

## BEVEZETÉS AZ UNIVERZÁLIS ALGEBRÁBA

**1. Algebra.** Ha  $A$  tetszőleges halmaz és  $n \in \mathbb{N}_0$ , az  $f : A^n \rightarrow A$  leképezéseket így nevezzük:  $n$ -áris művelet az  $A$  halmazon. 0-áris, 1-áris, 2-áris és 3-áris helyett megfelelően azt mondjuk, hogy nulláris, unáris, bináris és ternáris. Azt, hogy  $f$   $n$ -áris, úgy is kifejezhetjük, hogy  $f$  aritása  $n$ . Legyen  $F$  műveletek egy halmaza az  $A$  halmazon; ekkor az  $(A, F)$  párt *algebrának* nevezzük. Ezt az algebrát rövidebben  $A$  is jelölheti, ha nincs szükség a műveletek halmazának feltüntetésére. Az  $A$  halmaz az  $A$  algebra *alaphalmaza*,  $F$  elemei pedig  $A$  *alapműveletei*. Mivel szokásos az  $A^0 = \{\emptyset\}$  megállapodás, az  $A$  halmazon nulláris művelet mindig  $A$  valamely elemének a kijelölését jelenti, az unáris műveletek pedig  $A$  transzformációi (önmagába való leképezései). Ha  $f$  egy  $n$ -áris művelet jele  $A$ -n és  $a_1, \dots, a_n \in A$ , az  $f$  művelet *eredményét* az  $(a_1, \dots, a_n)$  elem- $n$ -esen (azaz utóbbi képét az  $f$  leképezésnél)  $f(a_1, \dots, a_n)$  jelöli. Természetes kivételek a nulláris műveletek; nulláris művelet által kijelölt elemet magának a műveletnek a jelével szoktuk jelölni. Unáris és bináris műveletek esetén is gyakran eltérünk e szabálytól, pl. „ $+(a_1, a_2)$ ” helyett a megszokott  $a_1 + a_2$ -t írjuk.

*Példák:* A csoportok, amelyek alapműveletei a bináris szorzás, az unáris inverzképzés ( $a \mapsto a^{-1}$ ) és a nulláris egységelem (amelyet jelölhetünk az „1” jellel akkor is, ha nem az 1 számról van szó). A csoportot másképpen is lehet definiálni, mi azonban a következőkben ezt a csoportfogalmat használjuk. Természetesen, itt most nem adtuk meg a csoport definícióját; az a három művelet közti bizonyos kapcsolatokat is tartalmaz, amelyeket később fogunk tárgyalni (hasonló igaz következő három példánkra is).

Az adott  $T$  test feletti vektorterek, amelyek alapműveletei a bináris összeadás, az unáris additív inverz-képzés ( $a \mapsto -a$ ), a nulláris additív egységelem (0) és a  $T$  elemeivel (a „skalárokkal”) való szorzások (amelyek unáris műveletek).

A gyűrűk, amelyek alapműveletei a bináris összeadás és szorzás, valamint az unáris additív (azaz összeadásra vonatkozó) inverzképzés és a nulláris additív egységelem (amelynek jele 0). Az egységelemes gyűrűk alapműveletei közé sorolhatjuk még a nulláris multiplikatív egységelemet.

A hálók, amelyek műveletei a bináris egyesítés és metszés. Csoport és vektortér alaphalmaza nem lehet üres, mivel ezek az algebrák tartalmazznak a nulláris műveletükkel kijelölt elemet. Ezzel ellentétben az üres halmazt a rajta értelmezett két üres bináris művelettel tekinthetjük hálónak. (Gyűrű alaphalmaza lehet-e üres?)

A halmazok üres művelethalmazzal ugyancsak algebrák.

**2. Típus.** Legyen  $M$  halmaz, és legyen  $\tau$  az  $M$  halmaz leképezése a nemnegatív egészek halmazába. Az  $(M, \tau)$  párt *típusnak* nevezzük. Itt  $M$  a típushoz tartozó *műveletjelek halmaza*,  $\tau$  pedig a típus *aritásfüggvénye*. Bármely  $m \in M$ -re a  $\tau(m)$  számot az  $m$  műveletjel *aritásának* nevezzük. Ha  $\tau(m) = n$ , azt is mondjuk, hogy  $m$  *n-áris műveletjel*. Most is használhatjuk a nulláris, ..., ternáris szavakat.

Tekintsünk egy  $(M, \tau)$  típust és egy  $A = (A, F)$  algebrát. Azt mondjuk, hogy  $(M, \tau)$  *interpretálható*  $A$ -ban, ha létezik a műveletjelek  $M$  halmazának a műveletek  $F$  halmazára való olyan leképezése, amelynél műveletjel és a hozzárendelt művelet aritása ugyanaz. Az ilyen leképezés neve:  $(M, \tau)$  *interpretációja*  $A$ -ban. Ha  $(M, \tau)$  interpretálható  $A$ -ban, akkor azt mondjuk, hogy  $A$   $(M, \tau)$  *típusú algebra*. Az interpretáció pedig a gyakorlatban azt jelenti, hogy megállapodunk,  $A$  minden egyes műveletét melyik  $M$ -beli műveletjellel jelöljük. Ilyen megállapodás többféleképpen is történhet, mert adott típusnak adott algebraiban különböző interpretációi lehetnek. Legyen pl.  $T$  az a típus, amelyben  $M = \{\cup, \cap\}$  és  $M$  mindkét elemének aritása 2. A  $T$  típusnak minden (legalább kételemű) hálóban két interpretációja van, hiszen a hálóbeli egyesítést is jelölheti  $\cap$  (és a metszést  $\cup$ ). Ezért ugyanaz az algebra két különböző háló is lehet: az egyik a másiknak a duálisa. Hogy ez ne okozzon félreértést, a továbbiakban adott típusú algebráról beszélve mindig adottnak tekintjük az interpretációt is.

Legyen  $T$  tetszőleges típus. A  $T$  típusú algebrákat *hasonló algebráknak* nevezzük, az összes  $T$  típusú algebraok osztályát pedig *hasonlósági osztálynak*. Hasonlósági osztály pl. az összes grupoidok (egyetlen kétváltozós műveletű algebra) osztálya. Vigyázat: az összes csoportok nem alkotnak hasonlósági osztályt, s hasonlóképpen az összes vektorterek, gyűrűk és hálók sem. Ugyanis pl. a két bináris műveletű algebra hasonlósági osztályában olyan algebra is vannak, amelyek műveletei nem asszociatívok, amelyek tehát nem hálók. A következőkben rendszerint rögzítünk egy — egyébként tetszőleges —  $T$  típust, s megfontolásainkban csupa  $T$  típusú (tehát hasonló) algebra szerepelnek.

**3. Term.** Legyen  $T = (M, \tau)$  tetszőleges típus. Az általánosság megszorítása nélkül feltehetjük, hogy  $M$  nem tartalmazza az  $x_1, x_2, \dots$  jeleket. Defináljuk a  $T$  típusú *termeket*. Minden termhez — a műveletekhez és műveletjelekhez hasonlóan — aritást fogunk rendelni, s minden nemnegatív egész  $n$ -re külön definiáljuk az *n-áris termeket*, a következőképpen:

- (1) Minden nulláris műveletjel  $n$ -áris term.
- (2) Az  $x_1, \dots, x_n$  jelek  $n$ -áris termék.
- (3) Ha  $k$  pozitív egész,  $m \in M$   $k$ -áris műveletjel és  $t_1, \dots, t_k$   $n$ -áris termék, akkor  $m(t_1, \dots, t_k)$   $n$ -áris term.
- (4) Ha  $n$ -áris termék egy  $H$  halmaza tartalmazza az (1) és (2) pontban megadott

$n$ -áris termeket, továbbá a (3) pontban megadott termképzési eljárás nem vezet ki belőle, akkor  $H$  az összes  $n$ -áris termék halmaza.

Habár magától értetődő, mégsem árt hangsúlyozni, hogy két termet csak akkor tekintünk egyenlőnek, ha jelről-jelre megegyeznek. Az  $x_1, x_2, \dots$  jeleket, hogy a műveletjelektől és a term definíciójában előforduló segédjelektől (zárójelek, vessző) megkülönböztessük, *határozatlanoknak* nevezzük. Konkrét típusoknál a termék jelölésében a fentebbiektől eltérhetünk; pl. az említett grupoidok esetén, ha az egyetlen kétváltozós művelet jele  $+$ , a ternáris  $+(+(x_1, x_2), x_3)$  termet a megszokottabb  $(x_1 + x_2) + x_3$  alakban írjuk. Az adott  $T$  típusú  $n$ -áris termék halmazát  $T_n$ , az összes termék  $\bigcup_{n=1}^{\infty} T_n$  halmazát pedig  $T$  jelöli.

Figyeljük meg a term definíciójának hasonlóságát a természetes számok Peano-féle axiómák segítségével történő bevezetéséhez. Ez nem véletlen; tekintsük ui. azt a típust, amely egy unáris  $'$  és egy nulláris  $1$  műveletből áll. Az ilyen típusú összes nulláris termék:  $1, 1', 1'', \dots$ , s ezekben felismerhetjük a természetes számokat. A termék képzésének (1) és (3) szabálya erre az esetre alkalmazva nem más, mint az első két Peano-axióma, a (4) szabály pedig a teljes indukció axiómája.

A definícióból következik, hogy ha  $k < n$  nemnegatív egészek, akkor az  $n$ -áris termék között ott vannak a  $k$ -áris termék is. Ezt figyelembe véve, a (3) szabály mutatja, hogy minden  $M$ -beli  $m$  műveletjelnek megfeleltethető egy vele megegyező arítású művelet az összes termék  $T$  halmazán, ti. azt a művelet, amely tetszőleges  $(t_1, \dots, t_k)$  term- $k$ -ashoz az  $m(t_1, \dots, t_k)$  termet rendeli. Előző megfigyelésünk szerint ez értelmes művelet-megadás, mert  $t_1, \dots, t_k$  mindegyikét tekinthetjük ugyanolyan — mondjuk,  $q$  — arításúnak; ekkor  $m$  eredménye ezen az elem- $k$ -ason ugyancsak  $q$ -áris lesz. A bevezetett megfeleltetés a  $T$  típus egy interpretációja az összes termék  $T$  halmazán. Ezzel az interpretációval  $T$  maga is egy  $T$  típusú algebra. Ezt az algebrát  $T$  típusú megszámlálható rangú termalgebrának nevezzük. Univerzális algebrai megfontolásokban gyakran van rá szükség, így érthető, hogy más neveken is találkozunk vele: termalgebra helyett nevezik kifejezésalgebrának, Peano-algebrának, abszolút szabad algebrának is. Egy időben az „anarchikus algebra” nevet is használták. Az öt név közül az első három az eddigiekből érthető (term helyett mondhatnánk kifejezést is), a két utolsó név értelme később derül ki.

A „megszámlálható rangú” jelző azt fejezi ki a „termalgebra” előtt, hogy az elemeit képező termekben az  $x_1, x_2, \dots$  határozatlanok mindegyike előfordul. Az előző bekezdés gondolatmenetét alkalmazhatjuk bármely rögzített  $n$  természetes számmal az összes  $n$ -áris termekre is. Ilyen módon a  $T_n$  halmazon kapunk egy  $T$  típusú algebrát. Ezt  $n$  rangú termalgebrának nevezzük.

Mint megfigyeltük, term arítása nem egyértelműen meghatározott; minden

termnek van azonban egyetlen minimális aritása. Ez a csak nulláris műveletjeleket tartalmazó termekre 0, más termre pedig a legnagyobb olyan  $n$ , amelyre a term tartalmazza az  $x_n$  határozatlan. Ha a term a határozatlanok közül pontosan  $k$  számú különbözőt tartalmaz, akkor azt mondjuk, hogy *látszólagos aritása  $k$* . A látszólagos aritás egyértelmű, és lehet kisebb a minimális aritásnál [!], de nagyobb nem.

**4. Termművelet.** Adott típusú algebra alaphalmazán az alpműveletekből további műveletek származtathatók. A típust és az interpretációt rögzítettnek tekintjük. Jelöljön  $t$  tetszőleges termet, amelynek minimális aritása  $k$ . Mint láttuk, ezt a termet tekinthetjük  $n$ -árisnak is, ha  $n \geq k$ . A  $t$  term részletes felírása helyett használhatjuk a  $t(x_1, \dots, x_n)$  jelölést, amellyel azt fejezzük ki, hogy a term részletes felírásában legfeljebb az  $x_1, \dots, x_n$  határozatlanok szerepelnek. A jelölés mutatja, hogy a  $t$  term minimális aritása legfeljebb  $n$ , és a termet  $n$ -árisnak tekintjük.

Legyen  $A$  tetszőleges algebra,  $t(x_1, \dots, x_n)$  tetszőleges term. Az  $(a_1, \dots, a_n) \mapsto t(a_1, \dots, a_n)$  műveletet  $t$ -hez tartozó *termműveletnek* nevezzük. Ezt az újabb műveletet a létrehozó term jelével, esetünkben  $t$ -vel jelöljük. A termművelet definíciója részletesebben azt jelenti, hogy a  $t$  termhez tartozó termművelet eredményét az  $(a_1, \dots, a_n) \in A^n$   $n$ -esen úgy nyerjük, hogy tekintjük  $t$  részletes felírását, benne  $x_i$ -et mindenütt  $a_i$ -vel helyettesítjük ( $i = 1, \dots, n$ -re), s az így kijelölt műveleteket  $A$ -ban elvégezzük. Ugyanezt pontosabban is megfogalmazhatjuk a term definíciója segítségével:

- (1) Ha  $t$  olyan  $n$ -áris term, amely nulláris műveletjel, a  $t$  termművelet  $A$ -ban a mindenütt  $c (\in A)$  eredményű  $n$ -áris művelet (más szóval a konstans  $c$  művelet), ahol  $c$  az  $A$  algebraiban a szóbanforgó nulláris műveletjellel jelölt nulláris művelet által kijelölt elem.
- (2) Minden  $i$ -re ( $i = 1, \dots, n$ ) az  $x_i$  termművelet az  $i$ -edik  $n$ -áris *projekció*, amely bármely  $A$ -ból képezett elem- $n$ -eshez annak  $i$ -edik komponensét rendeli.
- (3) Az  $m(t_1, \dots, t_k)$  alakú  $n$ -áris termhez (lásd az  $n$ -áris term definíciójának (3) pontját) tartozó termművelet eredménye a tetszőleges  $(a_1, \dots, a_n) \in A^n$  elem- $n$ -esen

$$m(t_1(a_1, \dots, a_n), \dots, t_k(a_1, \dots, a_n)).$$

Jelölje  $H$  mindazon termek halmazát, amelyekhez tartozó termműveletet a most felsorolt (1),(2),(3) szabályok meghatározzák. Akkor a termek képzésére vonatkozó (4) szabály szerint  $H = T_n$ , tehát az (1),(2),(3) szabályok minden termre meghatározzák a hozzá tartozó termműveletet. A termekre vonatkozó ilyen gondolatmenetet *induktív bizonyításnak* nevezzük. Az előző fejezetbeli, a természetes számokra vonatkozó megjegyzésünk mutatja, hogy ez a fogalom általánosítása a természetes számokra vonatkozó induktív bizonyítás fogalmának.

Az előzőekben az interpretációt kiterjesztettük a műveletjelekről az összes termek halmazára. Ez a „kiterjesztés” nem szó szerint értendő, hiszen a műveletjelek nincsenek ott a termek között. Az  $m$  műveletjelhez azonban ugyanaz a művelet tartozik, mint az  $m(x_1, \dots, x_k)$  termhez (amit a termműveletekre vonatkozó (2) és (3) szabályból látunk). Az alpműveletek tehát maguk is termműveletek.

A termműveleteket egyszerre definiáltuk az összes ugyanolyan típusú algebrára. Ha valamilyen fajta algebrák (pl. csoportok, stb.) mind ugyanolyan típusúak, akkor a rájuk használatos jelöléssel írhatjuk fel termműveleteiket. Pl.  $x_1 \cdot x_2^{-1} \cdot x_3$  ternáris termművelet minden csoporton (a zárójeleket elhagytuk, mert csoportban a két lehetséges zárójelezéssel adódó két termhez ugyanaz a termművelet tartozik);  $x_1 \cdot x_1 + x_1 + x_1$  (vagy ahogy egyszerűsítő megállapodásokkal élve rendszerint írjuk:  $x^2 + 2x$  — unáris termék felírásakor az 1 indexet az  $x$  mellől többnyire elhagyjuk) unáris termművelet minden gyűrűn (de ne gondoljuk, hogy a gyűrűk feletti polinomműveletek mind termműveletek!);  $x_1 \cup (x_1 \cap x_2)$  bináris termművelet minden hálón.

**5. Polinom.** A matematika egyik legfontosabb fogalma a polinom és a hozzá kapcsolódó polinomfüggvény. E fogalmak szembeötlően hasonlítanak a most bevezetett term és termművelet fogalmakhoz. A gyűrű feletti polinom a termhez hasonlóan definiálható (az alpműveletek itt a gyűrű alpműveletei), annyi különbséggel, hogy egyrészt a konstansok (tehát a gyűrűelemek) is polinomok és a nulláris műveletjelekhez és a határozatlanokhoz hasonlóan felhasználhatók újabb polinomok képzéséhez, másrészt polinomokat nem csak akkor tekintünk egyenlőnek, ha jelről-jelre megegyeznek (ti. akkor is, ha kanonikus alakjuk megegyezik). E különbségeket szem előtt tartva, gyűrű feletti polinomokhoz ahhoz hasonlóan rendelünk polinomfüggvényeket, ahogyan termekhez termműveleteket. Ez a hozzárendelés két egyenlőnek tekintett polinomhoz mindig ugyanazt a polinomfüggvényt rendeli. Ebből a megfontolásból ered a tetszőleges  $A$  algebra feletti  $n$  határozatlanú polinom következő definíciója. Rövidség kedvéért „ $p$  az  $A$  algebra feletti  $n$  határozatlanú polinom” helyett ezt írjuk:  $p \in A[x_1, \dots, x_n]$ .

- (1) Ha  $m$  nulláris műveletjel,  $m \in A[x_1, \dots, x_n]$ .
- (2)  $x_1, \dots, x_n \in A[x_1, \dots, x_n]$ .
- (2') Ha  $c \in A$ , akkor  $c \in A[x_1, \dots, x_n]$  (ezek a *konstans polinomok*).
- (3) Ha  $k$  pozitív egész,  $m$   $k$ -áris műveletjel és  $p_1, \dots, p_k \in A[x_1, \dots, x_n]$ , akkor  $m(p_1, \dots, p_k) \in A[x_1, \dots, x_n]$ .
- (4) Ha  $A$  feletti  $n$  határozatlanú polinomok egy  $H$  halmaza tartalmazza az (1), (2) és (2') pontban megadott polinomokat, továbbá a (3) pontban megadott polinomképzési eljárás nem vezet ki belőle, akkor  $H = A[x_1, \dots, x_n]$ .

A termekre használt rövid  $t(x_1, \dots, x_n)$  jelölést polinomokra is alkalmazzuk:

$p(x_1, \dots, x_n)$  olyan polinomot jelent, amelyben legfeljebb az  $x_1, \dots, x_n$  határozatlanok fordulnak elő. Ez a jelölés tehát nem mond semmit  $A$ -nak a  $p$  polinom felépítéséhez használt elemeiről.

Tetszőleges algebra feletti polinomnak nincs olyan elegáns kanonikus alakja, mint a gyűrű feletti polinomnak. Mindazonáltal létezik egyszerűen kezelhető felírása: minden  $A$  feletti  $p$   $n$ -áris polinomhoz létezik olyan  $t$   $n + k$ -áris term ( $k$  nemnegatív egész) és olyan  $a_1, \dots, a_k \in A$ , hogy

$$p(x_1, \dots, x_n) = t(x_1, \dots, x_n, a_1, \dots, a_k).$$

A jobboldalon  $x_1, \dots, x_n, a_1, \dots, a_k$  mind  $n$ -áris termek illetve  $n$ -áris konstans polinomok. Állításunk nyilvánvaló, ha  $p$  nulláris term, vagy határozatlan; míg ha  $p$  a  $c$  konstans polinom, akkor  $k$  választható 1-nek,  $t$   $x_{n+1}$ -nek,  $a_1$  pedig  $c$ -nek. Végül, ha

$$p(x_1, \dots, x_n) = m(p_1(x_1, \dots, x_n), \dots, p_k(x_1, \dots, x_n)),$$

és

$$p_1(x_1, \dots, x_n) = t_1(x_1, \dots, x_n, a_{n+1}, \dots, a_{n+i_1}),$$

$$p_2(x_1, \dots, x_n) = t_2(x_1, \dots, x_n, a_{n+i_1+1}, \dots, a_{n+i_1+i_2}),$$

...

$$p_k(x_1, \dots, x_n) = t_k(x_1, \dots, x_n, a_{n+i_1+\dots+i_{k-1}+1}, \dots, a_{n+i_1+\dots+i_k}),$$

akkor a  $p = m(p_1, \dots, p_k)$  egyenlőség jobboldalába az utóbbi egyenlőségek jobboldalát helyettesítve, és a kapott egyenlőségben minden  $a_j$  helyébe  $x_j$ -t írva megkapjuk azt az  $n + k$ -áris termet ( $k = i_1 + \dots + i_k$ ), amelyből — az  $a_j$ -ket visszaírva —  $p$ -t a kívánt alakban kapjuk. Az így nyert polinomot  *$p$  szabályos alakjának* nevezzük.

Az  $A$  algebra alaplmműveletei nemcsak a termeken, hanem az  $A$  feletti polinomokon is elvégezhetők. Így az  $A$  feletti összes polinomok, és hasonlóképpen minden  $n$ -re az  $A$  feletti  $n$ -áris polinomok is egy-egy  $A$ -hoz hasonló (azaz vele megegyező típusú) algebrát alkotnak, amelyet megfelelően  *$A$  feletti megszámlálható rangú*, ill.  *$n$  rangú polinomalgebrának* nevezünk.

Ahogy termhez termműveletet, polinomhoz polinomműveletet rendelhetünk. Az  $A$  feletti polinomműveletek definíciója azzal az egyetlen lényeges különbséggel kapható a termműveletek definíciójából, hogy tartalmazza a következő természetes megállapodást: a  $c \in A[x_1, \dots, x_n]$  polinomhoz tartozó polinomművelet minden  $A$ -ból vett elem- $n$ -eshez a  $c$  elemet rendeli. A term és a polinom definíciója közti kapcsolat mutatja, hogy minden alaplmművelet — mint termművelet — egyben polinomművelet is.

Az unáris polinomhoz tartozó polinomműveletet *transzlációnak* nevezzük. Unáris polinomot szabályos alakban írva látjuk, hogy  $A$  minden  $\varphi$  transzlációjához

van olyan nemnegatív egész  $k$ , olyan  $k+1$ -áris  $t$  term és olyan  $a_1, \dots, a_k \in A$  elemek, hogy minden  $a \in A$ -ra  $\varphi(a) = t(a, a_1, \dots, a_k)$ . E megfigyelésből az is következik, hogy algebra translációinak szorzata is transláció.

**6. Részalgebra.** Ha az  $A = (A, F)$  algebra alaphalmazának  $B$  olyan részhalmaza, amely zárt az  $F$ -beli műveletekre vonatkozóan, azaz minden nemnegatív egész  $n$ -re, minden  $n$ -áris  $m \in F$  műveletre és minden  $b_1, \dots, b_n \in B$  elem- $n$ -esre  $m(b_1, \dots, b_n) \in B$ , akkor  $(B, F|B)$   $A$ -hoz hasonló algebra; benne minden művelet az  $A$  algebra megfelelő műveletének  $B$ -re való *restrikciója* (megszorítása). Minden így előálló  $B = (B, F|B)$  algebrát  $A$  *részalgebrájának* nevezünk. A félreértés veszélye nélkül magát a  $B$  halmazt is nevezhetjük  $A$  részalgebrájának. Jelölés:  $B \leq A$ , vagy  $B \leq A$ .

A definíció mutatja, hogy minden részalgebra tartalmazza minden nulláris művelet eredményét. A részalgebrák nemcsak az alpműveletekre, hanem minden termműveletre is zártak. Ezt induktívan bizonyíthatjuk. *Algebra részalgebrái bármely halmazának metszete ugyancsak részalgebra* — ez nyilvánvaló a részalgebra és a halmazmetszet definíciójából. Ha  $H$  az  $A$  algebra alaphalmazának részhalmaza, akkor a  $H$ -t tartalmazó összes részalgebrák  $\overline{H}$  metszete is részalgebra. Másrészt, alkalmazzunk minden termműveletet minden  $H$ -beli elemekből képezett megfelelő elemszámú sorozatra. E műveletek összes eredményeinek  $H^*$  halmaza ( $H$ -t tartalmazó) részalgebra  $A$ -ban, mert a termművelet definíciójának (3) pontja szerint az alpműveletekre zárt. Mivel  $\overline{H}$   $H^*$ -nak és esetleges más részalgebráknak a metszete, azért  $\overline{H} \subseteq H^*$ . Másrészt  $H \subseteq \overline{H}$ , és a részalgebrák zártak a termműveletekre, így  $H^* \subseteq \overline{H}$ . Nyertük, hogy  $\overline{H} = H^*$ . A  $\overline{H}$  részalgebrát az  $A$ -ban  $H$  által generált részalgebrának, vagy röviden  $H$  generátumának nevezzük. Beláttuk, hogy tetszőleges  $a \in A$  akkor és csak akkor eleme  $H$  generátumának, ha létezik olyan  $n$  nemnegatív egész, olyan  $n$ -áris  $t$  term és olyan  $h_1, \dots, h_n \in H$ , hogy  $a = t(h_1, \dots, h_n)$ . Ha a  $H$  halmaz generátuma maga az  $A$  algebra, akkor azt mondjuk, hogy  $H$  generátorrendszere  $A$ -nak.

A nulláris termműveletek eredményei részalgebrát alkotnak, amely minden részalgebrának részhalmaza, tehát  $A$  legszűkebb részalgebrája. Ha a típus nem tartalmaz nulláris műveletjelet, akkor a legszűkebb részalgebra az üres (alaphalmazú) algebra. Természetesen minden algebra (a legbővebb) részalgebrája önmagának. Ezt a két részalgebrát *triviális részalgebrának* nevezzük. A triviális részalgebrák egybe is eshetnek (mikor?).

Algebra összes részalgebrái a tartalmazásra nézve részbenrendezett halmazt alkotnak. Ez a halmaz hálószerűen rendezett, mert benne bármely két részalgebrának van legkisebb közös alsó korlátja, ti. a metszetük, továbbá van legnagyobb közös felső korlátjuk is, ti. mindazon részalgebrák metszete, amelyek mindkette-

jüket tartalmazzák (legalább egy ilyen biztosan van: maga a tekintett algebra). Bármely algebra összes részalgebrái tehát hálót alkotnak. Ha egy hálószerűen rendezett halmaz olyan, hogy elemei *bármely halmazának* tartalmazza legkisebb közös alsó korlátját (és ebből következően [!] legkisebb közös felső korlátját is), akkor az elemei által alkotott hálót *teljes hálónak* nevezzük. Láthatóan, algebra összes részalgebráinak hálója teljes. Teljes háló — definíciójából következően — mindig korlátos. A részalgebrák teljes hálójának korlátai a triviális részalgebrák. Az  $A$  algebra részalgebra-hálójának szokásos jele  $\text{Sub } A$ .

**7. Lezárási operátor.** Az előző fejezetben tárgyalt  $H \mapsto \overline{H}$  megfeleltetés az  $A$  algebra  $A$  alaphalmazának részhalmazait ugyanezen halmaz részhalmazaiiba viszi át; szokásos elnevezéssel, a generálás (a generátum képzése) halmazoperátor, röviden *operátor*  $A$  hatványhalmazán (azaz részhalmazainak halmazán). A generálás három alaptulajdonsága:

- (1) Minden  $H \subseteq A$ -ra  $H \subseteq \overline{H}$  (a generálás *extenzív* operátor);
- (2) Ha  $H_1 \subseteq H_2$ , akkor  $\overline{H_1} \subseteq \overline{H_2}$  (a generálás *monoton* operátor);
- (3) Minden  $H \subseteq A$ -ra  $\overline{\overline{H}} = \overline{H}$  (a generálás *idempotens* operátor).

Az extenzív, monoton és idempotens halmazoperátort *lezárási operátornak* nevezzük. Tekintsünk egy tetszőleges lezárási operátort valamely  $A$  halmaz hatványhalmazán. Bármely  $H \subseteq A$  halmaz képét ennél az operátornál *zárt* halmaznak, s ha azt is meg akarjuk mondani, mely halmaz képe,  $H$  *lezártjának* nevezzük. A generálás tehát lezárási operátor, amelynél a zárt halmazok éppen a részalgebrák, és részhalmaz lezártja éppen a generátuma.

Mint láttuk, az  $A$  algebra részalgebrái bármely halmazának metszete is részalgebra. Tekintsük tetszőleges  $A$  halmaz hatványhalmazának olyan  $C$  részhalmazát, amelyben hozzá tartozó halmazok bármely halmazának metszete is benne van. Az ilyen  $C$ -t *lezárási rendszernek* nevezzük  $A$ -n. Algebra részalgebrái tehát lezárási rendszert alkotnak. Hasonlóan a részalgebrákhoz, tetszőleges  $A$  halmaz bármely lezárási rendszerében levő összes halmazok is korlátos teljes hálót alkotnak. (Maga az  $A$  halmaz minden esetben a lezárási rendszerhez tartozik, mint a lezárási rendszerben levő halmazok *üres* halmazának metszete.)

A generálás és a részalgebrák közötti kapcsolat általánosítható tetszőleges  $A$  halmaz lezárási operátoraira és lezárási rendszereire is a következő alakban: Bármely lezárási operátornál a zárt halmazok lezárási rendszert alkotnak. Ha pedig  $C$  lezárási rendszer, akkor az a *leképezés*, amely  $A$  minden részhalmazához az azt tartalmazó  $C$ -beli halmazok metszetét rendeli, lezárási operátor. Így módon  $A$  minden lezárási operátorához egy lezárási rendszerét rendelhetjük, minden lezárási rendszeréhez pedig egy lezárási operátort, és ez a két hozzárendelés egymásnak inverze (s ezért mindkettő bijektív).

Először azt mutatjuk meg, hogy lezárási operátornál zárt halmazok metszete is zárt. Legyen az operátor  $H \mapsto H^*$ ; azt kell belátnunk, hogy bármely  $I$  indexhalmazra és  $A$  zárt részhalmazainak bármely  $\{H_\alpha^* \mid \alpha \in I\}$  halmazára  $\bigcap_{\alpha \in I} H_\alpha^*$  zárt, azaz

$$\left(\bigcap_{\alpha \in I} H_\alpha^*\right)^* = \bigcap_{\alpha \in I} H_\alpha^*.$$

A  $*$  operátor extenzív, ezért a jobb oldal részhalmaza a bal oldalnak. Másrészt minden  $\beta \in I$ -re  $\left(\bigcap_{\alpha \in I} H_\alpha^*\right)^* \subseteq H_\beta^{**} = H_\beta^*$ , mivel a  $*$  operátor monoton és idempotens. Innen  $\left(\bigcap_{\alpha \in I} H_\alpha^*\right)^* \subseteq \bigcap_{\beta \in I} H_\beta^* = \bigcap_{\alpha \in I} H_\alpha^*$ , tehát a bal oldal is részhalmaza a jobb oldalnak. A második állítás triviálisan ellenőrizhető: a lezárási rendszerből létrehozott operátor valóban extenzív, monoton és idempotens.

A harmadik állítás belátásához meg kell mutatnunk, hogy ha  $\mathcal{C}$  lezárási rendszer  $A$ -n és  $H^*$  a  $\bigcap_{H \subseteq K \in \mathcal{C}} K$  metszetet jelöli, akkor  $A$ -nak pontosan azok a részhalmazai tartoznak  $\mathcal{C}$ -hez, amelyekre  $L^* = L$ . Ha  $L \in \mathcal{C}$ , akkor  $L^* = \bigcap_{L \subseteq K \in \mathcal{C}} K = L$ , mert a metszet „metszendői” között  $L$  is ott van; ha pedig  $L = L^*$ , akkor  $L = \bigcap_{L \subseteq K \in \mathcal{C}} K \in \mathcal{C}$ . Végül azt is igazolnunk kell, hogy ha  $H \mapsto H^*$  lezárási operátor  $A$ -n, akkor minden  $L \subseteq A$ -ra  $L^*$  éppen az  $L$ -t tartalmazó zárt halmazok  $M = \bigcap_{L \subseteq K^*} K^*$  metszete. Az  $M$  metszet részhalmaza  $L^*$ -nak, hiszen metszendői között  $L^*$  is ott van; másrészt, ha  $L \subseteq K^*$ , akkor  $L^* \subseteq K^*$ , ezért  $M$  minden metszendője tartalmazza  $L^*$ -ot, s így  $L^*$  részhalmaza  $M$ -nek.

Gondoljuk meg, elhagyható-e a lezárási operátor definíciójából az ott szereplő három tulajdonság valamelyike.

**8. Direkt szorzat.** Ha  $A$  és  $B$  hasonló algebrák, műveletjeik természetes módon interpretálhatók alaphalmazaik Descartes-szorzatán a következőképpen. Bármely  $k$  nemnegatív egészre,  $m$   $k$ -áris műveletjelre és  $a_1, \dots, a_k \in A$ ,  $b_1, \dots, b_k \in B$  elemekre legyen

$$m((a_1, b_1), \dots, (a_k, b_k)) = (m(a_1, \dots, a_k), m(b_1, \dots, b_k)).$$

Ezáltal az  $A \times B$  szorzathalmazt  $A$ -hoz (és  $B$ -hez) hasonló algebrává tettük, amelyet  $A$  és  $B$  *direkt szorzatának* nevezünk. Jelölése:  $A \times B$ . Magukat az  $A$  és  $B$  algebrákat e direkt szorzat *direkt tényezőinek* nevezzük.

Két algebra direkt szorzatában a műveleteket az alaphalmazt alkotó elem-párokon *komponensenként* végezzük: külön a párok első komponensein, és második komponensein. Ezt nyilvánvaló módon általánosíthatjuk elempárok helyett elem- $n$ -esekre, s ilyen módon  $n$  algebra direkt szorzatának a definíciójához jutunk. Hasonló

algebrák tetszőleges rendszerének direkt szorzatát lényegében ugyanígy vezethetjük be. Ehhez szükségünk van a kiválasztási függvény fogalmára.

Legyen  $I$  tetszőleges indexhalmaz,  $A_\alpha (\alpha \in I)$  pedig nemüres halmazok tetszőleges rendszere. Minden olyan  $\zeta : A_\alpha \mapsto c_\alpha$  leképezést, amelynél minden  $\alpha \in I$ -re  $c_\alpha \in A_\alpha$ , *kiválasztási függvénynek* nevezünk az  $A_\alpha (\alpha \in I)$  halmazrendszeren. Jelölje  $\prod_{\alpha \in I} A_\alpha$  az  $A_\alpha (\alpha \in I)$  halmazrendszeren értelmezett kiválasztási függvények halmazát. Ha minden  $A_\alpha$  egy  $\mathbf{A}_\alpha = (A_\alpha, F)$  algebra alaphalmaza, akkor az  $F$ -hez tartozó műveletjelek természetes módon interpretálhatók a  $\prod_{\alpha \in I} A_\alpha$  halmazon a következőképpen. Bármely  $k$  nemnegatív egészre,  $m \in F$   $k$ -áris műveletjelre és  $\zeta_i : A_\alpha \mapsto c_{\alpha i}$  ( $i = 1, \dots, k$ ) kiválasztási függvényekre legyen

$$m(\zeta_1, \dots, \zeta_k) = \zeta : A_\alpha \mapsto m(c_{\alpha 1}, \dots, c_{\alpha k}).$$

Ezáltal a  $\prod_{\alpha \in I} A_\alpha$  halmazt az  $\mathbf{A}_\alpha$  algebrákhoz hasonló algebrává tettük. Ezt az algebrát az  $\mathbf{A}_\alpha (\alpha \in I)$  algebrák *direkt szorzatának*, az  $\mathbf{A}_\alpha$  algebrákat pedig e direkt szorzat *direkt tényezőinek* nevezzük. A direkt szorzat jelölése:  $\prod_{\alpha \in I} \mathbf{A}_\alpha$ . Ha  $I$  kételemű (vagy általánosabban, véges) akkor ez a definíció két algebra (ill. véges számú algebra) direkt szorzatának definíciójába megy át. Ha minden  $\alpha \in I$ -re  $A_\alpha = A$ , akkor a direkt szorzatot *direkt hatványnak* nevezzük, és így jelöljük:  $\mathbf{A}^n$ , ahol  $n$  az  $I$  halmaz számossága. (Ha  $n = 2$ , direkt négyzetről beszélünk.)

A halmazelméleti *kiválasztási axióma* szerint *nemüres halmazok bármely rendszerén létezik kiválasztási függvény*. Ez pontosan azt (a nyilvánvalónak látszó ténnyt) jelenti, hogy *nemüres algebrák bármely rendszerének direkt szorzata nem üres*.

**9. Kongruencia.** Legyen  $\mathbf{A}$  tetszőleges algebra. Az  $A^2$  halmaz részhalmazai a *bináris relációk*  $A$ -n. Ha egy  $\rho \subseteq A^2$  reláció egyidejűleg ekvivalencia és részalgebrája  $\mathbf{A}^2$ -nek, akkor  $\rho$ -t az  $\mathbf{A}$  algebra *kongruenciájának* nevezzük. Ha  $a_1, a_2 \in A$  olyan elemek, hogy  $(a_1, a_2) \in \rho$ , akkor azt mondjuk, hogy  $a_1$  és  $a_2$  *kongruensek* ( $\rho$ -ra vonatkozóan).

Algebra kongruenciái tetszőleges halmazának metszete is kongruenciája az algebrának, mivel hasonló igaz ekvivalenciákra is, részalgebrákra is. Ezért bármely  $\mathbf{A}$  algebra összes kongruenciái lezárási rendszert, s ebből következően teljes hálót alkotnak. Ennek a hálónak alsó korlátja az egyenlőségreláció (ezt, részalgebraként tekintve, szokás  $\mathbf{A}^2$  *átlójának* nevezni), felső korlátja az univerzális reláció (azaz maga  $A \times A$ ). Ezek a *triviális kongruenciák*. Az  $\mathbf{A}$  algebra kongruenciahálójának szokásos jele  $\text{Con } \mathbf{A}$ .

Példa: algebrák direkt szorzatában minden direkt tényezőhöz rendelhetünk egy kongruenciát: tekintsük a  $\mathbf{D} = \prod_{\alpha \in I} \mathbf{A}_\alpha$  direkt szorzatot és legyen  $\beta \in I$ . Akkor

a  $D$  tetszőleges  $\zeta_1, \zeta_2$  elemeire a

$$(\zeta_1, \zeta_2) \in \pi_\beta \iff \zeta_1(\beta) = \zeta_2(\beta)$$

összefüggéssel definiált reláció láthatóan ekvivalencia és részalgebrája  $D$ -nek. Az így előálló kongruenciákat a *direkt szorzat természetes kongruenciáinak* nevezzük.

A kongruencia és a részalgebra definícióját összehasonlítva látjuk, hogy  $A$  kongruenciái pontosan az olyan  $\rho$  ekvivalenciák  $A$ -n, hogy bármely pozitív egész  $k$ -ra,  $m$   $k$ -áris alpműveletre és bármely  $a_1, \dots, a_k, b_1, \dots, b_k \in A$  elemekre

$$(a_1, b_1), \dots, (a_k, b_k) \in \rho \text{---ből következik } (m(a_1, \dots, a_k), m(b_1, \dots, b_k)) \in \rho. \quad (i)$$

A kongruenciák ezen egyszerű jellemzését tekinthetjük definíciójuknak is. Ha az (i) összefüggésben az  $a_i, b_j$  elemek valós számok,  $\rho$  pedig a  $\leq$  reláció, akkor (i) pontosan azt jelenti, hogy az  $m$  függvény (minden változójában) monoton növekvő. Azt, hogy (i) az alaphalmazon mindig teljesül, tetszőleges reláció esetén is szokás úgy kifejezni, hogy  $m$  *monoton  $\rho$ -ra nézve*. Ugyancsak szokásos beszédmód:  $m$  *megőrzi  $\rho$ -t*. A kongruenciák tehát azok az ekvivalenciák, amelyeket minden alpművelet megőrzi. Induktív bizonyítás mutatja, hogy a kongruenciákat minden termművelet és minden polinomművelet — speciálisan, minden transláció — ugyancsak megőrzi. Ezek az állítások meg is fordíthatók, ami termműveletekre és polinomműveletekre nyilvánvaló, hiszen az alpműveletek is termműveletek és polinomműveletek. Kevésbé nyilvánvaló, hogy megfordítható a translációkra vonatkozó állítás is: *ha a  $\rho$  ekvivalenciát minden transláció megőrzi, akkor  $\rho$  kongruencia*.

Legyen  $\rho$  ekvivalencia az  $A$  halmazon, amelyet az  $A$  algebra minden translációja megőrzi, és legyen  $m$   $A$   $k$ -áris alpművelete. Tegyük fel, hogy  $(a_1, b_1), \dots, (a_k, b_k) \in \rho$  ( $a_i, b_j \in A$ ), és tekintsük  $A$  következő translációit:

$$\begin{aligned} \tau_1 &= a \mapsto m(a, a_2, \dots, a_k), \\ \tau_2 &= a \mapsto m(b_1, a, a_3, \dots, a_k), \\ \tau_3 &= a \mapsto m(b_1, b_2, a, a_4, \dots, a_k), \\ &\dots \\ \tau_k &= a \mapsto m(b_1, \dots, b_{k-1}, a) \end{aligned}$$

(ahol pl.  $\tau_k$  ahhoz a polinomhoz tartozó polinomművelet, amely úgy keletkezik, hogy a  $t(x_1, x_2, \dots, x_k) = m(x_2, \dots, x_k, x_1)$  term képzése során az  $x_2, \dots, x_k$  határozatlanok helyett rendre a  $b_1, \dots, b_{k-1}$  konstansokat használjuk). Most, mivel a  $\tau_1, \tau_2, \dots$  translációk megőrzik  $\rho$ -t,  $(a_1, b_1), (a_2, b_2), \dots \in \rho$ -ból következik megfelelően

$$\begin{aligned} (m(a_1, a_2, a_3, \dots), m(b_1, a_2, a_3, \dots)) &\in \rho, \\ (m(b_1, a_2, a_3, \dots), m(b_1, b_2, a_3, \dots)) &\in \rho, \end{aligned}$$

és így tovább. Innen  $\rho$  tranzitivitását figyelembe véve kapjuk, hogy  $(m(a_1, \dots, a_k), m(b_1, \dots, b_k)) \in \rho$ , és ezt kellett belátnunk.

**10. Faktoralgebra.** Legyen  $\rho \in \text{Con } A$ . A  $\rho$  relációhoz, mint ekvivalenciához tartozó osztályozás  $a \in A$ -t tartalmazó osztályát jelölje  $\rho(a)$ , az összes különböző  $\rho(a)$  osztályok halmazát pedig  $A/\rho$ . Ezen a halmazon az alpműveleteket a következő módon vezethetjük be. Ha  $m$   $k$ -áris alpművelet és  $\rho(a_1), \dots, \rho(a_k) \in A/\rho$ , akkor legyen

$$m(\rho(a_1), \dots, \rho(a_k)) = \rho(m(a_1, \dots, a_k)). \quad (\text{ii})$$

Természetesen, a  $\rho(a_i)$  osztályokból az  $a_i$  elemek helyett más reprezentáns elemeket is választhattunk volna, pl. megfelelően a  $b_i$  elemeket (ekkor minden  $i$ -re  $\rho(a_i) = \rho(b_i)$ , másképpen  $(a_i, b_i) \in \rho$ ), és ezeket használva is megadhattuk volna az ezen osztályokon elvégzett  $m$  alpművelet eredményét:

$$m(\rho(a_1), \dots, \rho(a_k)) = m(\rho(b_1), \dots, \rho(b_k)) = \rho(m(b_1, \dots, b_k)),$$

ám ez az eredmény ugyanaz, mert a kongruencia definíciója szerint  $(m(a_1, \dots, a_k), m(b_1, \dots, b_k)) \in \rho$ . Ezt a megfigyelést úgy szoktuk kifejezni, hogy *kongruenciához tartozó osztályozás az alpműveletekkel kompatibilis* (azaz velük „összefér”). Indukcióval belátható, hogy kongruenciához tartozó osztályozás a termműveletekkel és a polinomműveletekkel is kompatibilis. Ezért a kongruenciához tartozó osztályozást röviden *kompatibilis osztályozásnak* nevezzük. Ennek osztályait szokás a szóbanforgó kongruencia *blokkjainak* nevezni.

Az ilyen úton nyert,  $A$ -val megegyező típusú  $A/\rho$  algebraikat  $A$  faktoralgebráinak nevezzük. Részletesebben beszélve azt mondjuk, hogy  $A/\rho$  az  $A$  algebra  $\rho$  kongruencia szerinti faktoralgebrája. Algebra bármely faktoralgebrájának alaphalmaza tehát az algebra valamely kompatibilis osztályozása összes osztályainak (más szóval *blokkjainak*) halmaza, amelyen az alpműveleteket a (ii) szabály szerint végezzük. Ugyanígy végezzük faktoralgebrában a termműveleteket és a polinomműveleteket is.

**11. Reláció által generált kongruencia.** Legyen  $\rho$  tetszőleges reláció  $A$ -n, és jelölje  $\bar{\rho}$  az  $A$  algebra összes,  $\rho$ -t tartalmazó kongruenciáinak metszetét. Ezt  $A$   $\rho$  által generált kongruenciájának nevezzük. A kongruencia-generálás a kongruenciák alkotta lezárási rendszerhez tartozó lezárási operátor az  $A^2$  halmazon. Általában  $\bar{\rho}$  bővebb, mint a  $\rho$ -t tartalmazó legszűkebb ekvivalencia, mert az nem szükségképpen részalgebrája  $A^2$ -nek; hasonlóképpen  $\bar{\rho}$  általában bővebb, mint  $A^2$   $\rho$  által generált részalgebrája.

Láttuk, hogy a részalgebra-generálás a termműveletek segítségével jellemezhető. A kongruencia-generálás — tehát a  $\rho \mapsto \bar{\rho}$  lezárási operátor — ennél bonyolultabb de használható módon transzlációk alkalmazásával írható le.

Legyen  $a, b \in A$ . Az  $a = c_0, c_1, \dots, c_n = b$  véges sorozatot  $A$ - $\rho$ -sorozatnak nevezzük, ha vagy  $n = 0$  (és így  $a = b$ ), vagy pedig minden  $i \in \{1, \dots, n\}$  indexre létezik  $A$ -nak olyan  $\tau_i$  translációja, és léteznek olyan  $a_{i-1}, a_i \in A$  elemek, hogy

- (1)  $(a_{i-1}, a_i) \in \rho$  vagy  $(a_i, a_{i-1}) \in \rho$ ,
- (2)  $\tau(a_{i-1}) = c_{i-1}$  és  $\tau(a_i) = c_i$ .

Ha ilyen sorozat létezik, akkor azt mondjuk, hogy  $a$  és  $b$  összeköthető  $A$ - $\rho$ -sorozattal. (Pl. a kongruenciák translációk segítségével történt jellemzésénél  $A$ - $\rho$ -sorozattal kötöttük össze  $m(a_1, \dots, a_k)$ -t és  $m(b_1, \dots, b_k)$ -t.)

*Malcev-lemma:* Legyen az  $A$  algebra és a  $\rho \in A^2$  reláció tetszőleges. Bármely  $a, b \in A$ -ra  $(a, b) \in \bar{\rho}$  akkor és csak akkor, ha  $a$  és  $b$  összeköthető  $A$ - $\rho$ -sorozattal.

A bizonyításhoz jelölje  $\bar{\rho}$  mindazon  $A$ -beli elempárok halmazát, amelyek összeköthetők  $A$ - $\rho$ -sorozattal. Először belátjuk, hogy  $\bar{\rho} \subseteq \bar{\rho}$ . Ehhez elég megmutatnunk, hogy  $\bar{\rho}$  kongruencia. Azt igazoljuk, hogy  $\bar{\rho}$  ekvivalencia, amelyet minden transláció megőriz. Az  $A$ - $\rho$ -sorozat definíciója szerint  $\bar{\rho}$  reflexív; szimmetrikus is, mert  $A$ - $\rho$ -sorozat fordított sorrendben is  $A$ - $\rho$ -sorozat; végül tranzitív, mert két  $A$ - $\rho$ -sorozatot egymás után írva is  $A$ - $\rho$ -sorozatot kapunk. Most tegyük fel, hogy  $a$  és  $b$  összeköthető  $A$ - $\rho$ -sorozattal, amelyben a  $c_1, \dots, c_{n-1}$  elemek és a  $\tau_1, \dots, \tau_n$  translációk lépnek fel. Akkor bármely  $\sigma$  translációra  $\sigma(a)$  és  $\sigma(b)$  is összeköthető  $A$ - $\rho$ -sorozattal, mégpedig olyanal, amelyben a  $\sigma(c_1), \dots, \sigma(c_{n-1})$  elemek és a  $\tau_i \cdot \sigma : a \mapsto \sigma(\tau_i(a))$  ( $i = 1, \dots, n$ ) translációk lépnek fel.

Már csak azt kell belátnunk, hogy  $\bar{\rho} \supseteq \bar{\rho}$ . Legyen  $a, b \in A$  összekötve az  $a = c_0, c_1, \dots, c_n = b$   $A$ - $\rho$ -sorozattal. Ha  $a = b$ , akkor  $(a, b) \in \bar{\rho}$ , mivel  $\bar{\rho}$  kongruencia s így reflexív. A translációk megőrzik a kongruenciákat, másrészt a kongruenciák szimmetrikusak; ezért  $i = 1, \dots, n$ -ra  $(c_{i-1}, c_i) \in \bar{\rho}$ . Végül  $\bar{\rho}$  tranzitív, s ebből következik  $(a, b) \in \bar{\rho}$ .

A Malcev-lemma alkalmazásaként leírjuk az algebraik részhalmazai által generált kongruenciákat, tehát adott  $A$  algebra alaphalmazának bármely  $H$  részhalmazához megadjuk a legszűkebb olyan kongruenciát, amelynek alkalmas blokkja tartalmazza  $H$ -t. Jelölje  $\chi$  a  $H \times H$  ( $\subseteq A \times A$ ) relációt  $A$ -n. Ekkor a keresett kongruencia  $\bar{\chi}$ , azaz mindazon párok halmaza ( $A \times A$ -ban) amelyek összeköthetők  $A$ - $\chi$ -sorozattal. Mivel  $\chi$  szimmetrikus, az  $A$ - $\chi$ -sorozatok definíciója az általános definíciónál valamivel egyszerűbb: olyan  $a = c_0, c_1, \dots, c_n = b$  sorozatok ezek, amelyekben bármely két szomszédos  $c_{i-1}, c_i$  elem két  $H$ -beli elemből ugyanazzal a  $\tau_i$  translációval nyerhető.

Eredményünket felhasználjuk a kongruenciák blokkjainak jellemzésére:

*Ljapin-Malcev-lemma:* A tetszőleges  $A$  algebra nemüres  $H$  részhalmazához akkor és csak akkor létezik  $A$ -nak olyan kongruenciája, amelynek  $H$  blokkja, ha  $A$

bármely  $\sigma$  translációjára és bármely  $h_1, h_2 \in H$  elemekre  $\sigma(h_1) \in H$ -ből következik  $\sigma(h_2) \in H$ .

A kongruenciák blokkjait tehát az jellemzi, hogy ezeket minden transláció vagy önmagukba, vagy komplementer halmazukba képezi le. A bizonyításhoz tegyük fel, hogy az  $A$  algebra  $H$  részhalmaza  $A$  valamely  $\rho$  kongruenciájának blokkja. Ha létezne olyan  $\sigma$  transláció és olyan  $h_1, h_2 \in H$  elemek, hogy  $\sigma(h_1) \in H$ , de  $\sigma(h_2) \notin H$ , akkor  $\sigma$  nem őrizné meg a  $\rho$  kongruenciát. Fordítva, tegyük fel, hogy  $H$  egyetlen kongruenciának sem blokkja  $A$ -ban. Akkor  $H$  nem blokkja a  $\chi$  kongruenciának sem, ahol  $\chi = H \times H$  (mint fentebb). Ezért létezik  $A$ -ban olyan  $a \in H$  és  $b \notin H$ , amelyek  $A$ - $\chi$ -sorozattal összeköthetők. Ha ennek a  $a = c_0, c_1, \dots, c_n = b$  sorozatnak a képzése során rendre a  $\sigma_1, \dots, \sigma_n$  translációk lépnek fel, és a sorozatban  $c_j$  a legkisebb indexű olyan elem, amely már  $H$ -n kívül van, akkor léteznek olyan  $h_1, h_2 \in H$  elemek, hogy  $\sigma_j(h_1) = c_{j-1} \in H$ , de  $\sigma_j(h_2) = c_j \notin H$ .

**12. Izomorfia.** Az összes valós számok additív csoportja bizonyos értelemben ugyanaz a csoport, mint a pozitív valós számok multiplikatív csoportja; ez teszi lehetővé, hogy a bonyolultabb szorzást logaritmusfüggvény segítségével az egyszerűbb összeadásra vezessük vissza. Ilyenfajta megfigyelések mindennaposak az algebrában. Ezt a jelenséget az *izomorfia* fogalommal tehetjük pontossá.

Legyenek  $A$  és  $B$  hasonló algebrák. Azt mondjuk, hogy  $A$  *izomorf*  $B$ -vel, ha létezik olyan  $\phi : A \rightarrow B$  bijektív leképezés, hogy minden nemnegatív egész  $k$ -ra,  $k$ -áris műveletjelre és  $a_1, \dots, a_k \in A$  elemekre

$$\phi(m(a_1, \dots, a_k)) = m(\phi(a_1), \dots, \phi(a_k)) \quad (\text{iii})$$

(szavakban:  $\phi$  az alaplmműveletekkel felcserélhető). Ezáltal hasonló algebrák bármely halmazán egy relációt definiáltunk, amelynek neve *izomorfia*, jele  $\cong$ . Magát  $\phi$ -t *izomorf leképezésnek* vagy *izomorfizmusnak* nevezzük. Hasonló algebrák bármely halmazán az *izomorfia ekvivalencia*; a reflexivitás, szimmetria és tranzitivitás belátásához csak azt kell meggondolnunk, hogy az identikus leképezés izomorfizmus, izomorf leképezés inverze is izomorf (indirekt módon igazoljuk!), és izomorf leképezések szorzata is izomorf. Az izomorfia szimmetriája miatt azt is mondhatjuk, hogy  $A$  és  $B$  *izomorfok*. (Vigyázat! Az „izomorf” szó leképezésre vonatkozva tulajdonságot, algebrákra vonatkoztatva viszonyt fejez ki.)

Izomorf leképezés részalgebrát részalgebrába, generátumot generátumba, kongruenciát kongruenciába visz át, emellett felcserélhető a termmműveletekkel és — bizonyos értelemben — a polinommműveletekkel. (Fogalmazzuk meg részletelesen és lássuk be ezeket a megállapításokat.) Mivel algebrák minden vizsgálatra érdemes tulajdonsága a műveletekkel írható le, és matematikai vizsgálatuk közben

elemeik mibenléte vagy jelölése érdektelen, az *izomorf algebraikat nem tekintjük különbözőeknek*, ahhoz hasonlóan, ahogyan az egybevágó háromszögeket sem tekintjük különböző alakzatoknak.

Az izomorfia fogalma lehetővé teszi, hogy a direkt szorzat fogalmat — amellyel adott algebraiból új algebrát „rakunk össze” — algebraik „felbontására” is felhasználjuk. Ha egy  $D$  algebra izomorf bizonyos  $A_\alpha$  algebrak direkt szorzatával, akkor azt mondjuk, hogy  $D$  *felbontható ezen algebrak direkt szorzatára*. Az  $A_\alpha$  algebraikat ilyenkor is  $D$  direkt tényezőinek nevezzük. Eltérően a csoportok ismert esetétől,  $D$  nem szükségképpen tartalmaz az  $A_\alpha$ -kkal izomorf részalgebraikat. Pl. két kételemű grupoid direkt szorzata, ahol egyikük művelete a Sheffer-művelet ( $00 = 1$ , különben  $xy = 0$ ), a másiké az implikáció ( $10 = 1$ , különben  $xy = 0$ ), nem tartalmaz a másodikkal izomorf részalgebraikat. Nyilvánvalóan minden algebra felbontható önmagának és az egyelemű algebrainak (ilyen minden hasonlósági osztályban van!) a direkt szorzatára. Ha egy algebra más módon nem is bontható fel kéttényezős direkt szorzatra, akkor *direkt felbonthatatlannak* nevezzük, egyébként *direkt felbonthatónak*.

Tekintsük a  $D = \prod_{\alpha \in I} A_\alpha$  direkt szorzatot, és legyen  $I = \bigcup_{\beta \in J} I_\beta$  az  $I$  indexhalmaz egy osztályozása. Akkor  $D$  felbomlik a  $\prod_{\alpha \in I_\beta} A_\alpha$  ( $\beta \in J$ ) algebrak direkt szorzatára. Az eredeti felbontást az utóbbi *finomításának* nevezzük (mert úgy keletkezik, hogy az utóbbi felbontás direkt tényezőit tovább bontjuk). Ha egy  $D$  algebra direkt felbonthatatlan, akkor kettőnél több algebra direkt szorzatára is csak úgy bontható fel, hogy a direkt tényezők egyike  $D$ , a többiek pedig egyeleműek, mert minden direkt felbontás valamely kéttényezős direkt felbontás (amely természetesen nem egyértelműen meghatározott) finomítása.

Az izomorfia egy másik alkalmazása direkt szorzatokra: tekintsük a  $D = \prod_{\alpha \in I} A_\alpha$  direkt szorzatot és legyen  $\beta \in I$ . Mint láttuk, a  $\pi_\beta$  reláció természetes kongruenciája  $D$ -nek (lásd a 9. fejezetet). A  $D/\pi_\beta$  faktoralgebra a  $\pi_\beta(\zeta)$  (kiválasztási függvényekből álló) osztályok alkotják. Ekkor  $D/\pi_\beta \cong A_\beta$ . Valóban, a  $\pi_\beta(\zeta) \mapsto \zeta(A_\beta)$  leképezés izomorfizmus: a  $\pi_\beta$  és  $\zeta$  leképezések definíciójából következik, hogy bijektív, továbbá az alpműveletekkel felcserélhető:

$$\begin{aligned}\pi_\beta(m(\zeta_1, \dots, \zeta_k)) &= m(\zeta_1, \dots, \zeta_k)(A_\beta) \\ &= m(\zeta_1(A_\beta), \dots, \zeta_k(A_\beta)) = m(\pi_\beta(\zeta_1), \dots, \pi_\beta(\zeta_k)).\end{aligned}$$

Ezzel megmutattuk, hogy *direkt szorzat természetes kongruenciák szerinti faktoralgebrai izomorfok a direkt szorzat megfelelő direkt tényezőivel*.

**13. Homomorfia.** Ha az izomorfizmus definíciójából elhagyjuk a bijektivitást követelményét, akkor a homomorfizmus definíciójához jutunk. *Homomorfizmusnak*

tehát algebrának hasonló algebrába való olyan  $\phi$  leképezését nevezzük, amelyre a (iii) szabály érvényes. Ha az  $A$  algebrának létezik homomorf leképezése a  $B$  algebrára, akkor azt mondjuk, hogy  $B$   $A$ -nak homomorf képe. (Nem [!] szokás azt mondani, hogy „ $A$  homomorf  $B$ -vel”, vagy hogy „ $A$  és  $B$  homomorfok”.) Homomorfizmus és izomorfizmus szorzata (akármilyen sorrendben) mindig homomorfizmus. Ebből következik, hogy ha  $A$ -nak  $B$  homomorf képe és  $B \cong C$ , akkor  $C$  is homomorf képe  $A$ -nak, s ez akkor is teljesül, ha  $A \cong B$  és  $B$ -nek homomorf képe  $C$ .

Példa: tetszőleges  $A$  algebra bármely faktoralgebrája  $A$ -nak homomorf képe. Valóban, ha  $\rho \in \text{Con } A$ , akkor az  $a \mapsto \rho(a)$  leképezés  $A$ -nak  $A/\rho$ -ra való homomorfizmusa. A (iii) szabály erre a leképezésre alkalmazva a faktoralgebra alaplíműleteinek definíciójába megy át. E példa állításának a megfordítása is érvényes „izomorfiaig terjedő pontossággal”:

*Homomorfia-tétel:* Algebra bármely homomorf képe izomorf az algebra valamely faktoralgebrájával.

Legyen  $A$  homomorf képe  $B$ , és legyen  $\phi$  az ezt biztosító homomorfizmus. Ugyanezt a  $\phi$  jelet használjuk egy reláció jelölésére is  $A$ -n: legyen  $(a_1, a_2) \in \phi$  akkor és csak akkor, ha  $\phi(a_1) = \phi(a_2)$ . Az, hogy a  $\phi$  leképezésre teljesül a (iii) szabály, éppen azt jelenti, hogy a  $\phi$  relációra teljesül a kongruenciák definíciójában látott (i) szabály. Emellett  $\phi$  ekvivalencia, ezért kongruenciája  $A$ -nak. Létezik tehát az  $A/\phi$  faktoralgebra. Megmutatjuk, hogy  $A/\phi \cong B$ . Az ehhez szükséges izomorfizmus az a leképezés, amely a tetszőleges  $\phi(a)$  kongruenciaosztálynak  $B$   $\phi(a)$  elemét felelteti meg. Ez a leképezés definíciója szerint bijektív, továbbá minden  $m$  alaplíművelettel felcserélhető: a  $\phi(a_1), \dots \in A/\phi$  faktoralgebra-elemeken az  $m$  műveletet és a leképezést akármelyik sorrendben is végezzük el, az eredmény  $m(\phi(a_1), \dots) \in B$ .

**14. Izomorfiatételek.** Ezek a tételek azt mondják ki, hogy adott algebrából részalgebra- és faktoralgebra-képzés bizonyos különböző módokon történő alkalmazásával előálló algebrák izomorfoknak bizonyulnak. Tekintsünk egy  $A$  algebrát. Legyen  $H \leq A$ ,  $\rho \in \text{Con } A$ . Jelölje  $\rho|H$  a  $\rho$  kongruencia  $H$ -ra való megszorítását, vagyis a  $\rho \cap (H \times H)$  relációt  $H$ -n. Mivel ekvivalencia részhalmazra való megszorítása ekvivalencia a részhalmazon, és részalgebrák metszete részalgebra,  $\rho|H$  kongruenciája  $H$ -nak. Jelölje továbbá  $\rho(H)$  mindazon  $a \in A$  elemek halmazát, amelyek kongruensek ( $\rho$ -ra vonatkozóan)  $H$  valamely elemével. A részalgebra és a kongruencia definíciójából következik, hogy  $\rho(H)$  részalgebra  $A$ -ban. Ezeket a jelöléseket együttesen is használhatjuk, pl.  $\rho|H$  a  $\rho$  kongruenciának a  $\rho(H)$  részalgebrára való megszorítását jelenti.

*Első izomorfia-tétel:*  $\rho(H) / (\rho|H) \cong H / \rho|H$ .

A bal oldal (azaz a bal oldali faktoralgebra) elemei  $\rho$  azon blokkjai, amelyek metszete  $H$ -val nem üres. Megmutatjuk, hogy a keresett izomorfizmus az a leképezés lesz, amely mindegyik ilyen  $\rho(h)$  ( $h \in H$ ) blokknak megfelelteti a  $H$ -val való metszetét. Ezek a metszetek éppen a jobb oldal elemei. Ezért a  $H$ -val való metszés a bal oldalnak a jobb oldalra való bijektív leképezése. Legyen  $k$  nemnegatív egész,  $m$   $k$ -áris alpművelet, és legyenek  $\rho(h_1), \dots, \rho(h_k)$  ( $h_1, \dots, h_k \in H$ ) a bal oldal tetszőleges elemei. Akkor

$$\begin{aligned} m(\rho(h_1) \cap H, \dots, \rho(h_k) \cap H) &= m((\rho|H)(h_1), \dots, (\rho|H)(h_k)) \\ &= (\rho|H)(m(h_1, \dots, h_k)) = \rho(m(h_1, \dots, h_k)) \cap H \\ &= m(\rho(h_1), \dots, \rho(h_k)) \cap H, \end{aligned}$$

tehát a  $H$ -val való metszés felcserélhető az alpműveletekkel.

Legyen  $\rho$  és  $\sigma$  olyan kongruenciája  $A$ -nak, hogy  $\rho \leq \sigma$ . Ekkor  $\sigma$  minden blokkja  $\rho$  bizonyos blokkjainak egyesítése. Tekintsük az  $A/\rho$  faktoralgebrán a  $\rho(a_1) \sim \rho(a_2) \iff (a_1, a_2) \in \sigma$  összefüggés által definiált  $\sim$  relációt, s ellenőrizzük, hogy  $\sim$  kongruenciája a faktoralgebrának. Használjuk  $\sim$  helyett a természetes  $\sigma/\rho$  jelölést.

*Második izomorfia-tétel:*  $(A/\rho) / (\sigma/\rho) \cong A/\sigma$ .

Itt a bal oldal elemei  $\rho$  blokkjainak olyan halmazai, amelyek  $\sigma/\rho$  egy-egy blokkját alkotják, s ennél fogva  $(\sigma/\rho)(\rho(a))$  alakban írhatók fel. Feleltessük meg ennek a „blokk-blokknak” a jobb oldal  $\sigma(a)$  elemét. Belátjuk, hogy ez a megfeleltetés lesz a keresett izomorfizmus. Azt, hogy bijektív,  $\sigma/\rho$  definíciójából látjuk. Megmutatjuk, hogy felcserélhető az alpműveletekkel. Ha először a megfelelő számú  $(\sigma/\rho)(\rho(a_1)), \dots \in (A/\rho) / (\sigma/\rho)$  elemeken végezzük el az  $m$  alpműveletet, s az eredményre alkalmazzuk a megfeleltetést,  $\sigma(m(a_1, \dots))$  adódik. Ha pedig ugyanezekre az elemekre előbb a megfeleltetést alkalmazzuk, s képeiken végezzük el az  $m$  műveletet, az eredmény  $m(\sigma(a_1), \dots)$ , s a két eredmény a faktoralgebra alpműveleteinek definíciója szerint ugyanaz.

Gondoljuk meg, hogy abban az esetben, amikor  $A$  csoport, a most bebizonyított két izomorfia-tétel az ismert két csoportelméleti izomorfia-tételbe megy át.

**15. Ekvivalens algebrák.** Ismeretes, hogy minden Boole-algebra tekinthető Boole-gyűrűnek: adott  $(A, \{\cup, \cap, \bar{\cdot}\})$  Boole-algebrán a gyűrűműveleteket interpretálhatjuk a Boole-algebra termműveleteivel:

$$x_1 + x_2 = (x_1 \cap \bar{x}_2) \cup (\bar{x}_1 \cap x_2), \quad x_1 \cdot x_2 = x_1 \cap x_2, \quad -x_1 = \bar{x}_1.$$

Továbbá minden Boole-gyűrű tekinthető Boole-algebrának: adott  $(A, \{+, \cdot, 1\})$  Boole-gyűrűn a Boole-algebra-műveleteket interpretálhatjuk a Boole-gyűrű termműveleteivel:

$$x_1 \cup x_2 = x_1 + x_2 + x_1 \cdot x_2, \quad x_1 \cap x_2 = x_1 \cdot x_2, \quad \bar{x}_1 = x_1 + 1.$$

Ezt a két művelet-átalakítást egymás után elvégezve a kiindulási alpműveleteket kapjuk vissza, akár Boole-algebra-műveletekből, akár Boole gyűrű-műveletekből indulunk ki. Ez a jelenség emlékeztet az izomorfia: úgy tűnik, hogy a Boole-algebrák lényegileg ugyanazok, mint a Boole-gyűrűk. Mindenesetre most nem izomorfia-ról van szó, mert a Boole-algebrák és a Boole-gyűrűk nem is hasonlóak.

Legyen adott két típus,  $(M_1, \tau_1)$  és  $(M_2, \tau_2)$ , és e típusok műveletjeinek egy-egy interpretációja ugyanazon az  $A$  halmazon. Így egy  $(A, F_1)$  első és egy  $(A, F_2)$  második típusú algebrát kapunk. Ha  $(A, F_1)$  összes termműveleteinek a halmaza ugyanaz, mint  $(A, F_2)$  összes termműveleteinek halmaza, akkor azt mondjuk, hogy  $(A, F_1)$  és  $(A, F_2)$  *ekvivalens algebrák*. A definícióból világos, hogy az algebrák ekvivalenciája a szó általános értelmében is ekvivalencia az  $A$  alaphalmazú algebrák bármely halmazán. Az algebrák ekvivalenciájának fogalmát kiterjeszthetjük különböző alaphalmazú algebrákra is: a tetszőleges típusú  $(A, F_1)$  és  $(B, F_2)$  algebrákat *ekvivalensnek* mondjuk, ha létezik az  $A$  alaphalmazon olyan  $(A, F_1)$ -gyel (az előző értelemben) ekvivalens,  $(B, F_2)$ -höz hasonló algebra, amely izomorf  $(B, F_2)$ -vel. Más szóval,  $A$  akkor és csak akkor és csak akkor ekvivalens  $B$ -vel, ha létezik  $A$ -nak  $B$ -re olyan  $\varphi$  bijektív leképezése és  $A$  termműveletei halmazának  $B$  termműveletei halmazára való olyan (aritást változtatlanul hagyó)  $\vartheta$  bijektív leképezése, hogy bármely nemnegatív egész  $k$ -ra,  $A$  bármely  $k$ -ásis  $t$  termműveletére és tetszőleges  $a_1, \dots, a_k$  elemeire

$$\varphi(t(a_1, \dots, a_k)) = (\vartheta(t))(\varphi(a_1), \dots, \varphi(a_k)).$$

Ez a reláció is ekvivalencia (a szó általános értelmében) algebrák bármely halmazán. Algebrák ekvivalenciája tehát lényegében azt jelenti, hogy ha termműveleteiket is alpműveleteknek tekintjük, akkor (újdonsült alpműveleteik jelölésétől eltekintve) izomorf algebrákká válnak. (Az alpműveletek jelölésének különbözőségét a  $\vartheta$  leképezés írja le.)

Minden Boole-algebra ekvivalens a belőle a fenti módon származtatható Boole-gyűrűvel (és viszont). Ha ugyanis két  $A$  alaphalmazú algebra olyan, hogy mindegyikük alpműveletei a másiknak termműveletei, akkor indukcióval igazolhatjuk, hogy mindegyikük termműveletei a másiknak is termműveletei, tehát a két algebra termműveleteinek halmaza ugyanaz.

Az izomorfia-hoz hasonlóan, algebrák ekvivalenciája is lehetővé teszi, hogy adott algebra helyett egy vele ekvivalens és valamilyen szempontból könnyebben vizsgálható algebrával dolgozzunk. (Az utóbbinak pl. megegyező alaphalmaz esetén ugyanazok lesznek a konstans műveletei és így a polinomműveletei is, mint az adott algebrának; ezért ugyanazon relációi lesznek kongruenciák, és í. t.) Egy konkrét példa: tekintsünk egy csoportot, amelynek exponense 2 (ami azt jelenti, hogy benne minden elem rendje 2, ahonnan az is következik, hogy a cso-

port Abel-féle). Ha csoportunkban alpműveletei — bináris összeadás, unáris additív inverz-képzés (ami esetünkben az identikus leképezés) és a 0 nulláris additív egységelem — mellé további alpműveletekként bevezetjük a  $GF(2)$  kételemű test egységelemével és zéruselemével való szorzásként az identikus leképezést ill. a 0 konstans leképezést, akkor ezáltal csoportunk alaphalmazán  $GF(2)$  feletti vektorteret vezettünk be (ellenőrizzük a vektortér definiáló tulajdonságainak teljesülését!), a csoport termműveleteinek halmazát azonban nem bővítettük. Eszerint minden 2 exponensű csoport ekvivalens egy  $GF(2)$  feletti vektortérrel. Megmutatjuk, hogy *bármely két megszámlálható 2 exponensű csoport izomorf egymással*. Ehhez elegendő azt belátni, hogy bármely két  $GF(2)$  feletti megszámlálható vektortér izomorf egymással. Ezt a következő gondolatmenet mutatja. A Zorn-lemma szerint egy ilyen vektortérben van maximális független elemrendszer; elemi halmazelmélettel látjuk, hogy az szükségképpen megszámlálható; végül a véges dimenziós vektorterekre használt megfontolással kapjuk, hogy *két* ilyen vektortér szükségképpen izomorf. A megszámlálható 2 exponensű csoportnak fontos szerepe van a diszkrét játékok elméletében: ez a nemnegatív egész számok csoportja a nim-összeadás (azaz kettes számrendszerben végzett számjegyenkénti modulo 2 összeadás) műveletére vonatkozóan.

**16. Szubdirekt szorzat.** Megvizsgáljuk a  $D = \prod_{\alpha \in I} A_\alpha$  direkt szorzat részalgebráit. Legyen  $C \leq D$ , és tekintsünk egy  $\beta \in I$  indexet. Az  $A_\beta$  direkt tényező mindazon elemei, amelyeket  $C$ -hez tartozó kiválasztási függvény  $A_\beta$ -n felvesz, a direkt szorzat alpműveleteinek definíciója szerint  $A_\beta$ -nak részalgebráját képezik. Ezt a részalgebrát  $C$   $\beta$ -vetületének nevezzük  $D$ -ben; jele  $C_\beta$ . Ha minden  $\beta \in I$ -re  $C_\beta = A_\beta$ , akkor azt mondjuk, hogy  $C$  az  $A_\alpha$  ( $\alpha \in I$ ) algebrák *szubdirekt szorzata*, ezeket az algebrákat pedig  $C$  *szubdirekt tényezőinek* nevezzük. Ellentétben a direkt szorzattal, a szubdirekt szorzat nem egyértelműen meghatározott: algebrák direkt szorzata egyben szubdirekt szorzatuk is, de pl. az  $A^2$  algebra átlója is szubdirekt szorzata  $A$  két példányának. A definícióból látszik, hogy *algebrák direkt szorzatának bármely részalgebrája a tekintett algebrák részalgebráinak szubdirekt szorzata*.

A direkt szorzat természetes kongruenciáit változtatlan módon vezethetjük be tetszőleges szubdirekt szorzatra. Ezeknek a természetes kongruenciák szerinti faktoralgebrái is izomorfok a megfelelő szubdirekt tényezőkkel, továbbá az összes természetes kongruenciák metszete az egyenlőségreláció. Ebből következik, hogy ha egy  $C$  algebra izomorf valamely  $A_\alpha$  ( $\alpha \in I$ ) algebrák szubdirekt szorzatával, akkor vannak olyan kongruenciái, amelyek metszete az egyenlőségreláció, s amelyek szerinti faktoralgebrák izomorfok az  $A_\alpha$  ( $\alpha \in I$ ) algebrákkal. Ennek a megfordítása is igaz, tehát *egy algebra akkor és csak akkor izomorf bizonyos algebrák szubdirekt szorzatával, ha vannak olyan kongruenciái, amelyek metszete az egyenlőség, s*

amelyek szerinti faktoralgebrák izomorfok azokkal az algebrákkal.

Csak az „akkor” állítást kell igazolnunk. Legyen a tekintett algebra  $C$ , a kongruenciák  $\rho_\alpha$  ( $\alpha \in I$ ), és legyen minden  $\alpha$ -ra  $C/\rho_\alpha \cong A_\alpha$ . Ezt az izomorfiát biztosító izomorfizmusnál tetszőleges  $c \in C$ -re legyen  $\rho_\alpha(c)$  képe  $a_\alpha^c$ . A  $C$  algebra keresett izomorfizmusa az  $A_\alpha$  algebrák szubdirekt szorzatára a

$$\phi = c \mapsto \zeta_c : A_\alpha \mapsto a_\alpha^c \quad (c \in C)$$

leképezés. Mivel az  $a_\alpha^c$  képelemek kimerítik  $A_\alpha$ -t,  $C$   $\phi$  melletti képének  $\alpha$ -vetülete  $A_\alpha$  minden  $\alpha \in I$ -re. A  $\phi$  leképezés injektív, ha ugyanis  $\phi(c) = \phi(c')$ , akkor  $a_\alpha^c = a_\alpha^{c'}$  minden  $\alpha \in I$ -re, amiből következik  $(c, c') \in \bigcap_{\alpha \in I} \rho_\alpha$ , s ez azt jelenti, hogy  $c = c'$ . Végül,  $\phi$  minden  $m$  alaplíművelettel felcserélhető:

$$m(\phi(c_1), \dots, \phi(c_k)) = m(\zeta_{c_1}, \dots, \zeta_{c_k}) = \zeta_{m(c_1, \dots, c_k)} = \phi(m(c_1, \dots, c_k)).$$

A most bizonyított tényből a következőt is leszűrhetjük. Legyenek  $\rho_\alpha$  ( $\alpha \in I$ ) az  $A$  algebra kongruenciái, és legyen  $\bigcap_{\alpha \in I} \rho_\alpha = \rho$ . Akkor  $A/\rho$  izomorf az összes  $A/\rho_\alpha$  algebrák szubdirekt szorzatával. Valóban, ekkor az  $A/\rho$  algebrában az egyenlőségreláció az összes  $\rho_\alpha/\rho$  kongruenciák metszete, ezért  $A/\rho$  izomorf az összes  $(A/\rho) / (\rho_\alpha/\rho)$  faktoralgebrák szubdirekt szorzatával; ezek azonban a második izomorfia-tétel szerint izomorfok a megfelelő  $A/\rho_\alpha$  algebrákkal.

Ha egy algebra izomorf bizonyos algebrák szubdirekt szorzatával, azt is mondhatjuk, hogy azok szubdirekt szorzatára bomlik (hasonlóan a direkt szorzatra vonatkozó szóhasználatához). Ha egy algebra egyenlőségtől (azaz egyenlőségrelációtól) különböző összes kongruenciájának metszete különbözik az egyenlőségtől, akkor az algebra kongruenciáinak bármely olyan halmazában, amelyek metszete az egyenlőség, elő kell fordulnia az egyenlőségnek. Ilyenkor tehát az algebra akárhogy is bomlik bizonyos algebrák szubdirekt szorzatára, azok között ott van maga az algebra is. Ebben az esetben az algebrát szubdirekt felbonthatatlannak (vagy szubdirekt irreducibilisnek) nevezzük. Minden algebrát saját egytényezős direkt (és így szubdirekt) felbontásának tekinthetünk (mert az egyetlen egyenlőségreláció metszete maga az egyenlőség).

Példák: Legyen  $p_1, p_2, \dots$  az összes prímszámok sorozata. Ha két egész szám mindegyik  $p_i$  modulusra nézve kongruens egymással, akkor szükségképpen egyenlők. Ezért az egész számok gyűrűje az összes mod  $p_i$  maradékosztálytestek szubdirekt szorzatára bomlik. Másrészt nevezzük egyszerűnek az olyan algebrát, amelynek csak triviális kongruenciái vannak (ez az egyszerű csoport és gyűrű fogalmának általánosítása). Minden egyszerű algebra szubdirekt felbonthatatlan.

**17. Birkhoff szubdirekt felbontási tétele.** Minden véges  $A$  algebra direkt felbonthatatlan algebrak direkt szorzatára bomlik. Valóban, ha  $A$  direkt felbontható, felbontása lépésenként addig finomítható, amíg csupa direkt felbonthatatlan direkt tényezőhöz jutunk. (Ezt  $A$  elemeinek száma szerinti teljes indukciós bizonyítással pontosíthatjuk.) Megfigyelésünk érvénye nem terjeszthető ki végtelen (alaphalmazú) algebraikra. Ellenpélda: egy megszámlálható 2 exponensű  $G$  csoport bárhogyan bomlik akárhány egynél több elemű csoport direkt szorzatára, azok között mindig van direkt felbontható. Valóban, a direkt tényezők, mivel mind  $G$  homomorf képei, maguk is véges, vagy megszámlálható 2 exponensű csoportok. Mindnyájan végesek nem lehetnek, mert akkor számuk megszámlálható lenne, márpedig megszámlálható egynél több elemű csoport direkt szorzata megszámlálhatónál több elemű. Van tehát köztük megszámlálható 2 exponensű csoport. Mint a 15. fejezetből tudjuk, ilyen csoport (izomorfiaig terjedő pontossággal) csak egy van. Az pedig direkt felbontható: tekintsük  $GF(2)$  feletti vektortérnek, egy bázisát bontsuk két részhalmazára, s akkor csoportunk e két részhalmaz generátumainak direkt szorzatára bomlik.

A szubdirekt felbonthatóság véges és végtelen algebraikra egységesen tárgyalható:

*Birkhoff tétele: Bármely algebra szubdirekt felbonthatatlan algebrak szubdirekt szorzatára bomlik.*

Legyen  $A$  tetszőleges algebra és legyenek  $a, b \in A$  különbözők. Tekintsük  $A$  mindazon  $\rho$  kongruenciáinak halmazát, amelyekre  $(a, b) \notin \rho$ , szavakban: amelyek szétválasztják  $a$ -t és  $b$ -t. Kongruenciák tartalmazás szerint növekvő láncának (azaz véges vagy végtelen sorozatának) egyesítése is kongruencia (gondoljuk meg), s ha  $e$  kongruenciák mindegyike szétválasztja  $a$ -t és  $b$ -t, akkor növekvő láncuk egyesítése is. Ezért a Zorn-lemma szerint  $A$   $a$ -t és  $b$ -t szétválasztó kongruenciái között van maximális; jelölje ezt  $\rho_a^b$ .

Megmutatjuk, hogy a  $A/\rho_a^b$  faktoralgebra szubdirekt felbonthatatlan. Ha ugyanis  $\rho'$  egyenlőségtől különböző kongruenciája  $\text{Con } A/\rho_a^b$ -nek, akkor az

$$(u, v) \in \rho^* \iff (\rho_a^b(u), \rho_a^b(v)) \in \rho'$$

által definiált  $\rho^*$  reláció kongruenciája  $A$ -nak, amely valódi módon tartalmazza  $\rho_a^b$ -t, és így  $(a, b) \in \rho^*$ , tehát  $(\rho_a^b(a), \rho_a^b(b)) \in \rho'$ . Nyertük, hogy  $(\rho_a^b(a), \rho_a^b(b))$  benne van  $A/\rho_a^b$  minden egyenlőségtől különböző kongruenciájában, tehát mindezek metszetében is. Másrészt  $\rho_a^b(a) \neq \rho_a^b(b)$  a  $\rho_a^b$  reláció definíciója miatt. Így  $A/\rho_a^b$  egyenlőségtől különböző kongruenciáinak metszete nem az egyenlőség.

Képezzük az összes különböző  $\rho_a^b$  kongruenciákat. Ezek metszete az egyenlőségreláció, mert köztük bármely  $a, b \in A$  elemeket szétválasztó kongruenciát találunk.

Ez azt jelenti, hogy  $A$  az  $e$  kongruenciák szerinti faktoralgebrák szubdirekt szorzatára bomlik, azokról pedig most láttuk be, hogy szubdirekt felbonthatatlanok.

**18. Lezárási operátorok algebrák osztályain.** Legyen adva hasonló algebráknak egy  $\mathcal{A}$  osztálya. Az  $\mathcal{A}$  osztályt *absztrakt osztálynak* nevezzük, ha bármely algebrájával együtt minden azzal izomorf algebrát is tartalmaz. A továbbiakban tekintett algebraosztályokról feltesszük, hogy absztrakt osztályok.

Jelölje  $S\mathcal{A}$  mindazon algebrák osztályát, amelyek izomorfok valamely  $\mathcal{A}$ -ba tartozó algebra valamely részalgebrájával. A részalgebra és az izomorfia definíciójából következik, hogy a  $\mathcal{A} \mapsto S\mathcal{A}$  megfeleltetés extenzív, monoton és idempotens (az utóbbi abból következik, hogy a „részalgebrája” reláció tranzitív).

Jelölje  $H\mathcal{A}$  mindazon algebrák osztályát, amelyek valamely  $\mathcal{A}$ -ba tartozó algebra homomorf képei. Az így definiált osztály is absztrakt algebraosztály, és a  $\mathcal{A} \mapsto H\mathcal{A}$  megfeleltetés is nyilvánvalóan extenzív és monoton, továbbá idempotens is (ez utóbbi a homomorfizáció és a második izomorfizáció következménye).

Jelölje továbbá  $P\mathcal{A}$  az összes olyan algebrák osztályát, amelyek izomorfok  $A$ -ba tartozó algebrák valamely rendszerének direkt szorzatával. Ennek a megfeleltetésnek is megvan az említett három tulajdonsága (az idempotensség itt a direkt szorzat finomíthatóságából következik). Ha itt direkt szorzat helyett szubdirekt szorzatot mondunk, a három tulajdonság változatlanul érvényes (és az idempotensség ugyanúgy látható be). Az így keletkező algebraosztályt  $P_s\mathcal{A}$  jelöli.

Jóllehet ezúttal nem halmazoperátorokkal van dolgunk, ezeket a megfeleltetéseket most is *lezárási operátoroknak* nevezzük. Ezekre az operátorokra nézve *zárt osztályok* azok az absztrakt algebraosztályok, amelyek algebráikkal együtt azoknak — megfelelően — összes részalgebráit, összes homomorf képeit (vagy, ami ugyanazt jelenti, faktoralgebráit), ill. összes direkt szorzatait is tartalmazzák.

Ezeket az operátorokat egymás után is alkalmazhatjuk. Ilyenkor, ahogyan általában leképezések esetén tesszük, operátorok esetén is ezek szorzatáról beszélünk, és ennek megfelelő jelölést alkalmazunk. A jelölés egyértelműsége érdekében megállapodunk, hogy pl.  $SP\mathcal{A}$  az  $\mathcal{A}$ -ba tartozó algebrák összes direkt szorzatainak összes részalgebrái izomorf képeinek osztálya. Szemmel láthatóan, bevezetett operátoraink szorzata is extenzív és monoton operátor, az azonban nem nyilvánvaló, hogy idempotens is. Az operátorok szorzása asszociatív művelet.

Legyen  $X, Y$  két operátor algebrák osztályain. Ha minden  $\mathcal{A}$  osztályra  $X\mathcal{A}$  részosztálya  $Y\mathcal{A}$ -nak, akkor azt mondjuk, hogy  $Y$  *bővebb* (és  $X$  *szűkebb*), s ezt így jelöljük:  $X \leq Y$ . A  $\leq$  reláció operátorok bármely halmazán részbenrendezés. Az operátorok szorzata  $e$  részbenrendezésre vonatkozóan monoton. Példa:  $P_s \leq SP$ .

A direkt szorzat és a részalgebra definíciójából közvetlenül következik, hogy *tetszőleges algebrák részalgebráinak direkt szorzata mindig részalgebrája a tekin-*

tett algebrák direkt szorzatának. Ez mutatja, hogy  $\mathbf{PS} \leq \mathbf{SP}$ . Ebből következik  $\mathbf{SP} \leq \mathbf{SPSP} \leq \mathbf{SSPP} = \mathbf{SP}$ , ami mutatja, hogy  $\mathbf{SP}$  idempotens, tehát  $\mathbf{SP}$  lezárási operátor. (Nem igaz  $\mathbf{PS} = \mathbf{SP}$ , azaz direkt szorzat részalgebrája nem mindig izomorf a direkt tényezők bizonyos részalgebráinak direkt szorzatával. Ellenpélda — erre is — a megszámlálható 2 exponensű csoport, amely két elemű csoportok megszámlálható rendszere direkt szorzatának részcsoportha, de nem izomorf két elemű csoportok részcsoportha semmilyen rendszerének direkt szorzatával. Gondoljuk meg, miért.)

Legyen  $\phi$  az  $\mathbf{A}$  algebrának  $\mathbf{A}_1$ -re,  $\psi$  pedig  $\mathbf{B}$ -nek  $\mathbf{B}_1$ -re való homomorf leképezése. Ekkor a  $\phi \times \psi : (a, b) \mapsto (\phi(a), \psi(b))$  leképezés  $\mathbf{A} \times \mathbf{B}$ -nek  $\mathbf{A}_1 \times \mathbf{B}_1$ -re való homomorfizmusa (ellenőrizzük!). Hasonló megállapítás igaz kéttényezős direkt szorzat helyett algebrák bármely rendszerének direkt szorzatára is. Innen következik, hogy *tetszőleges algebrák homomorf képeinek direkt szorzata mindig homomorf képe a tekintett algebrák direkt szorzatának*. Eszerint  $\mathbf{PH} \leq \mathbf{HP}$ , ahonnan az előző gondolatmenetet lemásolva kapjuk, hogy  $\mathbf{HP}$  is idempotens, tehát lezárási operátor. Ugyanez a megfontolás szubdirekt szorzatokra is megy, és azt adja, hogy  $\mathbf{P}_s\mathbf{H} \leq \mathbf{HP}_s$ , és  $\mathbf{HP}_s$  is lezárási operátor. (Direkt szorzat homomorf képe nem mindig direkt szorzata a direkt tényezők bizonyos homomorf képeinek. Valóban, tekintsünk két algebrát a  $\{0, 1\}$  halmazon egy-egy unáris művelettel, a nemidentikus permutációval ill. a konstans 0 leképezéssel; ezek direkt szorzatának van 3 elemű faktoralgebrája (ellenőrizzük), amely azonban nem lehet homomorf képeinek direkt szorzata, mert 3 prímszám [!].)

Legyen a  $\mathbf{A}$  algebra tetszőleges és  $\rho \in \text{Con } \mathbf{A}$ . Az  $\mathbf{A}/\rho$  faktoralgebra bármely részalgebráját alkotó blokkokban levő elemek halmaza részalgebra  $\mathbf{A}$ -ban. Ebből a homomorfizációt alkalmazva kapjuk, hogy *tetszőleges algebra homomorf képének részalgebrája mindig homomorf képe az algebra valamely részalgebrájának*. Innen  $\mathbf{SH} \leq \mathbf{HS}$ , tehát  $\mathbf{HS}$  is idempotens, és ezért lezárási operátor. (Algebra részalgebrájának homomorf képe nem mindig részalgebrája az algebra valamely homomorf képének. Mutassuk ezt meg, művelettáblázattal megadva olyan négy elemű grupoidot, amely egyszerű és nincs két elemű részcsoportha, de van olyan három elemű részgrupoidja, amelynek van két elemű faktorcsoportja.)

**19. Varietás.** Az olyan algebraosztályt, amely a  $\mathbf{H}$ ,  $\mathbf{S}$ ,  $\mathbf{P}$  operátorok mindegyikére nézve zárt, *varietásnak* nevezzük. Ha  $\mathcal{V}$  varietás, természetesen zárt a  $\mathbf{HSP}$  szorzatoperátorra vonatkozóan is. Ez a szorzat maga is lezárási operátor, ami az előző fejezetben látott összefüggések segítségével látható be: idempotens, mert

$$\mathbf{HSP} \leq \mathbf{HSPHSP} \leq \mathbf{HSHPS} \leq \mathbf{HHSSPP} = \mathbf{HSP}.$$

Másrészt algebrák bármely  $\mathcal{A}$  osztályára  $\mathbf{HSP } \mathcal{A}$  varietás; a három operátorra vonatkozó zártága ugyanazokkal az összefüggésekkel igazolható. Szűkebb varietás

nyilvánvalóan nem tartalmazhatja  $\mathcal{A}$ -t, ezért  $\mathbf{HSP} \mathcal{A}$ -t az  $\mathcal{A}$  osztály által generált varietásnak nevezzük, és  $\text{Var } \mathcal{A}$ -val is jelöljük. A varietások a szubdirekt szorzat által is jellemezhetők:

*Kogalovszkij tétele:*  $\mathbf{HSP} = \mathbf{HP}_s$ .

A bizonyításhoz belátjuk, hogy  $\mathbf{S} \leq \mathbf{HP}_s$ . Ehhez elegendő megmutatnunk, hogy bármely  $\mathbf{A}$  algebrára  $\mathbf{S} \{ \mathbf{A} \} \leq \mathbf{HP}_s \{ \mathbf{A} \}$ . Vegyük  $\mathbf{A}$  megszámlálhatóan végtelen példányának direkt szorzatát, s ennek az összes olyan kiválasztási függvényekből álló  $B$  részhalmazát, amelyek legfeljebb véges számú kivétellel  $\mathbf{A}$  minden példányához  $\mathbf{A}$ -nak ugyanazt az elemét rendelik. Ez a részhalmaz részalgebra a direkt szorzatban, továbbá az ilyen kiválasztási függvények által  $\mathbf{A}$  bármely rögzített példányából kiválasztott elemek között  $\mathbf{A}$  minden eleme előfordul. Így  $B \in \mathbf{P}_s \{ \mathbf{A} \}$ . Vezessük be  $B$ -n a következő  $\rho$  relációt: álljon két kiválasztási függvény ebben a relációban, ha legfeljebb véges számú kivétellel  $\mathbf{A}$  minden példányához  $\mathbf{A}$ -nak ugyanazt az elemét rendelik. Ellenőrizhetjük, hogy  $\rho \in \text{Con } B$ , és az  $B/\rho$  faktoralgebra izomorf  $\mathbf{A}$ -val. Az ehhez szükséges izomorfizmus az a leképezés, amely a véges számú hely kivételével mindenütt  $a$  ( $\in A$ ) értéket felvevő kiválasztási függvényekből álló blokkhoz magát az  $a$  elemet rendeli.

Ezután a tétel a

$$\mathbf{HSP} \leq \mathbf{HHP}_s \mathbf{P} \leq \mathbf{HP}_s \mathbf{P}_s = \mathbf{HP}_s \leq \mathbf{HSP}$$

tartalmazásokból következik; itt felhasználtuk a nyilvánvaló  $\mathbf{P} \leq \mathbf{P}_s$  összefüggést és az előző fejezetben látott példát.

Nevezzünk egy algebrát *megszámlálhatóan generáltnak*, ha létezik megszámlálható (azaz véges vagy megszámlálhatóan végtelen) generátorrendszere. Ha az  $\mathbf{A}$  algebra minden megszámlálhatóan generált részalgebrája egy  $\mathcal{V}$  varietáshoz tartozik, akkor  $\mathbf{A} \in \mathcal{V}$ .

Legyenek  $\mathbf{A}$  megszámlálhatóan generált részalgebrái  $\mathbf{A}_\alpha$  ( $\alpha \in I$ ). Tekintsük ezek rendszerén azokat a  $\zeta$  kiválasztási függvényeket, amelyekhez létezik olyan  $\beta \in I$  és  $a \in A$ , hogy minden olyan  $\gamma \in I$ -re, amelyre  $A_\beta \subseteq A_\gamma$ , teljesül  $\zeta(A_\gamma) = a$ . Ha  $\zeta_1, \dots, \zeta_k$  ilyen kiválasztási függvények és  $m$   $k$ -áris alapl művelet, akkor  $m(\zeta_1, \dots, \zeta_k)$  is ilyen. Valóban, ha  $\zeta_i$ -hez a  $\beta_i$  „küszöbindex” és az  $a_i \in A$  elem tartozik, akkor legyen az  $A_{\beta_1} \cup \dots \cup A_{\beta_k}$  halmaz generátuma az — ugyancsak megszámlálhatóan generált —  $\mathbf{A}_\delta$  részalgebra. Ekkor minden olyan  $\gamma \in I$ -re, amelyre  $A_\delta \subseteq A_\gamma$ ,  $\zeta_i(A_\gamma) = a_i$ , s ezért  $m(\zeta_1, \dots, \zeta_k)(A_\gamma) = m(a_1, \dots, a_k)$ . A tekintett kiválasztási függvények tehát egy  $\mathbf{D}$  részalgebrát alkotnak a  $\bigcap_{\alpha \in I} \mathbf{A}_\alpha$  direkt szorzatban. Bármely  $a \in A$ -hoz van olyan kiválasztási függvény, amely minden  $a$ -t tartalmazó  $\mathbf{A}_\alpha$ -ból  $a$ -t választja ki, ezért  $\mathbf{D}$  az  $\mathbf{A}_\alpha$  ( $\alpha \in I$ ) algebrák szubdirekt szorzata.

Vezessük be  $D$ -n a következő  $\rho$  relációt: legyen két kiválasztási függvény ebben a relációban, ha létezik olyan  $\beta \in I$  küszöbindex, hogy valahányszor  $A_\beta \subseteq A_\gamma$  ( $\gamma \in I$ ), mindannyiszor a két kiválasztási függvény  $A_\gamma$ -ból ugyanazt az elemet választja ki. Ellenőrizhetjük, hogy  $\rho \in \text{Con } \mathbf{H}$ , és az  $\mathbf{H}/\rho$  faktoralgebra izomorf  $\mathbf{A}$ -val. Az ehhez szükséges izomorfizmus az a leképezés, amely a valamely  $A_\alpha$ -nál bővebb  $A_\beta$ -kon mindenütt  $a (\in A)$  értéket felvevő kiválasztási függvényekből álló blokkhoz magát az  $a$  elemet rendeli. Nyertük, hogy

$$\mathbf{A} \in \text{HP}_s\{\mathbf{A}_\alpha | \alpha \in I\} \subseteq \text{HP}_s \mathcal{V} = \mathcal{V}.$$

**20. Azonosság.** Az adott típusú termekből álló párokat *azonosságoknak* nevezzük. Megállapodunk abban, hogy minden  $(t_1, t_2)$  azonosság két komponensét meg egyező arításúnak tekintjük. Vegyünk egy  $\mathbf{A}$  (ugyanolyan típusú) algebrát. Ha  $t_1$  és  $t_2$  ugyanazt a termműveletet határozza meg  $\mathbf{A}$ -n, azt mondjuk, hogy  $a(t_1, t_2)$  *azonosság teljesül* (vagy *érvényes*)  $\mathbf{A}$ -n. (Rövidebben:  $(t_1, t_2)$  *azonosság*  $\mathbf{A}$ -n, vagy  $t_1 = t_2$  *azonosság*  $\mathbf{A}$ -n.) Ha  $\mathcal{C}$  algebrák egy osztálya, és  $(t_1, t_2)$  teljesül minden  $\mathcal{C}$ -be tartozó algebrán, akkor azt mondjuk, hogy  $(t_1, t_2)$  *teljesül a  $\mathcal{C}$  osztályon*. Az  $\mathbf{A}$  algebrán, ill. a  $\mathcal{C}$  osztályon teljesülő összes azonosságok halmazát megfelelően  $\text{Id } \mathbf{A}$  és  $\text{Id } \mathcal{C}$  jelöli.

Definíciója szerint  $\text{Id } \mathcal{C}$  mindig reláció az adott típusú  $\mathbf{T}$  megszámlálható rangú termalgebrán; az is világos, hogy ekvivalenciareláció. A termműveletek definíciója mutatja, hogy  $\text{Id } \mathcal{C}$  kongruenciája  $\mathbf{T}$ -nek. Létezik tehát a  $\mathbf{T}/\text{Id } \mathcal{C}$  faktoralgebra. Ezt  $\mathcal{C}$  *megszámlálható rangú termművelet-algebrájának* nevezzük. Ha  $n$  nemnegatív egész, ehhez hasonló megfontolást végezhetünk és definíciót vezethetünk be az  $n$  rangú termalgebrán.

Algebra önmagába való homomorfizmusát az algebra *endomorfizmusának* hívjuk. Algebra  $\rho$  kongruenciáját *teljesen invariáns (kongruenciá)nak* nevezzük, ha  $\rho$  invariáns az algebra endomorfizmusaival szemben, azaz bármely  $\varepsilon$  endomorfizmusra  $(a, b) \in \rho$ -ból következik  $(\varepsilon(a), \varepsilon(b)) \in \rho$ . (Példa: ha egy  $\mathbf{G}$  véges csoportnak valamely  $\mathbf{N}$   $p$ -Sylow-csoportja normálosztó, akkor  $\mathbf{G} \mathbf{N}$  szerinti kongruenciája teljesen invariáns. Gondoljuk végig!) Az  $\text{Id } \mathcal{C}$  reláció a  $\mathbf{T}$  termalgebrának teljesen invariáns kongruenciája. Ennek belátásához vegyük észre, hogy  $\mathbf{T}$  bármely  $\varepsilon$  endomorfizmusát a határozatlanok halmazára való restrikciója teljesen meghatározza, ugyanis  $\varepsilon(t(x_1, \dots, x_n)) = t(\varepsilon(x_1), \dots, \varepsilon(x_n))$ , amit indukcióval igazolhatunk. Ebből az is látszik, hogy a határozatlanok  $\varepsilon(x_1), \dots$  képeit tetszésünk szerint választhatjuk. Eszerint  $\mathbf{T}$  minden endomorfizmusa valamely  $x_1 \mapsto s_1, \dots$  leképezés kiterjesztése az összes termek halmazára, ahol  $s_1, \dots$  tetszőleges termek. Ha a  $(t_1, t_2)$ , részletesebben  $(t_1(x_1, \dots, t_n), t_2(x_1, \dots, x_n))$

azonosság teljesül  $\mathcal{C}$ -n, akkor az azonosság teljesülésének definíciója szerint teljesül a  $(t_1(s_1, \dots, s_n), t_2(s_1, \dots, s_n))$  azonosság is, és ez éppen azt jelenti, hogy  $\text{Id } \mathcal{C}$  teljesen invariáns.

E megfigyelésünk megfordítása is igaz: a  $\mathbf{T}$  megszámlálható rangú termalgebra  $\rho$  bináris relációjához akkor és csak akkor létezik olyan  $\mathcal{C}$  osztály, hogy  $\rho = \text{Id } \mathcal{C}$ , ha  $\rho$   $\mathbf{T}$ -nek teljesen invariáns kongruenciája. Ennek eddig a „csak akkor” felét láttuk be. Az „akkor” igazolásához tegyük fel, hogy  $\rho$  teljesen invariáns kongruenciája  $\mathbf{T}$ -nek. Ekkor  $\mathcal{C}$ -nek választhatjuk az egyelemű  $\{\mathbf{T}/\rho\}$  osztályt. Megmutatjuk, hogy  $\rho = \text{Id } \{\mathbf{T}/\rho\}$ .

Először tegyük fel, hogy  $(t_1, t_2) \in \rho$ . Legyen  $t_1$  (és  $t_2$ )  $n$ -áris. Válasszuk ki  $\mathbf{T}/\rho$ -ból a tetszőleges  $\rho(s_1), \dots, \rho(s_n)$  elemeket, és legyen  $\varepsilon$   $\mathbf{T}$ -nek az az endomorfizmusa, amely  $i = 1, \dots, n$ -re az  $x_i$  határozatlant  $s_i$ -be viszi át. Akkor

$$\begin{aligned} t_1(\rho(s_1), \dots, \rho(s_n)) &= \rho(t_1(s_1, \dots, s_n)) = \rho(t_1(\varepsilon(x_1), \dots, \varepsilon(x_n))) \\ &= \rho(\varepsilon(t_1(x_1, \dots, x_n))) = \rho(\varepsilon(t_1)) = \rho(\varepsilon(t_2)) = \dots = t_2(\rho(s_1), \dots, \rho(s_n)). \end{aligned}$$

Innen látjuk, hogy  $\rho \subseteq \text{Id } \{\mathbf{T}/\rho\}$ . Most tegyük fel, hogy  $(t_1, t_2) \in \text{Id } \{\mathbf{T}/\rho\}$ . Akkor

$$\rho(t_1) = \rho(t_1(x_1, \dots, x_n)) = t_1(\rho(x_1), \dots, \rho(x_n)) = t_2(\rho(x_1), \dots, \rho(x_n)) = \dots = \rho(t_2),$$

azaz  $(t_1, t_2) \in \rho$ .

**21. Birkhoff varietástétele.** Ha hasonló algebrák valamely  $\mathcal{C}$  osztályához létezik azonosságoknak olyan  $\rho$  halmaza, hogy  $\mathcal{C}$  pontosan azokból az algebrákból áll, amelyeken a  $\rho$ -hoz tartozó azonosságok mind teljesülnek, akkor  $\mathcal{C}$ -t *azonosságokkal definiálható osztálynak* nevezzük. Ilyenkor  $\mathcal{C}$ -re használjuk az  $\text{Eq } \rho$  jelölést is.

A definícióból következik, hogy ha két term bizonyos algebrákon ugyanazt a termműveletet határozza meg, akkor ezeknek az algebráknak a részalgebráin, homomorf képein és direkt szorzatain is. Ebből következik, hogy minden azonosságokkal definiálható osztály varietás. Ennek a megfordítása is igaz:

*Birkhoff tétele: Minden varietás azonosságokkal definiálható osztály.*

*Birkhoff bizonyítása.* Legyen  $\mathcal{C}$  varietás. Sejthető, hogy a keresett azonosságthalmaz — amellyel  $\mathcal{C}$  definiálható — mindazon azonosságok halmaza lesz, amelyek  $\mathcal{C}$ -n teljesülnek. Ez azonban nem nyilvánvaló; elképzelhetnénk, hogy egy  $\mathbf{A}$  algebra nincs  $\mathcal{C}$ -ben és mégis teljesül rajta minden  $\text{Id } \mathcal{C}$ -be tartozó azonosság. Azt bizonyítjuk be, hogy ha  $\mathbf{A}$ -n teljesül minden  $\text{Id } \mathcal{C}$ -be tartozó azonosság, akkor  $\mathbf{A}$  megkapható  $\mathcal{C}$ -beli algebrákból homomorf kép, részalgebra és direkt szorzat (néhányszori) képzésével, s ezért  $\mathbf{A} \in \mathbf{HSP } \mathcal{C} = \mathcal{C}$ . A bizonyítás tehát azt is mutatja, hogy minden  $\mathcal{C}$  varietásra  $\text{Eq } \text{Id } \mathcal{C} = \mathcal{C}$ .

Tegyük fel, hogy  $\mathbf{A}$ -n teljesül minden  $\text{Id } \mathcal{C}$ -be tartozó azonosság. Rögzítsük  $\mathbf{A}$ -nak egy  $G = \{g_\alpha | \alpha \in J\}$  generátorrendszerét. Minden olyan  $(t_1, t_2)$

azonossághoz, amely *nem* tartozik  $\text{Id } \mathcal{C}$ -be, tekintsünk egy  $A_{t_1}^{t_2} \in \mathcal{C}$  algebrát, amelyen  $(t_1, t_2)$  nem teljesül. Minden így kiválasztott algebrába képezzük le  $G$ -t minden lehetséges módon, s minden leképezéshez külön-külön tekintsük  $A_{t_1}^{t_2}$  egy-egy példányát. Mindezek  $D$  direkt szorzata is  $\mathcal{C}$ -ben van. A  $G$  generátorrendszer minden egyes  $g_\alpha$  eleméhez természetes módon hozzárendelhetjük  $D$  egy elemét, mégpedig azt a kiválasztási függvényt, amely minden  $A_{t_1}^{t_2}$  algebrának a tetszőleges  $\varphi : G \rightarrow A_{t_1}^{t_2}$  leképezéshez tartozó példányából éppen a  $\varphi(g_\alpha)$  elemet választja ki. Legyen e kiválasztási függvény jele  $\Phi(g_\alpha)$ . Az összes  $g_\alpha$ -khoz ilyen módon rendelt kiválasztási függvények egy  $F$  részalgebrát generálnak  $D$ -ben, amely ugyancsak  $\mathcal{C}$ -be tartozik. A bizonyítással készen leszünk, ha megmutatjuk, hogy  $A$  homomorf képe  $F$ -nek.

Mivel  $F$  minden eleme valamely, a  $\Phi(G) = \{\Phi(g_\alpha) | \alpha \in J\}$  halmaz elemein elvégzett termművelet eredménye,  $F$ -nek  $A$ -ba való homomorf leképezésére a jelölt az a megfeleltetés, amely bármely nemnegatív egész  $n$ -re,  $n$ -áris  $t$  termre és  $F$  bármely  $\Phi(g_{\alpha_1}), \dots, \Phi(g_{\alpha_n})$  generátorelemeire  $F$   $t(\Phi(g_{\alpha_1}), \dots, \Phi(g_{\alpha_n}))$  eleméhez  $A$   $t(g_{\alpha_1}, \dots, g_{\alpha_n})$  elemét rendeli. Ez a megfeleltetés szürjektív, mert  $A$  minden eleme ugyancsak a  $G$  halmaz elemein elvégzett valamely termművelet eredménye. Ezért már csak azt kell belátni, hogy megfeleltetésünk *leképezés*, mert az alapműveletekkel való felcserélhetősége a termműveletek eredményére vonatkozó (3) szabályból következik.

Tegyük fel, hogy ez nem így van, azaz léteznek olyan  $t_1, t_2$  termek (feltehetjük, hogy mindkettő  $n$ -áris) és olyan  $\Phi(g_{\alpha_1}), \dots, \Phi(g_{\alpha_n}) \in \Phi(G)$  elemek, hogy

$$t_1(\Phi(g_{\alpha_1}), \dots, \Phi(g_{\alpha_n})) = t_2(\Phi(g_{\alpha_1}), \dots, \Phi(g_{\alpha_n})), \quad (\text{iv})$$

de  $t_1(g_{\alpha_1}, \dots, g_{\alpha_n}) \neq t_2(g_{\alpha_1}, \dots, g_{\alpha_n})$ . Megmutatjuk, hogy ekkor a  $(t_1, t_2)$  azonosság teljesül  $\mathcal{C}$ -ben, s ezért  $A$ -ban is, ami ellentmond a  $t_1(g_{\alpha_1}, \dots, g_{\alpha_n}) \neq t_2(g_{\alpha_1}, \dots, g_{\alpha_n})$  feltevésnek.

Ha  $(t_1, t_2)$  nem teljesül  $\mathcal{C}$ -ben, akkor van olyan  $A_{t_1}^{t_2} \in \mathcal{C}$ , amelyen nem teljesül, tehát vannak olyan  $a_1, \dots, a_n \in A_{t_1}^{t_2}$  elemek, hogy  $t_1(a_1, \dots, a_n) \neq t_2(a_1, \dots, a_n)$ . Legyen  $\varphi$   $G$ -nek olyan leképezése  $A_{t_1}^{t_2}$ -be, amelyre  $\varphi(g_{\alpha_i}) = a_i$  ( $i = 1, \dots, n$ ). Akkor a (iv) egyenlet baloldalán álló kiválasztási függvény az  $A_{t_1}^{t_2}$  algebra a  $\varphi$ -hez tartozó példányából  $t_1(a_1, \dots, a_n)$ -t, a (iv) jobboldalán álló kiválasztási függvény pedig az attól különböző  $t_2(a_1, \dots, a_n)$ -t választja ki, tehát (iv) nem igaz.

Birkhoff tétele (1935) volt az első igazi univerzális algebrai eredmény, abban az értelemben, hogy nem valamely, bizonyos algebrafajtákra már korábban is ismert tétel általánosításaként, hanem azonnal teljes általánosságban született meg. Bemutatjuk egy másik bizonyítását is.

*Imreh Balázs bizonyítása.* Tegyük fel, hogy  $\mathcal{C}$  varietás, és valamely  $A$  algebrán teljesül minden  $\text{Id } \mathcal{C}$ -hez tartozó azonosság. Be kell látnunk, hogy  $A \in \mathcal{C}$ .

Mint a varietásokat bevezető fejezetben láttuk, ehhez elegendő megmutatnunk, hogy  $\mathbf{A}$  minden megszámlálhatóan generált részalgebrája (amelyeken természetesen ugyancsak teljesülnek az  $\text{Id } \mathcal{C}$ -hez tartozó azonosságok)  $\mathcal{C}$ -be tartozik. Azt fogjuk igazolni, hogy ha egy tetszőleges megszámlálhatóan generált  $\mathbf{B}$  algebrán teljesülnek az  $\text{Id } \mathcal{C}$ -hez tartozó azonosságok, akkor  $\mathbf{B}$   $\mathcal{C}$ -beli algebrák szubdirekt szorzatának homomorf képe (s ezért  $\mathcal{C}$ -be tartozik).

Korábban megfigyeltük, hogy  $\text{Id } \mathcal{C}$  (teljesen invariáns) kongruencia a megszámlálhatóan generált  $\mathbf{T}$  termalgebrán. Minden megszámlálhatóan generált  $\mathbf{B}$  algebra homomorf képe  $\mathbf{T}$ -nek; tekintsük ugyanis  $\mathbf{B}$   $H = \{h_1, h_2, \dots\}$  generátorrendszerét (ha ez véges és  $k$  elemű, akkor legyen  $h_k = h_{k+1} = \dots$ ) és a határozatlanok halmazának  $H$ -ra való  $x_i \mapsto h_i$  leképezését; akkor a  $\phi : t(x_1, \dots, x_n) \mapsto t(h_1, \dots, h_n)$  leképezés, ahol  $t$  tetszőleges  $n$ -áris term,  $\mathbf{T}$ -nek  $\mathbf{B}$ -re való homomorfizmusa. A homomorfizmus bizonyításánál használt jelölést alkalmazva tekintsük  $\mathbf{T}$ -n a  $\phi$  relációt:  $(t_1, t_2) \in \phi$   $\mathbf{T}$ -ben akkor és csak akkor, ha  $\phi(t_1) = \phi(t_2)$   $\mathbf{B}$ -ben. Ez kongruenciája  $\mathbf{B}$ -nek és  $\mathbf{B} \cong \mathbf{T}/\phi$ . Vegyük észre, hogy az összes  $\text{Id } \mathcal{C}$ -beli azonosságok akkor és csak akkor teljesülnek  $\mathbf{T}/\phi$ -n — és ezért  $\mathbf{B}$ -n is —, ha  $\text{Id } \mathcal{C} \subseteq \phi$ .

Mint Birkhoff bizonyításában, tekintsünk most is minden olyan  $(t_1, t_2)$  azonossághoz, amely *nem* tartozik  $\text{Id } \mathcal{C}$ -be, egy olyan  $\mathbf{A}_{t_1}^{t_2} \in \mathcal{C}$  algebrát, amelyen  $(t_1, t_2)$  *nem* teljesül. Feltehetjük, hogy ezek mind megszámlálhatóan generáltak (miért?). Minden így kiválasztott algebrára képezzük le  $\mathbf{T}$ -t, megfelelően a  $\phi_{t_1}^{t_2}$  homomorfizmusokkal. Akkor az összes  $\phi_{t_1}^{t_2} \in \text{Con } \mathbf{T}$  kongruenciák metszete éppen  $\text{Id } \mathcal{C}$ , ahonnan következik, hogy  $\mathbf{T}/\text{Id } \mathcal{C}$  (azaz  $\mathcal{C}$  megszámlálható rangú termművelet-algebrája) izomorf az összes  $\mathbf{A}_{t_1}^{t_2} (\in \mathcal{C})$  algebrák valamely szubdirekt szorzatával. Ha  $\mathbf{B}$ -n teljesülnek az összes  $\text{Id } \mathcal{C}$ -beli azonosságok, akkor a fentebb  $\mathbf{B}$ -hez rendelt  $\phi$  kongruenciára  $\text{Id } \mathcal{C} \subseteq \phi$ . Innen a második izomorfizmus tétel szerint  $\mathbf{B} \cong \mathbf{T}/\phi \cong (\mathbf{T}/\text{Id } \mathcal{C}) / (\phi/\text{Id } \mathcal{C})$ , azaz  $\mathbf{B}$  izomorf  $\mathbf{T}/\text{Id } \mathcal{C}$  egy faktoralgebrájával, s ezért  $\mathbf{T}/\text{Id } \mathcal{C}$ -nak homomorf képe.

Ha már bebizonyítottuk Birkhoff tételét, akkor élesíthetjük a 19. fejezet végén kimondott és a második bizonyításban felhasznált állítást, amely szerint ha egy algebra minden megszámlálhatóan generált részalgebrája egy varietáshoz tartozik, akkor maga az algebra is ahhoz a varietáshoz tartozik. Nevezzünk egy algebrát végesen generáltnak, ha van véges generátorrendszere. Legyen  $\mathcal{P}$  algebrák egy tulajdonsága. Azt mondjuk, hogy az  $\mathbf{A}$  algebra *lokálisan*  $\mathcal{P}$  tulajdonságú, ha minden végesen generált részalgebrája  $\mathcal{P}$  tulajdonságú. Az ígért élesítés: *ha egy  $\mathbf{A}$  algebra lokálisan a  $\mathcal{V}$  varietáshoz tartozik, akkor  $\mathbf{A} \in \mathcal{V}$ . (Lássuk bel!)*

**22. Galois-kapcsolat.** Legyenek  $P$  és  $Q$  halmazok,  $\mu$  pedig egy megfeleltetés  $P$  és  $Q$  között, azaz  $\mu \subseteq P \times Q$ . Rendeljük  $P$  minden  $H$  részhalmazához  $Q$

mindazon elemeinek a halmazát, amelyek  $H$  minden elemével a  $\mu$  megfeleltetésben vannak; jelöljük ezt a halmazt  $\sigma(H)$ -val. Rendeljük továbbá  $Q$  minden  $K$  részhalmazához  $P$  mindazon elemeinek a halmazát, amelyekkel  $K$  minden eleme a  $\mu$  megfeleltetésben van; ezt a halmazt jelöljük  $\tau(K)$ -val. Ekkor  $\sigma\tau : H \mapsto \tau(\sigma(H))$   $P$  hatványhalmazának,  $\tau\sigma : K \mapsto \sigma(\tau(K))$  pedig  $Q$  hatványhalmazának önmagába való leképezése. Belátjuk, hogy mindkét leképezés lezárási operátor (megfelelően  $P$ -n és  $Q$ -n).

A  $\sigma$  és  $\tau$  leképezések definíciójából látszik, hogy  $\sigma\tau$  extenzív; ugyanígy  $\tau\sigma$  is. Mind  $\sigma$ , mind  $\tau$  *antimonoton*: ha  $H_1 \subseteq H_2$ , akkor  $\sigma(H_1) \supseteq \sigma(H_2)$ , és hasonló érvényes  $\tau$ -ra. Innen következik, hogy  $\sigma\tau$  monoton; ugyanígy  $\tau\sigma$  is. Megmutatjuk, hogy

$$\tau\sigma\tau = \tau, \quad \sigma\tau\sigma = \sigma. \quad (v)$$

Közülük elég az elsőt igazolnunk. Minden  $K \subseteq Q$ -ra  $(\tau\sigma\tau)(K) = (\sigma\tau)(\tau(K)) \supseteq \tau(K)$ , másrészt  $(\tau\sigma)(K) \supseteq K$  és ezért  $(\tau\sigma\tau)(K) = \tau((\tau\sigma)(K)) \subseteq \tau(K)$ . A belátt (v) egyenlőségből következik  $(\tau\sigma\tau)(K) = (\tau\sigma)(K)$ , tehát  $\tau\sigma$  idempotens; hasonlóképpen  $\sigma\tau$  is.

A 7. fejezetből tudjuk, hogy a zárt halmazok teljes hálót alkotnak  $P$  és  $Q$  hatványhalmazában egyaránt. Az, hogy  $\sigma\tau$  lezárási operátor, együtt az (v) összefüggéssel mutatja, hogy  $P$ -nek pontosan azok a  $H$  részhalmazai zártak, amelyekhez létezik olyan  $K \subseteq Q$ , hogy  $H = \tau(K)$ . Ugyanígy,  $Q$ -nak pontosan azok a  $K$  részhalmazai zártak, amelyekhez létezik olyan  $H \subseteq P$ , hogy  $K = \sigma(H)$ . Innen következik, hogy mind  $\sigma$ , mind  $\tau$  zárt halmazt zárt halmazba visz át, továbbá (v) szerint ezek a leképezések a zárt halmazok halmazán egymás inverzei. Eszerint  $\sigma$  és  $\tau$  bijektív — és mint már előbb észrevettük, antimonoton — módon képezi le  $P$  ill.  $Q$  zárt halmazainak halmazát egymásra. Mint megjegyeztük, ezek a zárt halmazok egy-egy teljes hálót alkotnak. Ez a két háló  $\sigma$  és  $\tau$  antimonotonsága miatt *duálisan izomorf*: van köztük olyan bijektív megfeleltetés, amelynél egyesítés képe (nem a képek egyesítése, hanem) a képek metszete, és hasonló igaz metszetre.

A két halmaz közötti adott tetszőleges megfeleltetésből a fenti módon származtatható lezárási rendszerek és a köztük bijektív megfeleltetést teremtő  $(\sigma, \tau)$  leképezéspár *Galois-kapcsolatot* létesít a két halmaz között. Az elnevezés Galois nevét őrzi, aki (1832-ben) bizonyos testek és csoportok között talált ilyen kapcsolatot, s ennek révén lehetővé tette annak az eldöntését, hogy mely polinomok zérushelyei gyökmennyiségek az együtthatóik által generált test felett. A legegyszerűbb eset: adott racionális együtthatós  $f$  polinomhoz legyen  $\mathbf{K}$  a legszűkebb számtest, amely  $f$  minden (komplex) zérushelyét tartalmazza, továbbá legyen  $\mathbf{G}$   $\mathbf{K}$  összes *automorfizmusainak* (önmagára való izomorf leképezéseinek) csoportja. Ezek (alaphalmazai) játsszák  $P$  és  $Q$  szerepét, s legyen  $r \in K$ -ra és  $\gamma \in G$ -re

$(r, \gamma) \in \mu$  akkor és csak akkor, ha  $\gamma(r) = r$ . Ekkor  $\mathbf{K}$ -ban a résztestek,  $\mathbf{G}$ -ben a részcsoporthoz tartozó elemek a zárt halmazok. További klasszikus példák – két matematikai és egy filozófiai (ismeretelméleti) példa – Galois-kapcsolatra:

- (1) Legyen  $I$  ideálja az  $\mathbf{R}$  kommutatív gyűrűnek. Mindazok az  $\mathbf{R}$ -beli elemek, amelyeknek valamely hatványa  $I$ -ben van, ugyancsak ideált alkotnak  $\mathbf{R}$ -ben, amelyet  $I$  radikáljának (vagy nilradikáljának) nevezünk. Tekintsük a komplex számtest feletti  $n$  változós polinomok  $\mathbf{C}[x_1, \dots, x_n]$  gyűrűjét és a  $\mathbf{C}^n$   $n$  dimenziós komplex vektorteret, és tekintsük közöttük a  $\mu = \{(f(x_1, \dots, x_n), (c_1, \dots, c_n)) : f(c_1, \dots, c_n) = 0\}$  megfeleltetést (amelyben tehát egy polinom és egy szám- $n$ -es pontosan akkor van, ha a szám- $n$ -es zérushelye a polinomnak). A  $\mu$ -höz tartozó Galois-kapcsolatban  $\mathbf{C}^n$  zárt részhalmazait algebrai sokaságoknak nevezzük (ezek vizsgálata a matematika *algebrai geometria* nevű területe), míg  $\mathbf{C}[x_1, \dots, x_n]$  zárt részhalmazai éppen azok az ideálok, amelyek egybeesnek saját radikáljukkal. Speciálisan, adott polinomhalmaz lezártja a benne levő polinomok által generált ideál radikálja. (Ez a nevezetes Hilbert-féle zérushelytétel.)
- (2) Tekintsük a racionális számok halmazán — vagyis a  $\mathbf{Q}$  racionális számtest két példány között — a  $\mu = \{(a, b) : a < b\}$  megfeleltetést, azaz a „kisebb” relációt. A  $\mu$ -höz tartozó Galois-kapcsolatban egymásnak megfelelő zárt halmazok éppen  $\mathbf{Q}$  Dedekind-szeletei (olyan  $H_1, H_2$  halmazpárok, hogy  $H_1 \cup H_2 = \mathbf{Q}$  és minden  $h_1 \in H_1, h_2 \in H_2$  racionális számokra  $h_1 < h_2$ ); Dedekind definíciója szerint ezek a szeletek a valós számok).
- (3) Tekintsük az összes dolgok  $D$  halmazát és az összes tulajdonságok  $T$  halmazát. (Aki halmazelméleti tanulmányai alapján kétli e halmazok létezését, gondoljon inkább a megnevezhető dolgok és leírható tulajdonságok halmazára — ezek együtt is csak megszámlálhatóan vannak.) Tekintsük a

$$\mu = \{(d, t) \in D \times T : a \text{ } d \text{ dolog } t \text{ tulajdonságú}\}$$

megfeleltetést. Az ehhez tartozó Galois-kapcsolatban egymásnak megfelelő  $F_1, F_2$  ( $F_1 \subseteq D, F_2 \subseteq T$ ) zárt halmazpárokat *fogalmaknak* nevezzük;  $F_1$  a szóban forgó fogalom *terjedelme*,  $F_2$  a *tartalma*.

Tekintsünk most egy  $\mathcal{S}$  hasonlósági osztályt és a termjeiből képezett összes párok halmazát, másszóval  $T^2$  alaphalmazát. Ezek között vegyük azt a megfeleltetést, amelyben  $A \in \mathcal{S}$  és  $(t_1, t_2) \in T^2$  akkor és csak akkor áll, ha  $(t_1, t_2)$  teljesül  $A$ -n. Az ehhez tartozó Galois-kapcsolatban algebraik bármely  $\mathcal{C}$  osztályához  $\sigma$  az  $\text{Id } \mathcal{C}$  azonosságalmazt rendeli,  $\tau$  pedig azonosságok bármely  $\rho$  halmazához az  $\text{Eq } \rho$  algebraosztályt. Ebből következik, hogy a zárt algebraosztályok pontosan a varietások, a zárt azonosságalmazok pedig  $T$  teljesen invariáns kongruenciái. Az

ezek által alkotott teljes hálók duálisan izomorfok. Ez a megfigyelés lehetővé teszi, hogy varietásokra vonatkozó egyes kérdések vizsgálatát visszavezzük a megszámlálhatóan generált termalgebra teljesen invariáns kongruenciáinak vizsgálatára.

Pl. minden hasonlósági osztály maga is varietás, amelyhez tartozó kongruencia az egyenlőségreláció  $T$ -n (mivel a  $T$  algebraiban csak a triviális  $t = t$  azonosságok teljesülnek); továbbá minden hasonlósági osztály tartalmaz olyan varietást, amelyben csak egyelemű algebra van (és természetesen az egyelemű algebra izomorfok), s ennek  $T$  teljes kongruenciája — a  $T \times T$  reláció — felel meg. Ezek a *triviális varietások*. Kevésbé nyilvánvaló példa az algebra és azonosságok közti Galois-kapcsolat alkalmazására a minimális varietások létezésének bizonyítása. Nevezzük egy korlátozott háló *atomjának* az olyan hálóelemet, amely minimális a 0-tól különböző elemek között; *duális atomon* pedig értsük a háló olyan elemét, amely maximális az 1-től különböző elemek között. Az összes adott típusú varietások teljes hálójának atomjait *minimális varietásoknak* nevezzük,  $T$  teljesen invariáns kongruenciái teljes hálójának duális atomjait pedig maximális teljesen invariáns kongruenciáknak. A  $\mathcal{V}$  varietás akkor és csak akkor minimális, ha minden egynél több elemű algebraja generálja.

*Ha egy varietás tartalmaz egynél több elemű algebrát, akkor tartalmaz minimális varietást.* Az algebra és azonosságok közti Galois-kapcsolat alapján ehhez elegendő megmutatnunk, hogy  $T$  minden  $\rho$  nemteljes teljesen invariáns kongruenciáját tartalmazza egy maximális teljesen invariáns kongruencia. Gondoljuk meg, hogy egy teljesen invariáns kongruencia akkor és csak akkor teljes, ha tartalmazza az  $(x_1, x_2)$  párt. (A „csak akkor” nyilvánvaló, az „akkor” pedig abból következik, hogy  $x_1$  és  $x_2$  helyébe a teljes invariancia miatt tetszőleges termeket írhatunk.) Azt kell tehát belátnunk, hogy a  $\rho$ -t tartalmazó, de  $(x_1, x_2)$ -t nem tartalmazó kongruenciák között van maximális. Ezt a Zorn-lemma azonnal mutatja, mert a mondott tulajdonságú kongruenciák bármely tartalmazás szerint rendezett halmazának egyesítése is ilyen tulajdonságú kongruencia.

(Figyelmeztetés: osztályoknak rendszerint olyan összességeket nevezünk, amelyekhez nem rendelhető számosság. Osztályok halmazáról — bizonyos halmazelméleti antinómiák elkerülése végett — nem beszélünk, legalábbis addig, amíg ki nem derül, hogy halmazuk létezik. A fenti megfontolásban ez kiderült, mert a varietások kölcsönösen egyértelmű módon megfeleltethetők  $T$  teljesen invariáns kongruenciáinak, amelyek halmazt alkotnak.)

**23. Szabad algebra.** Birkhoff varietástételének második bizonyításából az is látszik, hogy ha  $\mathcal{C}$  varietás és  $\vartheta = \text{Id } \mathcal{C}$ , akkor a  $T/\vartheta$  algebra és  $\vartheta(x_1), \vartheta(x_2), \dots$  generátorrendszerének a következő tulajdonsága van: e generátorrendszer bármely  $A \in \mathcal{C}$  algebraba való bármely leképezése folytatható (más szóval, kiterjeszt-

hető), mégpedig egyetlen módon,  $\mathbf{T}/\vartheta$ -nak  $\mathbf{A}$ -ba való homomorf leképezésévé. A Birkhofftól eredő bizonyításban pedig az ott előállított  $\mathbf{F}$  algebrának és  $\Phi(G)$  generátorrendszerének van ugyanilyen tulajdonsága (amit a bizonyítás közben ugyan nem mondtunk ki, de az ottani gondolatmenettel igazolható, ha azt az ott tekintett  $\mathbf{A}$  és annak  $G$  generátorrendszere helyett tetszőleges  $\mathcal{C}$ -beli algebrára és annak tetszőleges elemeire alkalmazzuk).

E megfigyelések a következő definíciót sugallják. Legyen  $\mathcal{C}$  algebrák egy osztálya,  $\mathbf{F} \in \mathcal{C}$  és  $G$  generátorrendszere  $\mathbf{F}$ -nek. Ha  $G$ -nek bármely  $\mathbf{A} \in \mathcal{C}$  algebrába való tetszőleges leképezése egyetlen módon folytatható  $\mathbf{F}$ -nek  $\mathbf{A}$ -ba való homomorfizmussá, akkor azt mondjuk, hogy  $\mathbf{F}$  *szabad algebra a  $\mathcal{C}$  osztályban a  $G$  szabad generátorrendszerrel* (vagy másképpen *a  $G$  halmaz által szabadon generált  $\mathcal{C}$ -szabad algebra*). Ha tehát  $\mathcal{C}$  varietás, akkor  $\mathbf{T}/\text{Id } \mathcal{C}$  (azaz a  $\mathcal{C}$  varietás termművelet-algebrája) szabad algebra  $\mathcal{C}$ -ben, amelynek a határozatlanokat tartalmazó blokkok szabad generátorrendszerét alkotják.

Imreh Balázs bizonyítása közben azt is láttuk, hogy  $\mathbf{T}$  szabad algebra az adott hasonlósági osztályban az  $x_1, x_2, \dots$  szabad generátorrendszerrel. Innen ered a 3. fejezetben említett „abszolút szabad algebra” elnevezés. A „szabad” jelző arra vonatkozik, hogy a generátorrendszer leképezései akadálytalanul kiterjeszthetők homomorfizmussá. Ez azt jelenti, hogy *szabad algebrán végzett  $t_1$  és  $t_2$  termműveletek (akkor és) csak akkor ugyanazok a műveletek, ha a  $\mathcal{C}$  osztályon teljesül a  $(t_1, t_2)$  azonosság*. Speciálisan, a  $t_1$  és  $t_2$  termek akkor és csak akkor jelölik a szabad algebra ugyanazon elemét, ha a  $\mathcal{C}$  osztályon teljesül a  $(t_1, t_2)$  azonosság. Ezért nem fordulhat elő a szabad generátorrendszer leképezéseinek az egész algebrára való kiterjesztésekor, hogy valamely (mondjuk,  $n$ -áris)  $t_1, t_2$  termekre és  $a_1, \dots, a_n$  elemekre  $t_1(a_1, \dots, a_n) \neq t_2(a_1, \dots, a_n)$ , jöllehet a szabad generátorokra — jelölje most ezeket  $y_1, y_2, \dots$  — fennáll  $t_1(y_1, \dots, y_n) = t_2(y_1, \dots, y_n)$ . Az azonosságokat egyes nyelveken (angol, orosz) „törvényeknek” is nevezik; ezért kapták a termalgebrák, amelyeken csak a  $(t, t)$  alakú triviális törvények érvényesek, az „anarchikus algebra” elnevezést.

E fejezet elején végzett megfigyeléseink mutatják, hogy bármely varietásban léteznek szabad algebrák akármilyen számosságú szabad generátorrendszerrel. *A szabad generátorrendszer számossága a szabad algebrát izomorfia erejéig meghatározza*, mert két szabad algebra szabad generátorrendszereinek egymásra való bijektív leképezései folytathatók homomorfizmussá, s ha ezek a bijektív leképezések éppen egymás inverzei, akkor homomorf folytatásaik szorzata az identikus leképezés, ahonnan következik, hogy ezek a folytatások is bijektívek, s ezért izomorfizmuskok. Ezért ezután szabad algebráról beszélve szabad generátorrendszere helyett rendszerint csak annak a számosságát említjük, s azt a szabad algebra

rangjának nevezzük; pl. *megszámlálható rangú szabad  $\mathcal{C}$ -algebra*,  *$n$  rangú szabad  $\mathcal{C}$ -algebra*, stb. Léteznek olyan varietások, amelyekben bizonyos különböző számosságú generátorrendszerek által szabadon generált szabad algebrák is izomorfok, ám ha a varietásban van egynél több elemű véges algebra, ez nem fordulhat elő (*Fujiwara tétele*). (Olyan varietásra, amelyben nincs nemtriviális véges algebra, a későbbiekben látunk példát.) Ha ugyanis egy ilyen  $\mathbf{A}$  algebrának  $k$  eleme van és az  $m$  elemű halmaz által szabadon generált szabad algebra izomorf az  $n$  ( $\neq m$ ) elemű halmaz által generálttal, akkor ezeknek a szabad algebra definíciója szerint az  $\mathbf{A}$  algebrába megfelelően  $k^m$  és  $k^n$  különböző homomorf leképezése létezik, s így  $k^m = k^n$ , mert két izomorf algebrának egy harmadikba ugyanannyi különböző homomorf leképezése van. Innen  $m = n$ . (Ezt az egyszerű megfontolást először Pollák Györgytől hallottam; ugyanabban az időben Jónsson és Tarski is felfedezték. Fujiwara bizonyítása hosszadalmas volt.)

Ha  $\mathcal{C}$  varietás, akkor azok a  $\mathcal{C}$ -n teljesülő azonosságok, amelyekben csak az  $x_1, \dots, x_n$  határozatlanok fordulnak elő, egy teljesen invariáns  $\vartheta_n$  kongruenciát képeznek az  $n$  rangú  $\mathbf{T}_n$  termalgebrában. A Birkhoff-tétel Imreh-féle bizonyításában elvégzett megfontolás  $\mathbf{T}$  és  $\vartheta = \text{Id } \mathcal{C}$  helyett  $\mathbf{T}_n$ -re és  $\vartheta_n$ -re alkalmazva mutatja, hogy a  $\vartheta_n(x_1), \dots, \vartheta_n(x_n)$  osztályok halmazának bármely  $\mathbf{A} \in \mathcal{C}$ -beli algebrába való bármely leképezése  $\mathbf{T}_n/\vartheta_n$   $\mathbf{A}$ -ba való leképezésévé folytatható. Ezért az  $n$  elem által generált (röviden  $n$  rangú) szabad algebra  $\mathcal{C}$ -ben éppen  $\mathbf{T}_n/\vartheta_n$ .

**24. Szabad algebrák véges algebra által generált varietásban.** Ha  $\mathcal{V}$  varietás és  $\mathbf{F}$  megszámlálható rangú szabad algebra  $\mathcal{V}$ -ben, akkor  $\mathbf{F}$  generálja  $\mathcal{V}$ -t. Valóban, ekkor bármely  $\mathbf{A} \in \mathcal{V}$  algebra minden megszámlálhatóan generált részalgebrája  $\mathbf{F}$  homomorf képe, maga  $\mathbf{A}$  pedig e részalgebrák szubdirekt szorzatának homomorf képe, tehát  $\mathbf{A}$  megkapható  $\mathbf{F}$ -ből a  $\mathbf{H}$ ,  $\mathbf{S}$ ,  $\mathbf{P}$  operátorok segítségével.

Tekintsünk most egy tetszőleges  $\mathbf{B}$  algebrát. Az általa generált  $\text{Var } \{\mathbf{B}\} = \mathbf{HSP} \{\mathbf{B}\}$  varietás szabad algebráit megkaphatjuk Birkhoff tétele eredeti bizonyításának gondolatát használva. Az a bizonyítás valamivel többet mutatott meg, mint a Birkhoff-tétel állítása; azt ti., hogy ha  $\mathcal{C}$  algebrák egy *tetszőleges* osztálya, akkor  $\mathcal{C}$ -ből az  $\mathbf{S}$  és  $\mathbf{P}$  operátorok segítségével képezhetünk olyan  $\mathbf{F}$  algebrát  $n$  elemű generátorrendszerrel, hogy e generátorrendszernek bármely leképezése tetszőleges  $n$  elem által generált és minden  $\text{Id } \mathcal{C}$ -beli azonosságot teljesítő  $\mathbf{A}$  algebra generátorrendszerére folytatható  $\mathbf{F}$ -nek  $\mathbf{A}$ -ra való homomorfizmusává. Mivel ez természetesen érvényes az  $\mathbf{A} \in \text{Var } \mathcal{C}$  algebrákra is, Birkhoff bizonyítási módszere  $n$  rangú szabad algebrát szolgáltat a  $\text{Var } \mathcal{C}$  varietásban.

Ezek szerint adott véges  $\mathbf{B}$  algebra által generált varietás  $n$  rangú szabad algebráját — egyszerűség kedvéért  $n$  most legyen természetes szám — a következőképpen csinálhatjuk meg. Vegyük a  $g_1, \dots, g_n$  jeleket; halmazukat képezzük le minden

lehetséges  $\phi$  leképezéssel  $B$ -be (most minden olyan  $(t_1, t_2)$  azonosságra, amely *nem* teljesül  $B$ -ben, maga  $B$  játssza a Birkhoff-féle bizonyításban látott  $A_{t_1}^{t_2}$  szerepét). Ilyen leképezés csak véges sok van; mindegyikükhöz tekintsük  $B$  egy példányát, és alkossuk meg mindezen példányok direkt szorzatát. Válasszuk ki e direkt szorzat azon  $\Phi_i$  elemeit, amelyeknek minden direkt tényezőbe eső komponense  $g_i$  képe abban a direkt tényezőben, és vegyük a  $\{\Phi_1, \dots, \Phi_n\}$  halmaz generátumát. Ez lesz az  $n$  rangú szabad algebra  $\text{Var } \{B\}$ -ben. Kis alaphalmazú  $B$ -re és kis  $n$ -re ez az eljárás ceruzával (még inkább számítógéppel) a gyakorlatban is elvégezhető. Példaként kiszámítjuk a 2 rangú szabad algebrát abban a varietásban, amelyet a  $\{0, 1\}$  alaphalmazú implikáció alpműveletű (lásd a 12. fejezetet) algebra generál.

|    | $\phi_1$ | $\phi_2$ | $\phi_3$ | $\phi_4$ |    | x  | y  | xy | yx | xx | z  |
|----|----------|----------|----------|----------|----|----|----|----|----|----|----|
| x  | 0        | 0        | 1        | 1        | x  | xx | xy | z  | x  | x  | xy |
| y  | 0        | 1        | 0        | 1        | y  | yx | xx | y  | z  | y  | yx |
| xy | 0        | 0        | 1        | 0        | xy | xx | xy | xx | xy | xy | xy |
| yx | 0        | 1        | 0        | 0        | yx | yx | xx | yx | xx | yx | yx |
| xx | 0        | 0        | 0        | 0        | xx | xx | xx | xx | xx | xx | xx |
| z  | 0        | 0        | 0        | 1        | z  | xx | xx | z  | z  | z  | xx |

Az első táblázat első két sora  $\Phi_1$  és  $\Phi_2$ . E soroknak pl. az első komponense  $g_1$  ill.  $g_2$  képe a konstans 0 leképezésnél, amelyet itt  $\phi_1$  jelöl. A rövidség kedvéért  $x$  és  $y$  jelöli ezeket a sorokat. A további sorokat az alap- és termműveletek komponensenkénti elvégzésével kapjuk  $x$ -ből és  $y$ -ből; az implikációt szorzásként jelöltük, a  $z$  jel  $x(xy)$  helyett áll. Hogy az összes termműveletek eredményét megkapjuk, az implikációt minden lehetséges sorrendben elvégezzük a már megkapott sorokon, mindaddig, amíg új sorokat kapunk. A lehetséges sorok száma  $2^4$ , tehát eljárásunk eredményeként legfeljebb ennyi sort kapunk — mint látjuk, esetünkben összesen 6 különböző sor lép fel, vagyis a keresett 2 rangú szabad algebra 6 elemű. (Gondoljuk meg, hogy általában bármely  $k$  elemű algebra által generált varietás  $n$  rangú szabad algebrája legfeljebb  $k^{k^n}$  elemű lehet.) A második táblázat az implikáció művelettáblázata a 2 rangú szabad algebrában; helyeit a komponensenkénti implikáció elvégzésével töltöttük ki.

Figyeljük meg, hogy a keresett szabad algebrát  $B$  négy példánya direkt szorzatának részalgebrájaként állítottuk elő; három példány is elég lett volna azonban, mert az első komponenseknek a számolásoknál nincs szerepe.

Ha kiindulási kételemű algebránk alpművelete implikáció helyett a Sheffer-művelet, akkor 16 elemű 2 rangú szabad algebrát kapunk. Ennek elemeit — ugyancsak elemnégyesek alakjában — nehézség nélkül meghatározhatjuk, de ha tényleg elvégezzük ezt a munkát, meggyőződünk róla, hogy az ilyen számolást jobb számítógépre bízni.

**25. Sima algebrák.** *Simának* nevezzük az olyan legalább két elemű véges algebrát, amely egyszerű, és legfeljebb egyelemű valódi részalgebrái vannak. Példák: minden kételemű algebra, minden prímszámrendű csoport. Algebra elemét *idempotensnek* nevezzük, ha önmagában részalgebrát alkot. *Idempotens algebrán* olyan algebrát értünk, amelynek minden eleme idempotens. Idempotens algebrák pl. a hálók.

A varietásokra eddig megismertek alkalmazásaként bebizonyítjuk Szendrei Ágnes következő tételét:

*Minden idempotens sima algebra minimális varietást generál.*

*Kearnes bizonyítása:* Előkészítő megfigyelések: (1) Ha  $B$  véges algebra, akkor  $HS\{B\}$  tartalmaz sima algebrát. (Valóban,  $B$ -ből a  $H$  és  $S$  operátorok véges számú alkalmazásával sima algebrát tartalmazó osztályhoz jutunk, de ekkor — a korábban látott  $SH \leq HS$  összefüggés alapján — már  $HS$  egyszeri alkalmazásával is.)

(2) Ha  $B$  sima, akkor  $HS\{B\}$ -ben minden legalább két elemű algebra izomorf  $B$ -vel.

(3) Amint láttuk, véges algebra által generált varietásban minden véges rangú szabad algebra véges, és ezért minden véges generátorrendszerű (röviden *végesen generált*) algebra (amely véges rangú szabad algebra homomorf képe) is véges. Más szóval, véges algebra által generált varietás *lokálisan véges*.

(4) Idempotens algebrában bármely kongruencia bármely blokkja részalgebra.

Tegyük fel, hogy  $A$  sima algebra, amely nem minimális varietást generál. Akkor  $\text{Var}\{A\}$ -ban van olyan  $B$  algebra, amely  $\text{Var}\{A\}$ -nál szűkebb varietást generál, de ekkor  $B$  bármely, két elem által generált részalgebrája is. Utóbbi véges lévén, (1) szerint alkalmas részalgebrájának van sima homomorf képe, amely ugyancsak  $\text{Var}\{A\}$ -nál szűkebb varietást generál. Ebből következik, hogy az  $A$  által generált varietásban van  $A$ -val nem izomorf sima algebra. A tétel bizonyításához tehát elegendő megmutatnunk, hogy idempotens sima  $A$  algebra által generált varietásban nem létezik  $A$ -val nem izomorf sima algebra.

Tegyük fel, hogy  $A$  idempotens sima algebra,  $B \in \text{Var}\{A\}$  is sima és  $A \not\cong B$ . Minden sima algebrának van legfeljebb két elemű generátorrendszere (mi több, minden kételemű részhalmaza generátorrendszere is). A szabad algebrák előző fejezetben tárgyalt konstrukciójából látjuk, hogy  $\text{Var}\{A\}$  2 rangú szabad algebrája  $A$  véges számú példánya direkt szorzatának részalgebrája, s azt is tudjuk, hogy  $B$  e részalgebrának homomorf képe. Van tehát  $A$ -nak olyan  $A^n$  direkt hatványa, amelynek van olyan  $C$  részalgebrája, amelynek  $B$  homomorf képe. Tekintsük  $B$  ilyen előállításai közül azt, amelyben  $C$ -nek a legkevesebb eleme van. Legyen  $\vartheta$   $C$ -nek olyan kongruenciája, hogy  $B \cong C/\vartheta$ . Jelölje  $\pi_1, \dots, \pi_n$   $A^n$  ter-

mészertes kongruenciáit. ( $A^n$  két eleme pontosan akkor van a  $\pi_i$  kongruenciában, ha  $i$ -edik komponensük ugyanaz.)

Ha valamely  $i$ -re  $\vartheta \supseteq \pi_i|C$ , akkor

$$B \cong C/\vartheta \cong (C/(\pi_i|C)) / (\vartheta/(\pi_i|C)).$$

Itt a második izomorfia a második izomorfizációból következik, a jobboldal „számlálója” pedig  $A$ -nak (pontosabban a vele izomorf  $A^n/\pi_i$ -nek) egy részalgebrájával (mégpedig  $\pi_i(C)/(\pi_i|_{\pi_i(C)})$ -vel) izomorf az első izomorfizáció szerint. Azt kaptuk, hogy  $B \in \text{HS}\{A\}$ . Innen (2) szerint  $B \cong A$ , de feltettük, hogy ez nem igaz. A kapott ellentmondás mutatja, hogy  $i = 1, \dots, n$ -re  $\vartheta \not\supseteq \pi_i|C$ .

Most rögzítsünk egy tetszőleges  $i$ -t. Van olyan  $c_1, c_2 \in C$ , hogy  $\vartheta(c_1) \neq \vartheta(c_2)$ , de  $\pi_i(c_1) = \pi_i(c_2)$ . Nyertük, hogy a  $\pi_i|C \in \text{Con } C$  kongruencia  $P = (\pi_i|C)(c_1)$  blokkja legalább két elemű. Ez a blokk (4) alapján részalgebra  $C$ -ben. Az első izomorfizáció szerint  $P/(\vartheta|P)$  izomorf  $C/\vartheta (\cong B)$  valamely részalgebrájával, minthogy pedig  $P/(\vartheta|P)$  ugyancsak legalább két elemű, izomorf magával  $B$ -vel. Nyertük, hogy  $A$  egy direkt hatványának  $P$  olyan részalgebrája, amelynek  $B$  homomorf képe. Mivel  $P \subseteq C$ , és feltevésünk szerint  $C$  a legkevesebb elemű *ilyen* részalgebra, következik  $P = C$ . Beláttuk, hogy minden  $i$ -re  $C$  blokkja a  $\pi_i$  kongruenciának, tehát blokkja e kongruenciák metszetének is. Az összes természetes kongruenciák metszete azonban az egyenlőségreláció, ezért  $|C| = 1$ . Eszerint  $B$  egyelemű, és így nem lehet sima; ellentmondás.

Példa: a kételemű félháló (másképpen: a minimum-művelet a  $\{0, 1\}$  alaphalmazon) idempotens sima algebra, tehát minimális varietást generál. Igazoljuk, hogy ez a varietás az összes félhálók (idempotens kommutatív félsoportok) varietása!

**26. Felcserélhető kongruenciák.** Az  $A$  halmaz (bináris) relációinak szorzatát a következő módon értelmezzük: ha  $\eta, \vartheta \in A^2$ , legyen ezek *szorzata* az az  $\eta \circ \vartheta \in A^2$  reláció, amelyre  $(a, c) \in \eta \circ \vartheta$  akkor és csak akkor, ha létezik olyan  $b \in A$ , hogy  $(a, b) \in \eta$  és  $(b, c) \in \vartheta$ . (Gondoljuk meg, hogy ha  $A$  bináris relációit úgy tekintjük, mint  $A$ -nak önmagába való „több-többértelmű leképezéseit”, akkor a relációk szorzása éppen a közösleges leképezés-szorítás általánosítása.)

Ha  $\eta \circ \vartheta = \vartheta \circ \eta$ , akkor azt mondjuk, hogy  $\eta$  és  $\vartheta$  *felcserélhető*. Példa: csoport bármely két kongruenciája felcserélhető. Ez annak figyelembe vételével egyszerűen belátható, hogy  $G$  csoport bármely  $\eta$  kongruenciájához van a csoportnak olyan  $N$  normálosztója, hogy bármely  $a, b \in G$ -re  $(a, b) \in \eta$  akkor és csak akkor, ha létezik olyan  $n \in N$ , amelyre  $a = bn$ . Az olyan algebrát, amelynek bármely két kongruenciája felcserélhető, *permutábilisnek* (vagy *kongruencia-felcserélhetőnek*) nevez-

zük. Ha egy varietás minden algebrája permutábilis, akkor ez *permutábilis varietás*. Előbbi példánk szerint a csoportok varietása permutábilis. (Hasonlóképpen a gyűrűké is — miért?)

Varietások bizonyos tulajdonságai azonosságok segítségével jellemezhetők. Az ilyen tulajdonságokat *Malcev-tulajdonságoknak*, az ezeket azonosságokkal leíró tételeket *Malcev-típusú tételeknek* nevezzük, mivel közös elődjük a következő tétel:

*Malcev tétele: Tetszőleges  $\mathcal{V}$  varietás akkor és csak akkor permutábilis, ha van olyan ternáris  $t$  term, hogy a  $t(x_1, x_1, x_2) = x_2$ ,  $t(x_1, x_2, x_2) = x_1$  azonosságok teljesülnek  $\mathcal{V}$ -ben.*

*Bizonyítás:* Először tegyük fel, hogy létezik a tételben megadott tulajdonságú  $t$  term. Legyen  $A \in \mathcal{V}$ ,  $\eta, \vartheta \in \text{Con } A$ . A két kongruencia szerepe szimmetrikus, ezért felcserélhetőségük igazolásához elegendő azt belátnunk, hogy  $\eta \circ \vartheta \subseteq \vartheta \circ \eta$ . Tegyük fel, hogy  $a, c \in A$ -ra létezik olyan  $b \in A$ , hogy  $(a, b) \in \eta$ ,  $(b, c) \in \vartheta$ . Azt kell megmutatnunk, hogy van olyan  $d \in a$ , hogy  $(a, d) \in \vartheta$ ,  $(d, c) \in \eta$ . E kongruencia-rendszer megoldása  $d = t(a, b, c)$ , mert a termműveletek megőrzik a kongruenciákat, s ezért  $a = t(a, b, b)$  a  $\vartheta$  relációban van  $t(a, b, c) = d$ -vel,  $t(a, b, c)$  pedig az  $\eta$  relációban van  $t(b, b, c) = c$ -vel.

A „csak akkor” bizonyításához a következő segédtételekre lesz szükségünk. Legyen  $F$  szabad algebra egy  $\mathcal{V}$  varietásban az  $Y$  szabad generátorrendszerrel. Tekintsünk egy ekvivalenciarelációt  $Y$ -on, amelynek  $n$  blokkja van. Jelölje  $\eta$  e reláció által generált kongruenciát  $F$ -en. Akkor  $F/\eta$   $n$  rangú szabad algebra a  $\mathcal{V}$  varietásban. A bizonyítást csak a legegyszerűbb nemtriviális esetre végezzük el, amikor is  $Y$  három elemű, és az ekvivalencia nem triviális; az általános eset ugyanúgy tárgyalható, csak a jelölés lenne nehezkesebb. Malcev tételének belátásához viszont éppen a tárgyalandó esetre lesz szükség.

Jelölje  $F_3$  a 3 rangú szabad algebrát  $\mathcal{V}$ -ben. Tudjuk, hogy  $F_3 \cong T_3/\rho$ , ahol  $\rho = \text{Id } \mathcal{V}$ , és a szabad generátorok  $\rho(x_1), \rho(x_2), \rho(x_3)$ . Ezek helyett írjunk röviden  $y_1, y_2, y_3$ -at. Jelölje továbbá  $\eta$   $F_3$ -nak az  $\{y_1, y_2\}$ , részhalmaz által generált kongruenciáját. Tekintsük az  $F_2$  2 rangú szabad algebrát is  $\mathcal{V}$ -ben a  $\{z_1, z_2\}$  szabad generátorrendszerrel. Az  $y_1, y_2 \mapsto z_1, y_3 \mapsto z_2$  leképezés folytatható  $F_3$ -nak  $F_2$ -re való  $\lambda$  homomorfizmusává. Ehhez a homomorfizmushoz a homomorfizmatétel bizonyításában látott módon  $F_3$ -nak egy ugyancsak a  $\lambda$  jellel jelölhető kongruenciája tartozik, amelyre érvényes  $F_3/\lambda \cong F_2$ . Megmutatjuk, hogy  $\lambda = \eta$ . Mivel  $\eta$  a legszűkebb olyan kongruencia, amely tartalmazza az  $(y_1, y_2)$  párt,  $\lambda \supseteq \eta$ . Másrészt  $F_3/\lambda$   $F_2$ -re való izomorfizmusát megszorozhatjuk azzal a  $\kappa : F_2 \rightarrow F_3/\eta$  szürjektív homomorfizmussal, amely a  $z_1 \mapsto \eta(y_1), z_2 \mapsto \eta(y_3)$  megfeleltetés folytatása. Ez a szorzat maga is szürjektív homomorfizmus, és minden  $\lambda(a) \in F_3/\lambda$  blokknak az  $\eta(a) \in F_3/\eta$  blokkot felelteti meg (amit termeken végzett indukció

mutat). Ezért  $\lambda$  egyetlen blokkja sem bontható fel  $\eta$  több blokkjának egyesítésére, azaz  $\lambda = \eta$ . Ezzel beláttuk, hogy  $\mathbf{F}_3/\eta$  2 rangú szabad algebra a  $\mathcal{V}$  varietásban az  $\{\eta(y_1), \eta(y_3)\}$  szabad generátorrendszerrel.

Most tegyük fel, hogy  $\mathcal{V}$  permutábilis. Jelölje  $\eta$  és  $\vartheta$  megfelelően  $\mathbf{F}_3$ -nak az  $\{y_1, y_2\}$ , ill.  $\{y_2, y_3\}$  részhalmaz által generált kongruenciáját. Akkor  $(y_1, y_3) \in \eta \circ \vartheta$ . Mivel  $\mathbf{F}_3$  minden eleme alkalmas  $t$  termmel  $t(y_1, y_2, y_3)$  alakban adható meg,  $\mathbf{F}_3$  permutabilitásából következik, hogy létezik olyan ternáris  $t$  term, hogy

$$(y_1, t(y_1, y_2, y_3)) \in \vartheta, \quad (t(y_1, y_2, y_3), y_3) \in \eta. \quad (\text{vi})$$

A segédétel mutatja, hogy (az ottani jelöléssel)  $\mathbf{F}_3/\eta$  2 rangú  $\mathcal{V}$ -szabad algebra az  $\eta(y_1), \eta(y_2)$  szabad generátorrendszerrel, és  $\mathbf{F}_3/\vartheta$  is 2 rangú szabad algebra  $\mathcal{V}$ -ben a  $\{\vartheta(y_1), \vartheta(y_2)\}$  szabad generátorrendszerrel.

Megállapodva az  $\eta(y_i) = u_i$ ,  $\vartheta(y_i) = v_i$  jelölésben, ami többek között az  $u_1 = u_2$  és  $v_2 = v_3$  egyenlőségeket is jelenti, a (vi) relációk a  $v_1 (= t(v_1, v_2, v_3)) = t(v_1, v_2, v_2)$  és  $u_1 = t(u_1, u_1, u_3)$  egyenletek alakjába írhatók át. Mivel  $\{v_1, v_2\}$  és  $\{u_1, u_3\}$  szabad algebra szabad generátorai, a tételben szereplő azonosságok valóban érvényesek  $\mathcal{C}$ -ben.

*Ha egy algebra permutábilis, akkor két kongruenciájának egyesítése a kongruenciahálóban megegyezik e kongruenciák szorzatával.* Ennek belátásához először vegyük észre, hogy két kongruenciát tartalmazó legszűkebb kongruencia éppen a két kongruencia közösleges egyesítésének lezártja. A Malcev-lemma alapján meggondolható, hogy ha  $\eta, \vartheta \in \text{Con } A$ , úgy  $(a, b) \in \eta \cup \vartheta$  akkor és csak akkor, ha léteznek olyan  $c_0 = a, c_1, \dots, c_n = b$  elemek  $A$ -ban, hogy

$$(c_0, c_1) \in \eta, (c_1, c_2) \in \vartheta, \dots, (c_{n-2}, c_{n-1}) \in \eta, (c_{n-1}, c_n) \in \vartheta.$$

Ám ha  $A$  permutábilis, ez azt jelenti, hogy  $(a, b) \in \eta \circ \vartheta$ . Ezért  $\overline{\eta \cup \vartheta} \subseteq \eta \circ \vartheta$ . Az ellenkező irányú tartalmazás nyilvánvaló.

Az előző megfigyelésből következik, hogy *ha egy permutábilis  $A$  algebra két kongruenciája egymás komplementuma a  $\text{Con } A$  hálóban, akkor  $A$  felbomlik e kongruenciák szerinti faktoralgebráinak direkt szorzatára.* Csoportokra ezt a tényt a csoportelméleti bevezetésben szokták bizonyítani. A kongruenciák felcserélhetőségének követelménye nélkül nem szükségképpen létezik direkt felbontás (a szubdirekt felbonthatóság természetesen mindig igaz). Ellenpélda a kételemű implikáció-algebra által generált varietás 2 rangú szabad algebrája, amelyet a 24. fejezetben határoztunk meg. Abban az  $\{x, z\}, \{xy, xx\}, \{y\}, \{yx\}$  és az  $\{x, xy\}, \{y, z, yx, xx\}$  blokkokkal rendelkező kongruenciák egymás komplementumai, de maga az algebra csak 6 elemű (a faktoralgebrák direkt szorzata pedig 8 elemű).

Állításunk igazolásához legyen  $A$  permutábilis, és legyenek  $\eta, \vartheta$  olyan kongruenciái, amelyek metszete az egyenlőség, egyesítése a teljes reláció. Minden  $c \in A$ -hoz rendeljük  $(A/\eta) \times (A/\vartheta)$   $(\eta(c), \vartheta(c))$  elemét. Mivel  $\eta \cap \vartheta$  az egyenlőség, ez a hozzárendelés injektív. Szürjektív is, amihez azt kell belátnunk, hogy bármely  $(\eta(a), \vartheta(b))$  pár felírható  $(\eta(c), \vartheta(c))$  alakban. Most  $\eta \cup \vartheta$  a teljes reláció, ezért  $(a, b) \in \eta \cup \vartheta$ , van tehát olyan  $c \in A$ , hogy  $(a, c) \in \eta$ ,  $(c, b) \in \vartheta$ . Ekkor  $(\eta(a), \vartheta(b)) = (\eta(c), \vartheta(c))$ . Végül a definíciójából látszik, hogy hozzárendelésünk felcserélhető az alpműveletekkel.

**27. Varietás bővítése varietással.** Legyenek  $G, A, B$  csoportok. Ha  $G$ -nek van olyan  $N$  normálosztója, hogy  $N \cong A$  és  $G/N \cong B$ , akkor azt mondjuk, hogy  $G$   $A$ -nak  $B$ -vel való bővítése. Az összes csoportok varietást alkotnak; ennek részvarietásai pl. az Abel-csoportok varietása és az adott  $n$  exponensű csoportok varietása. Ismeretes, hogy ha  $\mathcal{A}$  és  $\mathcal{B}$  csoportok két varietása, akkor az  $\mathcal{A}$ -ba tartozó csoportok  $\mathcal{B}$ -be tartozó csoportokkal való összes bővítései ugyancsak varietást alkotnak. Megmutatjuk, hogy ez a tény csupán azon múlik, hogy a csoportok egységelemek és kongruenciáik felcserélhetők.

Tekintsünk egy  $A$  algebrát és egy  $m = m(x_1, \dots, x_k)$   $k$ -áris termet. Ha léteznek olyan  $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_k, b, c \in A$ , hogy

$$m(a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_k) \neq m(a_1, \dots, a_{i-1}, c, a_{i+1}, \dots, a_k),$$

akkor azt mondjuk, hogy  $m$   $A$ -ban lényegesen függ  $x_i$ -től. Ha egy  $\mathcal{V}$  varietásban van olyan  $A$  algebra, hogy  $m$   $A$ -ban lényegesen függ  $x_i$ -től, akkor azt mondjuk, hogy  $m$   $\mathcal{V}$ -ben lényegesen függ  $x_i$ -től. Ha  $m$   $A$ -ban (vagy  $\mathcal{C}$ -ben) pontosan  $l$  számú határozatlantól függ lényegesen, akkor azt mondjuk, hogy  $m$  lényegében  $l$ -áris, vagy  $m$  lényeges aritása  $l$  (megfelelően  $A$ -ban vagy  $\mathcal{C}$ -ben). A lényeges aritás legfeljebb akkora, mint a látszólagos aritás, hiszen a term felírásában nem szereplő határozatlan nem befolyásolhatja a megfelelő termművelet eredményeit. Példa: csoportban az  $x_2 \cdot x_2^{-1}$  term (amelyhez bináris vagy magasabb aritású termművelet tartozik) minimális aritása 2, látszólagos aritása 1, lényeges aritása 0. Ha  $\mathcal{V}$  részvarietása  $\mathcal{W}$ -nek, akkor  $m$  lényeges aritása  $\mathcal{V}$ -ben legfeljebb akkora, mint  $\mathcal{W}$ -ben; ez a definíció közvetlen következménye. Speciálisan, az egyelemű algebrákból álló triviális varietásokban minden term lényeges aritása 0, míg a hasonlósági osztályokban minden term lényeges aritása egyenlő látszólagos arításával. Az utóbbi megállapítás abból következik, hogy a megszámlálható rangú termalgebrában minden term lényegesen függ minden benne előforduló határozatlantól.

Ez az észrevétel tetszőleges varietásra is igaz a következő gyengébb formában. A tetszőleges  $m$  term akkor és csak akkor függ az  $x_i$  határozatlantól a  $\mathcal{V}$  varietásban, ha függ tőle a varietás megszámlálható rangú  $\mathbf{F}$  szabad algebrájában. (Az „akkor” nyilvánvaló; ha pedig  $m$  nem függ  $x_i$ -től  $\mathbf{F}$ -ben, és  $\mathbf{F}$

szabad generátorrendszere  $y_1, y_2, \dots$ , akkor  $m(y_1, \dots, y_{i-1}, y_{k+1}, y_{i+1}, \dots, y_k) = m(y_1, \dots, y_{i-1}, y_{k+2}, y_{i+1}, \dots, y_k)$ , ahonnan — a szabad generátorrendszer leképezéseinek folytathatóságát felhasználva — következik, hogy  $m$  nem függ  $x_i$ -től  $\mathcal{V}$  egyetlen algebrájában sem.) Innen következik, hogy *term lényeges aritása egy varietásban egyenlő e term aritásával a varietás megszámlálható rangú szabad algebrájában.*

Ha egy varietásban van olyan lényegében nulláris term (amely, persze, lehet nullánál nagyobb látszólagos aritású, vagy pl. nulláris alapművelet-term is), amely által kijelölt elem idempotens (azaz egyelemű részalgebrát képez) a varietás minden algebrájában, akkor a varietást *poláris* varietásnak, a szóban forgó termet ill. termműveleteket *pólustermeknek* ill. *pólusműveleteknek*, az általuk kijelölt elemet pedig *pólusnak* nevezzük. Az egységelem pólus minden csoportban, amelyet az 1 nulláris term művelete jelöl ki (vagy ha a csoportot olyan típusú algebrának tekintjük, hogy csak a szorzás és az inverzképzés az alapműveletei, akkor pl.  $x_1 \cdot x_1^{-1}$  a pólus-term); a zéruselem pólus minden gyűrűben. A csoportok és a gyűrűk varietása tehát poláris. Algebra minden részalgebrája tartalmazza a nulláris termműveletek eredményeit, ezért minden algebrának legfeljebb egy pólusa van. Ebből következik, hogy ha  $t_1$  és  $t_2$  pólustermek egy  $\mathcal{V}$  varietásban, akkor  $(t_1, t_2) \in \text{Id } \mathcal{V}$ .

Poláris varietás algebráiban bármely kongruencia pólust tartalmazó blokkja részalgebra (miért?). A továbbiakban jelölje 0 az éppen tekintett poláris varietás pólus-termjét, valamint az általa kijelölt elem(ek)et. Ha  $\mathbf{C}$ ,  $\mathbf{A}$  és  $\mathbf{B}$  egy poláris varietás algebrái, és van olyan  $\rho \in \text{Con } \mathbf{C}$ , hogy  $\rho(0) \cong \mathbf{A}$  és  $\mathbf{C}/\rho \cong \mathbf{B}$ , akkor azt mondjuk, hogy  $\mathbf{C}$   $\mathbf{A}$ -nak  $\mathbf{B}$ -vel való bővítése.

*Tétel (Malcev):* Legyen  $\mathcal{V}$  poláris permutábilis varietás. Ha  $\mathbf{A}$ ,  $\mathbf{B}$  részvarietásai  $\mathcal{V}$ -nek, akkor az  $\mathbf{A}$ -ba tartozó algebrák  $\mathbf{B}$ -be tartozó algebrákkal való összes bővítései ugyancsak varietást alkotnak.

*Bizonyítás (Tőke Pál):* Megmutatjuk, hogy a mondott bővítések osztálya zárt a  $\mathbf{H}$ ,  $\mathbf{S}$  és  $\mathbf{P}$  operátorokra nézve.

**H.** Legyen  $\mathbf{C} \in \mathcal{V}$ ,  $\mathbf{A} \in \mathcal{A}$ ,  $\mathbf{B} \in \mathcal{B}$ , és legyen  $\rho \in \text{Con } \mathbf{C}$  olyan, hogy  $\rho(0) \cong \mathbf{A}$  és  $\mathbf{C}/\rho \cong \mathbf{B}$ . A homomorfiatétel alapján elegendő megmutatnunk, hogy  $\mathbf{C}$  bármely  $\eta$  kongruenciájára  $\mathbf{C}/\eta$  valamely  $\mathcal{A}$ -ba tartozó algebrának valamely  $\mathcal{B}$ -be tartozó algebrával való bővítése. Feltehetjük, hogy  $\rho(0) = \mathbf{A}$ . Mivel  $\rho \cup \eta \supseteq \rho$ , a második izomorfiatétel szerint  $(\mathbf{C}/\eta) / ((\rho \cup \eta)/\eta) \cong \mathbf{C}/(\rho \cup \eta)$ . Itt a jobb oldal  $\mathbf{C}/\rho$ -nak, s vele együtt  $\mathbf{B}$ -nek is homomorf képe, ezért a jobb oldal, s vele együtt a bal oldal is a  $\mathcal{B}$  varietásba tartozik.  $\mathbf{C}/\eta$  pólusa  $\eta(0)$ , ezért  $(\mathbf{C}/\eta) / ((\rho \cup \eta)/\eta)$  pólusa  $((\rho \cup \eta)/\eta)(\eta(0))$ , amelyet tehát mindazok az  $\eta(u)$  blokkok alkotnak, melyekre  $u$  az  $\eta \circ (\rho \cup \eta)$  relációban van 0-val. Minthogy  $\mathcal{V}$  permutábilis,  $\eta \circ (\rho \cup \eta) = \rho \circ \eta$ ; ehhez azt is figyelembe kell vennünk, hogy  $\eta \circ \eta = \eta$ , ami a reflexivitás és tranzitivitás következménye. Innen kapjuk, hogy  $(\mathbf{C}/\eta) / ((\rho \cup \eta)/\eta)$  pólusa  $\eta(\mathbf{A}) / (\eta|\eta(\mathbf{A}))$ . Ez

$C/\eta$  részalgebrája, amely az első izomorfia-tétel szerint izomorf  $A/(\eta|A)$ -val. Az utóbbi pedig, mint  $A$  homomorf képe, az  $\mathcal{A}$  varietásba tartozik.

S. Legyenek  $A, B, C, \rho$  ugyanazok, mint az előző megfontolásban. Tegyük fel, hogy  $D$  részalgebra  $C$ -ben. Az első izomorfia-tétel szerint  $\rho(D)/(\rho|_{\rho(D)}) \cong D/(\rho|D)$ . A bal oldal  $C/\rho$  részalgebrája, tehát  $\mathcal{B}$ -be tartozik; ezért a jobb oldal is. Készen leszünk, ha belátjuk, hogy  $(\rho|D)(0) \in \mathcal{A}$ . De  $(\rho|D)(0) = A \cap D$ , ami  $A$  részalgebrája, tehát valóban  $\mathcal{A}$ -ba tartozik.

P. Az egyszerűség kedvéért a direkt szorzatra vonatkozó zártságot csak két algebra direkt szorzatára mutatjuk meg; az általános eset ugyanúgy kezelhető. Legyen  $A, B \in \mathcal{V}$ ,  $\rho_1 \in \text{Con } A$ ,  $\rho_1(0) \in \mathcal{A}$ ,  $A/\rho_1 \in \mathcal{B}$ ,  $\rho_2 \in \text{Con } B$ ,  $\rho_2(0) \in \mathcal{A}$ ,  $A/\rho_2 \in \mathcal{B}$ . Ha  $\alpha \subseteq A^2$ ,  $\beta \subseteq B^2$ , definiáljuk  $A \times B$ -en az  $\alpha \dot{\times} \beta$  relációt a következő módon: ha  $a_1, a_2 \in A$ ,  $b_1, b_2 \in B$ , legyen

$$((a_1, b_1), (a_2, b_2)) \in \alpha \dot{\times} \beta \iff (a_1, b_1) \in \alpha \text{ és } (a_2, b_2) \in \beta.$$

( $\alpha \times \beta$  — a halmazelméleti szorzat — nem ugyanezt jelenti!) Megmutatjuk, hogy

$$(A_1 \times B_2) / (\rho_1 \dot{\times} \rho_2) \cong (A_1 / \rho_1) \times (B_1 / \rho_2)$$

és

$$(\rho_1 \dot{\times} \rho_2)((0, 0)) = \rho_1(0) \times \rho_2(0),$$

ami elegendő is a bizonyításhoz. A kívánt izomorfizmus:  $(\rho_1 \dot{\times} \rho_2)(a, b) \mapsto (\rho_1(a), \rho_2(b))$ . A definíciók közvetlenül mutatják, hogy ez a leképezés bijektív. Felcserélhető az alapl műveletekkel is:

$$\begin{aligned} m((\rho_1 \dot{\times} \rho_2)(a_1, b_1), \dots, (\rho_1 \dot{\times} \rho_2)(a_k, b_k)) &= (\rho_1 \dot{\times} \rho_2)(m((a_1, b_1), \dots, (a_k, b_k))) \\ &= (\rho_1 \dot{\times} \rho_2)(m(a_1, \dots, a_k), m(b_1, \dots, b_k)) \\ &= (\rho_1(m(a_1, \dots, a_k)), \rho_2(m(b_1, \dots, b_k))) \\ &= (m(\rho_1(a_1), \dots), m(\rho_2(b_1), \dots, \rho_2(b_k))) \\ &= m((\rho_1(a_1), \rho_2(b_1)), \dots, (\rho_1(a_k), \rho_2(b_k))) \end{aligned}$$

Másrészt  $(\rho_1 \dot{\times} \rho_2)((0, 0))$  definíció szerint azon párok halmaza, amelyek első komponense  $\rho_1$ , második komponense  $\rho_2$  relációban van a (megfelelően  $A$ - ill.  $B$ -beli) 0 elemmel, s ez volt a másik bizonyítandó.

**28. Egyszerű algebra varietásban.** Birkhoff szubdirekt felbontási tételéből következik, hogy minden varietásban van szubdirekt irreducibilis algebra (s ennél valamivel több is: *bármely varietást generálják a szubdirekt irreducibilis algebrai*). Az az erősebb állítás azonban, hogy minden varietásban van egyszerű algebra, nem

nyilvánvaló. Ha egy varietásban van nemtriviális (azaz egynél több elemű) véges algebra, akkor annak van maximális kongruenciája is, és az a szerinti faktoralgebrája egyszerű algebra a tekintett varietásban. Nem minden varietásban van azonban nemtriviális véges algebra. Tekintsük a nullákból és egyesekből álló olyan megszámlálható sorozatok halmazát, amelyekben csak véges számú egyes van. Vezessünk be rajta egy bináris  $f$  műveletet, a fésűs egyesítést ( $f((a_0, a_1, \dots), (b_0, b_1, \dots)) = (a_0, b_0, a_1, b_1, \dots)$ ), és két unáris műveletet, a páros és a páratlan indexű elemekből álló sorozatok képzését ( $e(a_0, a_1, a_2, a_3, \dots) = (a_0, a_2, \dots)$ ,  $o(a_0, a_1, a_2, a_3, \dots) = (a_1, a_3, \dots)$ ). Megmutatjuk, hogy ez a  $\mathbf{C}$  algebra olyan varietást generál, amelyben nincs nemtriviális véges algebra.  $\mathbf{C}$ -ben teljesülnek a következő azonosságok:  $(f(e(x_1), o(x_1)), x_1)$ ,  $(e(f(x_1, x_2)), x_1)$ ,  $(o(f(x_1, x_2)), x_2)$ . Ezek teljesülnek tehát a  $\mathbf{C}$  által generált  $\mathcal{V}$  varietás minden algebrájában. Legyen  $A \in \mathcal{V}$ . Megmutatjuk, hogy  $A^2$  bijektív módon leképezhető  $A$ -ra, ami lehetetlen, ha  $A$  egynél több elemű véges halmaz. A bijektív leképezés  $(a_1, a_2) \mapsto f(a_1, a_2)$ . Az első azonosság alapján ez szürjektív, a másik két azonosságból pedig következik, hogy ha két elempár képe ugyanaz, akkor azok első és második komponense is ugyanaz, tehát a leképezés injektív.

Ahhoz, hogy belássuk egyszerű algebra létezését minden varietásban, előbb egy — a szóban forgó problémától látszólag távoli — Malcev típusú tételt fogunk bebizonyítani. Ez a tétel azokat a varietásokat jellemzi, amelyek nemtriviális algebraiban nincs idempotens elem. Ilyen pl. a Boole-gyűrűk varietása. (Meglépően hangzik, lássuk bel!).

*Tétel: Bármely  $\mathcal{V}$  varietásra a következő két állítás ekvivalens:*

- (1)  $\mathcal{V}$  egynél több elemű algebraiban nincs idempotens elem.
- (2) Van olyan  $n$  nemnegatív egész, olyan  $t_1, \dots, t_n$  ternáris termek és olyan  $f_1, \dots, f_n, g_1, \dots, g_n$  unáris termek, hogy  $\mathcal{V}$ -ben teljesülnek az

$$\begin{aligned} &(x_1, t_1(x_1, x_2, f_1(x_1))), \\ &(t_i(x_1, x_2, g_i(x_1)), t_{i+1}(x_1, x_2, f_{i+1}(x_1))) \quad (i = 1, \dots, n-1), \\ &(t_n(x_1, x_2, g_n(x_1))) \end{aligned}$$

*azonosságok.*

*Bizonyítás:* (1)  $\Rightarrow$  (2). Ha a  $\mathcal{V}$  varietás triviális, (2)  $n = 0$ -val teljesül. Egyébként  $\mathcal{V}$  egynél nagyobb rangú szabad algebrainak szabad generátorai különbözök. Figyeljük meg, hogy  $\mathcal{V}$ -beli algebra nemtriviális részalgebrája az algebra egyetlen kongruenciájának sem lehet blokkja, mert különben a kongruencia szerinti (nemtriviális) faktoralgebra idempotens eleme lenne. Tekintsük az  $\{y_1, y_2\}$  szabad generátorrendszerű  $\mathbf{F}_2$   $\mathcal{V}$ -szabad algebraiban az  $y_1$  (egy) elem(ű halmaz) által generált  $\mathbf{F}_1$  részalgebrát. Jelölje  $\psi$   $\mathbf{F}_2$ -nek az  $\mathbf{F}_1$  halmaz által generált kongruenciáját.

Ennek egy blokkja tartalmazza  $F_1$ -et, s ezért részalgebra  $F_2$ -ben. Mint láttuk, ez a blokk csak triviális részalgebra lehet, és így nem más mint  $F_2$  (egy elemű nem lehet, mert akkor  $y_1$  idempotens elem lenne  $F_2$ -ben). Nyertük, hogy  $\psi$  a teljes reláció  $F_2$ -n. Ezért  $(y_1, y_2) \in \psi$ .

Amint a 9. fejezetben láttuk, van olyan  $n$  természetes szám, olyan  $z_0 = y_1, z_1, \dots, z_n = y_2 \in F_2$  elemek, olyan  $(u_i, v_i) \in F_1^2$  elempárok, és  $F_2$ -nek olyan  $\tau_1, \dots, \tau_n$  translációi, hogy  $\tau_i(u_i) = z_{i-1}$ ,  $\tau_i(v_i) = z_i$   $i = 1, \dots, n$ -re. Mivel  $F_1$ -nek  $y_1$  egy elemű generátorrendszere, az  $u_i, v_i$  elemek bizonyos  $f_i, g_i$  unáris termműveletek eredményei  $y_1$ -en. A translációk szabályos felírására emlékezve látjuk, hogy mindegyik  $\tau_i$  egy-egy  $y \mapsto s_i(y, w_2(y_1, y_2), \dots, w_k(y_1, y_2))$  alakban felírható leképezés, ahol  $s_i$  alkalmas term, a  $w_j$ -k pedig a translációban felhasznált  $F_2$ -beli konstansokat — mint  $\{y_1, y_2\}$  generátumának elemeit — előállító termek. Jelölje  $t_i = t_i(x_1, x_2, x_3)$  az  $s_i(x_3, w_2(x_1, x_2), \dots, w_k(x_1, x_2))$  termet. Akkor  $F_2$ -ben teljesülnek a következő egyenlőségek:  $y_1 = t_1(y_1, y_2, f_1(y_1))$ ,  $(z_1 = ) t_1(y_1, y_2, g_1(y_1)) = t_2(y_1, y_2, f_2(y_1))$ ,  $\dots$ ,  $t_n(y_1, y_2, g_n(y_1)) = y_2$ . Mivel  $y_1, y_2 \in \mathcal{V}$ -beli szabad algebra szabad generátorai, a 23. fejezetben tett megállapítás szerint az ezen egyenlőségek oldalaiból képezett párok  $\mathcal{V}$ -ben érvényes azonosságok.

(2)  $\Rightarrow$  (1). Tegyük fel, hogy az  $A \in \mathcal{V}$  algebrának van idempotens  $a$  eleme. Megmutatjuk, hogy  $A = \{a\}$ . Legyen  $b \in A$  tetszőleges. Képezzük a (2)-ben felsorolt azonosságok két oldalán álló bináris termekhez tartozó termműveletek eredményét az  $(a, b)$  helyen. Felhasználva, hogy  $a$  idempotens, nyerjük:  $a = t_1(a, b, f_1(a)) (= t_1(a, b, a)) = t_1(a, b, g_1(a)) = t_2(a, b, f_2(a)) = t_2(a, b, g_2(a)) = \dots = t_n(a, b, a) = t_n(a, b, g_n(a)) = b$ , amit bizonyítani kellett.

Az ígért tétel mostmár egyszerűen bizonyítható.

*Magari tétele: Minden varietásban van egyszerű algebra.*

*Bizonyítás:* Ha a  $\mathcal{V}$  varietásban létezik egynél több elemű  $A$  algebra idempotens  $a$  elemmel, akkor legyen  $b$  egy további elem  $A$ -ban, és tekintsük az  $A$ -ban az  $\{a, b\}$  halmaz által generált  $B$  részalgebrát. E részalgebra  $a$ -t és  $b$ -t szétválasztó kongruenciáinak tartalmazás szerint részbenrendezett halmaza eleget tesz a Zorn-lemma feltételének, van tehát köztük maximális. Ha  $\rho$  ilyen,  $\rho$  egyben maximális nemteljes kongruenciája is  $B$ -nek, mert ha  $\rho_1 \supsetneq \rho$  és  $\rho_1 \neq \rho$ , akkor  $(a, b) \in \rho_1$ , ezért  $\rho_1$   $a$ -t tartalmazó blokkja  $a$ -t és  $b$ -t tartalmazó részalgebra  $B$ -ben, azaz maga  $B$ , tehát  $\rho_1$  teljes.

Ha pedig a  $\mathcal{V}$  varietásban egynél több elemű algebrának nincs idempotens eleme, akkor tekintsünk  $\mathcal{V}$ -ben egy egyetlen  $c$  elem által generált  $C$  algebrát, és alkalmazzuk az  $f_i, g_i$  ( $i = 1, \dots, n$ ) termműveleteket  $c$ -re:  $f_1(c), \dots, g_n(c)$ . Legyen most  $\rho$   $C$ -nek maximális olyan kongruenciája, amely ez utóbbi elemek közül legalább kettőt szétválaszt — a Zorn-lemma szerint ilyen is létezik. Ez a  $\rho$  max-

imális nemteljes kongruenciája  $C$ -nek, mert, ha  $\rho_1 \supseteq \rho$  és  $\rho_1 \neq \rho$ , akkor az előző tétel azonosságai alapján, felhasználva a  $\rho_1(f_1(c)) = \dots = \rho_1(g_n(c))$  egyenlőségeket is, kapjuk, hogy  $C/\rho_1$ -ben bármely  $d \in C$ -re  $\rho_1(c) = \rho_1(d)$ , azaz  $\rho_1$  teljes.

Mindkét esetben találtunk  $\mathcal{V}$ -ben olyan algebrát, amelynek van maximális nemteljes kongruenciája. A második izomorfiatétel szerint azonban algebra maximális nemteljes kongruencia szerinti faktoralgebrája — amely, mint az algebra homomorf képe, maga is  $\mathcal{V}$ -ben van — egyszerű.

**29. Modulusok varietásai.** Legyen  $R$  tetszőleges egységelemes gyűrű. Az  $M$  algebrát  $R$  feletti modulusnak vagy röviden  $R$ -modulusnak nevezzük, ha  $M$  műveletei a következők:

összeadás, amelyet a szokásos módon jelölünk, s amelyre nézve  $M$  Abel-csoport (ezt a modulus Abel-csoportjának nevezzük);

az  $R$  elemeivel való szorzások; ezeket egyváltozós műveleteknek tekintjük, s

az  $a \in M$  elemnek az  $R$ -beli  $r$  elemmel való megszorozása eredményét  $ar$  jelöli;

és ezekre a műveletekre — az Abel-csoportok azonosságain túl — az alábbi azonosságok teljesülnek:

$$\forall r \in R \quad (x + y)r = xr + yr,$$

$$\forall r, s \in R \quad x(r + s) = xr + xs,$$

$$\forall r, s \in R \quad x(rs) = (xr)s.$$

Ha ezeken kívül az  $R$ -beli 1 egységelemre az  $x1 = x$  azonosság is teljesül, akkor azt mondjuk, hogy  $M$  unitér modulus  $R$  felett. Ha hangsúlyozni akarjuk, hogy az  $ar$  alakú műveleti eredményekben az  $R$  gyűrű elemét mindig jobbról írjuk (lehetne következetesen mindig balról is), akkor a modulus *jobbmodulusnak* mondjuk.

A vektortér az unitér modulus speciális esete: ha  $R$  test, akkor az unitér modulus definíciója éppen a vektortér definíciójába megy át. Minden Abel-csoportot tekinthetünk az egész számok  $\mathbb{Z}$  gyűrűje feletti modulusnak; ha  $n \neq 0$ , akkor  $an$  jelentse  $|n|$  számú  $a$  vagy  $-a$  összegét aszerint, hogy  $n$  pozitív vagy negatív, és legyen mindig  $a0 = 0$ . A fentebbi azonosságok ekkor láthatóan teljesülnek. (A vektorteret és az Abel-csoportot rendszerint *balmodulusként* írjuk, ami pl. az Abel-csoportok esetében csupán annyit jelent, hogy az  $n$  tagú  $a + \dots + a$  összeget  $an$  helyett mindig  $na$  jelöli.) Továbbá minden gyűrűt tekinthetünk önmaga feletti modulusnak; az azonosságok egyszerűen a disztributivitás és az asszociativitás miatt teljesülnek. A továbbiakban modulusról beszélve mindig jobbmodulusra gondolunk. Ugyanúgy, mint vektorterekben, modulusokban is megmutatható, hogy ha  $a = 0$  vagy  $r = 0$ , akkor  $ar = 0$ . (Vektorterekben a „csak akkor” is igaz, modulusokban azonban nem; gondoljunk egy zérusosztót tartalmazó gyűrűre, mint önmaga feletti modulusra.)

Ha  $R$  egységelemes gyűrű, az összes  $R$ -modulusok osztálya varietás, mert azonosságokkal — ti. éppen a fentebbi azonosságokkal — definiálható osztály. Jelölje  $\mathcal{M}_R$ . Ebben az osztályban minden  $t(x_1, \dots, x_n)$  term átírható  $x_1 t_1 + \dots + x_n t_n$  normálalakba ( $t_1, \dots, t_n \in R$ ), ami éppúgy látható be, ahogyan az adott test feletti vektorterek osztályára vonatkozó hasonló állítás. Így tehát bármely egységelemes  $R$ -re az  $R$ -modulusokban a termfüggvények éppen a (rögzített együttható-sorozatú) lineáris kombinációk képzését jelentik.

$R$ -modulusok kongruenciái Abel-csoportjuknak is kongruenciái, ezért ezek a modulus Abel-csoportjának részcsoportjai szerinti osztályozásokhoz tartozó ekvivalencia-relációk. Nem minden  $K$  részcsoport szolgáltat azonban kongruenciát. Ehhez az kell, hogy a  $K$  részcsoport szerinti osztályozás kompatibilis legyen az  $R$  elemeivel való szorzásokkal is, tehát bármely  $a \in M$  és  $r \in R$  esetén az  $(a + K)r (= ar + Kr)$  halmaz is valamelyik  $K$  szerinti osztályba tartozzék. Ez igaz, ha  $K$  részmodulusa  $M$ -nek, mert ekkor  $Kr \subseteq K$ , és így  $(a + K)r \subseteq ar + K$ . Ha viszont a  $K$  részcsoport nem részmodulus, akkor van olyan  $r \in R$  és  $k \in K$ , hogy  $kr \notin K$ . Másrészt  $0 \in K$  és  $0r = 0$ , így a  $K$  szerinti osztályozás  $K (= 0 + K)$  osztályának elemei  $r$ -rel való szorzásnál legalább két különböző osztályba kerülnek, tehát az osztályozás nem kompatibilis. Nyertük, hogy modulus kongruenciái éppen a részmodulusai szerinti osztályozásokhoz tartozó ekvivalencia-relációk. Bármely  $M$  modulus minden  $\theta$  kongruenciájához létezik tehát  $M$ -nek egyetlen olyan  $K$  részmodulusa, hogy  $K$  a  $\theta$  kongruenciának (hosszadalmasabban mondva: a  $\theta$  kongruenciához tartozó osztályozásnak) osztálya; azért egyetlen, mert különböző részmodulusok szerinti osztályozás is különböző. Másrészt  $M$  minden  $K$  részmodulusához létezik  $M$ -nek egyetlen olyan  $\theta$  kongruenciája, amelynek  $K$  osztálya, ti. a  $K$  szerinti osztályozáshoz tartozó ekvivalencia-reláció; azért egyetlen, mert különböző osztályozások nem lehetnek ugyanazon részmodulus szerinti osztályozások.

**30. A modulus-varietások jellemzése.** Bármely  $A$  algebra esetén feleltessük meg egymásnak  $A$  egy részalgebráját és egy kongruenciáját, ha az a részalgebra annak a kongruenciának osztálya. Nevezzük ezt (az  $A$  részalgebrái és kongruenciái közötti) *természetes megfeleltetésnek*. A természetes megfeleltetés általában nem bijektív  $\text{Sub}(A)$  és  $\text{Con}(A)$  között; gondoljuk meg ezt a harmadfokú teljes permutációcsoport példáján (s keressünk olyan példát is, amelyben csak triviális részalgebra van, de sok kongruencia). Az előző fejezetben azonban beláttuk, hogy abban az esetben, amikor  $A$  modulus, ez a megfeleltetés bijektív  $\text{Sub}(A)$  és  $\text{Con}(A)$  között. E megfigyelésünk nem fordítható meg; ellenpélda az  $Q = \{1, -1, i, -i, j, -j, k, -k\}$  csoport, az ún. *kvaterniócsoport*, amelynek elemei a kvaternió-ferdetest egységei, a szokásos kvaterniószorzással. Hogy erről meggyőződjünk, keressük meg  $Q$  részcsoportjait, és mutassuk meg, hogy mindegyik normálosztó. Emellett azt is meg

tudjuk mutatni, hogy nem létezik olyan modulus, amely ekvivalens  $Q$ -val.

Valóban, tegyük fel, hogy létezik olyan  $R$  egységelemes gyűrű, hogy a  $Q$  kvaterniócsoport ekvivalens egy  $R$ -modulussal. Ennek a modulusnak a kvaterniócsoport-beli szorzás term-művelete, van tehát olyan  $r_1, r_2 \in R$ , hogy minden  $x, y \in Q$ -ra  $x \circ y = xr_1 + yr_2$  (megkülönböztetésül a gyűrűelemekkel való szorzásoktól, a kvaterniócsoport szorzását köröcskével jelöltük). Feltevésünkéből úgy jutunk majd ellentmondáshoz, hogy belátjuk, hogy a  $Q$  kvaterniócsoport szorzása ugyanaz a művelet, mint a  $Q$  modulus összeadása, és ez lehetetlen, mert a kvaterniócsoport nem Abel-csoport. Azt nem tudjuk, hogy a  $Q$  modulusban melyik elem az additív egységelem; mindenesetre ezt az elemet  $0$ -val fogjuk jelölni. Rögzített  $b \in Q$ -ra az  $a \mapsto a \circ b$  leképezés a  $Q$  halmaznak permutációja. Ha  $b = 0$ , ez a leképezés éppen az  $r_1$ -gyel való szorzás a  $Q$  modulusban, tehát az  $r_1$ -gyel való szorzás permutáció. Ugyanígy látható be, hogy az  $r_2$ -vel való szorzás is. Ezért létezik olyan  $s, t \in Q$ , hogy  $sr_1 = 0, tr_2 = 0$ . Akkor minden  $a \in Q$ -ra  $ar_1 = ar_1 + tr_2 = a \circ t$  és  $ar_2 = sr_1 + ar_2 = s \circ a$ . Speciálisan,  $0 \circ t = 0r_1 = 0$ ,  $s \circ 0 = 0r_2 = 0$ , s innen következik, hogy  $s$  és  $t$  mindegyike a kvaterniócsoport egységeleme. Nyerjük minden  $a, b \in Q$ -ra:

$$a \circ b = ar_1 + br_2 = (a \circ t) + (s \circ b) = a + b.$$

Példánk mutatja: abból, hogy egy  $A$  algebrán a természetes megfeleltetés bijektív, nem következik, hogy  $A$  ekvivalens valamely modulussal. Varietásokra azonban szerencsésebb a helyzet: alkalmas (és természetes) módon definiálva varietások ekvivalenciáját, érvényes a következő

**Tétel.** *A természetes megfeleltetés akkor és csak akkor bijektív egy  $\mathcal{V}$  varietás minden algebráján, ha létezik olyan  $R$  egységelemes gyűrű, hogy  $\mathcal{V}$  ekvivalens az összes  $R$ -modulusok  $\mathcal{M}_R$  varietásával.*

**Bizonyítás.** A feltétel elegendő, mert teljesülése esetén  $\mathcal{V}$  minden  $A$  algebrája ekvivalens egy  $M$   $R$ -modulussal (ugyanazon az alaphalmazon), s így  $A$  és  $M$  részalgebrái ugyanazok a halmazok, továbbá  $A$  és  $M$  kongruenciái ugyanazok az ekvivalencia-relációk.

A szükségesség igazolásához tegyük fel, hogy  $\mathcal{V}$  minden algebráján a természetes megfeleltetés bijektív. Először belátjuk, hogy  $\mathcal{V}$ -ben van poláris művelet. Jelölje  $F_\infty$  a megszámlálható rangú  $\mathcal{V}$ -szabad algebrát az  $\{x_1, x_2, \dots\}$  szabad generátorrendszerrel. Az  $F_\infty$  algebrán az egyenlőség-kongruenciának létezik egyetlen olyan osztálya, amely részalgebra. Van tehát olyan  $t = t(x_1, \dots, x_n)$   $\mathcal{V}$ -term, hogy minden  $f = f(x_1, \dots, x_k)$   $\mathcal{V}$ -termre  $f(t, \dots, t) = t$ . Megmutatjuk, hogy a

$t$  termfüggvénynek nincs lényeges változója  $\mathcal{V}$ -ben. Tegyük fel, hogy pl. az első változója lényeges és tekintsük a  $t' = t(x_{n+1}, x_2, \dots, x_n)$  termet. Ekkor  $t = t'$  nem azonosság, tehát  $t \neq t'$   $F_\infty$ -ben. Másrészt minden  $f$  termre  $f(t', \dots, t') = t'$   $F_\infty$ -ben, mert ez az egyenlőség  $f(t, \dots, t) = t$ -ből az  $x_1 \mapsto x_{n+1}$  helyettesítéssel áll elő. Eszerint  $t'$  is részalgebra  $F_\infty$ -ben, tehát ott az egyenlőség-kongruenciának két különböző osztálya is részalgebra, ellentmondásban a természetes megfeleltetés bijektív voltával. Hasonlóan igazolható, hogy a  $t$  termfüggvény más változóitól sem függ  $\mathcal{V}$ -ben. Kaptuk, hogy a  $t$  termfüggvény poláris művelet  $\mathcal{V}$ -ben. A továbbiakban  $t$  helyett  $0$ -t írunk.

Szükségünk lesz két segédtétele:

1. Ha az  $A$  algebrán a természetes megfeleltetés bijektív, akkor a természetes megfeleltetés izomorfizmus a  $\text{Sub}(A)$  és  $\text{Con}(A)$  hálók között.

A bizonyításhoz legyen  $B$  részalgebra  $A$ -ban, és jelölje  $\beta$  azt a kongruenciát  $A$ -ban, amelynek osztálya a  $B$  halmaz. Akkor  $\beta$  egyben a legszűkebb olyan kongruencia is  $A$ -ban, amelynél  $B$  minden eleme ugyanabba az osztályba tartozik. Ezért  $\beta$   $B$ -ből a részhalmazokra vonatkozó Malcev-lemma segítségével kapható meg. Ha  $C$   $A$ -nak  $B$ -nél bővebb részalgebrája, és  $C$  a  $\gamma$  kongruenciának osztálya, akkor a Malcev-lemma mutatja, hogy  $\gamma$  bővebb, mint  $\beta$ . Eszerint a természetes megfeleltetés monoton (azaz tartalmazást megőrző) bijekció a  $\text{Sub}(A)$  és  $\text{Con}(A)$  hálók között. Általánosan igaz azonban, hogy hálónak hálóra való bijektív és monoton leképezése izomorfizmus (igazolása egyszerű).

2. Legyen a  $\mathcal{V}$  varietás minden algebráján a természetes megfeleltetés bijektív. Ha  $A \in \mathcal{V}$ ,  $B, C \leq A$ ,  $B \cap C = \{0\}$ , és  $[B \cup C] = A$ , akkor  $A \cong B \times C$ , és létezik olyan  $\varphi : A \rightarrow B \times C$  szürjektív izomorfizmus, amelynél minden  $b \in B$ -re  $\varphi(b) = (b, 0)$ , és minden  $c \in C$ -re  $\varphi(c) = (0, c)$ .

A bizonyításhoz most is jelölje  $\beta$  ill.  $\gamma$  azokat a kongruenciákat  $A$ -ban, amelyeknek osztálya a  $B$  ill.  $C$  részalgebra. Belátjuk, hogy minden  $a \in A$ -hoz létezik egyetlen olyan  $a_b \in B$ , hogy  $a\gamma a_b$ , és ugyancsak egyetlen olyan  $a_c \in C$ , hogy  $a\beta a_c$ . Van olyan  $t_a \stackrel{\sim}{=} t_a(x_1, \dots, x_k, x_{k+1}, \dots, x_{k+l})$   $\mathcal{V}$ -term, hogy  $a = t_a(b_1, \dots, b_k, c_{k+1}, \dots, c_{k+l})$ . Ekkor

$$a\gamma t_a(b_1, \dots, b_k, 0, \dots, 0) \in B,$$

és

$$a\beta t_a(0, \dots, 0, c_{k+1}, \dots, c_{k+l}) \in C.$$

Így a keresett elemek  $a_b = t_a(b_1, \dots, b_k, 0, \dots, 0)$ ,  $a_c = t_a(0, \dots, 0, c_{k+1}, \dots, c_{k+l})$ . Tekintsünk két olyan elemet  $B$ -ben, amelyek a  $\gamma$  relációban vannak  $a$ -val. Ezek a  $\gamma|_B$  relációban vannak, amely  $B$ -nek kongruenciája, s  $\{0\}$  az egyetlen olyan osztálya, amely részalgebra. Ezért  $\gamma|_B$  az egyenlőség-reláció  $B$ -n, így a tekintett két

elem egyenlő. Nyertük, hogy  $a_b$  valóban egyértelműen meghatározott. Ugyanígy igazoljuk  $a_c$  unicitását. Mind az  $a \mapsto a_b$ , mind az  $a \mapsto a_c$  leképezés homomorf (gondoljuk meg).

Legyen  $\varphi(a) = (a_b, a_c)$ . Megmutatjuk, hogy  $\varphi$  a keresett izomorfizmus. Ha  $\varphi(a) = \varphi(a')$ , akkor  $a(\beta \cap \gamma)a'$  és az 1. segédtétel szerint  $\beta \cap \gamma$  az egyenlőség-reláció, így  $a = a'$ , tehát  $\varphi$  injektív. A  $\varphi$  leképezés definíciójából következik, hogy  $b \in B$ -re  $\varphi(b) = (b, 0)$ , és  $c \in C$ -re  $\varphi(c) = (0, c)$ . Azt, hogy  $\varphi$  a műveletekkel felcserélhető, egyszerűség kedvéért egy kétváltozós  $*$  művelet példáján mutatjuk be:

$$\varphi(a) * \varphi(a') = (a_b, a_c) * (a'_b, a'_c) = (a_b * a'_b, a_c * a'_c) = ((a * a')_b, (a * a')_c) = \varphi(a * a').$$

Még azt kell belátnunk, hogy  $\varphi$  szürjektív. Mint látjuk,  $\varphi(A) = \{\varphi(a) | a \in A\}$ . A val izomorf részalgebrája a  $B \times C$  direkt szorzatnak, úgy tekinthetjük tehát, hogy  $A$  be van ágyazva  $B \times C$ -be. E beágyazásban  $B$ -t a  $(B, 0) = \{(b, 0) | b \in B\}$ ,  $C$ -t pedig a  $(0, C) = \{(0, c) | c \in C\}$  részalgebra jelenti. Feltevésünk szerint  $[(B, 0) \cup (0, C)] = \varphi(A)$ . Másrészt  $B \times C \in \mathcal{V}$ , ezért  $B \times C$ -n is bijektív a természetes megfeleltetés. A  $(B, 0)$  részalgebra annak a kongruenciának osztálya, amelyben akkor van két elempár, ha második komponensük ugyanaz,  $(0, C)$  pedig azé, amelyet a megegyező első komponensű elempárok alkotnak. E két kongruencia egyesítése a teljes kongruencia, azaz a  $\text{Con}(B \times C)$  háló egységeleme, mert bármely párból bármely másik pár megkapható két lépésben úgy, hogy az első lépésben az első komponens, a másodikban a másodikat hagyjuk változatlanul. Az 1. segédtétel szerint ekkor ennek a két kongruenciának megfelelő részalgebrák  $[(B, 0) \cup (0, C)]$  egyesítése a  $\text{Sub}(B \times C)$  hálóban ugyancsak az egységelem lesz, vagyis  $[(B, 0) \cup (0, C)] = B \times C$ . Ezért  $\varphi(A) = B \times C$ , tehát  $\varphi$  valóban szürjektív, s ezzel a 2. segédtétel bizonyítása kész.

Jelölje  $F_n$  az  $n$  rangú  $\mathcal{V}$ -szabad algebrát az  $\{x_1, \dots, x_n\}$  szabad generátorrendszerrel. Jegyezzük meg, hogy  $F_n$ -ben az  $F_1 = [x_1], [x_2], \dots, [x_n]$  részalgebrák mind izomorfok. Megmutatjuk, hogy  $F_n$  izomorf  $F_1$   $n$  példányának  $[x_1] \times \dots \times [x_n]$  direkt szorzatával, és van  $F_n$ -nek  $[x_1] \times \dots \times [x_n]$ -re való olyan  $\varphi$  izomorfizmusa, amelynél minden  $t(x_1)$  termre és minden  $i$ -re ( $i = 1, \dots, n$ )  $\varphi(t(x_i)) = (\dots, 0, t(x_i), 0, \dots)$ , ahol a jobb oldalon  $t(x_i)$  az  $i$ -edik helyen áll. (Ilyenkor röviden azt fogjuk mondani, hogy  $\varphi$  kielégíti az unáris term-feltételt.) Állításunk nyilvánvaló  $n = 1$ -re. Tegyük fel, hogy  $F_{n-1} \cong [x_1] \times \dots \times [x_{n-1}]$ , és az unáris term-feltételt kielégítő  $\chi$  szürjektív izomorfizmus létezik. Alkalmazzuk  $F_n$ -re és két részalgebrájára,  $F_{n-1}$ -re és  $[x_n]$ -re a 2. segédtételt. E két részalgebra metszetében levő  $(f(x_1, \dots, x_{n-1}) = g(x_n))$  alakú termek lényegileg 0-változósak  $\mathcal{V}$ -ben. Ha létezne e metszetben két különböző elem, akkor ezek az elemek (pl.)  $[x_n]$  minden részalgebrájában benne lennének, s így az egyenlőség-reláció egyetlen osztálya sem lehetne részalgebra, ellentmondásban a természetes

megfeleltetés bijektív voltára vonatkozó feltevessel. Ezért a két részalgebra metszete  $\{0\}$ . Egyesítésük  $F_n$  részalgebra-hálójában nyilvánvalóan  $F_n$ . A 2. segédétel szerint  $F_n \cong F_{n-1} \times [x_n]$ , és van olyan  $\psi : F_n \rightarrow F_{n-1} \times [x_n]$  szürjektív izomorfizmus, hogy minden  $f = f(x_1, \dots, x_{n-1}) \in F_{n-1}$ -re  $\psi(f) = (f, 0)$ , és minden  $t = t(x_n) \in [x_n]$ -re  $\psi(t) = (0, t)$ . Minden  $g = g(x_1, \dots, x_n) \in F_n$ -hez rendeljük a  $\varphi(g) = (g_1, \dots, g_{n-1}, g_n)$  elem- $n$ -est, ahol  $g_1, \dots, g_{n-1}$   $\psi(g)$  első komponense  $\chi$  melletti képének komponensei,  $g_n$  pedig  $\psi(g)$  második komponense. Mivel  $\psi$  és  $\chi$  szürjektív izomorfizmusok,  $\varphi$  is az lesz, és ellenőrizhető, hogy kielégíti az unáris term-feltételt is. Az  $F_n$  szabad algebrának az  $[x_1] \times \dots \times [x_n]$  direkt szorzatra való most leírt (szürjektív, és az unáris term-feltételt kielégítő) izomorfizmusát a rövidség kedvéért *kanonikus izomorfizmusnak* nevezzük.

Az előző számolás megmutatta, hogy  $\mathcal{V}$ -ben a véges rangú szabad algebrák 1 rangúak direkt szorzatai. Ezt felhasználva most már nem nehéz megtalálni  $\mathcal{V}$ -ben az összeadás szerepét játszó műveletet és felépíteni azt a gyűrűt, amely feletti modulusokkal ekvivalensek a  $\mathcal{V}$ -beli algebrák. Mint igazoltuk, létezik  $F_2$ -nek  $\varphi$  kanonikus izomorfizmusa  $[x_1] \times [x_2]$ -re. Legyen  $p = p(x_1, x_2)$  az az eleme  $F_2$ -nek, amelyre  $\varphi(p) = (x_1, x_2)$ . Írjunk  $p(x_1, x_2)$  helyett a továbbiakban  $x_1 + x_2$ -t, és nevezzük a  $p$  termműveletet összeadásnak.

Megmutatjuk, hogy 0 az összeadásra vonatkozóan egységelem, továbbá az összeadás asszociatív és kommutatív. Érvényes

$$(x_1, x_2) = \varphi(x_1 + x_2) = \varphi(x_1) + \varphi(x_2) = (x_1, 0) + (0, x_2) = (x_1 + 0, 0 + x_2),$$

ahonnan  $x_1 + 0 = x_1$  és  $0 + x_1 = x_1$ . Ezután tekintsük  $F_4$  kanonikus izomorfizmusát  $[x_1] \times [x_2] \times [x_3] \times [x_4]$ -re. Nem okoz félreértést, ha most ezt jelöljük  $\varphi$ -vel. Belátunk az összeadásra egy olyan azonosságot, amelyből az asszociativitás és a kommutativitás is következik.

$$\begin{aligned} (x_1 + x_2) + (x_3 + x_4) &= \varphi^{-1}((\varphi(x_1) + \varphi(x_2)) + (\varphi(x_3) + \varphi(x_4))) \\ &= \varphi^{-1}(((x_1, 0, 0, 0) + (0, x_2, 0, 0)) + ((0, 0, x_3, 0) + (0, 0, 0, x_4))) \\ &= \varphi^{-1}((x_1, x_2, 0, 0) + (0, 0, x_3, x_4)) \\ &= \varphi^{-1}(x_1, x_2, x_3, x_4), \end{aligned}$$

és ugyanilyen módon kapjuk, hogy  $(x_1 + x_3) + (x_2 + x_4) = \varphi^{-1}(x_1, x_2, x_3, x_4)$ . Innen kapjuk az

$$(x_1 + x_2) + (x_3 + x_4) = (x_1 + x_3) + (x_2 + x_4)$$

azonosságot. Ha ebben  $x_2 = 0$ -t helyettesítünk, az összeadás asszociativitását, ha pedig  $x_1 = x_4 = 0$ -t, akkor az összeadás kommutativitását kapjuk.

Megmutatjuk, hogy  $\mathcal{V}$  algebráiban az összeadásra vonatkozóan minden elemnek van inverze, és azt minden algebrában ugyanaz a term jelöli ki. Olyan  $r = r(x_1)$

termet kell tehát találnunk, amelyre az  $x_1 + r(x_1) = 0$  azonosság teljesül. Ebből a célból tekintsük  $F_3$ -nak az  $S = [x_1, x_2 + x_3, x_3]$  részalgebráját. A  $\mathcal{V}$ -re vonatkozó feltevés szerint  $S \subseteq F_3$  valamely kongruenciájának osztálya, ezért a Ljapin–Malcev-lemma szerint minden  $\tau$  egyváltozós polinomfüggvényre vagy  $\tau(S) \subseteq S$ , vagy  $\tau(S) \cap S = \emptyset$  igaz. Tekintsük  $F_3$ -on a  $\tau : a \mapsto x_2 + a$  egyváltozós polinomfüggvényt. Akkor  $x_3 \in S$  és  $\tau(x_3) = x_2 + x_3 \in S$ , ezért  $x_1 \in S$ -ből következik  $\tau(x_1) = x_2 + x_1 (= x_1 + x_2) \in S$ . Létezik tehát olyan  $s = s(x_1, x_2, x_3) \in \mathcal{V}$ -term, hogy  $x_1 + x_2 = s(x_1, x_2 + x_3, x_3)$ .

Az additív inverz megkereséséhez és a további megfontolásokhoz szükségünk lesz egy azonosságra (pontosabban azonosság-seregére). Megmutatjuk, hogy minden  $n$ -re és minden  $t = t(x_1, \dots, x_n) \in \mathcal{V}$ -termre a

$$t(x_1, \dots, x_n) = t(x_1, 0, \dots, 0) + t(0, x_2, 0, \dots, 0) + \dots + t(0, \dots, 0, x_n)$$

azonosság teljesül  $\mathcal{V}$ -ben. Ez azt jelenti, hogy minden  $n$ -áris term felbontható  $n$  számú unáris term összegére. Jelölje  $\varphi : F_n$  kanonikus izomorfizmusát  $[x_1] \times \dots \times [x_n]$ -re. Elegendő belátnunk, hogy az igazolandó azonosság két oldalának  $\varphi$  melletti képe ugyanaz. Figyeljük meg, hogy a kanonikus izomorfizmusnál  $F_n$   $x_1 + \dots + x_n$  elemének képe  $(x_1, \dots, x_n)$ , és általánosabban, tetszőleges  $u_1, \dots, u_n$  unáris termekre  $u_1(x_1) + \dots + u_n(x_n)$  képe  $(u_1(x_1), \dots, u_n(x_n))$ . Ezt alkalmazva nyerjük:

$$\begin{aligned} \varphi(t(x_1, \dots, x_n)) &= t(\varphi(x_1), \dots, \varphi(x_n)) \\ &= t((x_1, 0, \dots, 0), (0, x_2, 0, \dots, 0), \dots, (0, \dots, 0, x_n)) \\ &= (t(x_1, 0, \dots, 0), t(0, x_2, 0, \dots, 0), \dots, t(0, \dots, 0, x_n)) \\ &= \varphi(t(x_1, 0, \dots, 0) + t(0, x_2, 0, \dots, 0) + \dots + t(0, \dots, 0, x_n)). \end{aligned}$$

A most igazolt azonosságot nevezzük *felbontási azonosságnak*. Azt az előző azonosságot, amely az összeadást a Ljapin–Malcev-lemma segítségével kapott  $s$  termmel fejezi ki, a következő alakba írhatjuk át a felbontási azonosság segítségével:

$$\begin{aligned} x_1 + x_2 &= s(x_1, 0, 0) + s(0, x_2 + x_3, 0) + s(0, 0, x_3) \\ &= s(x_1, 0, 0) + s(0, x_2, 0) + s(0, x_3, 0) + s(0, 0, x_3). \end{aligned}$$

Legyen ezúttal  $\varphi : F_3$ -nak  $[x_1] \times [x_2] \times [x_3]$ -ra való kanonikus izomorfizmusa. Azonosságunk két oldalának  $\varphi$  melletti képe ugyanaz. Részletesen:

$$(x_1, x_2, 0) = (s(x_1, 0, 0), s(0, x_2, 0), s(0, x_3, 0) + s(0, 0, x_3)).$$

Innen — többek között — következik az  $s(0, x_1, 0) = x_1$  és az  $s(0, x_1, 0) + s(0, 0, x_1) = 0$  azonosság, amelyek egybevetésével kapjuk, hogy  $x_1 + s(0, 0, x_1) = 0$ .

A keresett  $r_1(x_1)$  term tehát nem más, mint  $s(0, 0, x_1)$ . Így a  $\mathcal{V}$ -beli algebrákban az összeadásra vonatkozóan minden  $a$  elemnek van inverze, mégpedig  $s(0, 0, a)$ . Ezzel azt is beláttuk, hogy az összeadásra nézve  $\mathcal{V}$  algebrai Abel-csoportok.

A felbontási azonosság mutatja, hogy  $\mathcal{V}$ -ben minden term legfeljebb egy generátort tartalmazó termék összege, s ezért minden termfüggvény lényegileg legfeljebb egyváltozós termfüggvények összege. Gondoljuk meg, hogy bármely egységelemes  $R$  gyűrű feletti összes unitér jobbmodulusok varietásában az egyváltozós termfüggvények éppen az  $R$  elemeivel való szorzások, és az  $R$  különböző elemeivel való szorzások különböző termfüggvények (ha ugyanis  $r_1, r_2 \in R$  és  $r_1 \neq r_2$ , akkor  $R$ -ben, mint  $R$ -modulusban,  $1r_1 \neq 1r_2$ ). Ez adja az ötletet, hogy azt az egységelemes gyűrűt keresve, amely feletti unitér jobbmodulusok varietása ekvivalensnek bizonyul majd  $\mathcal{V}$ -vel,  $\mathcal{V}$  legfeljebb egy generátort tartalmazó különböző termjeire gondoljunk. Ezek  $F_1$  különböző elemeivel jelölhetők. Az eddigiekben máris láttuk, hogy  $F_1$  az összeadás műveletével — vagyis az  $f + g = (f + g)(x_1) = f(x_1) + g(x_1)$  művelettel — Abel-csoport. A szorzást  $F_1$ -ben termék szuperpozíciójával (egymásba helyettesítésével) definiáljuk:  $fg = (fg)(x_1) = g(f(x_1))$ . Ez a művelet nyilvánvalóan asszociatív, továbbá az összeadásra nézve disztributív: ha  $f, g, h (= h(x_1)) \in F_1$ , akkor

$$\begin{aligned} ((f + g)h)(x_1) &= h((f + g)(x_1)) \\ &= h(f(x_1) + g(x_1)) = (fh)(x_1) + (gh)(x_1) = (fh + gh)(x_1), \end{aligned}$$

és hasonlóan következik a másik oldali disztributivitás is. Így tehát  $F_1$  a bevezetett két művelettel gyűrű, amelynek egységeleme az  $x_1$  unáris term. Jelölje ezt a gyűrűt  $R$ .

Megmutatjuk, hogy  $\mathcal{V}$ -ben minden  $A$  algebra  $R$ -modulus, ha benne az összeadást a fentebb vizsgált módon, az  $R$  elemeivel való szorzásokat pedig minden  $a \in A$ -ra és  $f \in R$ -re az  $af = f(a)$  szabállyal értelmezzük. Az előzőekben már láttuk, hogy  $A$  az összeadásra nézve Abel-csoport. Teljesülnek a modulus-azonosságok is: minden  $a, b \in A$ -ra és  $f, g \in R$ -re

$$\begin{aligned} a(f + g) &= (f + g)(a) = f(a) + g(a) = af + ag, \\ (a + b)f &= f(a + b) = f(a + 0) + f(0 + b) = af + bf, \\ a(fg) &= g(f(a)) = g(af) = (af)g, \\ a1 &= (x_1|_{x_1=a}) = a. \end{aligned}$$

A felbontási azonosság szerint  $\mathcal{V}$ -ben minden  $f(x_1, \dots, x_n)$  term  $x_1f_1 + \dots + x_nf_n$  ( $f_i \in R$ ) alakban is írható, tehát a  $\mathcal{V}$ -termek egyben  $\mathcal{M}_R$ -termek is. Másrészt nyilvánvaló, hogy az  $\mathcal{M}_R$ -termek mind  $\mathcal{V}$ -termek. Még azt kell észrevennünk,

hogy ha  $f = g$  azaz  $f(x_1, \dots, x_n) = g(x_1, \dots, x_n)$  azonosan teljesül  $\mathcal{V}$ -ben, akkor ennek az azonosságnak az  $x_1 f_1 + \dots + x_n f_n = x_1 g_1 + \dots + x_n g_n$  alakjában  $f_i = g_i$  igaz  $i = 1, \dots, n$ -re. Ez  $F_1 \in \mathcal{V}$ -ben  $x_k = \delta_i^k, k = 1, \dots, n$  helyettesítéssel látható be. Ezzel a bizonyítás kész.

**31. Klón.** Tekintsünk egy adott típusú  $\mathbf{A}$  algebrát.  $\mathbf{A}$  összes termműveleteinek halmaza is, összes polinomműveleteinek halmaza is rendelkezik a következő két tulajdonsággal:

- (1) Tartalmazza az összes projekció-műveleteket.
- (2) Zárt az összetett függvények képzésére nézve.

A (2) tulajdonság részletesebben a következőt jelenti: Ha  $f$   $n$ -áris (pl.) termművelet,  $g_1, \dots, g_n$  pedig  $k$ -áris termműveletek, akkor

$$(a_1, \dots, a_k) \mapsto f(g_1(a_1, \dots, a_k), \dots, g_n(a_1, \dots, a_k))$$

is  $(k$ -áris) termművelet. Ilyen fogalmazásban (2) nyilvánvaló a termék és termműveletek definíciójából. (Összetett függvények belső függvényeit mindig tekinthetjük megegyező arításúnak; pl.  $xy + \sin x$  második belső függvényét is tekinthetjük kétváltozós függvénynek, ti. olyannak, amely csak az első változójától függ.) Műveletekből összetett függvény képzését szokás a műveletek *szuperpozíciójának* vagy *kompozíciójának* is nevezni.

Adott halmaz műveleteinek az (1) és (2) tulajdonsággal rendelkező  $C$  halmazát *klónnak* nevezzük. Néha szükséges lehet klón helyett *műveletklón*t mondani (mert a klón szót műveleteken kívül más algebrai objektumokra is alkalmazzuk).

A fenti két tulajdonsága számos más művelethalmaznak megvan. Példák:

- Az összes műveletek egy adott  $A$  halmazon ( $A$  teljes műveletklónja, jele  $O_A$ ).
- Az összes (akármilyen arítású) projekciók (ugyanott).
- Az összes folytonos (akárhány változós, valós értékű) valós függvények.
- Az összes (minden változójukban) monoton növekvő valós függvények.

További, algebrai jellegű példákat kapunk, ha tekintünk egy tetszőleges  $M$  halmazt, s annak egy nemtriviális  $K$  részhalmazát (vagy egy nemtriviális  $\rho$  kongruenciáját), s mindazon  $f$  műveleteket vesszük  $M$ -en, amelyekre vonatkozóan  $K$  részalgebrája (ill.  $\rho$  kongruenciája) az  $(M, f)$  algebrának. Azt, hogy  $K$  részalgebrája  $(M, f)$ -nek, szokás úgy is kifejezni, hogy  $K$  *zárt  $f$ -re nézve*, vagy,  $f$  *megőrzi  $K$ -t*.

A  $C$  klónban levő  $k$ -áris műveletek halmazát a klón  $k$ -adik *emeletének* nevezzük és  $C_k$ -val jelöljük. A szuperpozíció tekinthető a klón elemein (azaz műveleteken) végzett általánosított műveletnek: míg az  $M$  halmazon értelmezett művelet  $M^n$ -nek  $M$ -be való leképezése (egy bizonyos  $n$ -re), addig a szuperpozíció  $C_n \times C_k^n$  leképezése  $C_k$ -ba (minden  $n$ -re és  $k$ -ra). Ennek megfelelően az (univerzális) algebra-alapfogalmai klónokra is alkalmazhatók. Klón *részklónján* olyan

részhalmazát értjük, amely maga is klón (azaz tartalmazza a projekciókat és zárt a szuperpozícióra nézve). Klón összes részklónjai lezárási rendszert, s ezért teljes hálót alkotnak. E háló atomjait és duális atomjait (azaz duális hálójának atomjait) megfelelően *minimális* ill. *maximális klónoknak* nevezzük. Adott  $C$  klón *generátorrendszerén*  $C$  elemeinek olyan  $F$  halmazát értjük, hogy  $F$ -beli műveletekből és projekciókból bármely  $C$ -beli elem (azaz művelet) előáll véges számú szuperpozícióval. Bármely algebra alpműveletei generátorrendszerét képezik az algebra termműveletei klónjának; az összes (egyváltozós) konstans függvényekkel együtt pedig az algebra összes polinomműveleteinek a klónját generálják. Műveletek adott  $F$  halmaza által generált klón — az algebraék esetéhez hasonlóan — úgy is jellemezhető, mint az  $F$ -et tartalmazó összes klónok metszete, vagy mint az  $F$ -et tartalmazó legszűkebb klón. A minimális és maximális klónok pedig a generálás segítségével is jellemezhetőek.  $C$  minimális klón, ha tartalmaz nemprojekciót, és minden benne lévő nemprojekció generátorrendszere;  $C$  maximális klón, ha nem az összes műveletek klónja, de bármely hozzá nem tartozó művelettel együtt már az összes műveletek klónját generálja.

Legalább két elemű véges halmaz klónjainak hálója végtelen, de legfeljebb kontinuum számosságú, mert véges halmazon csak megszámlálhatóan végtelen különböző művelet van. A kételemű halmaz klónjai alkotta hálót *Post-hálónak* nevezzük (első teljes leírását Post adta 1921-ben). A Post-háló megszámlálhatóan végtelen; ennek az egyszerű ténynek nem ismeretes egyszerű bizonyítása.

*Janov-Mucsnyik-tétel:* Legalább három elemű véges halmaz klónhálója kontinuum számosságú. A tekintett halmaz legyen  $k = \{0, 1, \dots, k-1\}$ . A bizonyításhoz megadunk egy olyan megszámlálhatóan végtelen  $M$  művelethalmazt, amelynek egyetlen művelete sincs benne az összes többi  $M$ -beli műveletek által generált klónban. Ekkor  $M$  különböző részhalmazai különböző klónokat generálnak.

Álljon  $M$  az összes  $f_i$  műveletekből ( $i = 2, 3, \dots$ ), ahol

- $f_1$  aritása  $i$ ,
- $a_1, \dots, a_i \in M$ -re  $f_i(a_1, \dots, a_i) = 1$ , ha egy kivétellel mindegyik  $a$  2, a kivétel  $a$  pedig 1,
- $f_i(a_1, \dots, a_i) = 0$  minden más esetben.

Láthatóan minden  $f_i$  lényeges aritása  $i$  (azaz  $f_i$  értéke ténylegesen függ mindegyik változója értékétől). Jelöljük  $M_i$ -vel az  $M$ -ből  $f_i$  elhagyásával keletkező művelethalmazt. Tegyük fel, hogy valamely  $i$ -re  $f_i$ -t tartalmazza az  $M_i$  által generált klón. Akkor van olyan  $j$ , és vannak olyan  $g_1, \dots, g_j$  termműveletek  $M_i$  felett, hogy

$$(*) \quad f_i(= f_i(x_1, \dots, x_i)) = f_j(g_1, \dots, g_j).$$

Különböztessünk meg három esetet:

- (1) Ha  $g_1, \dots, g_j$  mind projekciók, akkor közöttük nem fordulhat elő  $i$ -nél nagyobb indexű projekció. Nem lehetséges továbbá  $i > j$ , mert ekkor  $f_i$ -nek  $i$ -nél kevesebb lényeges változója lenne. Ezért  $j > i$ , s így az  $f_j$  argumentumában álló projekciók között vannak egyenlők. Az általánosság megszorítása nélkül feltehető  $g_1 = g_2 = x_i$ . Ha most  $(*)$ -ba  $x_1 = 1$ -et és  $x_2 = \dots = x_i = 2$ -t helyettesítünk, akkor a baloldal értéke 1, a jobboldalé 0; ellentmondás.
- (2) Ha csak egyetlen  $g$  — mondjuk,  $g_1$  — nem projekció, és  $g_2 = x_i$ , akkor  $(*)$ -ba  $x_i = 1$ -et, minden más változóba 2-t helyettesítve ugyanazt az ellentmondást kapjuk, mint az előző esetben.
- (3) Ha legalább két különböző  $g$  — mondjuk,  $g_1$  és  $g_2$  — nem projekció, akkor megint az  $x_1 = 1, x_2 = \dots = x_i = 2$  helyettesítés vezet ellentmondásra.

**32. Primál algebrák.** Ha egy véges  $(A, F)$  algebra termműveleteinek klónja  $O_A$  (vagyis az algebra alaphalmazán értelmezhető minden művelet termművelet), akkor  $(A, F)$ -et *primál* algebrának nevezzük. Az olyan algebrát pedig, amelynek alaphalmazán minden lehetséges művelet polinomművelet, *függvényteljes* algebrának mondjuk. A polinomok és termek közötti kapcsolat mutatja, hogy ha egy függvényteljes algebrában minden unáris konstans művelet termművelet, akkor az az algebra primál. Jegyezzük meg, hogy ha egy klón tartalmazza az unáris konstans műveleteket, akkor bármely  $n$ -re tartalmazza az  $n$ -áris konstans műveleteket is, ti. az unáris  $c$  konstans műveletet külső függvényként szuperponálva bármelyik  $n$ -áris projekcióval az  $n$ -áris  $c$  konstans műveletet kapjuk.

Minden véges test függvényteljes. Ezt a tényt a klasszikus algebra Lagrange-féle interpolációs tétele szokásos bizonyításának gondolatát utánozva láthatjuk be. Azt a bizonyítást megvizsgálva kiválaszthatjuk a bizonyítás során ténylegesen használt feltevéseket, s így a következő általánosabb megállapítást kapjuk:

*Werner–Wille-lemma:* Ha egy  $A$  halmazon  $+$  és  $\cdot$  művelet, valamint  $a$   $0, 1 \in A$  elemek olyanok, hogy  $0$  egységeleme  $+$ -nak és zéruseleme  $\cdot$ -nak, míg  $1$  egységeleme  $\cdot$ -nak, akkor bármely  $A$  alaphalmazú algebra, amelynek polinomműveletei között ott van  $+$  és  $\cdot$ , valamint  $A$  minden elemének a karakterisztikus függvénye, függvényteljes.

A bizonyításhoz jelölje  $a \in A$  karakterisztikus függvényét  $\chi_a$  (ez unáris művelet, amelyre  $\chi_a(x) = 1$ , ha  $x = a$ ; másutt  $\chi_a(x) = 0$ ), továbbá jelölje  $(a_1, \dots, a_n)$  karakterisztikus függvényét  $A^n$ -ben  $\chi_{(a_1, \dots, a_n)}$  (ez  $n$ -áris!). Akkor bármely rögzített  $(a_1, \dots, a_n) \in A^n$ -re

$$\prod_{i=1}^n \chi_{a_i}(x_i) = \chi_{(a_1, \dots, a_n)}(x_1, \dots, x_n),$$

továbbá bármely  $n$ -áris műveletre  $A$ -n és tetszőleges  $(b_1, \dots, b_n) \in A^n$ -re

$$f(b_1, \dots, b_n) = \sum_{(a_1, \dots, a_n) \in A^n} f(a_1, \dots, a_n) \cdot \chi_{(a_1, \dots, a_n)} f(b_1, \dots, b_n),$$

ahol  $f(a_1, \dots, a_n)$   $n$ -áris konstans művelet; ui. ekkor a jobboldalnak egyetlen nemzérus tagja van, és az  $f(b_1, \dots, b_n)$ .

A véges testek függvényteljessége a Werner–Wille-lemma speciális esete, mert véges testben az elemek karakterisztikus függvényei polinomműveletek:  $k$  elemű testben minden  $x$  testelemre  $\chi_a(x) = 1 - (x - a)^{k-1}$ . (Alkalmazzuk a csoportelméleti Lagrange-tételt a test multiplikatív csoportjára.)

A következő tétel mutatja, hogy bármely véges halmaz teljes műveletklónjának létezik egyetlen műveletből álló generátorrendszere. Az ilyen műveletet *Sheffer-műveletnek* nevezzük. (Sheffer kételemű halmazon talált ilyen műveletet, tehát az összes Boole-függvények között — azaz a  $\{0, 1\}$  halmaz teljes műveletklónjában — talált egyelemű generátorrendszert.)

*Webb tétele:*  $A \setminus \{0, 1, \dots, m-1\}$  halmazon

$$a \circ b = \max\{a, b\} + 1 \pmod{m}$$

*Sheffer-művelet.*

A bizonyításhoz elegendő megmutatni, hogy a  $\circ$  művelet által generált klón tartalmaz a Werner–Wille-lemma feltételeinek eleget tevő  $+$  és  $\cdot$  műveleteket, és tartalmazza az összes konstans műveleteket, valamint  $0, 1, \dots, m-1$  karakterisztikus függvényét (az utóbbiakban az  $1$  elem szerepét  $m-1$  tölti be). Azt látjuk be, hogy mindezek termműveletek az egyetlen  $\circ$  alapművelet felett. Jelölje  $p$  az  $x \circ x$  termet. Akkor  $p(x)$  az  $x + 1 \pmod{m}$  művelet, és  $p^{m-1}(x \circ y) = \max\{x, y\}$ . A maximum-művelet tehát termművelet, emellett teljesíti a  $+$ -ra kirótt feltételeket. A  $c$  konstans műveletet a  $p^{c+1}(\max\{x, p(x), \dots, p^{m-1}(x)\})$  termművelet adja, míg  $c$  karakterisztikus függvénye  $p(\max\{p(x), \dots, p^{m-c-2}(x), p^{m-c}(x), \dots, p^m(x)\})$ . A  $\cdot$  művelettel szemben támasztott feltételeket a  $\min$  művelet teljesíti, amely a  $\max$  műveletből „tükrözéssel” így nyerhető:

$$\min\{x, y\} = m - 1 - \max\{m - 1 - x, m - 1 - y\}.$$

Most már csak az  $x \mapsto m - 1 - x$  unáris műveletet kell  $\circ$  feletti termműveletként előállítanunk. Eközben használhatjuk a termművelet alakjában már felírt műveleteket:

$$m - 1 - x = \max\{p^{m-0}(\max\{\chi_0(x), 0\}), \dots, p^{m-(m-1)}(\max\{\chi_{m-1}(x), m - 1\})\}.$$

**33. Maximális klónok.** A Webb-tételből következik, hogy ha egy véges  $M$  halmaz valamely  $C$  klónja nem egyenlő  $O_M$ -mel, akkor létezik  $M$ -en olyan maximális klón, amely  $C$ -t tartalmazza. Valóban, a  $C$ -t tartalmazó, de Sheffer-műveletet nem tartalmazó klónok olyan részbenrendezett halmazt alkotnak, amelyben minden rendezett részhalmaznak van felső korlátja, ti. a belé tartozó klónok egyesítése. Ezért a Zorn-lemma szerint a  $C$ -t tartalmazó, de Sheffer-műveletet nem tartalmazó klónok között van maximális; ez azonban  $M$  összes klónjai között is maximális lesz.

Két példát mutatunk be maximális klónra. Legyen  $S$  nemtriviális részhalmaza az  $A$  halmaznak. Mindazon műveletek  $A$ -n, amelyekre nézve  $S$  zárt, maximális klónt alkotnak. A bizonyításhoz legyen  $f$  olyan  $k$ -áris művelet  $A$ -n, amelyre nézve  $S$  nem zárt,  $g$  pedig tetszőleges  $n$ -áris művelet  $A$ -n. Legyenek  $c_1, \dots, c_k \in S$  olyan elemek, hogy  $f(c_1, \dots, c_k) = c \notin S$ . Defináljuk az  $n+1$ -áris  $h$  műveletet a következőképpen:

$$h(a_1, \dots, a_n, a_{n+1}) = \begin{cases} g(a_1, \dots, a_n), & \text{ha } a_{n+1} = c \\ c_k, & \text{ha } a_{n+1} \neq c. \end{cases}$$

Akkor  $S$  zárt  $h$ -ra nézve, és — természetesen —  $S$  ugyancsak zárt az  $x_i$   $n$ -áris projekciókra és a  $c_i$   $n$ -áris konstans műveletekre nézve. A

$$g = g(x_1, \dots, x_n) = h(x_1, \dots, x_n, f(c_1, \dots, c_n))$$

egyenlőség mutatja, hogy  $A$ -n minden művelet előáll szuperpozícióval  $S$ -t megőrző műveletekből és bármely további műveletből; ezért az  $S$ -t megőrző műveletek valóban maximális klónt alkotnak.

A másik példa Šlupecki következő tételéből folyik, amelyet később bizonyítottunk: Legalább három elemű véges halmazon az összes unáris műveletek együtt bármely lényegében legalább 2 aritású szűrjektív művelettel a halmaz teljes műveletklónját generálják. (Szűrjektív a művelet, ha értékkészlete az alaphalmaz.) A lényegében legalább 2 aritású szűrjektív műveletet lényeges műveletnek nevezzük. A definícióból következik, hogy az összes nemlényeges műveletek klónt alkotnak, s a Šlupecki-tétel szerint legalább három elemű halmazon az összes nemlényeges műveletek klónja maximális, továbbá ez az egyetlen maximális klón ott, amelynek első emelete az összes unáris műveletekből áll.

*Kuznyecov tétele:* Véges halmazon csak véges számú maximális klón van. A Boole-függvények elméletének klasszikus eredménye, hogy kételemű halmazon pontosan öt maximális klón van; lásd Czédli Gábor *Boole-függvények* c. könyvét (Polygon, 1995). Ezért a továbbiakban feltesszük, hogy halmazunk legalább három elemű. A bizonyításhoz elegendő belátnunk, hogy különböző maximális klónok első emelete is különböző (mivel az utóbbiak a tekintett véges halmaz teljes transzformációmonoidjának részmonoidjai). Ha a két különböző maximális klón közül az

egyik az összes nemlényeges műveletek klónja, akkor ennek első emelete az előző bekezdés végén tett megjegyzés szerint nem lehet más maximális klón első emelete. Most már csak azt kell belátnunk, hogy halmazunk teljes transzformációmonoidjának bármely  $S$  valódi részmonoidja legfeljebb egy maximális klón első emelete.

Legyen  $S$  egy  $C$  maximális klón első emelete. Mindazok a műveletek, amelyeket külső függvényként bármilyen  $S$ -beli műveletekkel szuperponálva  $S$ -beli műveleteket kapunk, klónt alkotnak (ellenőrizzük). Jelölje ezt a klónt  $C_1$ . Bármely  $k$ -áris  $f \in C$  műveletre és  $s_1, \dots, s_k \in S$  unáris műveletekre az  $f(s_1(x), \dots, s_k(x))$  unáris művelet  $C$ -be, és így  $S$ -be tartozik. Ezért  $C \subseteq C_1$ . Mivel  $C$  maximális klón, és  $S$  nem tartalmaz minden transzformációt, szükségképpen  $C = C_1$ .

Kuznyecov tételének kiegészítéséül jegyezzük meg, hogy nem minden transzformációmonoid első emelete valamely maximális klónnak. (Pl. az egyetlen identikus leképezés sem; lássuk be ezt!)

*A véges  $A = (A, F)$  algebra akkor és csak akkor primál, ha  $F$ -et  $A$  egyetlen maximális klónja sem tartalmazza.* Ez következik a jelen fejezet első állításából, meg abból a tényből, hogy  $F$ -et és  $A$  termműveleteinek klónját  $A$ -nak ugyanazok a klónjai tartalmazzák.

**34. Shupecki tétele.** Bebizonyítjuk az előző fejezetben kimondott és alkalmazott tételt. Felhasználjuk a Werner–Wille-lemma következő élesebb alakját:

Legyen adva a legalább három elemű véges  $A$  halmaz és  $A$ -nak egy  $B$  részhalmaza. Ha az  $A$ -n értelmezett  $+$  és  $\cdot$  műveletek, valamint a  $0, 1 \in B$  elemek olyanok, hogy minden  $b \in B$ -re  $b+0 = 0+b$ ,  $b \cdot 0 = 0$ ,  $b \cdot 1 = b$ , akkor bármely olyan művelet  $A$ -n, amelynek értékkészlete  $B$ -be esik, polinomművelet a  $+$  és  $\cdot$  műveletekből, valamint  $A$  minden elemének a karakterisztikus függvényéből álló alpművelet-halmaz felett. (A lemma eredeti alakjára adott bizonyítás erre az alakra is jó.)

Hogy ne kelljen nehézkes jelöléseket használnunk, a tételt csak bináris szürjektív műveletre igazoljuk; az általános eset hasonlóan igazolható. Nevezzük az  $A^2$  halmaz  $A_1 \times A_2$  ( $A_1, A_2 \subseteq A$ ) alakú részhalmazát  $t$ -négyzetnek, ha  $|A_1| = |A_2| = t$ .

*Jablonszkij-lemma:* Ha az  $A$  halmazon egy  $\circ$  lényeges bináris művelet legalább három különböző értéket vesz fel, akkor van olyan 2-négyzet is, amelyen az a művelet legalább három különböző értéket vesz fel. (Lássuk be!) A Jablonszkij-lemmából következik:

- (1) Ha az  $A$  halmazon egy  $\circ$  lényeges bináris művelet legalább  $k$  különböző értéket vesz fel, akkor van olyan  $k-1$ -négyzet is, amelyen a művelet legalább  $k$  különböző értéket vesz fel.
- (2) Ha  $A$  és  $\circ$  ugyanaz, mint a lemmában, akkor van olyan 2-négyzet és olyan  $c \in A$ , hogy  $\circ$  a  $c$  értéket azon a 2-négyzeten pontosan egyszer veszi fel.

A Słupecki-tétel bizonyítása: Legyen  $\mathbf{A} = (A; T_A, \circ)$  legalább három elemű algebra, ahol  $T_A$  az  $A$  halmaz összes transzformációinak halmazát jelöli,  $\circ$  pedig lényeges bináris művelet. Megmutatjuk, hogy minden  $(2 \leq) t (\leq |A|)$  természetes számra bármely olyan  $g$  művelet  $A$ -n, amelynek értékkészlete  $t$  elemű,  $\mathbf{A}$ -nak termművelete. Legyen  $g$  értékkészlete  $t = \{0, 1, \dots, t-1\}$ . Indukcióval bizonyítunk.

$t = 2$ . A Jablonszkij-lemma második következménye szerint van olyan  $(a_0, a_1) \times (b_0, b_1) \subseteq A^2$  2-négyzet és olyan  $c \in A$ , hogy  $\circ$  a  $c$  értéket ezen a 2-négyzeten pontosan egyszer veszi fel. Feltéhetjük, hogy  $a_1 \circ b_1 = c$ . Legyen  $\phi_1, \phi_2 \in T_A$  olyan, hogy  $\phi_1(i) = a_i$ ,  $\phi_2(i) = b_i$ , ha  $i \in \{0, 1\}$ . Defináljuk a  $\cdot$  és  $+$  műveleteket: minden  $x, y \in A$ -ra legyen

$$x \cdot y = \chi_c(\phi_1(x) \circ \phi_2(y)), \quad x + y = \chi_0(\chi_0(x) \cdot \chi_0(y)).$$

Akkor minden  $x \in \{0, 1\}$ -re  $0 + x = x + 0 = x$ ,  $x \cdot 1 = x$ ,  $x \cdot 0 = 0$ . Most az állítás a Werner-Wille-lemma élesebb alakjából következik.

$t - 1 \rightarrow t$ . Az elemek jelölését szükség esetén megváltoztatva, a Jablonszkij-lemma első következménye szerint létezik olyan  $C \times D \subseteq A^2$   $t - 1$ -négyzet, amelyen  $g$  felveszi értékkészletének mind a  $t$  elemét. Minden  $0 \leq i < t$ -re válasszunk olyan  $c_i \in C$ ,  $d_i \in D$  elemeket, hogy  $c_i \circ d_i = i$ . Ha  $g$   $k$ -áris, definiáljuk az ugyancsak  $k$ -áris  $g_1, g_2$  műveleteket úgy, hogy valahányszor  $g(r_1, \dots, r_k) = i$ , mindannyiszor  $g_1(r_1, \dots, r_k) = c_i$  és  $g_2(r_1, \dots, r_k) = d_i$  teljesüljön. Ekkor  $g_1$  és  $g_2$  értékkészlete  $t - 1$  elemű, ezért — indukciófeltevés szerint —  $g_1$  és  $g_2$   $\mathbf{A}$ -nak termművelete. Másrészt

$$g(r_1, \dots, r_k) = (i = c_i \circ d_i) = g_1(r_1, \dots, r_k) \circ g_2(r_1, \dots, r_k),$$

ami mutatja, hogy  $g$  termművelete  $\mathbf{A}$ -nak, és ezt akartuk bizonyítani.

**35. A Słupecki-tétel alkalmazásai.** Néhány egyszerű alkalmazást mutatunk be.

A papír-kő-olló játékban két gyerek egyszerre mutatja tenyerét (papír), öklét (kő) vagy szétnyitott mutató- és középső ujját (olló). Az olló nyer a papír ellen, a papír a kő ellen (a kő becsomagolható), a kő az olló ellen. A játék szabályát a következő grupoidművelet táblázatába foglalhatjuk:

|  |   |   |   |
|--|---|---|---|
|  | 0 | 0 | 2 |
|  | 0 | 1 | 1 |
|  | 2 | 1 | 2 |

(0, 1 és 2 a papírt, a követ és az ollót jelöli ilyen sorrendben.) Nevezzük az így megadott algebrát papír-kő-olló-grupoidnak; műveletét jelölje  $\circ$ .

*Quackenbush tétele:* A papír-kő-olló-grupoid függvényteljes. Mint táblázata mutatja,  $\circ$  lényeges művelet. Nem nehéz belátni, hogy  $\mathbf{3} = \{0, 1, 2\}$  összes permutációi (és így összes transzpozíciói is) együtt egy kételemű értékkészletű transzformációjával generálják az összes transzformációk félcsoportját. A játék szabálya mutatja, hogy a (012) ciklus automorfizmusa grupoidunknak. Ezért elegendő pl. a (01) transzpozíciót és egy kételemű értékkészletű transzformációt előállítanunk a grupoid polinomfüggvényeként; utána a tétel a Šlupecki-tételből következik. Az  $x \circ 0$  transláció értékkészlete kételemű. Másrészt,

$$(01) = (x \circ 1 \circ 2 \circ 0) \circ (x \circ 2) \circ (x \circ 1 \circ 2 \circ 0 \circ 1).$$

(Szokásos megállapodás, hogy a műveletek elvégzésének sorrendjét kijelölő zárójelzés hiányában mindig a két balszélső elemen végezzük el a műveletet, majd e művelet eredményén és a tőle közvetlenül jobbra álló elemen, stb. Próbáljuk egyszerűbb polinomművelettel kifejezni (01)-et!)

Az alábbi  $t$  művelet bármely halmazon bevezethető. Neve: *ternáris diszkriminátor*.

$$t(x, y, z) = \begin{cases} x, & \text{ha } x \neq y \\ z, & \text{ha } x = y. \end{cases}$$

*Werner tétele:* Ha egy legalább három elemű véges algebrán a ternáris diszkriminátor polinomfüggvény, akkor az algebra függvényteljes.

A ternáris diszkriminátor definícióját „dualizálva” a  $d$  duális diszkriminátor műveletet kapjuk:

$$d(x, y, z) = \begin{cases} x, & \text{ha } t(x) = z \\ z, & \text{ha } t(x) = x. \end{cases}$$

A duális diszkriminátor mindig termművelet a ternáris diszkriminátor felett. Valóban,

$$d(x, y, z) = t(x, t(x, y, z), z).$$

Ezért Werner tétele következik a duális diszkriminátorra vonatkozó megfelelő tételből:

*Fried-Pixley-tétel:* Ha egy legalább három elemű véges algebrán a duális diszkriminátor polinomfüggvény, akkor az algebra függvényteljes. Elegendő azt igazolnunk, hogy bármely  $m \geq 3$  természetes számra az  $\mathbf{M} = (\mathbf{m}, d)$  algebra függvényteljes. Ellenőrizhető, hogy  $d$  lényeges, továbbá  $d$ -t definíciójából következően  $\mathbf{m}$  minden permutációja megőrzi. Ezért most is elegendő belátnunk, hogy a (01) transzpozíció és valamely  $m - 1$  elemű értékkészletű transzformáció  $\mathbf{M}$ -nek polinomfüggvénye.

Definiáljuk a  $g_k$  polinomműveleteket a következő módon:

$$g_1(x) = d(1, d(2, d(0, x, 2), 1)0),$$

$$g_k(x) = d(k, x, g_{k-1}(x)).$$

Akkor  $k > 1$ -re  $g_k$  értékkészlete  $k+1$  elemű, és  $g_{m-1}$  éppen a (01) transzpozíció.

**36. Rosenberg tétele.** A 33. fejezet utolsó állítása szerint a véges halmazok összes maximális klónjainak ismeretében elvben eldönthető, hogy egy véges algebra primál-e (és hasonlóképpen az is, hogy függvénytjeljes-e). Pontosabban és részletesebben, ha adva van minden véges halmaz összes maximális klónjainak olyan leírása, amellyel bármely műveletről algoritmussal eldönthető, hogy mely maximális klónok tartalmazzák, akkor az is eldönthető algoritmussal, hogy egy véges sok alpműveletű véges algebra primál-e (vagy függvénytjeljes-e).

Ilyen leírást nyújt a maximális klónokról Rosenberg tétele, amely ezért a szóban forgó vizsgálatok terén „nagyagyú”. (Gondoljuk meg, Słupecki tételére lehet-e építeni algebra primál voltát eldöntő algoritmust!?)

A tétel kimondása is sok előkészületet igényel, bizonyítása hosszú és bonyolult. Ezért a tétel kimondására és alkalmazásának bemutatására szorítkozunk.

Legyen  $n$  természetes szám. Az  $A$  halmazon értelmezett  $n$ -áris reláción  $A^n$  tetszőleges részhalmazát értjük. Azt mondjuk, hogy az  $A$ -n értelmezett  $f$   $k$ -áris művelet megőrzi a  $\rho$  ( $\subseteq A^n$ ) relációt, ha valahányszor az  $a_{ij}$  ( $i = 1, \dots, k$ ;  $j = 1, \dots, n$ )  $A$ -beli elemekből képezett

$$\begin{array}{ccc} a_{11} & \dots & a_{1k} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nk} \end{array}$$

mátrix minden oszlopában levő elem- $n$ -es a  $\rho$  relációban van, akkor az  $f$  műveletnek a mátrix sorain való elvégzése útján keletkező

$$(f(a_{11}, \dots, a_{1k}), \dots, f(a_{n1}, \dots, a_{nk}))$$

elem- $n$ -es is a  $\rho$  relációban van. Pl. unáris relációt éppen az általa kijelölt részhalmazt megőrző műveletek, ekvivalenciarelációt a hozzátartozó osztályozást megőrző műveletek őrzik meg. A klón és a relációmegőrzés definícióját egybevetve világos, hogy bármely  $\rho$  relációt megőrző összes műveletek klónt alkotnak. (Hasonló igaz adott relációk mindegyikét megőrző műveletekre.) Ezt a klónt  $\text{Pol } \rho$  fogja jelölni. A definíciót átfogalmazhatjuk: az  $f$  művelet pontosan akkor őrzi meg a  $\rho \subseteq A^n$  relációt, ha  $\rho$  részalgebrája az  $(A^n; f)$  algebrának.

Rosenberg tételében hat fajta reláció szerepel, s a tétel azt mondja ki, hogy bármely  $A$  véges halmazon minden maximális klón megadható  $\text{Pol } \rho$  alakban, ahol  $\rho$  a hat relációfajta valamelyikéhez tartozik. A Rosenberg-relációk a következők:

- (1) Minden olyan részbenrendezés  $A$ -n, amelyre vonatkozóan van legkisebb és legnagyobb elem  $A$ -ban.
- (2) Olyan kvaternáris  $\rho$  reláció, amelyhez  $A$ -n értelmezhető olyan elemi  $p$ -csoport (vagyis azonos prímszám rendű csoportok direkt szorzata), hogy  $a, b, c, d \in A$ -ra  $(a, b, c, d) \in \rho \Leftrightarrow a + b = c + d$ . (Ilyen  $\rho$  csak prímszámosságú halmazon létezik.)
- (3) Olyan bináris  $\rho$  reláció, amelyhez létezik  $A$ -nak olyan fixpont nélküli, prímszámrendű (vagyis azonos prímszám hosszúságú ciklusok szorzataként felírható)  $\pi$  permutációja, hogy  $a, b \in A$ -ra  $(a, b) \in \rho \Leftrightarrow \pi(a) = b$ .
- (4)  $A$  minden nemtriviális ekvivalenciarelációja.
- (5)  $A$  minden centrális relációja. (Az  $n$ -áris  $\rho$  centrális, ha
  - nemtriviális,
  - invariáns változói permutációival szemben,
  - tartalmaz minden olyan elem- $n$ -est, amelyben vannak azonos elemek,
  - $A$ -nak van olyan nemtriviális  $C$  részhalmaza (a reláció centruma), hogy  $\rho$  tartalmaz minden olyan elem- $n$ -est, amelyben van  $C$ -beli elem.
- (6)  $A$  minden nemtriviális relációja, amely  $n$ -reguláris valamely  $n (> 2)$  természetes számra. (Az  $n$ -áris  $\rho$   $n$ -reguláris, ha vannak  $A$ -nak olyan  $\pi_1, \dots, \pi_t$  osztályozásai ( $t \geq 1$ ), amelyek mindegyike  $n$  blokkból áll, mindegyikből egyszerre tetszőlegesen kiválasztva egy-egy blokkot, azok metszete nem üres, s amelyek meghatározzák  $\rho$ -t a következő értelemben:  $\rho$  azokból az elem- $n$ -esekből áll, amelyekben mindegyik osztályozáshoz van legalább két olyan elem, amely annak az osztályozásnak ugyanazon blokkjában van.)

A fenti felsorolás (többek között) mutatja, hogy primál algebra műveletei nem lehetnek monotonok legkisebb és legnagyobb elemmel bíró részbenrendezésre vonatkozóan (speciálisan, nem rendezhető hálószerűen), nem rendelkezhet fixpont nélküli, prímszámrendű automorfizmussal, szükségképpen egyszerű, nem rendelkezhet nemtriviális részalgebrával (egyeleművel sem!).

Speciálisan, a primál algebrák mind simák. Az utolsónak említett tulajdonság oka, hogy a nemtriviális unáris relációk mind centrálisak. A legalább bináris centrális relációt nem megőrző műveletek nem jellemezhetők ilyen egyszerűen. A (2) típusú relációt a benne szereplő ( $p$  elemű test feletti vektortérrel ekvivalens, tehát annak is tekinthető) Abel-csoport feletti  $\varepsilon_1(x_1) + \dots + \varepsilon_k(x_k) + c$  alakú műveletek (és csak ezek) őrzik meg, ahol mindegyik  $\varepsilon_i$  a vektortér lineáris transzformációja,  $c$  pedig

a csoport eleme. A (6) típusú relációnak speciális esete  $n$  elemű halmazon az az  $n$ -áris reláció, amelyben egy elem- $n$ -es pontosan akkor van, ha komponensei nem mind különbözők. Ezt a relációt a nemlényeges műveletek és csak ezek őrzik meg (lássuk bel!).

Ha a Rosenberg-relációk segítségével algebra függvényteljességét akarjuk eldönteni, akkor nem kell figyelembe vennünk az (1) típusú unáris és a (3) típusú relációkat, mert ezeket a konstans műveletek úgysem őrzik meg. Példaként megadjuk a csoportok függvényteljességének szükséges és elegendő feltételét:

*Maurer-Rhodes-tétel:* Véges csoport akkor és csak akkor függvényteljes, ha egyszerű és nem kommutatív. A bizonyításhoz megmutatjuk, hogy ilyen csoport művelete nem őrizhet meg egyetlen — figyelembe veendő — Rosenberg-relációt sem.

(1) Véges csoport alaphalmazának nincs olyan részbenrendezése, amelyet a csoportművelet megőrizne. (Lássuk be.)

(2) Ilyen típusú reláció nem fordulhat elő, mert egyszerű nemkommutatív csoport elemeinek száma nem lehet prímszám. (Miért?)

(4) Algebra egyszerűsége azt jelenti, hogy alpműveletei nem őriznek meg nemtriviális ekvivalenciát.

(5) Legyen  $\rho$  legalább  $k$ -áris ( $k > 1$ ) centrális reláció, amelyet valamely csoport művelete megőriz. Legyen  $1$  a csoport egységeleme,  $c$  pedig eleme  $\rho$  centrumának. Akkor bármely  $g_1, \dots, g_k$  csoportelemekre

$$(g_1, \dots, g_k) = (c, g_2 c^{-1}, g_3, \dots, g_k) \cdot (c^{-1} g_1, c, 1, \dots, 1) \in \rho,$$

tehát  $\rho$  triviális; ellentmondás.

(6) Bármely  $k$ -áris reguláris reláció tartalmaz minden olyan  $k$ -ast, amelyben nem minden komponens különböző. Az előző eset jelölését használva:

$$(g_1, \dots, g_k) = (g_1, g_2, g_2, g_4, \dots, g_k) \cdot (1, 1, g_2^{-1} g_3, 1, \dots, 1),$$

tehát  $\rho$  ebben az esetben is triviális.

**37. Minimális klónok.** A definíció szerint, egy  $C$  klón akkor és csak akkor minimális, ha bármely  $f \in C$  nemprojekció műveletre  $C = [f]$ ; másképpen, bármely  $f, g \in C$  műveletekre, ahol  $f$  nem projekció,  $g$  termmművelet  $f$  felett. A minimális klónt generáló minimális (lényeges) aritású műveletet *minimális műveletnek* nevezzük.

A továbbiakban felhasználjuk azt a nyilvánvaló tényt, hogy bármely  $f$  műveletből változói azonosításával vagy permutációjával  $[f]$ -be tartozó művelet jön létre. (Ilyenkor nem csupa különböző projekciókat vagy megváltoztatott sorrendű projekciókat használunk belső függvényekként az  $f$  külső függvényhez.)

Ha egy  $C$  minimális klónban minden művelet lényeges aritása 1, akkor generátorművelete vagy prímszámrendű permutáció, vagy *retrakció*, azaz idempotens transzformáció. Ha van  $C$ -ben legalább 2 lényeges aritású  $f$  művelet, akkor  $[f]$ -be tartozik az unáris  $f_1 = f(x, \dots, x)$ , amely felett  $f$  nem lehet termművelet. Így  $f_1$  az identikus leképezés, tehát  $f$  idempotens. Tegyük fel, hogy  $f$  minimális. Ha  $f$  ternáris, akkor bármely két változóját azonosítva kisebb aritású termműveletet kapunk  $f$  felett, és ez csak projekció lehet. Nyolc lehetőség van ( $x$ -et és  $y$ -t írunk  $x_1$  és  $x_2$  helyett):

$$\begin{aligned} f(x, x, y) &= x \ x \ x \ x \ y \ y \ y \ y \\ f(x, y, x) &= x \ x \ y \ y \ x \ x \ y \ y \\ f(y, x, x) &= x \ y \ x \ y \ x \ y \ x \ y \end{aligned}$$

Az első esetben  $f$ -et *többségi műveletnek*, az utolsó esetben *kisebbségi műveletnek* nevezzük. A második, harmadik és ötödik esetben bármely két változó azonosításával  $f$ -ből *ugyanaz* a projekció keletkezik (ti. megfelelően az első, második és harmadik ternáris projekció). Ekkor  $f$  ternáris *szemiprojekció*; így nevezzük minden, tetszőleges aritású műveletet, amelyből változói bármely azonosításakor ugyanaz a projekció lesz. Belátjuk, hogy a fennmaradó három esetben  $f$  nem generálhat minimális klónt. A negyedik és a hetedik esetből a hatodik változók permutálásával keletkezik, ezért elég a hatodik esetet vizsgálnunk. Ebben az esetben  $f$ -ből ugyanúgy kapunk többségi függvényt, ahogy a 35. fejezetben a ternáris diszkriminátorból előállítottuk a duális diszkriminátort.  $f$  azonban nem kapható meg termműveletként többségi műveletből, ugyanis a többségi művelet feletti ternáris termműveletek maguk is mind többségi műveletek. (Ezt induktívan bizonyíthatjuk.)

Ha az  $f$  minimális művelet legalább négy változós, akkor szükségképpen szemiprojekció. Ez következik az alábbi tényből:

*Świerczkowski-lemma:* Ha egy  $f$  legalább négy lényeges változós műveletből bármely két lényeges változója azonosításakor projekció keletkezik, akkor  $f$  szemiprojekció. Ennek igazolásához elég azt belátnunk, hogy, ha az  $f(x_1, x_1, x_3, x_4, \dots)$ ,  $f(x_1, x_2, x_1, x_4, \dots)$  termműveletek projekciók, akkor ez a két termművelet egybeesik. (Más változó-azonosításokra „arasolással” juthatunk ugyanehhez a konklúzióhoz.)

Rövidség kedvéért  $f(x_1, x_2, x_3, x_4, \dots)$  helyett  $xyuv \dots$ -t írunk. Tegyük fel, hogy a felírt két termművelet különböző projekció; mondjuk, az  $i$ -edik és a  $j$ -edik. Most a lehetséges eseteket megvizsgálva mindig ellentmondást kapunk, pl. két konkrét esetben a következőképpen:

$$\begin{aligned} i = 1 &\Rightarrow xxuv = x \Rightarrow xxv = x \\ j = 4 &\Rightarrow xyv = v \Rightarrow xv = v \end{aligned}$$

és

$$i = 3 \Rightarrow xxvv = v \Leftrightarrow xyvv = v$$

$$j = 2 \Rightarrow xyxx = y \Leftrightarrow xyvv = y.$$

Az előző megfontolásokkal igazoltuk a következőt:

*Rosenberg osztályozási tétele: Véges halmazon minden minimális művelet vagy unáris, vagy bináris idempotens, vagy többségi, vagy kisebbségi, vagy szemiprojekció. Rosenberg azt is megmutatta, hogy kisebbségi minimális művelet csak 2-hatvány elemszámú halmazon létezik, s ott az egy elemi 2-csoport  $x + y + z$  termművelete. Nem ismeretes a minimális klónoknak a maximálisokéhoz hasonló teljes leírása. (Ismertek a két és három elemű halmaz összes minimális klónjai, valamint a szemiprojekciók kivételével a négy elemű halmazéi is.)*

Az osztályozási tételből következik, hogy véges halmazon csak véges számú minimális klón van (mert  $n$  elemű halmazon nincs  $n$ -nél nagyobb arítású szemiprojekció.)

*Véges halmazon minden klón tartalmaz minimális klónt.* Ennek belátásához nevezzünk egy  $C$  klónt  $n$ -speciálisnak, ha  $C$ -ben minden nemprojekció lényeges arítása legalább  $n$ , és van olyan  $n$ -áris művelet  $C$ -ben, amely generálja  $C$ -t. Minden nemtriviális  $B$  klónnak van  $n$ -speciális részklónja valamely  $n$ -re, ti. egy benne lévő minimális arítású nemprojekció illet generál. A Świerczkowski-lemmából folyik, hogy  $n$  nem lehet nagyobb, mint a tekintett véges  $M$  halmaz elemeinek száma. Innen következik, hogy  $B$ -nek legfeljebb véges sok speciális részklónja van. Utóbbiak halmazában létezik (tartalmazás szerint) minimális. Ez  $M$  összes klónjainak halmazában is minimális; ha nem lenne az, akkor egy valódi nemtriviális részklónjára ugyanezt a gondolatmenetet alkalmazva  $B$ -nek még szűkebb speciális részklónját kapnánk.

Példák minimális klónokra:

1. Bármely félháló (=idempotens kommutatív félcsoport) termműveleteinek klónja minimális. Félhálónak minden  $n$ -re egyetlen  $n$  lényeges arítású termművelete van:  $t_n = x_1 x_2 \dots x_n$ . Ha  $k < n$ , akkor  $t_k$   $t_n$ -ből változók azonosításával keletkezik. Ha pedig  $k = n + 1$ , akkor  $t_k = t_2(x_1, t_n(x_2, \dots, x_{n+1}))$  (itt a belső függvények arítása  $n + 1$ ). Így félháló minden termművelete benne van bármely nemtriviális termművelete generátumában.

2. Nevezzük *kváziprojekciónak* az olyan  $f = f(x_1, \dots, x_n)$  ( $n > 2$ ) szemiprojekciót, amelyhez létezik olyan  $j \in \{1, \dots, n\}$ , hogy valahányszor  $f$  alaphalmazának  $a_1, \dots, a_n$  elemei páronként különbözők, mindannyiszor  $f(a_1, \dots, a_n) = a_j$ . Ha  $f$  alaphalmaz  $k$  elemű, és  $k < n$ , akkor  $f$  projekció, máskülönben  $f$  lényeges arítása  $n$ . Megmutatjuk, hogy  $n$  elemű halmazon az  $n$ -áris kváziprojekciók (együtt az összes projekciókkal) minimális klónt alkotnak. Adott  $n$ -áris  $f$  kváziprojekció

által generált klón csak kváziprojekciókat tartalmaz, és tartalmazza az összes  $n$ -áris kváziprojekciót (lássuk be). Nem tartalmazhat azonban  $n$ -nél kisebb aritású nemtriviális kváziprojekciót. Valóban, ha az alaphalmaz  $\{0, 1, 2, \dots\}$  és  $k < n$ , akkor minden  $n$ -áris kváziprojekció megőrzi a  $\rho = \{(0, 1), (1, 0), (2, 0), \dots, (k-1, 0)\}$  relációt, de egyetlen nemtriviális  $k$ -áris kváziprojekció sem őrzi meg (ellenőrizzük), s ezért az utóbbi nem lehet az előző által generált klónban.

Másrészt, ha  $k < n$ ,  $k$ -áris kváziprojekció  $n$  elemű halmazon nem generál minimális klónt, mert belőle szuperpozícióval kaphatunk  $n$ -áris kváziprojekciót ott. (Ehhez elég belátnunk, hogy  $k+1$ -áris kváziprojekciót kaphatunk belőle.)

3. Legyen  $p$  prímszám,  $V$  vektortér a  $p$  elemű test felett. Akkor az összes idempotens lineáris kombinációk mint termműveletek egy  $C_p$  minimális klónt alkotnak (az idempotensség itt azt jelenti, hogy a lineáris kombináció együtthatóinak összege 1). A  $p = 2$  esetben e klón nemtriviális műveletei éppen az  $x_1 + x_2 + \dots + x_{2k+1}$  ( $k \geq 1$ ) lineáris kombinációk, s épp úgy, mint az 1. példában, látjuk, hogy  $C_2$ -t minden nemtriviális eleme generálja. Legyen ezután  $p > 2$ . Jelölje  $B$  a  $C_p$ -ben levő bináris műveletek halmazát, és jelölje  $m = m(x, y, z)$  az  $x - y + z \in C_p$  műveletet. Ekkor  $C_p$  minimális volta a következő észrevételekből folyik:

(i)  $B \supseteq [m]$ . Valóban,  $ax + (1-a)y = m(x, y, m(x, y, \dots m(x, y, x) \dots))$ , ahol  $m$   $a-1$ -szer szerepel.

(ii) Minden  $0 < k < p$ -re  $x - ky + kz \in [B]$ . Választhatjuk ugyanis az  $u, v, w$  testelemeket úgy, hogy teljesüljön

$$x - ky + kz = u(vx + (1-v)y) + (1-u)(wx + (1-w)z).$$

(iii)  $[B] = C_p$ . Ezt aritás szerinti indukcióval láthatjuk be, felhasználva (ii)-t.

(iv) Bármely  $C_p$ -beli nemtriviális műveletből változók alkalmas azonosításával nemtriviális bináris művelet keletkezik.

(v) Ha  $f \in C_p$  nemtriviális bináris művelet, akkor  $m \in [f]$ . Ennek belátásához írjunk  $xy$ -t  $ax + (1-a)y$  helyett, és igazoljuk az  $x - y + z = xy^{c-1}(zy^{d-1})$  összefüggést, ahol  $c$  és  $d$  megfelelően  $a$  ill.  $1-a$  rendjét jelöli a  $p$  elemű test multiplikatív csoportjában.

**38. Galois-kapcsolat műveletek és relációk között.** Tekintsük az  $A$  véges halmaz összes műveleteinek  $O_A$  halmazát és  $A$  összes (tetszőleges véges változószámú) relációinak  $R_A$  halmazát. Az „ $f$  megőrzi  $\rho$ -t” ( $f \in O_A$ ,  $\rho \in R_A$ ) megfeleltetés Galois-kapcsolatot létesít  $O_A$  és  $R_A$  között. Meghatározzuk e Galois-kapcsolat zárt művelet- ill. relációhalmazait.

A Galois-kapcsolatokra vonatkozó általános meggondolások (22. fejezet) szerint egy  $O$  művelethalmaz pontosan akkor zárt, ha van olyan  $R$  relációhalmaz, hogy  $O$  az  $R$ -beli relációkat megőrző műveletekből áll. Ezért a zárt művelethalmazok szükségképpen klónok.

Most  $R_A$ -n műveleteket definiálunk. A  $\rho$   $m$ -áris és  $\sigma$   $n$ -áris reláció *szorzata* az az  $m+n$ -áris  $\rho \times \sigma$  reláció, amelyre

$$(a_1, \dots, a_m, a_{m+1}, \dots, a_{m+n}) \in \rho \times \sigma \Leftrightarrow (a_1, \dots, a_m) \in \rho \text{ és } (a_{m+1}, \dots, a_{m+n}) \in \sigma.$$

Ez a szorzat különbözik a bináris relációk szokásos szorzatától (az utóbbi maga is bináris), amelyet félreértés elkerülése érdekében megfeleltetés-szorzatnak nevezhetünk. Természetes módon bevezethetjük kettőnél több reláció szorzatát (speciálisan, reláció hatványát) is.

Legyen  $\rho \in R_A$   $n$ -áris, és legyen  $1 \leq i_1, \dots, i_k \leq n$ , ahol a különböző indexű  $i$ -k maguk is különbözők. Sorozatukat jelölje  $I$ . A  $\rho$  reláció  $I$ -*megszorítása* az a  $k$ -áris  $\rho_I$  reláció, amelyre

$$(a_1, \dots, a_k) \in \rho_I \iff \exists (b_1, \dots, b_n) \in \rho \text{ úgy, hogy } a_1 = b_{i_1}, \dots, a_k = b_{i_k}.$$

Legyen  $\rho \in R_A$   $n$ -áris, és legyen  $\varepsilon$  ekvivalenciareláció az  $\{1, \dots, n\}$  halmazon. A  $\rho$  reláció  $\varepsilon$ -*átlója* az az  $n$ -áris  $\rho_\varepsilon$  reláció, amelyre

$$(a_1, \dots, a_n) \in \rho_\varepsilon \iff (a_1, \dots, a_n) \in \rho, \text{ és } a_i = a_j \text{ ha } (i, j) \in \varepsilon.$$

Ha  $A$  relációinak egy  $R$  halmaza tartalmazza az unáris üres és az unáris teljes relációt, továbbá zárt a szorzatok, megszorítások és átlók képzésére nézve, akkor  $R$ -t *relációklónnak* nevezzük. Képzési módjukból következik, hogy relációklón részklónjai is természetes módon definiálhatók, és mindig teljes hálót alkotnak. Adott  $R$  relációhalmaz által generált relációklón jele (hasonlóan a műveletklónok esetéhez):  $[R]$ . Adott halmaz összes relációinak a klónja a halmaz összes relációklónja alkotta háló egységeleme, míg e háló zéruseleme a halmaz összes diagonális relációból áll (*diagonálisnak* nevezzük az  $n$ -áris  $\rho$  relációt az  $A$  halmazon, ha  $\rho$  üres, vagy ha létezik az  $\{1, \dots, n\}$  halmazon olyan  $\varepsilon$  ekvivalencia, hogy  $\rho$  azokból az  $(a_1, \dots, a_n)$   $n$ -esekből áll, amelyekre  $a_i = a_j$ , valahányszor  $(i, j) \in \varepsilon$ ).

A relációklónok a definíciójukban közvetlenül szereplő reláció-műveleteken túl további műveletekre nézve is zártak. Ilyenek a következők:

- *Változók permutálása.* Legyen  $\rho$   $n$ -áris, és legyen  $\pi$  az  $\{1, \dots, n\}$  halmaz egy permutációja. Akkor a  $\rho_I$  „megszorítás”  $\rho$ -ból a változók  $\pi$  permutációjával keletkezik.

- *Változók azonosítása.* Ez nem más, mint átlóképzés: pl.  $\rho$  első két változójának azonosítása a  $\rho_\varepsilon$  relációt adja, ahol  $\varepsilon$  egyetlen legalább két elemű blokkja  $\{1, 2\}$ .
- *Fiktív változó bevezetése.* Ez az eljárás  $n$ -áris relációból  $(n + 1)$  aritásút hoz létre, mégpedig  $\rho$ -ból a  $\rho \times A$  relációt.
- *Változó megkettőzése.* Vegyük pl. a  $\rho \times = (n + 2)$  aritású reláció átlóját a  $\varepsilon = \{\{1\}, \dots, \{n - 1\}, \{n, n + 1\}, \{n + 2\}\}$  ekvivalencia szerint, majd ennek megszorítását az első  $n + 1$  index sorozatára. (Ezzel az utolsó változót kettőztük meg.)
- *Bináris relációk megfeleltetés-szorzása.* A  $\rho \circ \sigma$  (megfeleltetés-)szorzatot úgy kapjuk meg, hogy a (négy változós)  $\rho \times \sigma$  szorzatnak képezzük az  $\varepsilon$ -átlóját a  $\varepsilon = \{\{1\}, \{2, 3\}, \{4\}\}$  ekvivalencia szerint, majd a kapott ternáris relációt megszorítjuk az  $I = (1, 3)$  sorozatra.
- *Egyenlő aritású relációk metszetének képzése.* (Hogyan keletkezik szorzással, megszorítással és átlóképzéssel?)

A reláció-műveletek definíciójából látjuk, hogy ha valamely művelet megőrzi bizonyos relációkat, akkor megőrzi azok szorzatait, megszorításait és átlóit is; nyilvánvaló emellett, hogy minden művelet megőrzi az unáris üres és az unáris teljes relációt. Ezért a műveletek és relációk közötti Galois-kapcsolat zárt relációhalmazai szükségképpen relációklónok.

Megmutatjuk, hogy véges halmazokon a klónokra és relációklónokra vonatkozó megfigyeléseink megfordítása is igaz:

*A véges halmazok műveleteinek és relációinak dualitástétele (Geiger; Bodnarsuk–Kaluzsnyin–Kotov–Romov):* Véges halmazon a műveletek és relációk közötti Galois-kapcsolat zárt művelethalmazai éppen a műveletklónok, zárt relációhalmazai pedig éppen a relációklónok.

Következmények:

1. Véges halmazon minden  $O$  műveletklónhoz létezik olyan  $R$  relációhalmaz (speciálisan, olyan relációklón is), hogy  $O$  pontosan a minden  $R$ -beli relációt megőrző műveletekből áll; és minden  $R$  relációklónhoz létezik olyan  $O$  művelethalmaz (speciálisan, olyan műveletklón is), hogy  $R$  pontosan azokból a relációkból áll, amelyeket minden  $O$ -ba tartozó művelet megőriz.

2. Véges halmaz műveletklónjainak hálójá duálisan izomorf relációklónjainak hálójával.

A bizonyításhoz szükségünk lesz néhány megfigyelésre és terminológiai megál-

lapodásra. Legyen  $\rho$  egy  $n$ -áris reláció az  $A$  halmazon. Ha az

$$\begin{array}{ccc} a_{11} & \dots & a_{1k} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nk} \end{array}$$

mátrix minden oszlopa a  $\rho$  relációban van, akkor  $k$  méretű  $\rho$ -mátrixnak nevezzük. Ha  $|\rho| = m$ , akkor  $\rho$ -t megadhatjuk egy  $m$  méretű  $\rho$ -mátrixszal, amelynek oszlopai az összes (különböző)  $\rho$ -beli elem- $n$ -esek. Bármely  $f$   $k$ -áris művelet a  $t$  elemű  $A$  halmazon ugyancsak megadható egy  $t^k \times k + 1$  típusú mátrixszal, amelynek sorai az összes különböző  $(a_1, \dots, a_k, f(a_1, \dots, a_k))$  ( $a_i \in A$ ) elem- $(k+1)$ -esek. Egyszerűség kedvéért feltehetjük, hogy  $A = \{0, 1, \dots, t-1\}$ , és a mátrix sorai lexikografikus rendezésben következnek egymás után. Az így kapott mátrix az  $f$  művelet mátrixa, az általa megadott reláció pedig az  $f$  művelet relációja. Az  $f$  művelet abszcisszájának nevezzük a mátrixa első  $k$  oszlopából álló mátrixot, ordinátájának a mátrixa utolsó oszlopát. Az olyan mátrixot, amelynek sorai mind különbözők és lexikografikus sorrendben követik egymást, továbbá oszlopai is mind különbözők, szabályosnak nevezzük. Bármely  $M$  mátrixból képezhető szabályos  $M'$  mátrix úgy, hogy többször előforduló oszlopai közül csak egyet-egyet hagyunk meg, majd hasonlóan járunk el a többször előforduló sorokkal, s végül a sorokat lexikografikus sorrendben írjuk egymás alá. Ha ezek a mátrixok megfelelően egy  $\mu$  és egy  $\mu'$  reláció mátrixai, akkor  $[\mu] = [\mu']$ . (Ehhez figyeljük meg, hogy  $\mu$  és  $\mu'$  megkaphatók egymásból olyan műveletekkel, amelyekre nézve a relációklónok zártak.)

Legyen  $C$  műveletklón az  $A$  halmazon, és álljon  $C_k$ , a  $C$  klón  $k$ -adik emelete az  $f_1, \dots, f_n$  műveletekből. Azt a  $t^k \times k + n$  típusú mátrixot, amelynek első  $k$  oszlopa az  $f_i$  műveletek (közös) abszcisszája, utolsó  $n$  oszlopa pedig ezeknek a műveleteknek az ordinátái, a  $C$  klón  $k$ -adik mátrixának, az általa megadott relációt  $C$   $k$ -adik relációjának nevezzük, és megfelelően beszélünk műveletklón  $k$ -adik abszcisszájáról és ordinátájáról is. (Jegyezzük meg, hogy ekkor az ordináta mindig tartalmazza az abszcisszát [!], mert műveletklón  $k$ -adik emelete tartalmazza a  $k$ -áris projekciókat; továbbá adott alaphalmazon műveletklón  $k$ -adik abszcisszája minden műveletklónra ugyanaz.) A  $C$  klón  $k$ -adik relációját  $\text{Rel } C_k$ -val jelöljük.

Ha  $O$  művelethalmaz  $A$ -n, mindazon relációk halmazát, amelyeket az  $O$  halmazba tartozó műveletek mindegyike megőriz,  $\text{Inv } O$  jelöli. Mindig érvényes  $\text{Pol Inv } O \supseteq O$ . Ezért a dualitástétel első állításának a bizonyításához elegendő megmutatnunk, hogy bármely  $C$  műveletklónra  $\text{Pol Inv } C \subseteq C$ .

Jelöljük  $R(C)$ -vel a  $C$  klón (összes különböző emeletekhez tartozó) relációinak halmazát. Belátjuk, hogy

$$\text{Pol Inv } C \subseteq \text{Pol } R(C) \subseteq C.$$

Az első tartalmazás abból következik, hogy bármely  $f \in C$  művelet  $C$  minden relációját megőrzi. Legyen pl.  $f$   $n$ -áris; , megmutatjuk, hogy megőrzi  $C$   $k$ -adik relációját. Ezen reláció mátrixának minden oszlopa együtt az elé írt közös ordinátaoszlopokkal egy-egy  $C_k$ -beli  $g_i$  művelet mátrixa (az ordinátába eső oszlopok a projekciókéi). Mivel  $f(g_1, \dots, g_n) \in C$ , ennek a műveletnek az ordinátán felvett értékei is  $C$   $k$ -adik relációjának egy oszlopát alkotják, ami éppen azt jelenti, hogy  $f$  megőrzi ezt a relációt.

Másrészt, ha  $f$   $n$ -áris, de  $f \notin C$ , akkor  $f$ -nek az ordinátán felvett értékei *nem* alkotják  $C_n$ -nek oszlopát, így  $f$  nem őrzi meg  $C$   $n$ -edik relációját. Ebből következik a második tartalmazás.

A dualitástétel második állításának igazolásához azt kell megmutatnunk, hogy bármely  $R$  relációklónra  $\text{Inv Pol } R \subseteq R$ . Tekintsünk egy  $\sigma \in \text{Inv Pol } R$  relációt (amelyet tehát megőrzi minden olyan művelet, amely minden  $R$ -beli relációt megőrzi). Tegyük fel, hogy  $\sigma$   $n$ -áris és  $k$  méretű. Azt kell belátnunk, hogy  $\sigma \in [R]$  ( $= R$ ).

Előkészületül bebizonyítjuk, hogy létezik olyan  $\rho$  reláció, hogy  $\rho$ -t ugyanazok a  $k$ -áris műveletek őrzik meg, amelyek mindegyik  $R$ -beli relációt megőrzi (azaz  $(\text{Pol } R)_k = (\text{Pol } \rho)_k$ ). Ahhoz hasonló fogást alkalmazunk, amellyel Birkhoff bizonyította a varietás-tételét, olyan algebrát keresve, amelyben pontosan azok az azonosságok teljesülnek mint egy tekintett varietásban. Jelölje  $F$  azoknak a  $k$ -áris műveleteknek a halmazát, amelyek nem minden  $R$ -beli relációt őriznek meg. Minden  $f \in F$  művelethez válasszunk ki egy  $\tau_f \in R$  relációt, amelyet  $f$  nem őriz meg. Megmutatjuk, hogy az összes  $\tau_f$  relációk szorzata — jelölje máris  $\rho$  — rendelkezik a kívánt tulajdonsággal. Minden  $\tau_f$  megszorítása  $\rho$ -nak, ezért ha egy  $k$ -áris  $g$  művelet megőrzi  $\rho$ -t, akkor mindegyik  $\tau_f$ -et is, ezért  $g$  nem lehet azonos egyetlen  $f \in F$ -fel sem, vagyis  $g$  minden  $R$ -beli relációt megőrzi. Eszerint  $(\text{Pol } \rho)_k \subseteq (\text{Pol } R)_k$ . Az ellenkező irányú tartalmazás pedig abból következik, hogy  $\rho$  — mint  $R$ -beli relációk szorzata — maga is  $R$ -be tartozik.

Most belátjuk, hogy

$$(*) \quad \sigma \in [\text{Rel } (\text{Pol } \rho)_k],$$

és

$$(**) \quad \text{Rel } (\text{Pol } \rho)_k \in [\rho].$$

Figyelembe véve, hogy  $\rho \in R$ , a  $(*)$  és  $(**)$  összefüggésekből következni fog  $\sigma \in R$ , amit bizonyítani akarunk.

$(*)$  bizonyítása:

Feltehetjük, hogy  $\sigma$  szabályos reláció (ha nem lenne az, tekinthetnénk helyette azt a  $\sigma'$  szabályos relációt, amelyre  $[\sigma] = [\sigma']$ ). Gondoljuk meg, hogy bármely  $k$  méretű szabályos reláció mátrixa (eltekintve oszlopai sorrendjétől, amely egy relációnak mátrixszal való megadása esetén nem lényeges) részmátrixként benne van bármely műveletklón  $k$ -adik abszcisszájában. Ekkor tehát  $\sigma$  mátrixa részmátrixként benne van a  $\text{Rel}(\text{Pol } \rho)_k$  reláció mátrixának első  $k$  oszlopában (és, mondjuk, az  $i_1, \dots, i_n$  indexű sorokból áll). Mivel ez a reláció, mint láttuk, egyenlő  $\text{Rel}(\text{Pol } R)_k$ -val, és  $\sigma$ -t a  $\text{Pol } R$ -be tartozó műveletek mind megőrzik, ezért abban a mátrixban, amelyet  $\text{Rel}(\text{Pol } \rho)_k$  mátrixának az  $i_1, \dots, i_n$  indexű sorai alkotnak, minden oszlop már az abszcisszába eső oszlopok — azaz a  $\sigma$ -t alkotó oszlopok — között is előfordul. Ebből folyik, hogy  $\sigma$  az  $I = (i_1, \dots, i_n)$  sorozatra való megszorítással keletkezik  $\text{Rel}(\text{Pol } \rho)_k$ -ból, tehát  $(*)$  valóban igaz.

(\*\*) bizonyítása:

Először tekintsük az  $A$  halmaz összes olyan  $k$ -változós megfeleltetéseit önmagába, amelyek minden elem- $k$ -ashoz hozzárendelik  $A$ -nak legalább egy elemét. Ezek közül kiválogatjuk a  $(\text{Pol } \rho)_k$ -ba tartozó  $f$  műveleteket. Utóbbiak a következő tulajdonságaikkal jellemezhetők:

- Bármely  $k$  méretű reláció mátrixának sorain elvégezve az  $f$  megfeleltetést mindig egyetlen elemet kapunk eredményül.
- Bármely  $k$  méretű  $\rho$ -mátrix sorain elvégezve az  $f$  megfeleltetést, az eredmény mindig  $\rho$  mátrixának valamelyik oszlopa.

Most megalkotunk egy mátrixot; ezt  $(\text{Pol } \rho)_k$  *preabszcisszájának* fogjuk nevezni. Ehhez egymás alá írjuk az összes különböző  $k$  méretű  $\rho$ -mátrixokat, majd alájuk mindazokat a különböző  $k$  elemű sorozatokat ( $A$ -ból), amelyek egyetlen  $k$  méretű  $\rho$  mátrixban sem fordulnak elő annak soraként. Ha  $s$  számú ilyen sorozat van,  $\rho$  aritása  $p$ , mérete  $q$ , akkor a preabszcissza típusa  $(p \cdot q^k + s) \times k$ .

Ha a preabszcissza mellé további oszlopként  $A$  elemeit írjuk, mégpedig

- (i) minden  $\rho$ -mátrix mellé a  $\rho$  reláció (mátrixának) egy-egy tetszőleges oszlopát,
- (ii) a további sorok után  $A$  tetszőleges elemét,

akkor a kapott mátrix általában nem lesz egy művelet mátrixa (ui. a preabszcisszában ugyanaz a sor többször is előfordulhat, ilyenkor utánuk  $A$  különböző elemei állhatnak, emellett a sorok nem lesznek lexikografikusan rendezve). Ha azonban az (i) és (ii) szabályt betartva felírjuk az összes lehetséges oszlopokat (köztük ott lesznek a preabszcissza oszlopai is), akkor egy olyan  $\rho_0$  reláció mátrixát kapjuk, amely benne van a  $\rho$  által generált relációklónban, továbbá  $\text{Rel}(\text{Pol } \rho)_k \in [\rho_0]$  is teljesül.

Valóban,  $\rho_0$  előáll  $\rho$   $q^k$  számú példánya és  $A$  (vagyis az unáris teljes reláció)  $s$  számú példánya szorzataként. Másrészt tekintsük  $\rho_0$  változóin azt a  $\pi$  ekvivalen-

ciát, amelyben az  $i$ -edik és  $j$ -edik változó pontosan akkor van, ha a preabszcissza  $i$ -edik és  $j$ -edik sora egyenlő. Képezzük  $\rho_0$   $\pi$ -átlóját, majd — ha annak mátrixa nem szabályos — helyettesítsük a belőle nyerhető szabályos mátrixú relációval. Az így nyert reláció éppen  $\text{Rel}(\text{Pol } \rho)_k$ .

A most bizonyított tétel relációklónokra vonatkozó része algebrák hatványai részalgebráira vonatkozó állításként is megfogalmazható: Legyen  $R$  valamely véges  $A$  halmaz véges kitevőjű hatványai nemüres részhalmazainak egy halmaza. Akkor és csak akkor létezik olyan  $A$  alaphalmazú  $A$  algebra, hogy  $R$  éppen  $A$  véges direkt hatványai összes részalgebráinak alaphalmazából áll, ha  $R$  tartalmazza az  $A$  halmazt, továbbá az  $R$ -beli halmazok Descartes-szorzatait, bármely  $R$ -beli halmaz átlós részhalmazait és vetületeit. (Az utóbbiak definíciója ugyanaz, mint relációk átlói és megszorításaié.) Az  $A^n$  algebra bármely  $B$  részalgebrájának átlós részhalmazai  $B$ -nek részalgebrái, vetületei pedig homomorf képei. Ez adja a gondolatot, hogy a 18. fejezetben látottakhoz hasonlóan vizsgáljuk a  $H$  (megszorítás-képzés),  $S$  (átlóképzés) és  $P$  (szorzás) operátorokat véges halmaz összes relációinak halmazán. Könnyen belátható, hogy bármely  $R$  relációhalmazra  $[R] = HSP(R \cup \{A\}) \cup \{\emptyset\}$ .

*Gyakorló feladat:* Bármely  $M$  halmazon az összes idempotens műveletek klón alkotnak. Hány klón tartalmazza ezt véges  $M$  esetén? (Használjuk a dualitástételt és az előző bekezdés megfontolásait.)

**39. Sheffer-relációk.** Ezeket a Sheffer-műveletekhez hasonlóan definiáljuk: az  $A = \{0, 1, \dots, n-1\}$  halmazon értelmezett  $\rho$  reláció *Sheffer-reláció*, ha  $[\rho] = R_A$ .

*Minden legalább három elemű véges  $A$  halmazon létezik Sheffer-reláció.* Ilyen például a  $\rho = \{(a, b, c) \mid a \leq b, b \neq c\}$  ternáris reláció. Ennek a bizonyításához először vegyük észre, hogy a dualitástétel szerint  $\rho$  akkor és csak akkor Sheffer, ha a  $\rho$ -t megőrző műveletek  $\text{Pol } \rho$  klónja csak a projekciókat tartalmazza. Másrészt  $\rho$ -t pontosan azok a műveletek őrzik meg, amelyek a  $\leq$  és a  $\neq$  relációt megőrzik (ez abból következik, hogy  $[\rho] = [\leq, \neq]$ , ti.  $\rho$ -ból  $\leq$  és  $\neq$  megszorítással keletkezik, míg az utóbbiaknak éppen  $\rho$  a megfeleltetés-szorzata).

Ezért csak azt kell belátnunk, hogy ha egy  $A$ -n monoton  $f$  művelet megőrzi az egyenlőtlenség relációt, akkor  $f$  szükségképpen projekció. Tegyük fel, hogy ez nem így van: legyen  $f$  nemtriviális. Akkor az  $[f]$  klón tartalmaz minimális klónt, s ezért létezik olyan  $m$  minimális művelet, amely monoton és az egyenlőtlenséget is megőrzi. Alkalmazzuk Rosenberg osztályozási tételét. Az unáris eset kizárható, mert  $A$  monoton és kölcsönösen egyértelmű transzformációja csak az identikus leképezés lehet. Ha  $m$  többségi, vagy kisebbségi ternáris művelet vagy szemiprojekció, akkor nem őrzik meg az egyenlőtlenséget. Ha  $m$  többségi, akkor pl.  $m(0, 1, 2) = 0$  esetén ezt  $m(1, 0, 0) = 0$  mutatja, és hasonlóan gondolkodhatunk, ha  $m(0, 1, 2) = 1$  vagy 2, vagy ha  $m(0, 1, 2) > 2$ . Ugyanez az okoskodás használható

kisebbségi műveletre és szemiprojekcióra is. (Az utóbbiak egyébként monotonok sem lehetnek — lássuk be!)

Az az eset maradt hátra, amikor  $m$  bináris monoton művelet  $A$ -n, amely megőrzi az egyenlőtlenséget. Azt kell megmutatnunk, hogy  $m$  projekció. Teljes indukcióval belátjuk, hogy 1-től  $n - 1$ -ig minden  $k$ -ra  $m$  projekció a  $\{0, \dots, k\}$  halmazon. Jelöljük  $m$ -et szorzás módjára. Ha  $k = 1$ , akkor  $0 \cdot 1 \neq 1 \cdot 0$ , és  $m$  — mint minimális művelet — idempotens, így  $m$  valóban projekció. Legyen  $k > 1$ . Tegyük fel, hogy állításunk igaz  $k - 1$ -re, és a  $\{0, \dots, k - 1\}$  halmazon  $m$  első projekció. Ekkor bármely  $i \neq i' (< k)$ -ra  $i \cdot k \neq i' \cdot k - 1 = i'$ , tehát csak  $i \cdot k = i$  lehetséges. Végül  $k \cdot i \neq k' \cdot i' = k'$ , ha  $k \neq k'$ , ezért szükségképpen  $k \cdot i = k$ , azaz  $m$  a  $\{0, \dots, k\}$  halmazon is első projekció.