vee \ldots \vee \Phi_n$. Ennek a kiértékelése pontosan akkor 1, ha valamelyiküknek – például Φ_1-nek – a kiértékelése 1. Mint az előző meggondolás során láttuk, ez pontosan akkor 1, ha majdnem minden komponensre 1. Így a tétel állítása tetszőleges ítéletre igaz.

Legyen most Φ egy olyan zárt formula, amelyben n darab határozatlan szerepel, és tegyük fel, hogy az állítás igaz minden olyan zárt formulára, amelyben a határozatlanok száma kevesebb, mint n.

Legyen először $\Phi = (\forall \mathbf{x})\Psi$ alakú. Ez a formula az ultraszorzaton pontosan akkor igaz, ha $\mathbf{x}$ helyébe bármely $\widetilde{a}$ vektort írva a formula igaz. Ez pedig azt jelenti, hogy a komponensekben bármit helyettesítve a formula majdnem mindenütt igaz. Ha $\Phi = (\exists \mathbf{x})\Psi$ alakú, akkor van olyan $\widetilde{a}$ behelyettesítés, amelyre a formula igaz, azaz majdnem mindenütt igaz, tehát majdnem mindenütt van olyan behelyettesítés, amelyre a formula igaz. (Könnyen látható, hogy a gondolatmenetek „akkor és csak akkor” jellegűek.) ■

Az alábbiakban az ultraszorzat két alkalmazását adjuk. Az első az úgynevezett teljességi tétel.

14.15. Tétel. *Legyen adva egy relációalgebra-típus és egy hozzá tartozó Σ végtelen zárt formulahalmaz. Ha e halmaz minden véges részhalmazához található olyan relációalgebra, amelyen e részhalmaz minden eleme igaz, akkor létezik olyan algebra is, amelyen a formulák mindegyike igaz.*

Bizonyítás. Tekintsünk minden egyes véges Σ_i formularészhalmazhoz egy-egy, a tételben megkívánt tulajdonságú $\mathfrak{A}_i$ relációalgebrát, ahol i egy I indexhalmazon fut végig. Az I indexhalmaz elemei tehát bijektíven megfeleltethetők a formulahalmaz véges részhalmazainak.

Az I indexhalmazon egy mértéket fogunk definiálni. Ehhez először megadunk bizonyos részhalmazokat, amelyektől megkívánjuk, hogy 0 mértékűek legyenek. Tekintsük az adott formulák egy tetszőleges véges Σ_i részhalmazát, és vegyük I-nek azt az $I(\Sigma_i)$ részhalmazát, amely azokból a j indexekből áll, amelyekre $\mathfrak{A}_j$-ben a Σ_i elemei közül legalább egy nem igaz. Legyen 0 mértékű minden olyan halmaz, amelyik az $I(\Sigma_i)$-kből egy véges indexhalmaz hozzávételével keletkezik, továbbá ezek minden részhalmaza is. Mindenekelőtt kimutatjuk, hogy ezek a halmazok a részhalmazhálóban ideált alkotnak. Ezeknek a részhalmazoknak a halmaza definíció szerint öröklődő. A $\Sigma_1 \cup \Sigma_2$ formulahalmaz valamelyik eleme pontosan akkor nem teljesül egy $\mathfrak{A}_j$ algebrában, ha ez a formula vagy Σ_1-ben van, vagy Σ_2-ben. Így $I(\Sigma_1) \cup I(\Sigma_2) = I(\Sigma_1 \cup \Sigma_2)$, amiből következik, hogy valóban ideált definiáltunk. Ez az ideál nem tartalmazza az egész I halmazt. Ugyanis végtelen sok olyan algebra van, amely előre megadott formulákat kielégít; ezért egyetlen $I(\Sigma_i)$ halmaznak és egyetlen véges halmaznak az egyesítése nem lehet az egész halmaz; és természetesen ezek részhalmaza sem lehet I. Így van olyan prímideál, amely a megadott 0 mértékű halmazok mindegyikét tartalmazza – ezért valóban definiáltunk egy 0–1 mértéket.

Tekintsünk most egyetlen σ formulát. Ez a formula igaz az $I(\{\sigma\})$ halmaz komplementerén. Mivel $I(\{\sigma\})$ 0 mértékű, ezért a σ formula majdnem mindenütt igaz, tehát igaz a vizsgált ultraszorzatban is. Így az ultraszorzatban minden egyes formula igaz. ■

A másik alkalmazásként megmutatjuk, hogy a természetes számokat „nem lehet formulákkal egyértelműen definiálni”. A természetes számokat relációstruktúrának tekinthetjük, ahol az alábbi műveletek és relációk szerepelnek.

1) Egy nullváltozós művelet, az 1.

2) Egy egyváltozós művelet, a rákövetkezés: $f(n)$ az n természetes szám rákövetkezője.

3) Egy kétváltozós $a + b$ művelet, az összeadás, és egy kétváltozós ab művelet, a szorzás.

4) Egy kétváltozós reláció, a „kisebb-egyenlő”: $a \leq b$.

Ezekre a műveletekre és relációkra a következő „axiómák teljesülnek” (azaz a következő formuláktól kívánjuk meg, hogy realizációjuk kiértékelése 1 legyen):

1. 0 nem rákövetkező. Ez $(\forall \mathbf{x})\Phi$ alakú formula, ahol Φ az $\mathbf{e}(f(\mathbf{x}), 0)$ komplementere.

2. Különböző elemek rákövetkezője is különböző. (Itt és a későbbiekben a $\Phi \vee \Psi'$ formula helyett azt írjuk, hogy $\Psi \Rightarrow \Phi$.) Ezzel a jelöléssel megfogalmazva a következő formulát kapjuk:

$$(\forall \mathbf{x})(\forall \mathbf{y})[\mathbf{e}(f(\mathbf{x}), f(\mathbf{y})) \Rightarrow \mathbf{e}(\mathbf{x}, \mathbf{y})].$$

(Itt tehát a $\Rightarrow$ jel a logikai „ha..., akkor...” megfelelője.)

3. A teljes indukció axiómája. Ezt mindenekelőtt megfogalmazzuk szavakkal:

Bármely olyan formula, amelyre igaz az alábbi két feltétel, igaz minden n-re:

(I) Igaz a formula $n = 1$-re.

(II) Valahányszor igaz n-re, úgy igaz $f(n)$-re is.

Ennek az axiómának a formális megfogalmazásában két probléma is felmerül. Az egyik az, hogy a formulában szerepelhetnek még más határozatlanok is, amelyeknek minden esetben ugyanazt az értéket kell adni. A másik az, hogy a két feltételben szereplő határozatlanokat lehet ugyanazoknak választani, de a végkövetkeztetésben szereplőket nem. Evégett ugyanazt a formulát kétszer kell felírni, de mindkét esetben csak a határozatlanokat kell megváltoztatni. Ennek okáért, ha egy formula véges sok határozatlan „generálta” formula, akkor ezeket a határozatlanokat mint „változókat” kiírjuk. Ha egy változó helyébe mást írunk, az tulajdonképpen egy másik formulát jelent, amely az elsőből egy „endomorfizmussal” kapható meg. Így a teljes indukció a következőképpen írható:

$$(\forall \mathbf{X})\big\{\big(\Phi(0, \mathbf{x}_1, \ldots, \mathbf{x}_k) \wedge \big[\Phi(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_k) \Rightarrow \Phi(f(\mathbf{x}_0), \mathbf{x}_1, \ldots, \mathbf{x}_k)\big]\big) \Rightarrow$$
$$\Rightarrow \Phi(\mathbf{y}, \mathbf{x}_1, \ldots, \mathbf{x}_k)\big\},$$

ahol $\mathbf{X} = \{\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}\}$. (Láthatjuk, hogy a teljes indukció valójában nem egyetlen axióma, hanem minden egyes Φ formulához tartozik egy-egy axióma.)

4. Összefüggés a kétváltozós műveletek és a rákövetkezés között. Legyen az összeadásnak, illetve a szorzásnak megfelelő jel $\mathbf{s}$, illetve $\mathbf{p}$. Ekkor a következő formuláknak kell teljesülniük:

$$(\forall \mathbf{x})[\mathbf{e}(\mathbf{s}(\mathbf{x}, 0), \mathbf{x})], \qquad (\forall \mathbf{xy})[\mathbf{e}(\mathbf{s}(\mathbf{x}, f(\mathbf{y})), f(\mathbf{s}(\mathbf{x}, \mathbf{y})))],$$

$$(\forall \mathbf{x})[\mathbf{e}(\mathbf{p}(\mathbf{x}, 0), 0)], \qquad (\forall \mathbf{xy})[\mathbf{e}(\mathbf{p}(\mathbf{x}, f(\mathbf{y})), \mathbf{s}(\mathbf{p}(\mathbf{x}, \mathbf{y}), \mathbf{x}))].$$

5. Végezetül a „kisebb-egyenlő” definiálása következik. Legyen $\mathbf{r}(\mathbf{x}, \mathbf{y})$ az a relációszimbólum, amelynek realizálása (értelemszerűen) $x \leq y$. Erre a következőket kívánjuk

meg:

$$(\forall \mathbf{xy})(\exists \mathbf{z})[\mathbf{r}(\mathbf{x}, \mathbf{y}) \Leftrightarrow \mathbf{e}(\mathbf{s}(\mathbf{x}, \mathbf{z}), \mathbf{y})],$$

ahol $\Phi \Leftrightarrow \Psi$ a $(\Phi \vee \Psi') \wedge (\Psi \vee \Phi')$ formula rövidítése.

A fenti formulák tartalmazzák az összes axiómát, amelyet a természetes számoktól meg szoktunk kívánni.

Legyen most $\mathfrak{N}$ a fenti axiómarendszernek az a modellje, amelyből az 1–5. axiómákat leszűrtük: az „igazi" természetes számok alkotta relációstruktúra. Ebben bármely természetes számnál csak véges sok kisebbet találhatunk. Tekintsük most e modellnek egy – végtelen – ultraszorzatát (az indexek legyenek 1, 2, ... stb.). A 14.14. tétel szerint ez az ultraszorzat ugyancsak modellje lesz a fenti axiómarendszernek. Megmutatjuk, hogy ebben a modellben a megemlített tulajdonság nem teljesül. Legyen $\tilde{\mathbf{n}}$ az ultraszorzatnak az az eleme, amelynek minden egyes komponense az $n \in \mathfrak{N}$ (szám); és legyen $\tilde{\mathbf{d}}$ a diagonális elem, azaz $\tilde{\mathbf{d}}$-nek az i-edik komponense legyen az $i \in \mathfrak{N}$. Ekkor azt kapjuk, hogy $\tilde{\mathbf{0}} < \tilde{\mathbf{1}} < \ldots < \tilde{\mathbf{n}} < \ldots < \tilde{\mathbf{d}}$; hiszen a megfelelő relációk véges sok hely kivételével teljesülnek. A kapott modell tehát nem a „megszokott", és mégis minden igaz rá, amit az eredetire a fenti axiómarendszerből be lehet bizonyítani. A fenti tényt röviden úgy fejezzük ki, hogy *a természetes számoknak létezik nem standard modellje*.

Megjegyezzük a következőket. Az ultraszorzat segítségével bebizonyítható, hogy az összeadás és szorzás művelete nem definiálható a rákövetkezés segítségével, még rekurzívan sem. Legyen $\mathfrak{A}$ az a relációstruktúra, amely úgy van rendezve, mint a természetes számok, és a $\mathfrak{B}$ struktúra legyen úgy rendezve, hogy a természetes számok „után" még ott vannak az egész számok – a szokásos rendezéssel. Kimutatható, hogy ezeknek (csak a rákövetkezést és rendezést figyelembe véve!) létezik izomorf „ultrahatványuk", ami azt jelenti, hogy ugyanazokat az axiómákat elégítik ki. Márpedig a $\mathfrak{B}$ struktúrában nem lehet definiálni az összeadást úgy, hogy az kielégítse a megkövetelt axiómákat. (Erről könnyen meg lehet győződni!) Sőt, hasonló módon azt is beláthatjuk, hogy az összeadás definíciója sem elegendő; a szorzást még ennek birtokában sem lehet definiálni a többiekből.

Az ultraszorzat segítségével igen egyszerűen bizonyítható, hogy – általában – nem axiomatizálhatók olyan feltételek, amelyekben valaminek a végességét kötjük ki. Példaként tekintsük azt, hogy a test karakterisztikája véges. Ha elkészítjük az összes véges prímtest ultraszorzatát, akkor a kapott struktúra test lesz, de 0 karakterisztikájú. Egyébként nemcsak az igaz, hogy testek ultraszorzata test, hanem például az integritási tartományoké integritási tartomány (általában, ha a feltételeket formulákkal megfogalmazhatjuk, akkor az ultraszorzat is eleget tesz a feltételeknek).

15. Kategóriák

15.1. Objektumok és morfizmusok

Algebrai, de más matematikai struktúrák vizsgálatában is igen fontosak a „megengedett" leképezések viselkedései. Ezen azt értjük, hogy e leképezéseket bizonyos esetekben összeszorozhatjuk, és a szorzásról leolvasható formális tulajdonságok sok mindent elárulnak a struktúrákról. Az így kialakuló képben az egyes matematikai objektumokat mint egy „fekete dobozt" tekintjük, belső szerkezetüket egyáltalán nem vizsgáljuk. Az objektumok közötti leképezések veszik át a főszerepet; és az egész „rendszerről" csak annyit tudunk mondani, amennyit a leképezések lehetővé tesznek. Az így kialakult rendszereket *kategóriáknak* nevezzük. A kategóriákban az „objektumokról" nem tesszük fel (és nem is tehetjük fel), hogy halmazt alkotnak, ennek következtében a kategóriák alkalmasak például a matematika halmazelméleti megalapozására is.

A különböző, konkrétan megadott kategóriák esetében a leképezéseknek más és más speciális tulajdonsága van. Ennek megfelelően az egyes esetekben konkrétan vizsgált kategóriáknál rendszerint bizonyos többletfeltételt is kirónak. Az általános esetben viszonylag kevés olyan eredmény bizonyítható, amelyet ne lehetne a kategóriaelméleti fogalmak nélkül is bizonyítani. Amennyiben speciális kategóriákat nézünk, akkor a kategóriaelméleti vizsgálatok már sok lényeges új eredményt hozhatnak. Tekintettel arra, hogy e témakör vizsgálatában nem kívánunk túl mélyre bocsátkozni, ezért elsősorban csak arra szorítkozunk, hogy az eddigi fogalmak egy részét kategóriaelméleti „nyelven" is definiáljuk. Ez – esetünkben – főleg az említett fogalmak jobb megértését biztosítja.

15.1. Definíció. Tekintsünk egy $\mathcal{C}$ osztályt, amely „objektumokból" és „morfizmusokból" áll. Az objektumok alkotta osztályt $\mathrm{Ob}\mathcal{C}$, a morfizmusok alkotta osztályt $\mathrm{Mor}\mathcal{C}$ jelöli. ($\mathcal{C}$ tehát $\mathrm{Ob}\mathcal{C}$ és $\mathrm{Mor}\mathcal{C}$ diszjunkt egyesítése.) $\mathcal{C}$-t kategóriának nevezzük, ha az alábbiak teljesülnek:

(1) Minden $\mathrm{Ob}\mathcal{C}$-beli A, B elempárhoz ki van jelölve $\mathrm{Mor}\mathcal{C}$ elemeinek egy $\hom(A, B)$ halmaza, amelynek az elemeit A-ból B-be való (homo)morfizmusoknak nevezzük. Feltesszük továbbá, hogy a $\hom(A, B)$ és $\hom(C, D)$ halmazok diszjunktak, kivéve, ha $A = C$ és $B = D$. (Lényeges, hogy $\hom(A, B)$ csak halmaz lehet, és a definícióban A és B sorrendje is számít.)

(2) Tetszőleges $u \in \hom(A, B)$ és $v \in \hom(B, C)$ elemekhez hozzá van rendelve a $\hom(A, C)$-nek egy (egyértelműen meghatározott) vu eleme, amelyet a fenti két elem szorzatának nevezünk.

(3) A morfizmusok szorzása asszociatív, ha elvégezhető. Azaz, tetszőleges $u \in \hom(A, B)$, $v \in \hom(B, C)$ és $w \in \hom(C, D)$ esetén érvényes a $(wv)u = w(vu)$ összefüggés. (Az asszociativitást biztosító feltételt úgy is fogalmazhatjuk, hogy léteznek a wv és vu szorzatok.)

(4) Minden A objektumhoz létezik egy $1_A \in \hom(A, A)$ identitás, amelyre tetszőleges B objektum és $u \in \hom(A, B)$, illetve $v \in \hom(B, A)$ esetén teljesül az $u1_A = u$, illetve az $1_A v = v$ összefüggés. □

Az eddigieknek megfelelően az $u \in \hom(A, B)$ esetben használni fogjuk az $u : A \to B$, illetve az $A \xrightarrow{u} B$ jelölést is.

15.2. Tétel. *Minden e identitáshoz van olyan u morfizmus, hogy az eu vagy ue szorzatok valamelyike létezik. E tulajdonság a 15.1. definíció* (4) *pontjával együtt értelemszerűen jellemzi az identitásokat.*

Bizonyítás. Az $u = e$ választásra mindkét szorzat létezik.

Tegyük most fel, hogy e rendelkezik a két megkívánt tulajdonsággal. Legyen $e \in \in \hom(A, B)$ és tegyük fel például, hogy létezik ue. Ebből először is az következik, hogy $u \in \hom(B, C)$ egy alkalmas C objektummal. Az $ue = u$ feltételből azonnal következik az is, hogy $\hom(A, C) = \hom(B, C)$; tehát $A = B$.

Mivel $\hom(A, A)$ bármely két elemének létezik a szorzata, és e szorzat ugyancsak eleme $\hom(A, A)$-nak, továbbá $\hom(A, A)$ halmaz, ezért a szorzás asszociativitásának a következtében $\hom(A, A)$ félcsoport. E félcsoportnak e is és 1_A is egységeleme; s az egységelem egyértelműsége miatt csak $e = 1_A$ lehetséges. ■

Megjegyzések. 1. A 15.2. tétel első állítása természetesen akkor is igaz, ha e helyett tetszőleges a morfizmust tekintünk. Azért mondtuk ki a tételt mégis a fenti alakban, mert ezzel az identitásokat jellemezhettük.

2. A fenti tétel módot ad arra, hogy a kategóriákat csupán a morfizmusok felhasználásával definiálhassuk. Eszerint egy kategória morfizmusokból álló osztály, amelynek bizonyos elemeit összeszorozhatjuk. Ha létezik az ab és bc szorzat, akkor léteznek az $(ab)c$ és $a(bc)$ szorzatok is; és ezek megegyeznek. Egy e morfizmust identitásnak nevezünk, ha az ue, illetve ev létezéséből $ue = u$, illetve $ev = v$ következik. Megköveteljük még, hogy bármely u morfizmushoz létezzék bal oldali és jobb oldali identitás, azaz olyan e és f identitás, amelyekre $eu = uf = u$ teljesül. Végül még azt is feltesszük, hogy egy-egy rögzített e és f identitáspár esetén azok az u elemek, amelyek mind az $eu = u$, mind az $uf = u$ feltételt kielégítik, halmazt alkotnak.

3. Az identitások egyértelműsége ebben a felépítésben is igaz, és belátható, hogy az identitásokkal egyértelműen helyettesíthetjük az objektumokat. □

Ha kategóriákra példákat sorolunk fel, akkor meg kell mondani, hogy mik az objektumok, mik a morfizmusok és mit értünk morfizmusok szorzatán. Ha csupán az objektumokat mondjuk meg, akkor ezt úgy értjük, hogy a morfizmusok a megfelelő struktúrakörben a „szokásosak"; és a leképezések szorzása a morfizmusszorzás. Így beszélhetünk „a csoportok", „a gyűrűk" kategóriájáról stb. Lehet, mint említettük, hogy a morfizmusok nem a „természetesen adottak". Például vehetjük a kategória objektumainak a csoportokat, de morfizmusoknak csak azokat a homomorfizmusokat, amelyeknél a kép véges indexű (nem kapunk viszont kategóriát akkor, ha azt tesszük fel, hogy a kép véges csoport, mert az identitás általában nem ilyen).

Ha algebrai struktúrák egy kategóriáját vizsgáljuk, akkor itt az injektív, illetve a szürjektív leképezéseknek bizonyos egyszerűsítési tulajdonságai vannak. E tulajdonságok tetszőleges kategóriában értelmezhetők.

15.3. Definíció. Egy $\mathcal{C}$ kategória u, illetve v morfizmusát monomorfizmusnak, illetve epimorfizmusnak nevezzük, ha az $ux = uy$, illetve $xv = yv$ feltételből $x = y$ következik. □

Megjegyzés. A halmazok és az (összes) leképezések kategóriájában a monomorfizmusok pontosan az injektívek, az epimorfizmusok pontosan a szürjektívek. Hasonló a helyzet több olyan kategóriában is, amelynek az objektumai adott varietások elemei és a morfizmusok a homomorfizmusok, Általában azonban ez nem így van. Tekintsük például a következő kategóriát: Egyetlen objektuma az egész számok halmaza legyen. A φ leképezés minden n egész számhoz rendelje $(n + 1)$-et, kivéve 0-hoz, amelyhez 0-t rendeljen. A morfizmusok álljanak ennek a leképezésnek a hatványaiból, beleértve az identikus leképezést is. Könnyen belátható, hogy e leképezések mindegyike a kategóriának

monomorfizmusa is és epimorfizmusa is; de az identitástól eltekintve egyikük sem injektív és egyikük sem szürjektív. □

Látjuk tehát, hogy az injektivitást, illetve a szürjektivitást kategóriaelméleti módon általánosan csak gyengítve fogalmazhattuk meg. Volna arra is mód, hogy e tulajdonságoknál erősebb fogalmakat vigyünk át kategóriaelméleti nyelvre. Ugyanis, ha egy homomorfizmusnak létezik bal oldali (jobb oldali) inverze, akkor ebből következik, hogy a homomorfizmus injektív (szürjektív). A félcsoportoknál látottakhoz hasonló módon belátható, hogy e feltételek – megfelelően – indukálják, hogy monomorfizmusról, illetve epimorfizmusról van szó, bármely kategória esetében.

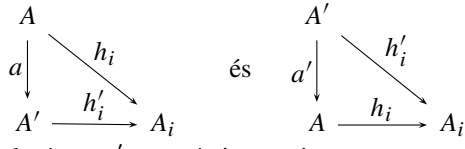
Az invertálható morfizmusok a modulusok kategóriájában alkalmasak voltak a direkt összeadandó megfogalmazására. Erre általános esetben nincs mód, hiszen egy homomorfizmus magja általában nem jellemezhető részstruktúrával. Így a kategóriaelméleti átfogalmazás sem sikerülhet ezen az úton. Megadható viszont az izomorfizmus fogalma az invertálható morfizmusok segítségével. Erre annál is inkább szükség van, mert az említett példában láttuk, hogy egy morfizmus lehet egyszerre monomorfizmus is és epimorfizmus is anélkül, hogy akár injektív, akár szürjektív volna.

15.4. Definíció. A $\mathscr{C}$ kategória egy i morfizmusát izomorfizmusnak nevezzük, ha található hozzá olyan j morfizmus, amelyre mind ij, mind ji identitás. Ekkor a két morfizmust egymás inverzének nevezzük. □

Noha az invertálható morfizmusok segítségével nem fogalmazható meg teljes általánosságban a direkt szorzat, mégis megadható a direkt szorzat általános analogonja, kiindulva abból a megfontolásból, hogy a direkt szorzat a „legkisebb" olyan objektum, amely a komponensekre „függetlenül" levetíthető:

15.5. Definíció. Legyen adva a $\mathscr{C}$ kategória objektumainak egy $\mathscr{A} = \{A_i \mid i \in I\}$ halmaza. Tetszőleges $\mathscr{C}$-beli A objektum esetén e halmaznak egy $\mathbf{h} : A \to \mathscr{A}$ kúpján morfizmusok egy $\{h_i : A \to A_i \mid i \in I\}$ halmazát értjük.

A $\mathbf{h} : A \to \mathscr{A}$ és a $\{h'_i : A' \to A_i \mid i \in I\}$ kapcsolattal megadott $\mathbf{h}' : A' \to \mathscr{A}$ kúpokat ekvivalenseknek nevezzük, ha léteznek olyan $a : A \to A'$ és $a' : A' \to A$ morfizmusok, amelyekre tetszőleges $i \in I$ esetén az



diagramok kommutatívak, és a, a' egymás inverzei.

A $\mathbf{h} : A \to \mathscr{A}$ kúpot univerzálisnak nevezzük, ha bármely, a $\{g_i : B \to A_i \mid i \in I\}$ kapcsolattal megadott $\mathbf{g} : B \to \mathscr{A}$ kúphoz létezik olyan egyértelműen meghatározott $a : B \to A$ morfizmus, amelyre tetszőleges $i \in I$ esetén az

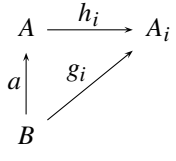


diagram kommutatív. □

Látható, hogy az univerzális kúp pontosan a direkt szorzat fogalmát takarja. Világos, hogy tetszőleges kategória esetén nem kell minden lehetséges direkt szorzatnak léteznie. Az azonban szükséges, hogy amennyiben a kategóriában létezik direkt szorzat, akkor az egyértelmű legyen.

15.6. Tétel. *Ha egy kategóriában – rögzített A-hoz és $\mathcal{A}$-hoz – létezik univerzális kúp, akkor ez, ekvivalenciától eltekintve, egyértelmű.*

Bizonyítás. Legyen $\mathbf{h} : A \to \mathcal{A}$ és $h' : A' \to \mathcal{A}$ két univerzális kúp. Ekkor – az univerzális kúp definíciója szerint – léteznek olyan $a : A \to A'$ és $a' : A' \to A$ morfizmusok, hogy a megfelelő $h_i : A \to A_i$ és $h'_i : A' \to A_i$ leképezésekre $h_i a' = h'_i$ és $h'_i a = h_i$ teljesülnek ($A_i \in \mathcal{A}$).

Ebből azonnal kapjuk, hogy minden i indexre fennállnak a $h_i a' a = h_i$ és $h'_i aa' = h'_i$ összefüggések. Emellett minden i indexre eleve teljesülnek az alábbiak: $h_i 1_A = h_i$ és $h'_i 1_{A'} = h'_i$. Tekintettel arra, hogy feltételünk szerint mindkét kúp univerzális volt, a megfelelő homomorfizmusok egyenlők: $a'a = 1_A$ és $aa' = 1_{A'}$. Ez pedig éppen a két kúp ekvivalenciáját jelenti. ■

Célszerű tudatosítani magunkban, hogy a direkt szorzat fenti definíciója nem csak a figyelembe vett objektumoktól függ, hanem attól is, hogy milyen más morfizmusok vannak még a kategóriában. Éppen ezért, ha a vizsgált kategóriát valamilyen módon „növeljük” vagy „csökkentjük”, akkor a direkt szorzat általában megváltozik.

A direkt szorzatnak létezik kategóriaelméleti „duálisa” is, amikor a szereplő „nyilak” mindegyikének megfordítjuk az irányát. Így definiálhatjuk a $\mathbf{h} : \mathcal{A} \to A$ úgynevezett *ko-kúpot* mint egy $\{h_i : A_i \to A \mid A_i \in \mathcal{A}, i \in I\}$ halmazt.

A $\mathbf{h} : \mathcal{A} \to A$ és $\mathbf{h}' : \mathcal{A} \to A'$ ko-kúpok *ekvivalenciája* olyan $a : A \to A'$ és $a' : A' \to A$ morfizmusok létezését jelenti, amelyek egymás inverzei, és amelyekre a $h'_i = ah_i$ és $h_i = a'h'_i$ diagram-kommutativitási feltételek teljesülnek.

Az univerzalitás szerepét a „*ko-univerzalitás*” veszi át: Ez tetszőleges $\mathbf{g} : \mathcal{A} \to B$ ko-kúphoz olyan egyértelmű $a : A \to B$ morfizmus létezését kívánja meg, amelyre a kommutativitást biztosító $g_i = ah_i$ feltételek teljesülnek.

A ko-szorzat definíciójára valójában nem lesz szükség, mert ez megkapható automatikusan az „oppozit” kategória (l. 15.9. definíció) tárgyalásából.

Felsorolunk néhány jól ismert kategóriát, megadva, hogy ezekben mi a ko-szorzat:

A halmazok kategóriájában a ko-szorzat a diszjunkt egyesítés. Ugyancsak a diszjunkt egyesítés a ko-szorzat minden olyan kategóriában, amely unáris algebrák egy varietása. Az Abel-csoportok vagy általában a modulusok kategóriájában a ko-szorzat a direkt összeg. A csoportok kategóriájában a ko-szorzat az úgynevezett szabad szorzat. Ezt általában nem vizsgáljuk, csak annyit jegyzünk meg róla, hogy egyetlen elemmel generált végtelen ciklikus csoportok szabad szorzata izomorf ezen elemek generálta szabad csoporttal.

Megjegyezzük még, hogy definiálható a szubdirekt szorzat is, felhasználva azt a tulajdonságot, hogy a szereplő morfizmusok „összességükben injektívek”.

Első pillanatra meglepőnek tűnik, hogy a direkt szorzattal ellentétben a „rész és a faktor” fogalma tetszőleges kategóriára nem általánosítható. Ez nemcsak azért van így, mert

nem tudjuk értelmezni az injektivitást és a szürjektivitást. Kategóriák esetében ugyanis csak „részként való beágyazásról" vagy „homomorf képről" lehetne beszélni; nincs valamiféle „értelmes" eljárás annak a kitüntetésére, hogy a „beágyazottak", illetve „képek" közül melyiket tekintsük résznek, illetve faktornak. Ezen úgy lehet segíteni, hogy „az összes olyat tekintjük, amely ugyanúgy viselkedik". Például a rész esetén a következőképpen járhatunk el: $h : B \to A$ és $g : C \to A$ az A-nak ekvivalens részei, ha közöttük megadott megfelelő a és b morfizmusokra $ah = g$ és $bg = h$ teljesül. Itt h, g monomorfizmusok és ab, ba mindegyike identitás. Ezek után az egymással ekvivalens részeket lehet részobjektumoknak tekinteni.

A fentiek után „következő" univerzális algebrai konstrukció a szabad algebra volt. Itt teljesen újszerű nehézség lép színre. A szabad algebrák definiálásakor ugyanis meg kell adni egy szabad generátorrendszert, és ennek egy *halmazleképezését* kell kiterjeszteni *algebrahomomorfizmussá*. Ennek megfelelően, kétféle kategóriát kell figyelembe venni: a halmazok és a vizsgált struktúrák kategóriáját. Azt tehát, hogy egy algebra szabad, csak e két kategória között fennálló kapcsolattal tudjuk megfogalmazni. A következő részben e kapcsolatot fogjuk részletesebben megvizsgálni.

E vizsgálatok előtt még felhívjuk valamire a figyelmet. Azoknak a kategóriáknak az objektumai, amelyekkel eddig találkoztunk, mind olyanok voltak, hogy egy-egy halmazt „kiterjesztettünk" valamilyen struktúrává. Ezeknek a struktúráknak tehát volt egy tartóhalmazuk. A „megengedett" (homo)morfizmusok mindig halmazleképezések voltak. Ilyen esetekben *konkrét kategóriákról* beszélünk. Nem minden kategória konkrét; például, ha a kategóriának egyetlen objektuma van, az a, és egyetlen morfizmusa, az 1_a, amely egymagában egy egyelemű csoport, akkor ez nem konkrét kategória, hiszen a nem egy halmaz és 1_a nem egy leképezés. Persze létezik ezzel „izomorf(?)" konkrét kategória, amelynek egyetlen objektuma az egyelemű csoport és egyetlen morfizmusa e csoport identitása. A továbbiakban ezzel a kérdéssel is foglalkozunk kicsit részletesebben.

15.2. Funktorok

A funktorokat – „formai szempontból" – úgy tekinthetjük, mint kategóriák közti homomorfizmusokat.

15.7. Definíció. A $\mathcal{C}$ kategóriából a $\mathcal{D}$ kategóriába képező $\Phi : \mathcal{C} \to \mathcal{D}$ funktoron a következőket értjük:

(1) Minden $A \in \mathrm{Ob}\mathcal{C}$-hez hozzá van rendelve egy $\Phi(A) \in \mathrm{Ob}\mathcal{D}$ objektum, és minden $u \in \mathrm{Mor}\mathcal{C}$-hez egy $\Phi(u) \in \mathrm{Mor}\mathcal{D}$ morfizmus.

(2) $\Phi(1_A) = 1_{\Phi(A)}$.

(3) Φ szorzattartó: Ha $\Phi(uv) = \Phi(u)\Phi(v)$, akkor kovariáns funktorról beszélünk; a $\Phi(uv) = \Phi(v)\Phi(u)$ esetben pedig kontravariánsról.

Azt az $I_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$ funktort, amely $\mathcal{C}$ minden objektumának és morfizmusának önmagát felelteti meg, a $\mathcal{C}$ identitásfunktorának nevezzük. □

Megjegyzés. Ez a definíció a 9.33. definíció általánosítása. □

Értelmezhetjük a funktorok szorzatát, amelyről triviálisan belátható, hogy ismét funktor:

15.8. Tétel. *Ha $\Phi : \mathcal{C} \to \mathcal{D}$ és $\Psi : \mathcal{D} \to \mathcal{E}$ funktorok, akkor a $\Psi\Phi(A) = \Psi(\Phi(A))$ és $\Psi\Phi(u) = \Psi(\Phi(u))$ definícióval egy $\Psi\Phi : \mathcal{C} \to \mathcal{E}$ funktort nyerünk, amelyet az eredeti két funktor (szereplő sorrendben vett) szorzatának nevezünk.*

Ha mindkét tényező kovariáns vagy mindkét tényező kontravariáns, akkor a szorzat kovariáns; ha a két tényező egyike kovariáns és a másik kontravariáns, akkor a szorzat kontravariáns. ■

Az alábbiakban belátjuk, hogy minden kontravariáns funktor visszavezethető egy kovariáns funktorra, felhasználva az úgynevezett oppozit (ellentétes) kategóriát; és egy erre képező rögzített kontravariáns funktort.

15.9. Definíció. A $\mathcal{C}$ kategória $\mathcal{C}^{\mathrm{op}}$ oppozit kategóriáját a következőképpen értelmezzük:

(1) Legyen $\mathrm{Ob}\mathcal{C}^{\mathrm{op}} = \mathrm{Ob}\mathcal{C}$ és $\mathrm{Mor}\mathcal{C}^{\mathrm{op}} = \mathrm{Mor}\mathcal{C}$.

(2) Az oppozit kategóriában az A, B objektumpárhoz hozzárendelt morfizmushalmazra legyen $\hom^{\mathrm{op}} = \hom(B, A)$.

(3) Az oppozit kategória morfizmusaira a következőképpen definiálunk szorzást az eredeti kategóriában megadott szorzás felhasználásával: Ha $u \in \hom^{\mathrm{op}}(A, B)$ és $v \in \hom^{\mathrm{op}}(B, C)$, akkor ezek $u \circ v$ szorzata legyen vu.

15.10. Tétel. *A 15.9. definícióban kategóriát definiáltunk. $(\mathcal{C}^{op})^{op} = \mathcal{C}$. Minden objektumnak, illetve morfizmusnak önmagát megfeleltetve egy $\nabla_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}^{op}$ kontravariáns funktort kapunk. A $\nabla_{\mathcal{C}}$ funktor után a $\nabla_{\mathcal{C}^{op}}$ funktort alkalmazva, az identitásfunktort nyerjük. Bármely kontravariáns $\Phi : \mathcal{C} \to \mathcal{D}$ funktorhoz létezik olyan egyértelműen meghatározott Ψ_1 és Ψ_2 kovariáns funktor, amelyekre $\Phi = \Psi_1\nabla_{\mathcal{C}} = \nabla_{\mathcal{D}}\Psi_2$ teljesül.*

Bizonyítás. Csupa nyilvánvaló állítást kell belátni; így megelégszünk ezek felsorolásával. Először is be kell látni, hogy a definiált szorzás valóban értelmezett. Ezután be kell látni a szorzás asszociativitását; majd azt, hogy 1_A az oppozit kategóriában is identitás. A további állítások is triviálisan beláthatók. ■

A szabad algebrák általánosítása előtt még szükségünk van a természetes transzformáció fogalmára.

15.11. Definíció. Legyen $\Phi : \mathcal{C} \to \mathcal{D}$ és $\Psi : \mathcal{C} \to \mathcal{D}$ két kovariáns funktor. Ezeknek egy $\chi : \Phi \to \Psi$ természetes transzformációján olyan $\chi : \mathrm{Ob}\mathcal{C} \to \mathrm{Mor}\mathcal{D}$ megfeleltetést értünk, amelynek a következő tulajdonságai vannak:

(1) $\chi(A) \in \hom(\Phi(A), \Psi(A))$.

(2) Ha $A, B \in \mathrm{Ob}\mathcal{C}$ és $u \in \hom(A, B)$, akkor a

$$\begin{array}{ccc} \Phi(A) & \xrightarrow{\Phi(u)} & \Phi(B) \\ {\scriptstyle\chi(A)}\downarrow & & \downarrow{\scriptstyle\chi(B)} \\ \Psi(A) & \xrightarrow{\Psi(u)} & \Psi(B) \end{array}$$

diagram kommutatív.

Ha $\chi(A)$ mindig izomorfizmus, akkor természetes izomorfizmusról beszélünk. □

A természetes transzformáció valójában annak a fogalomnak a pontos megfogalmazása, amely az előzőekben már olyan sokszor előfordult. A definíció azt fejezi ki, hogy a $\Phi(A)$-t $\Psi(A)$-ba vivő morfizmus előre és „egységesen" lett kiválasztva. Ez a morfizmus persze az A-tól függ, de a „megadásmód" már független. Érdemes végignézni, hogy a szereplő konkrét esetek valóban természetes transzformációk voltak. Mi itt most csak egyetlen példát nézünk meg.

A 9.64. tétel szerint: „Létezik egy $\mathrm{Hom}(\mathcal{A}, \mathcal{B}) \otimes \mathcal{C} \to \mathrm{Hom}(\mathcal{A}, \mathcal{B} \otimes \mathcal{C})$ természetes homomorfizmus".

A kényelem kedvéért Abel-csoportokra szorítkozzunk. A $\mathcal{C}$ kategória objektumai legyenek az Abel-csoportokból képezett (A, B, C) alakú rendezett hármasok. A morfizmusok csoporthomomorfizmus-hármasok; amelyeket a „variancia" figyelembevételével a következőképpen definiálunk: $(\alpha, \beta, \gamma) : (A, B, C) \to (A', B', C')$ azt jelenti, hogy $\alpha : A \leftarrow A'$, $\beta : B \to B'$, $\gamma : C \to C'$ egy-egy homomorfizmus. (Az első komponensben valójában az Abel-csoportok oppozit kategóriája szerepel.)

A $\mathcal{D}$ kategória elemei az Abel-csoportok, a morfizmusok a homomorfizmusok.

A 9.36. és a 9.54. tétel alapján mind $\Phi(A, B, C) = \mathrm{Hom}(A, B) \otimes C$, $\Phi(\alpha, \beta, \gamma) = \mathrm{Hom}(\alpha, \beta) \otimes \gamma$, mind $\Psi(A, B, C) = \mathrm{Hom}(A, B \otimes C)$, $\Psi(\alpha, \beta, \gamma) = \mathrm{Hom}(\alpha, \beta \otimes \gamma)$ egy-egy funktort definiál, amelyekre

$$\Phi : \mathcal{C} \to \mathcal{D} \qquad \text{és} \qquad \Psi : \mathcal{C} \to \mathcal{D} \qquad \text{igaz.}$$

E definíciókkal az adódik, hogy $f \in \mathrm{Hom}(A, B)$, $c \in C$ és $g \in \mathrm{Hom}(A, B \otimes C)$ esetén

$$\Phi(\alpha, \beta, \gamma) : f \otimes c \to \beta f \alpha \otimes \gamma c \qquad \text{és} \qquad \Psi(\alpha, \beta, \gamma) : g \to (\beta \otimes \gamma) g \alpha.$$

Mármost, a kívánt természetes transzformáció $\chi(A, B, C) : f \otimes c \to g$, ahol tetszőleges A-beli a-ra $g(a) = f(a) \otimes c$.

A kapott morfizmusokat megfelelően χ-vel, illetve χ'-vel jelölve, azt kell belátni, hogy

$$(\beta \otimes \gamma)[\chi(f \otimes c)]\alpha = \chi'(\beta f \alpha \otimes \gamma c).$$

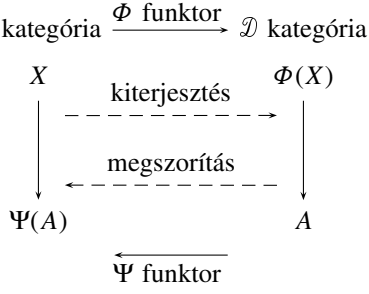
Ezek egyenlősége azt jelenti, hogy minden A-beli a elemet ugyanabba visznek. Ez a $(\beta \otimes \gamma)(f(\alpha a) \otimes c) = (\beta f(\alpha a)) \otimes \gamma c$ teljesülését kívánja meg, ami a tenzorszorzat tulajdonságai alapján igaz. (Megjegyezzük, hogy a fenti bizonyítást a modulusok esetén már az első kötetben elvégeztük, itt most csak azt néztük végig, hogy az ottani bizonyítás valóban a kívánt természetes transzformáció létezését adta.)

Ezek után rátérünk a szabad algebrák fogalmának az általánosítására. Mindenekelőtt tekintsünk egy X halmazt, és legyen $\Phi(X)$ az X generálta szabad algebra. Ez azt jelenti, hogy bármely A algebra esetén tetszőleges X-ből A-ba menő leképezés kiterjeszthető $\Phi(X)$-ből A-ba menő homomorfizmussá. Az első, amit észre kell venni, hogy két, különböző típusú morfizmus szerepel; a megadott halmazleképezés és a kiterjesztett algebrahomomorfizmus. A homomorfizmussal nincs is semmi probléma, mert algebrát képez algebrába. Ezzel szemben a megadott leképezés „más típusú" objektumok között adott. Éppen ezért célszerű ezt a leképezést úgy kezelni, hogy az nem az A algebrába, hanem annak a tartóhalmazába képez, jelölje e tartóhalmazt $\Psi(A)$.

Eddigi megállapításainkat tehát a következőképpen foglalhatjuk össze. Adott két kategória, a halmazok $\mathcal{C}$ kategóriája és az algebrák $\mathcal{D}$ kategóriája. Adott ezenkívül egy Φ, illetve Ψ leképezés, amelyek $\mathrm{Ob}\mathcal{C}$-t $\mathrm{Ob}\mathcal{D}$-be, illetve $\mathrm{Ob}\mathcal{D}$-t $\mathrm{Ob}\mathcal{C}$-be képezik.

Mielőtt a megfogalmazásban tovább mennénk, belátjuk, hogy az adott konkrét esetben ezek a megfeleltetések „kiterjeszthetők" funktorokká. Legyen ugyanis $f : X \to Y$ tetszőleges halmazleképezés. Mivel $\Phi(X)$ az X generálta szabad algebra, ezért f egyértelműen kiterjeszthető $\Phi(X)$-nek $\Phi(Y)$-ba való homomorfizmusává. Jelöljük ezt a homomorfizmust $\Phi(f)$-fel. Világos, hogy ha létezik a gf szorzat, akkor teljesül a $\Phi(gf) = \Phi(g)\Phi(f)$ összefüggés; továbbá a kiterjesztés egyértelműsége miatt az identitásnak identitás felel meg. ψ viszont triviálisan funktornak tekinthető; egyszerűen csak azt kell tenni, hogy minden algebrahomomorfizmusnak önmagát – mint halmazleképezést – feleltetjük meg.

Visszatérve az előbbi megállapításokra, a következőket mondhatjuk. Valahányszor megadunk egy $f : X \to \Psi(A)$ „halmazhomomorfizmust", ehhez mindig egyértelműen találhatunk egy $f^* : \Phi(X) \to A$ algebrahomomorfizmust, ami f kiterjesztése. Ez a megfeleltetés fordított irányban is létrehozható: a $g : \Phi(X) \to A$ algebrahomomorfizmusnak a megszorítása ugyanis egy $g' : X \to \Psi(A)$ halmazhomomorfizmust ad. Ezen felül nyilvánvalóan teljesül az $(f^*)' = f$ és $(g')^* = g$ összefüggés. Ezt a helyzetet rajzban is ábrázolhatjuk:



Tekintettel arra, hogy a halmazleképezés algebrahomomorfizmussá való kiterjesztése, valamint e homomorfizmusnak a generátorhalmazra való megszorítása teljesen egyöntetűen történt, ezért úgy látszik, hogy itt egy „természetes" izomorfizmus létezik. Ennek a megfogalmazása azonban újabb bonyodalmat okoz. Hiszen egy természetes izomorfizmus objektumok közti izomorfizmusok rendszere. Itt viszont a $\hom(X, \Psi(A))$-t kellene izomorf módon leképezni a $\hom(\Phi(X), A)$-ba. Ezt a látszólagos ellentmondást úgy oldhatjuk fel, hogy olyan kategóriát tekintünk, amelynek az objektumai a $\hom(\square, \square)$ alakú halmazok. Evégett elegendő az összes halmazok kategóriáját tekinteni. A továbbiakban az összes halmazok kategóriáját $\mathscr{S}$-sel fogjuk jelölni.

Mivel természetes izomorfizmusról csak akkor tudunk beszélni, ha két funktor adott, ezért két olyan funktort kellene keresni, amely „valahonnét" az $\mathscr{S}$-be képez úgy, hogy az objektumoknak mindig a $\hom(\square, \square)$ alakú halmaz felel meg. Ha megnézzük, hogy e halmaznak mitől kell függnie, akkor látjuk, hogy mindkét esetben egy $\mathscr{C}$-beli és egy $\mathscr{D}$-beli objektumtól függ, sőt, ugyanattól az objektumpártól. Ezek után remélhető, hogy itt valóban két funktor szerepel, amelyek a $\mathscr{C} \times \mathscr{D}$ kategóriát képezik le az $\mathscr{S}$-be. Ehhez természetesen meg kell adni a morfizmusok képeit is, és meg kell nézni, hogy a vizsgált funktorok kovagy kontravariánsak-e.

Belátjuk, hogy e funktorok első komponensükben kontravariánsak, másodikban kovariánsak. Más szóval mindkét funktor a $\mathscr{C}^{\mathrm{op}} \times \mathscr{D}$ kategóriát képezi $\mathscr{S}$-be. A $\mathscr{C}^{\mathrm{op}} \times \mathscr{D}$ kategóriában az objektumok és a morfizmusok a következőképpen adhatók meg. Az objektumok olyan (X, A) párok, amelyekre $X \in \mathrm{Ob}\mathscr{C}$ és $A \in \mathrm{Ob}\mathscr{D}$. Egy $(u, v) : (X, A) \to (Y, B)$

morfizmus pedig olyan párral adható meg, amelyre $u : Y \to X$ és $v : A \to B$. Két funktort adunk meg, a $\Sigma_1 : \mathscr{C}^{\mathrm{op}} \times \mathscr{D} \to \mathscr{S}$ és a $\Sigma_2 : \mathscr{C}^{\mathrm{op}} \times \mathscr{D} \to \mathscr{S}$ funktort:

1. Az objektumok képét a kívánalmaknak megfelelően definiáljuk: $\Sigma_1 : (X, A) \to \hom(X, \Psi(A))$ és $\Sigma_2 : (X, A) \to \hom(\Phi(X), A)$.

2. A morfizmusok képének meghatározása végett tekintsünk egy morfizmuspárt: $X \xrightarrow{u} Y$ és $A \xrightarrow{v} B$.

Tekintettel arra, hogy mind $\Sigma_1(u, v)$, mind $\Sigma_2(u, v)$ morfizmushoz (pontosabban leképezéshez) rendel morfizmust, ezért hatásukat célszerűbb diagramokon megadni. A

$$f \xrightarrow{\Sigma_1(u,v)} \Phi(v) f u \qquad \text{és} \qquad g \xrightarrow{\Sigma_2(u,v)} v g \Phi(u)$$

leképezések kommutatívvá teszik – megfelelően – az alábbi diagramokat:

$$\begin{array}{ccc} X & \xleftarrow{u} & Y \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \Phi(v) f u} \\ \Psi(A) & \xrightarrow[\Psi(v)]{} & \Psi(B) \end{array} \qquad \text{és} \qquad \begin{array}{ccc} \Phi(X) & \xleftarrow{\Phi(u)} & \Phi(Y) \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle v g \Phi(u)} \\ A & \xrightarrow[v]{} & B \end{array} .$$

Végső célunk most annak a bizonyítása, hogy a kiterjesztés valójában Σ_1-nek Σ_2-be való természetes izomorfizmusa. Az (X, A) objektumnak megfelelő $\chi(X, A)$ leképezés már adott, tehát e leképezés a kiterjesztés; és azt kell belátnunk, hogy az alábbi diagram kommutatív:

$$\begin{array}{ccc} \hom(X, \Psi(A)) & \xrightarrow{\Sigma_1(u,v)} & \hom(Y, \Psi(B)) \\ {\scriptstyle \chi(X,A)}\downarrow & & \downarrow{\scriptstyle \chi(Y,B)} \\ \hom(\Phi(X), A)) & \xrightarrow{\Sigma_2(u,v)} & \hom(\Phi(Y), B \end{array} .$$

A kommutativitás bizonyítása végett tekintsük a $\hom(X, \Psi(A))$ egy tetszőleges $f : X \to \Psi(A)$ elemét. Ennek képét a két úton kiszámolva: először vízszintesen, majd függőlegesen haladva $(\Psi(v) f u)^*$, a másik úton pedig $v f^* \Phi(u)$ adódik (a * jel a leképezések homomorfizmussá való kiterjesztését jelöli). Az elsőnek Y-ra való megszorítása, mint láttuk, $\Psi(v) f u$. A másodiknak az Y-ra való megszorítását a következőképpen határozhatjuk meg. Mivel $\Phi(u)$ az u-nak a kiterjesztése, ezért az Y halmazon mindketten ugyanúgy hatnak, így $\Phi(u)$-nak az Y-ra való megszorítása u. Ezután f^*-ot u-nak a képére, azaz X-re kell megszorítani, ami nem más, mint f. Végül v megszorítása következik, ami definíció szerint $\Psi(v)$. A kommutativitás tehát igaz.

Mielőtt a kapott eredményt tételszerűen megfogalmaznánk, elnevezzük azt a kapcsolatot, amely a $\mathscr{C}$ és $\mathscr{D}$ kategória vizsgált funktorai között fennáll:

15.12. Definíció. Legyenek adva a $\mathscr{C}$ és $\mathscr{D}$ kategóriák úgy, hogy mindkét esetben minden egyes $\hom(\square, \square)$ egy rögzített $\mathscr{K}$ kategória objektuma.

Legyenek $\Phi : \mathscr{C} \to \mathscr{D}$ és $\Psi : \mathscr{D} \to \mathscr{C}$ funktorok, és definiáljuk a $\Sigma_i : \mathscr{C}^{\mathrm{op}} \times \mathscr{D} \to \mathscr{K}$ funktorokat $(i = 1, 2)$ a következőképpen:

$$\Sigma_1(X, A) = \hom(X, \Psi(X)) \qquad \text{és} \qquad \Sigma_2(X, A) = \hom(\Phi(X), A);$$

továbbá, ha a megfelelő kategóriákban $u : Y \to X$ és $v : A \to B$, akkor adott $f \in \in \hom(X, \Psi(A))$ és $g \in \hom(\Phi(X), A)$ esetén legyen $\Sigma_1(u, v) : f \to \Psi(v) f u$ és $\Sigma_2(u, v) : g \to vg\Phi(u)$.

Ha létezik egy $\chi : \Sigma_1 \to \Sigma_2$ természetes izomorfizmus, akkor azt mondjuk, hogy (Φ, Ψ) a $\mathcal{K}$-ra nézve adjungált pár (Φ a Ψ-nek bal oldali és Ψ a Φ-nek jobb oldali adjungáltja). □

15.13. Tétel. *A szabad generálás és a tartóhalmazképzés $\mathcal{S}$-re nézve adjungált pár.*

Hasonló eredmény mondható ki, ha például az egyik funktor minden félcsoportnak megfelelteti az általa generált félcsoportalgebrát (rögzített test felett) és a másik funktor minden e test feletti algebrának megfelelteti a multiplikatív félcsoportját.

Még egy tételt bizonyítunk be, amely az előzőtől egészen elütő típusú adjungált párra ad példát.

15.14. Tétel. *Legyen S egy kommutatív gyűrű, $\mathcal{C} = \mathcal{D}$ az unitér S-modulusok kategóriája. Rögzített B modulus esetén a Φ, illetve Ψ funktor feleltesse meg minden egyes A, illetve C modulusnak az $A \times B$, illetve* $\mathrm{Hom}(B, C)$ *modulust.*

Ekkor (Φ, Ψ) az unitér S-modulusok kategóriájára nézve adjungált pár.

Bizonyítás. Mivel tetszőleges A, B unitér S-modulusokra $\mathrm{Hom}(A, B)$ is unitér S-modulus, ezért $\mathcal{K}$-nak valóban választhatjuk a fenti kategóriát. Bizonyítandó a $\hom(A, \Psi(C))$ és $\hom(\Phi(A), C)$ közötti természetes izomorfizmus létezése. Ez a fenti funktorok definíciója szerint $\mathrm{Hom}(A, \mathrm{Hom}(B, C))$ és $\mathrm{Hom}(A \times B, C)$ természetes izomorfizmusát jelenti. Márpedig ez nem más, mint a 9.63. tétel állítása. ■

15.3. Kategóriák realizációja

Amikor konkrét kategóriákról beszéltünk, akkor megemlítettük azt a lehetőséget, hogy olyan kategóriák is tekinthetők konkrétnak, amelyeket így tudunk ábrázolni, realizálni. Ehhez szükségünk van a „részkategória" és a „beágyazás" fogalmára, amely kategóriák esetében éppen úgy nem egyértelmű, mint a relációstruktúráknál.

15.15. Definíció. Legyen $\mathcal{C}$ egy adott kategória, és adott $A, B \in \mathrm{Ob}(\mathcal{C})$ esetén jelölje $\hom_{\mathcal{C}}(A, B)$ a megfelelő $\mathcal{C}$-beli morfizmusok halmazát.

$\mathcal{C}' \subseteq \mathcal{C}$ a $\mathcal{C}$-nek részkategóriája, ha a következők teljesülnek:

(1) $\mathrm{Ob}\mathcal{C}'$ része (részosztálya) $\mathrm{Ob}\mathcal{C}$-nek.

(2) Bármely $A, B \in \mathrm{Ob}(\mathcal{C}')$ esetén $\hom_{\mathcal{C}'}(A, B)$ része (részhalmaza) $\hom_{\mathcal{C}}(A, B)$-nek.

(3) Ha A egy $\mathcal{C}'$-beli objektum, akkor a $\mathcal{C}'$-beli $1'_A$ identitás megegyezik a $\mathcal{C}$-beli 1_A identitással.

(4) Ha $u, v \in \mathrm{Mor}\mathcal{C}'$, és $\mathcal{C}$-ben létezik az uv szorzat, akkor ez a szorzat $\mathcal{C}'$-ben is létezik és megegyezik az eredetivel.

Ha a (2)-ben szereplő halmazok mindig egyenlők (azaz bármely $A, B \in \mathrm{Ob}(\mathscr{C}')$ esetén $\hom_{\mathscr{C}'}(A, B) = \hom_{\mathscr{C}}(A, B)$), akkor teljes részkategóriáról beszélünk. □

15.16. Definíció. Egy $\Phi : \mathscr{C} \to \mathscr{D}$ funktor hű(séges), ha bármely $A, B \in \mathrm{Ob}\mathscr{C}$ esetén a $\Phi : \hom_{\mathscr{C}}(A, B) \to \hom_{\mathscr{D}}(\Phi(A), \Phi(B))$ leképezés injektív.

Egy $\Sigma : \mathscr{C} \to \mathscr{S}$ hű funktort felejtő funktornak nevezünk ($\mathscr{S}$ a halmazok kategóriája).

Egy $\mathscr{C}$ kategória konkretizálható, ha létezik egy $\Sigma : \mathscr{C} \to \mathscr{S}$ felejtő funktor. Ekkor azt mondjuk, hogy $(\mathscr{C}, \Sigma)$ egy konkrét kategória. □

Megjegyzések. 1. Ha Φ hű, attól még lehetséges, hogy különböző (A, B) és (C, D) párokra, ha $A \xrightarrow{u} B$ és $C \xrightarrow{v} D$, akkor $\Phi(u) = \Phi(v)$.

2. A konkretizálható kategória itt definiált fogalma nem „egészen" ugyanaz, mint a konkrét kategória „naiv" leírása. Természetesen a funktorral való definíció precízebb, de zavaró az a különbség, hogy itt különböző $\mathscr{C}$-beli objektumokhoz tartozhat ugyanaz a halmaz. Ezen viszont könnyen segíthetünk a funktor megváltoztatásával. Adott $\Sigma : \mathscr{C} \to \mathscr{S}$ felejtő funktorhoz definiáljuk a $\Sigma' : \mathscr{C} \to \mathscr{S}$ felejtő funktort a következőképpen: Ha A egy $\mathscr{C}$-beli objektum, akkor legyen $\Sigma'(A) = \{(x, A) \mid x \in \Sigma(A)\}$ (mivel A egy objektum, ennek van értelme), ha $A \xrightarrow{u} B$, akkor legyen $\Sigma' : (x, A) \mapsto ([\Sigma(u)](x), \Sigma(A))$, ahol x végigfut $\Sigma(A)$ elemein. Könnyen látható, hogy ez a funktor eleget tesz a szemlélet kívánalmainak. (Az világos, hogy a „naiv" definíció esetében az itteni definíció szerint is konkrét kategóriát kapunk. Ebben az esetben *természetes felejtő funktorról* vagy *tartóhalmazfunktorról* beszélünk.)

3. A $(\mathscr{C}, \Phi)$ konkrét kategória esetén $\Phi(A)$ az A objektum *tartóhalmaza*, míg a $\Phi(u)$ leképezés az u morfizmus *tartóleképezése*.

4. Igazából tetszőleges hű funktor is nevezhető felejtő funktornak. Ilyen felejtő funktort kapunk, ha egy gyűrűben „elfelejtjük" a szorzást, vagy ha egy csoportban „elfelejtjük" az invertálást. A „célkategóriában" minden esetben több objektum is van. Az utóbbi esetben minden félcsoport-homomorfizmus egy csoporthomomorfizmus „képe", az előbbi esetben viszont a „*tartó Abel-csoportnak*" van olyan homomorfizmusa, amely nem gyűrűhomomorfizmus. □

A gyűrű-tartócsoport és csoport-félcsoport esetek különbözősége alapján indokolt a következő

15.17. Definíció. A $\Phi : \mathscr{C} \to \mathscr{D}$ funktort teljesnek nevezzük, ha minden $\mathscr{C}$-beli A, B objektumpárhoz és minden $\mathscr{D}$-beli $v \in \hom_{\mathscr{D}}(\Phi(A), \Phi(B))$ morfizmushoz létezik olyan $\mathscr{C}$-beli $A \xrightarrow{u} B$ morfizmus, amelyre $v = \Phi(u)$.

A $\Phi : \mathscr{C} \to \mathscr{D}$ funktor egy-egyértelmű, ha különböző objektumok képe különböző; és tetszőleges $\mathscr{C}$-beli A, B párra Φ injektív módon képezi le $\hom_{\mathscr{C}}(A, B)$-t $\hom_{\mathscr{D}}(\Phi(A), \Phi(b))$-re.

Egy teljes és egy-egyértelmű $\Phi : \mathscr{C} \to \mathscr{D}$ funktor neve teljes beágyazás. Ha ilyen funktor létezik, akkor azt mondjuk, hogy $\mathscr{C}$ teljesen beágyazható $\mathscr{D}$-be. □

Megjegyzések. 1. Egy teljes funktor esetében természetesen lehet különböző morfizmusoknak ugyanaz a képe. Ha a funktor egy-egyértelmű, akkor ez nem lehetséges.

2. A teljes beágyazás azt jelenti, hogy az első kategória izomorf a másodiknak egy teljes részkategóriájával.

Egy kategóriát úgy tudunk elképzelni, hogy vesszük halmazok egy osztályát, és ezeken bizonyos halmazleképezéseket. Ez egy konkrét kategória. A másik lehetőség az, hogy veszünk „pontokat” és közöttük húzott nyilakat (bármely két pont között halmaznyit). Ha ahelyett, hogy veszünk pontokat, azt mondjuk – amit még el lehet képzelni –, hogy vesszük pontok egy halmazát, akkor egy „kis kategóriához” jutunk.

15.18. Definíció. Ha egy kategóriában az objektumok száma halmaznyi, akkor kis kategóriának nevezzük. □

15.19. Tétel. *Minden kis kategória konkretizálható.*

Bizonyítás. A bizonyítás elve ugyanaz, mint a csoportokra vonatkozó Cayley-tételé, illetve ennek félcsoportokra vonatkozó általánosításáé.

Legyen $\mathcal{C}$ egy kis kategória és definiáljuk a $\Sigma: \mathcal{C} \to \mathcal{S}$ funktort a következőképpen.

Minden objektumot helyettesítsünk a „belefutó” nyilakkal:

$\mathcal{C}$-beli A objektumra és x morfizmusra legyen $x \in \Sigma(A)$, pontosan akkor, ha van olyan $\mathcal{C}$-beli B objektum, hogy $x \in \hom(B, A)$.

$\mathcal{C}$-beli $A \xrightarrow{u} B$ morfizmus esetén, tetszőleges $x \in \Sigma(A)$ elemre legyen $\Sigma(u) : x \mapsto ux$.

Annak a bizonyítását, hogy ez valóban egy teljes beágyazás, az olvasóra bízzuk. ■

Megjegyzés. A fenti beágyazást felhasználva meg lehet mutatni, hogy egy kis kategóriát algebrák osztályába is be lehet ágyazni (teljes beágyazással). A technikai jellegű bizonyítás azon múlik, hogy felismerhető elemekkel, illetve műveletekkel „kódolunk”. □

Nem kell azt gondolni, hogy minden kategória konkretizálható. Az előző tétel alapján csak olyan kategória adhat ellenpéldát, amelynek az objektumai egy valódi osztályt alkotnak. Előkészületül egy olyan feltételt mutatunk meg, amely halmazok kategóriájában teljesül.

Tekintsük a halmazok kategóriáját. Legyen $A, B \in \mathcal{S}$ rögzített. Tetszőleges $X \xrightarrow{a} A$ és $X \xrightarrow{b} B$ esetén a direkt szorzat tulajdonsága szerint e két leképezés keresztülvezethető az $A \times B$ direkt szorzaton: $a = a_1 x$, $b = b_1 x$, ahol $X \xrightarrow{x} A \times B$. Mint minden leképezés, x is (egyértelműen) felbontható $x = uv$ alakba, ahol $X \xrightarrow{v} P$ szürjektív és $P \xrightarrow{u} A \times B$ injektív. Ez utóbbi azt jelenti, hogy P tekinthető az $A \times B$ részhalmazának, így „kiválasztására” halmaznyi lehetőség van. Tekintsük végül az $a' = a_1 u$ és $b' = b_1 v$ leképezéseket. Ezekre vonatkozik *Isbell feltétele*:

15.20. Tétel. *Tetszőleges $A \xrightarrow{f} Y$ és $B \xrightarrow{g} Y$ esetén $fa = gb$ pontosan akkor igaz, ha $fa' = gb'$.*

Bizonyítás. Ha $fa' = gb'$, akkor $fa = fa'v = gb'v = gb$. Ha viszont $fa'v = fa = gb = gb'v$, akkor v szürjektivitása miatt v epimorfizmus, tehát $fa' = gb'$. ■

15.21. Következmény. *Legyen az* $X \xrightarrow{a} A$, $X \xrightarrow{b} B$, $Z \xrightarrow{c} A$, $Z \xrightarrow{d} B$ *leképezésekre* $(a, b) \sim (c, d)$, *ha bármely* $A \xrightarrow{f} Y$ *és* $B \xrightarrow{g} Y$ *leképezések esetén az* $fa = gb$ *és* $fc = gd$ *feltételek bármelyikéből következik a másik.*

Ekkor $\sim$ *egy ekvivalenciareláció, és az ekvivalenciaosztályok halmaznyian vannak.*

Bizonyítás. $\sim$ triviálisan ekvivalenciareláció. A 15.20. tétel szerint a két feltétel helyett írható (a megfelelő a', b', c', d' leképezésekkel) $fa' = gb'$ és $fc' = gd'$. A lehetséges (a', b') párokra annyi lehetőség van, ahány $P \subseteq A \times B$ létezik; azaz halmaznyi. ■

Ezek után megadjuk az Isbell által konstruált példát:

15.22. Tétel. *Létezik nem konkretizálható kategória.*

Bizonyítás. Olyan kategóriát kell konstruálni, amelyikre nem teljesül a 15.21. korollárium feltétele. Mivel kis kategória konkretizálható, ezért a szereplő kategória objektumai valódi osztályt kell, hogy alkossanak.

Legyen I egy valódi osztály (például a számosságok osztálya).

$\mathcal{C}$ objektumai legyenek X_i, Y_i $(i \in I)$ és még két objektum, A és B. Megadjuk a morfizmusokat:

(1) Bármely $\mathcal{C}$-beli C objektumra $\hom(\mathcal{C}, \mathcal{C})$ egyetlen eleme 1_C.

(2) A $\hom(X_i, A)$, $\hom(X_i, B)$, $\hom(A, Y_j)$, $\hom(B, Y_j)$ halmazoknak egyetlen elemük van – megfelelően – a_i, b_i, f_j, g_j.

(3) $\hom(X_i, Y_i)$ kételemű, ezeket $a_{i,i}$, $b_{i,i}$ jelöli; míg $i \neq j$ esetén $\hom(X_i, Y_j)$ egyetlen eleme $a_{i,j}$.

(4) Az összes többi $\hom(\square, \square)$ üres.

A szorzás definíciója következik. Az triviális, ha valamelyik tényező az identitás. Egyébként csak $X \to A$ és $A \to Y$, illetve $X \to B$ és $B \to Y$ alakú morfizmusoknak létezhet szorzata. Legyen

$$f_j a_i = a_{i,j} \quad (i, j \in I) \qquad \text{és} \qquad g_j b_i = \begin{cases} b_{i,i}, & \text{ha } j = i \\ a_{i,j}, & \text{máskor.} \end{cases}$$

Könnyen ellenőrizhető, hogy $i \neq j$ esetén (a_i, b_i) és (a_j, b_j) nem ekvivalensek. Mivel I valódi osztály, ezért $\mathcal{C}$ nem konkretizálható. ■

Térjünk most vissza a 15.19. tételre és az utána következő megjegyzésre. A tételben szereplő Σ funktorról nem tettük fel, hogy teljes. Ez nem is tehető fel. Egy n elemű A halmaz esetén a $\hom_{\mathcal{S}}(A, A)$ elemszáma n^n, ami például nem lehet három. Így annak a kis kategóriának, amely egy objektumból, valamint az objektumot önmagába „képező” háromelemű csoportból áll, nincs hű reprezentációja $\mathcal{S}$-ben.

Mint a csoportok automorfizmuscsoportjának vizsgálatánál láttuk, a csoportok kategóriájában sem létezik hű reprezentáció. Ezzel szemben – meglepő módon – létezik hű reprezentáció a testek kategóriájában. Nevezetesen a $\mathbb{Q}(\alpha)$ test automorfizmuscsoportja a háromelemű ciklikus csoport, ha α az $x^3 - 3x + 1$ polinom gyöke (ezt láttuk!). Az is igaz,

hogy bármely csoporthoz létezik olyan test, amelynek az összes endomorfizmusai e csoporttal izomorf csoportot alkotnak.

Persze a testek kategóriája sem tartalmazhat minden lehetőséget, mert testek körében minden homomorfizmus injektív. Vannak viszont olyan kategóriák, amelyekben minden kis kategória hűen ábrázolható. Ilyenek például a hurokmentes (irányított vagy irányítatlan) gráfok, a félcsoportok és az egyértelmű faktorizációval rendelkező integritási tartományok kategóriája. Speciálisan minden csoport fellép, mint e struktúrák valamelyikének az automorfizmuscsoportja. Ezen utóbbi tételeknek a bizonyításánál nem kerülhetők el a kategóriák.

Feladatok

1. Adjunk meg „igazi” algebrák egy kategóriájában olyan i, j morfizmuspárt, amelyre ij identitás, de ji nem.

2. Legyen $\mathcal{R}$ a kommutatív gyűrűk kategóriája. Bizonyítsuk be, hogy ha $f : R \to K$ a hányadostestbe való beágyazás, akkor f nem csak monomorfizmus, de epimorfizmus is.

3. Bizonyítsuk be, hogy a $\mathbb{Z} \to \mathbb{Q}$ beágyazás nem csak a gyűrűk kategóriájában, de a csoportokéban is epimorfizmus.

4. Legyen $\mathcal{C}$ algebrák egy kategóriája és legyen $\Sigma : \mathcal{C} \to \mathcal{S}$ a tartóhalmazfunktor. Bizonyítsuk be, hogy ha a $\mathcal{C}$-beli f morfizmusra $\Sigma(f)$ izomorfizmus, akkor f is az.

5. Legyen $\mathcal{G}$ a hurokmentes gráfok kategóriája (ennek objektumai olyan $G = (X, V)$ párok, amelyekben X egy halmaz ($X \in \mathcal{S}$), $V \subseteq X \times X$ egy irreflexív és szimmetrikus reláció és morfizmusai olyan $f : G_1 \to G_2$ megfeleltetések, ahol az $f : X_1 \to X_2$ függvényre $(x, y) \in V_1$ esetén $(f(x), f(y)) \in V_2$ teljesül). Legyen $\Sigma : \mathcal{G} \to \mathcal{S}$ a tartóhalmazfunktor. Mutassuk meg, hogy van $\mathcal{G}$-ben olyan f morfizmus, amely nem izomorfizmus, noha $\Sigma(f)$ az.

Betűrendes mutató

0–1 mérték 369
2-bővítés 227

Abel-csoport 93
–, szabad 116
additív inverz, ellentett 152
adjungált pár 384
alaptest 178
algebra 286
–, Boole- 352
–, ciklikus 31
–, csoport- 287
–, félcsoport- 286
–, kifejezés- 313
–, Lie- 305
–, reláció- 366
–, szabad 314
–, szubdirekt irreducibilis 325
–, triviális 37
algebrai bővítés 188
– –, véges 188
– elem 178
– függés 200, 201
– háló 48
– lezárás 50
– struktúra (általános) 27
alsó korlát 20
általános lineáris csoport 141
– n-edfokú polinom 220
antiszimmetrikus reláció 17
archimedesi elrendezés 364
Artin-gyűrű, bal oldali 281
asszociált elemek 168
atom 354
–, duális (koatom) 354
atomos háló 354
automorfizmus 32
–, belső 101
–, relatív 207
azonosság algebrában 320
– algebrák egy osztályában 320
azonossághalmaz modellje 321
azonosságokkal definiálható osztály 321
azonosságokkal definiált osztály 321

balannullátor 156
balideál 154
–, nilpotens 281
balinverz (jobbinverz) monoidban 65
bal oldali (jobb oldali)
  egyszerűsítési szabály 73
bal oldali modulus 238
– – nullosztó 153
balzérus félcsoport 64
bázis 94
bázistranszformáció, elemi 143
beágyazás, teljes 385
behelyettesítés 324
belső automorfizmus 101
– direkt szorzat 93
biadditív függvény 262
bihomomorfizmus 262
bijekció 18
bináris művelet 27
binom 214
Boole-algebra (Boole-háló) 352
– -gyűrű 354
– -háló (Boole-algebra) 352
bővítés, algebrai 188
– Galois-csoportja 207
–, normális 206
–, szeparábilis 198
–, testé 178
–, tiszta transzcendens 202
–, véges 188
–, véges algebrai 188

Cartan-részalgebra 306
centralizátor 105
centrum 101
ciklikus (rész-)csoport 78
– algebra 31
– permutálás 127

ciklus 252
– hossza 128
ciklustényező 127

csillag, Lie-algebráé 307
csoport 72
– -algebra 287
– exponense 94
– -karakter 290
– kommutátorlánca 123
– rendje 79
– reprezentációja 288
–, *p*- 94
–, általános lineáris 141
–, ciklikus 78
–, egyszerű 88
–, elrendezett 358
–, feloldható 122
–, homológia- 252
–, nilpotens 125
–, permutáció- 125
–, projektív lineáris 142
–, részbenrendezett 357
–, speciális lineáris 142
–, szabad 115
–, szimmetrikus 125
–, szimplektikus 146
–, torzió- 97
–, triviális 78
–, unitér 146
csoportok direkt szorzata 89
–, hálószerűen rendezett 358
–, kivételes Lie-típusú 147
–, klasszikus egyszerű 147
–, ortogonális 146
csúcs (gráfban) 248

Dedekind-gyűrű 273
definiáló reláció 116
déloszi probléma (kockakettőzés) 228
Descartes-szorzat 15
diagram 248
–, kommutatív 249
diagramvadászat 258
dimenziófüggvény 348
direkt összeg, ideáloké 179
– –, modulusoké 239
direkt szorzat 36
– –, belső, külső 93
– –, csoportoké 89
– –, diszkrét 93
– –, modulusoké 239
– –, relációalgebráké 367
– –, teljes (komplett) 93
diszjunkt (idegen) halmazok 14
– permutálások 127
diszkrét direkt szorzat 93
disztributív háló 338
duális atom (vagy koatom) 354
– ideál (filter, szűrő) 333
– prímideál 336
dualitási elv (részbenrendezett halmazoké) 41
Dynkin-diagram 308

egész, részgyűrű felett 268
egzakt sorozat 250
egy-egyértelmű funktor 385
egyenlő számosságok 25
egyértelmű faktorizáció (felbontás) 169
egyesítés 14
egyesítés-, metszetfélháló 46
egység 168
egységelem 152
–, bal oldali, jobb oldali 63
egységelemes félcsoport 64
egységgyök, primitív 214
egyszerű bővítés, testé 178
– csoport 88
– –, sporadikus (szórványos) 147
– csoportok, klasszikus 147
– ideál 157
– testbővítés 178
egyszerűsítési szabály, bal oldali, jobb oldali 73
ekvivalenciareláció 22
ekvivalens halmazok 24
ekvivalens kúpok 377

elem, algebrai 178
–, pozitív 359
–, prímtulajdonságú 169
– rendje 80
–, transzcendens 178
elemének lenni 13
elemi bázistranszformáció 143
– formula 368
– ítéletek 367
– mátrixátalakítások 143
elemosztály konjugáltja 101
elemrendszer, független 94
ellentett (additív inverz) 152
előjelszabályok 151
elrendezés, archimedesi 364
– kiterjesztése 362
elrendezett csoport 358
– integritási tartomány 360
endomorfizmus 32
epimorfizmus 376
értékelés, kitevő- 364
–, nemarchimedesi 364
–, testé 362
– -gyűrű 163
értékkészlet 17
értelmezési tartomány 17
euklideszi gyűrű 171
– szerkesztés 226
exponens, csoporté 94

faktor 35
faktoralgebra 35
–, relációalgebráé 367
faktorcsoport 87
faktorgyűrű 157
faktorizáció (felbontás), egyértelmű 169
faktormodulus 239
félcsoport 56
–, balzérus 64
–, idempotens 67
–, jobbzérus 64
–, szabad kommutatív 66
–, szabadon generált 61
–, zéruselemes 64
félcsoportalgebra 286
felejtő funktor 385
félháló, egyesítés-, metszet- 46
félig egzakt sorozat 249
féligegyszerű gyűrű 281
féligegyszerű Lie-algebra 306
feloldható csoport 122
– Lie-algebra 306
felső korlát 20
ferdetest 154
feszített részstruktúra 40
filter, fő- 333
–, duális ideál 333
finomítás, láncé 348
–, normálláncé 118
–, valódi 118
formálisan valós test 298
formula (elemi) 368
formula, zárt 368
formulák algebrában való realizációja 368
formulák, nyílt 368
főfilter 333
főideál 155, 333
főideálgyűrű 171
főkongruencia 327
főpolinom 178
Frobenius-automorfizmus 205
funktor 253, 379
–, egy-egyértelmű 385
–, felejtő 385
–, hű(séges) 385
–, identitás- 379
–, kovariáns, kontravariáns 253, 379
–, teljes 385
függés, algebrai 200, 201
független elemrendszer 94
függvény 17
–, biadditív 262
–, injektív 18
függvények kompozíciója 18
függvények szorzata 18

Galois-csoport, bővítésé 207
Galois-megfeleltetés, Galois-kapcsolat 44
–, homogén 44
– -sel indukált lezárás 44

generált részalgebra 31
– részfélcsoport 58
generátor, szabad 115
generátorrendszer 31
generátum 31
gráf (irányított) éle 248
– csúcsai (vagy szögpontjai) 248
–, hurokmentes 17
–, irányítatlan 17
–, irányítatlan hurokmentes 17
–, irányított 17, 248
–, páros 81

gyök, ideálé 183
gyökkifejezés 214
gyökökkel elérhető test 214
gyűrű 150
–, Boole- 354
–, Dedekind- 273
–, értékelés- 163
–, euklideszi 171
–, faktor- 157
–, féligegyszerű 281
–, főideál- 171
–, hányados- 158
–, integrálisan zárt 269
–, kommutatív 150
–, lokális 161
–, maradékosztály- 157
–, Noether- 164
–, null- 151
–, nullkarakterisztikájú 177
–, nullosztómentes 153
–, p karakterisztikájú 177
–, polinom- 164
– radikálja 179
–, radikálmentes 281
–, teljes mátrix- 281
–, zéró- 151
gyűrű feletti polinomok 165
gyűrűösszeadás 150
gyűrűszorzás 150

halmaz 13
– hatványa 15
–, induktív 21
–, irányított 50
– komplementuma 15
halmazok, diszjunkt 14
– ekvivalenciája 24
–, idegen 14
–, páronként idegen 14
halmazrendszer 14
háló 46, 331
–, algebrai 48
–, atomos 354
–, Boole- 352
–, disztributív 338
– ideálja 333
–, kompakt 47
–, kompaktul generált 48
–, komplementumos 335
–, korlátos 335
–, moduláris 338
– nulleleme (egységeleme) 46
–, relatív komplementumos 335
hálószerűen rendezett csoport 358
hányados, ideáloké 179
hányadosgyűrű 158
határfüggvény 251
határozatlan 164
hatvány 58
–, Lie-algebráé 305
hatványhalmaz 15
homogén Galois-megfeleltetés 44
homológiacsoport 252
homomorfizmus 32, 366
– magja 87
homomorfizmustétel 87
hossz, ciklusé 128
–, sorozaté 249
hű(séges) funktor 385

ideál (duális ideál) 336
–, bal- 154
–, egyszerű 157
–, fő- 155, 333
– gyöke 183
– (hálóban) 51
–, hálóé 333
–, irreducibilis 180

–, jobb- 154
–, kétoldali 154
– lezártja 183
–, Lie-algebráé 305
–, maximális 157
–, prím- 161
–, primér 180
– radikálja 179
–, valódi 336
ideálháló 51
ideálok direkt összege 179
– hányadosa 179
– összege 179
– szorzata 179
idegen (diszjunkt) permutálások 127
– halmazok 14, 15
idempotens elem 63
– félcsoport 67
– művelet 56
identitás 375
identitásfunktor 379
indexhalmaz 14
indukált részbenrendezés 19
injekció 18
injektív függvény 18
– modulus 255
integrálisan zárt gyűrű 269
integritási tartomány 153
– –, elrendezett 360
– –, rendezhető 360
– –, részbenrendezett 359
intervallum 333
–, relatív komplementumos 335
intervallumok izomorfizmustétele 347
invariáns részcsoport (normálosztó) 82
inverz, additív (ellentett) 152
–, morfizmusoké 377
inverzelem 65
irányított él (gráfban) 248
– gráf 248
– halmaz 50
irreducibilis elemek 169
– ideál 180
– reprezentáció 288
irredundáns metszet-előállítás 349
irreflexív reláció 17
ítéletek kiértékelése 367
–, elemi 367
izomorfizmus 32, 377
–, részcsoportoké 119
–, természetes 380
izomorfizmustétel, intervallumoké 347
izomorfizmustételek 87
izomorf normálláncok 118

Jacobi-azonosság 305
Jacobson-radikál 293
jobbannullátor 156
jobbideál 154
jobb oldali modulus 238
– – nullosztó 153
jobbzérus félcsoport 64
jólrendezés 20

karakter, csoport- 290
karakterisztikus (teljesen karakterisztikus) részcsoport 102
kategória 375
–, kis 386
–, konkrét 385
–, konkretizálható 385
–, oppozit 380
–, rész- 384
–, teljes rész- 385
képhalmaz 18
kétoldali ideál 154
– modulus 238
kiértékelés, ítéleteké 367
–, konkrét ítéleté 367
kifejezésalgebra 313
kifejezés típusa 313
Killing-féle forma 306
kis kategória 386
kiterjesztés, elrendezésé 362
kitevőértékelés 364
kivételes Lie-típusú csoportok 147
klasszifikációs tétel 147
klasszikus egyszerű csoportok 147
Klein-féle négyescsoport 136
ko-kúp 378
ko-szorzat 100

ko-univerzalitás 378
kockakettőzés (déloszi probléma) 228
kommutatív diagram 32, 249
– gyűrű 150
– test 153
kommutátor 103
– -lánc, csoporté 123
– -részcsoport 103
–, záródó 123
kompakt háló 47
kompaktul generált (háló) 48
kompatibilis osztályozás 34
– reláció 357
komplementer hálóban 335
komplementum 15
– normál 106
– relatív 335
komplementumos háló 335
komplexus 75
– konjugáltja 101
komponens 15, 38
kompozíció, függvényeké 18
–, relációké 16
kompozíciólánc 118
kongruencia 34
kongruenciareláció 34
konjugált 206
–, elemosztályé 101
–, komplexusé 101
– résztestek 212
konkrét ítélet kiértékelése 367
– kategória 385
konkretizálható kategória 385
kontravariáns funktor 253, 379
konvex részháló 333
korlát, alsó, felső 20
korlát, legnagyobb alsó, legkisebb felső 20
korlátelemek 331
korlátos háló 335
kovariáns funktor 253, 379
kovéges 138
kölcsönös kommutátorcsoport 103
környégyszögesítés 229
körosztási polinom 214
kötetlen változó 368
kötött változó 368
követés 332
közbülső test 199
kúp 377
–, univerzális 377
kúpok ekvivalenciája 377
különbség 15
külső direkt szorzat 93
kvaternió 301
–, tiszta 302

lánc 251, 335
– finomítása 348
–, maximális 348
–, növő 41
–, stabilizálódó 41
–, szigorúan növő 41
lefelé induktív 41
legkisebb elem 19
– felső korlát 20
legnagyobb alsó korlát 20
– elem 20
leképezés 17
lezárás 42
–, Galois-megfeleltetéssel indukált 44
–, ideálé 183
Lie-algebra 305
– csillaga 307
–, féligegyszerű 306
–, feloldható 306
– hatványai 305
– ideálja 305
–, nilpotens 306
– radikálja 306
Lie-típusú csoportok, kivételes 147
lineáris csoport, általános 141
– –, projektív 142
– –, speciális 142
lokális gyűrű 161

mag, ekvivalenciarelációé 23
–, homomorfizmusé 87
–, pozitív 361
majdnem gyűrű 151
maradékosztály 157
– -gyűrű 157

mátrixátalakítások, elemi 143
mátrixgyűrű, teljes 281
mátrixok, speciális 143
maximális elem 20
– ideál 157
– lánc 348
– normálosztó 88
maximumfeltétel 41
mellékosztály, bal oldali, jobb oldali 79
mérték, 0–1 369
–, triviális 370
metszet 14
metszet-előállítás, irredundáns 349
metszetirreducibilis elem 349
minden **x**-re 369
minimális elem 19
– (egyszerű) modulus 243
– generátorrendszer 31
modell, azonossághalmazé 321
moduláris háló 338
modulus, bal oldali 238
–, faktor- 239
–, injektív 255
–, jobb oldali 238
–, kétoldali 238
–, minimális vagy egyszerű 243
–, nemtriviális 238
–, nemtriviális rész- 243
–, projektív 255
–, rész- 239
–, szabad 239
–, triviális 238, 240
–, triviális rész- 243
–, unitér 240
modulusok direkt összege 239
– – szorzata 239
monoid 65
monomorfizmus 376
monstrum 147
morfizmus 375
– inverze 377
művelet, n-változós, bináris, unáris, nulláris 27
műveleti zártság 30
művelettartó leképezés 32
n-változós művelet 27
negatív kitevőjű hatvány 66
nemarchimedesi értékelés 364
nemtriviális modulus 238
– normálosztó 82
– részmodulus 243
neutrális elem, bal oldali, jobb oldali 63
nilpotens balideál 281
– csoport 125
– Lie-algebra 306
Noether-gyűrű 164
normális bővítés 206
– részcsoport (normálosztó) 82
normalizátor 105
normál komplementum 106
normállánc 118
– finomítása 118
–, valódi 118
normállláncok izomorfizmusa 118
normálosztó (invariáns részcsoport), normális részcsoport 82
–, maximális 88
–, nemtriviális (valódi) 82
–, triviális 82
növő lánc 41
nulláris művelet 27
nullelem 151
– (egységelem) (hálóban) 46
–, bal oldali, jobb oldali 63
nullgyűrű 151
nullkarakterisztikájú gyűrű 177
nullosztó, bal oldali, jobb oldali 153
nullosztómentes gyűrű 153
nullosztópár 153
nyílt formulák 368

objektum 375
oppozit kategória 380
ortogonális csoportok 146
osztály 13
osztályozás 15
osztó 168
osztórendszer 158
öröklődő részhalmaz (duálisan) 335
összeg, ideáloké 179

p-csoport 94
p karakterisztikájú gyűrű 177
p-Sylow részcsoport 109
pálya 127
– triviális, valódi 127
páronként idegen halmazok 15
páros gráf 81
partíció 15
permutációcsoport 125
permutálás 125
–, ciklikus 127
– tartóhalmaza 127
– típusa 130
permutálások, idegen vagy diszjunkt 127
polinom, általános n-edfokú 220
–, fő- 178
–, körosztási 214
–, primitív 172
–, szeparábilis 198
polinomgyűrű 164
–, véges sok határozatlanú 165
polinomok gyűrű felett 165
polinomrendszer 207
pozitív kúp 357
– mag 361
pozitivitási tartomány 359
primér ideál 180
prímideál 161, 336
–, duális 336
primitív egységgyök 214
– polinom 172
prímtulajdonságú elem 169
projektív lineáris csoport 142
– modulus 255

R-homomorfizmus 239
radikál, gyűrűé 179
–, ideálé 179
–, Jacobson- 293
–, Lie-algebráé 306
radikálmentes gyűrű 281
ráképezés 18
rákövetkező 20
realizáció 28
–, formuláké, algebrában 368
–, relációneveké 366
reflexív reláció 17
reláció 16, 366
–, antiszimmetrikus 17
–, definiáló 116
–, diagonális 16
–, heterogén 16
–, homogén 16
– inverze 16
–, irreflexív 17
– kiterjesztése 17
–, kompatibilis 357
–, komplementer 16
– megszorítása 17
–, reflexív 17
–, szigorúan antiszimmetrikus 17
–, szimmetrikus 17
–, teljes 16
–, tranzitív 17
–, trihotom 17
–, univerzális 16
–, üres 16
relációalgebra 366
– faktoralgebrája 367
– részalgebrája 367
– típusa 366
relációalgebrák direkt szorzata 367
(reláció)homomorfizmus 40
relációk kompozíciója 16
– részbenrendezése 23
– szorzata 16
relációnevek realizációja 366
relációstruktúra 40
relatív automorfizmus 207
– komplementum 335
– komplementumos háló 335
– komplementumos intervallum 335
rend, csoporté 79
–, elemé 80
rendezés 20
rendezhető integritási tartomány 360
reprezentáció, csoporté 288
–, hű 288
–, irreducibilis 288

reprezentánsrendszer, bal oldali, jobb oldali, kétoldali 81
részalgebra 29
–, relációalgebráé 367
részalgebraháló 51
részbenrendezés 18
részbenrendezett csoport 357
– integritási tartomány 359
részcsoport 76
–, ciklikus 78
–, invariáns (normálosztó) 82
–, karakterisztikus (teljesen karakterisztikus) 102
–, normális (normálosztó) 82
–, *p*-Sylow 109
–, triviális 78
–, valódi 78
részcsoportok izomorfizmusa 119
részgyűrű, triviális 154
–, valódi 154
részhalmaz 14
–, (duálisan) öröklődő 335
részhalmazháló 51
részháló, konvex 333
részkategória 384
–, teljes 385
részmodulus 239
–, nemtriviális 243
–, triviális 243
részstruktúra, feszített 40
résztest, konjugáltak 212

sorozat 249
–, egzakt 250
–, félig egzakt 249
– hossza 249
speciális lineáris csoport 142
– mátrixok 143
sporadikus (szórványos) egyszerű csoport 147
stabilizálódó lánc 41
stabilizátor (elemé) 125
sűrűségi tétel 245
szabad Abel-csoport 116
– algebra 314
– csoport 115
– félcsoport 61
– generátor 115
– generátorok 61
– generátorrendszer 61
– kommutatív félcsoport 66
– modulus 239
szabadon generált félcsoport 61
szabályos *n*-szög szerkesztése 229
számosságok, egyenlő, kisebb, nagyobb 25
szemidirekt (féldirekt) szorzat 106
szeparábilis bővítés 198
– polinom 198
szerkesztés, euklideszi 226
–, szabályos *n*-szögé 229
szerkeszthetőség 226
szigorúan antiszimmetrikus reláció 17
szigorúan növő lánc 41
szimmetrikus csoport 125
– reláció 17
szimplektikus csoport 146
szimplex 251
szorzat 15, 152, 375
szorzat, függvényeké 18
–, ideáloké 179
–, relációké 16
–, szemidirekt (féldirekt) 106
–, úté 249
szögharmadolás 228
szögpont (gráfban) 248
szubdirekt felbontás 325
– –, triviális 325
– irreducibilis algebra 325
– komponens 325
– szorzat 325
szürjekció 18
szürjektív 18
szűrő, duális ideál 333

tartócsoport, gyűrűé 150
–, modulusé 238
tartóhalmaz 28
–, permutálásé 127
teljes beágyazás 385
– funktor 385
– inverz kép 18
– (komplett) direkt szorzat 93
– mátrixgyűrű 281
– rendezés (elrendezés) 20
– részkategória 385
tenzorszorzat 263
természetes izomorfizmus 380
– számok nem standard modellje 374
– transzformáció 380
test 153
–, alap- 178
– értékelése 362
–, ferde- 154
–, formálisan valós 298
–, gyökökkel elérhető 214
–, kommutatív 153
–, közbülső 199
–, tökéletes 198
–, valósan zárt 297
testbővítés 178
–, egyszerű 178
típus 28
–, kifejezésé 313
–, permutálásé 130
–, relációalgebráé 366
tiszta kvaternió 302
– transzcendens bővítés 202
torziócsoport 97
többszörös 168
tökéletes test 198
törtideál 272
transzcendenciabázis 201
transzcendenciafok 201
transzcendens bővítés, tiszta 202
– elem 178
transzformáció, természetes 380
transzpozíció 129
tranzitív (permutálás) 125
– reláció 17
trihotom reláció 17
triviális algebra 37
– csoport 78
– mérték 370
– modulus 238, 240
– normálosztó 82
– pálya 127
– részcsoport 78
– részgyűrű 154
– részmodulus 243
– szubdirekt felbontás 325

ultrafilter (ultraszűrő) 336
ultraszorzat 370
ultraszűrő (ultrafilter) 336
unáris művelet 27
unitér csoport 146
– modulus 240
univerzális algebra, tartó 366
– kúp 377
út (diagramban) 249
– szorzata 249
üres halmaz 14

valódi finomítás 118
– ideál (duális ideál) 336
– normállánc 118
– normálosztó 82
– pálya 127
– rész 14
– részcsoport 78
– részgyűrű 154
valósan zárt test 297
változó, kötetlen 368
–, kötött 368
van olyan **x**, amire 369
varietás 318
véges algebrai bővítés 188
– bővítés 188
végesen generált 31

záródó kommutátorlánc 123
zárt formula 368
zérógyűrű 151
zéruselem, bal oldali, jobb oldali 64
zéruselemes félcsoport 64

Irodalomjegyzék

A.1. Magyar nyelvű általános:

Bálintné Szendrei Mária, Czédli Gábor, Szendrei Ágnes: *Absztrakt algebrai feladatok*. Tankönyvkiadó, 1985.

Csákány Béla: *Algebra (kézirat).* Tankönyvkiadó, 1973.

Fried Ervin: *Absztrakt algebra elemi úton.* Műszaki Kiadó, 1972.

Fuchs László: *Algebra (kézirat).* Tankönyvkiadó, 1963.

Klukovits Lajos: *Klasszikus és lineáris algebra.* Polygon, 2000.

A. G. Kuros: *Felsőbb algebra.* Tankönyvkiadó, 1967.

Rédei László: *Algebra.* Akadémiai Kiadó, 1954.

I. R. Safarevics: *Algebra.* TypoTex, 2000.

Schmidt Tamás: *Algebra (kézirat).* Tankönyvkiadó, 1977.

Szele Tibor: *Bevezetés az algebrába.* Tankönyvkiadó, 1953–1977.

Szendrei János: *Algebra és számelmélet.* Tankönyvkiadó, 1975.

A.2. Magyar nyelvű speciális:

S. Burris, H. P. Sankappanavar: *Bevezetés az univerzális algebrába.* Tankönyvkiadó, 1988.

Czédli Gábor: *Hálóelmélet.* Jatepress, 1999.

Czédli Gábor, Szendrei Ágnes: *Geometriai szerkeszthetőség.* Polygon, 1997.

Freud Róbert: *Lineáris algebra.* ELTE Eötvös Kiadó, 1996.

I. M. Gelfand: *Előadások a lineáris algebrából.* Akadémiai Kiadó, 1955.

A. G. Kuros: *Csoportelmélet.* Akadémiai Kiadó, 1955.

Rózsa Pál: *Lineáris algebra és alkalmazásai.* Tankönyvkiadó, 1991.

Szász Gábor: *Bevezetés a hálóelméletbe.* Akadémiai Kiadó, 1959.

B.1. Idegen nyelvű általános:

P. M. Cohn: *Algebra.* Chichester, 1977.

O. Haupt: *Einführung in die Algebra I., II.* Akademische Verlag, Több kiadás.

N. Jacobson: *Basic Algebra.* Freeman, 1974.

S. Lang: *Algebra.* Addison–Wesley, 1965.

S. McLane: *Algebra.* Macmillan, 1967.

L. H. Rowen: *Algebra.* Wellesley, 1994 (4.)

B. L. van der Waerden: *A history of algebra.* Springer, 1985.

B. L. van der Waerden: *(Moderne) Algebra.* Springer, Több kiadás.

B.2. Idegen nyelvű speciális:

E. Artin: *Galoissche Theorie.* Teubner, 1959.
R. Baer: *Linear algebra and projective geometry.* Academic Press, 1952.
K. A. Baker, R. Wille: *Lattice theory and its applications.* Heldermann, 1995.
G. Birkhoff: *Lattice theory.* Amer. Math. Soc., 1967.
P. M. Cohn: *Universal algebra.* Reidel Publ. Co., 1981.
J. H. Davenport & al.: *Computer algebra.* Academic Press, 1988.
Y. Diers: *Categories of commutative algebras.* Clarendon Press, 1992.
D. J. Dixon: *Analytic pro-p groups.* Cambridge University Press, 1991.
K. Doerk: *Finite soluble groups.* de Gruyter, 1992.
D. Eisenbud: *Commutative algebra with a view toward algebraic geometry.* Springer, 1995.
O. Endler: *Valuation theory.* Springer, 1972.
A. Fröhlich: *Galois module structure of algebraic integers.* Springer, 1983.
Fuchs László: *Abelian Groups.* Akadémiai Kiadó, Több kiadás.
Fuchs László: *Infinite Abelian groups.* Academic Press 1970. I. kötet, 1973. II. kötet.
Fuchs László: *Partially ordered algebraic systems.* Pergamon Press, 1963.
S. I. Gelfand, Y. I. Manin: *Method of homological algebra.* Springer, 1996.
J. Golan: *Modules and structure of rings.* Dekker, 1991.
G. Grätzer: *General lattice theory.* Akademie–Verlag, 1978.
E. Hecke: *Vorlesungen über die Theorie der algebraischen Zahlen.* Akademische Verlag, 1954.
H. Herrlich, H. Porst: *Category theory at work.* Heldermann, 1991.
J. Humphreis: *Introduction to Lie algebras and representation theory.* Springer, 1980.
Kertész Andor: *Vorlesungen über artinsche Ringe.* Akadémiai Kiadó, 1968.
T. Y. Lam: *Exercises in classical ring theory.* Springer, 1995.
R. Lidl, H. Niederreiter: *Finite fields.* Addison–Wesley, 1983.
S. MacLane: *Homology.* Springer, 1963.
R. Pierce: *Associative algebras.* Springer-Verlag (Heidelberg), 1982.
A. Pultr, V. Trnková: *Combinatorial, algebraic and topological representations of groups, semigroups and categories.* Academia Prague, 1980.
O. Zariski, P. Samuel: *Commutative algebra.* Van Nostrand, Több kiadás.