

Algebra - 1

Jegyzőkönyv, BME, 2026 ősz

Sági Gábor*

2026 ősz

HUN-REN Rényi Alfréd Matematikai Kutatóintézet és
BME Matematika Intézet, Algebra és Geometria Tanszék
e-mail: sagi@renyi.hu

**Minden visszajelzést szívesen veszek.
1.3.0 Verzió.**

*Ez az anyag néhány hallgatóm (névsor szerinti sorrendben):

Balog Benjámin, Domokos Norbert, Gegő Levente, Kárpáti Noémi, Máthé Zsolt

hathatós segítségével jött létre. Ha valakit kihagytam, elnézést kérek – kérem szóljon, korrigálom azonnal. Hallgatóim precíz munkájáért, lelkesedésükért, nagyon hálás vagyok, hatalmas köszönet érte.

Előszó (vázlat; a végén írom meg)

Mi ez az anyag? Ez az iromány egy elektronikus segédlet, mely a BME-n, 2026 őszén, másaodéves matematikus hallgatók számára tartott „Algebra - 1” kurzushoz készült. Csakúgy, mint az előző tanévben, ennek az irománynak az első, nyers változatát néhány lelkes hallgatóm készítette; ezzel kapcsolatban az alábbi, „Hogy jött létre ez az anyag?” kezdetű bekezdésre utalok.

Mint a korábbi félévekben, ez az iromány is azért kapta a „Jegyzőkönyv” címet, mert egyetlen célja, hogy - a lehetőségekhez képest - minél pontosabban lehessen rekonstruálni, hogy mi hangzott el az egyes előadásokon.

Ez az iromány nem könyv, nem egyetemi jegyzet: az áttekinthetőség, tömörség érdekében a szövegbe rövidítések, sőt akár képletek ékelődnek úgy, ahogy egy klasszikus, nyomtatott anyagban megengedhetetlen lenne.

Hogyan használd ezt az anyagot?...

Hogy jött létre ez az anyag? Ez az anyag is úgy jött létre, hogy néhány hallgatóm szerkeszthető LaTeX file-á alakította az előadásokon készített kézzel írt jegyzeteit. Külön öröm számomra, hogy azok a hallgatóim, akik az előző tanévben részt vettek már hasonló segédletek előállításában, nem egyszerűen folytatják ezt a munkát, hanem műfajt teremtettek: a kezdeményezésükben rejlő lehetőségeket felismerve, létrejött egy intézményesített segédletíró kurzus, hogy idejükért, energiájukért oktatási krediteket is kapjanak, emellett jegyzetkészítési tapasztalataikat átadják a többi (akár fiatalabb) hallgatónak.

Ennek a Jegyzőkönyvnek az elkészítésében (névsor szerinti sorrendben) a következő hallgatóim vettek részt:

Balog Benjámin, Domokos Norbert, Gegő Levente, Kárpáti Noémi, Máthé Zalán

Ha valakit kihagytam volna, akkor elnézését kérem. Kérem, hogy jelezze, korrigálom azonnal.

HATALMAS KÖSZÖNET minden hallgatónak, aki közreműködött ennek az anyagnak az elkészítésében!!!! Lelkesedésükért nagyon hálás vagyok! Az általuk átadott nyers szöveget ebben a szemeszterben is nagy örömmel, szeretettel csinosítottam tovább; azt kívánom, Ti is ilyen örömmel olvassátok.

Budapest, 2026 ősz.

Sági Gábor

Tartalomjegyzék

0. Jelölések	4
1. Általános algebra	5
1.1. Termek és azonosságok	7
1.2. Algebrák konstrukciói: Reduktumképzés	8
1.3. Algebrák konstrukciói: Részalgebrák	8
1.4. Algebrák konstrukciói: Faktoralgebrák, homomorf kép	11
1.5. Algebrák konstrukciói: Direktszorzat	19
1.6. Összefoglalás	20
2. Félcsoportok	21
3. Csoportok	25
3.1. Részcsoportok	27
3.2. Mellékosztályok, Lagrange tétele	28

0. Jelölések

Gyorsírási jelölések, rövidítések

- TFH: Tegyük fel, hogy;
- ACSA: Akkor és csak akkor;
- $\exists$: Létezik;
- $\forall$: Minden;
- $\exists!$: Pontosan egy van;
- $\dots \Rightarrow \dots$: Ha... akkor... .

További jelölések

- $\in$: eleme;
- $\subset$ illetve $\subseteq$: valódi részhalmaz, illetve részhalmaz;
- $\cap$: metszet;
- $\cup$: unió;
- $A \setminus B$ vagy $A - B$: az A és B halmazok különbsége;
- $\mathbb{N}$: természetes számok halmaza ($\mathbb{N} = \{0, 1, 2, 3, \dots\}$);
- $\mathbb{N}^+$: pozitív egész számok halmaza ($\mathbb{N}^+ = \{1, 2, 3, \dots\}$);
- $\mathbb{Z}$: egész számok halmaza;
- $\mathbb{Q}$: racionális számok halmaza;
- $\mathbb{R}$: valós számok halmaza.

1. Általános algebra

Ebben a fejezetben megismerkedünk néhány konstrukcióval, módszerrel és tétellel, melyek egyszerre alkalmazhatók félcsoportokra, csoportokra, gyűrűkre, vektorterekre és még sokminden másra is. A Bevezetés az Algebrába - 1 Jegyzőkönyv 4. fejezetéből már ismerős absztrakciós szinten mozogva bővebben kifejtjük az ott bevezetett fogalmakat és konstrukciókat, sőt, egy picit tovább is megyünk az ott kijelölt irányban.

1.1. Definíció (Hasonlósági típus). Az $\langle F, \varrho \rangle$ pár egy *hasonlósági típus*, ha

$$\varrho: F \longrightarrow \mathbb{N}.$$

Itt F a műveletnevek halmaza, és minden $f \in F$ esetén $\varrho(f)$ az f változóinak száma.

1.2. Definíció (Algebra). Legyen $\langle F, \varrho \rangle$ hasonlósági típus. Az

$$\mathcal{A} = \langle A, f^{\mathcal{A}} \rangle_{f \in F}$$

$\langle F, \varrho \rangle$ típusú algebra, ha

- $A \neq \emptyset$; ez az *alaphalmaz*;
- minden $f \in F$ esetén

$$f^{\mathcal{A}}: A^{\varrho(f)} \longrightarrow A$$

függvény; ez az f -hez tartozó *művelet*.

Figyeljük meg, hogy magát az algebrát az írott $\mathcal{A}$ betűvel jelöltük, míg alaphalmazát a megfelelő nyomtatott A betűvel. Ezzel hangsúlyozva, hogy az algebra az alaphalmaz és a műveletek együttese. Ezt a különbségtételt egyes esetekben nagyvonalúan kezeljük: ha félreértés nem fenyeget (mert pl. a műveletek világosak a szövegkörnyezetből), akkor néha csak az alaphalmazt adjuk meg, mégis algebráról beszélünk majd.

1.3. Példa. Legyen $F = \{i, f, g\}$, és a hasonlósági típust adja meg

$$\begin{array}{c|ccc} h & i & f & g \\ \hline \varrho(h) & 0 & 2 & 2 \end{array}.$$

A következők mind $\langle F, \varrho \rangle$ típusú algebrák (az alábbi példák mindegyikében a műveletek értelmezéseinek jobboldalain mindig a szokásos összeadás, szorzás, hatványozás áll).

1. $\mathcal{A} = \langle \mathbb{C}, i^{\mathcal{A}}, f^{\mathcal{A}}, g^{\mathcal{A}} \rangle$, ahol

$$i^{\mathcal{A}} = 0, \quad f^{\mathcal{A}}(x, y) = x + y, \quad g^{\mathcal{A}}(x, y) = xy.$$

2. $\mathcal{B} = \langle \mathbb{Q}, i^{\mathcal{B}}, f^{\mathcal{B}}, g^{\mathcal{B}} \rangle$, ahol

$$i^{\mathcal{B}} = 0, \quad f^{\mathcal{B}}(x, y) = x + y, \quad g^{\mathcal{B}}(x, y) = xy.$$

3. $\mathcal{C} = \langle \mathbb{Q}, i^{\mathcal{C}}, f^{\mathcal{C}}, g^{\mathcal{C}} \rangle$, ahol

$$i^{\mathcal{C}} = 0, \quad f^{\mathcal{C}}(x, y) = xy, \quad g^{\mathcal{C}}(x, y) = x + y.$$

$\mathcal{C}$ -ben az előző példához képest az f és g műveletek fel vannak cserélve: f jelöli a szorzást, g az összeadást. Tehát $\mathcal{B}$ és $\mathcal{C}$ különböző algebrák.

$\mathcal{A}$ és $\mathcal{B}$ gyűrű, $\mathcal{C}$ viszont nem az, mert az összeadás nem disztributív a szorzásra.

4. $\mathcal{D} = \langle \mathbb{N}, i^{\mathcal{D}}, f^{\mathcal{D}}, g^{\mathcal{D}} \rangle$, ahol

$$i^{\mathcal{D}} = 17, \quad f^{\mathcal{D}}(x, y) = x^3 + 2y, \quad g^{\mathcal{D}}(x, y) = y^{y^y}.$$

Itt $g^{\mathcal{D}}$ olyan kétváltozós függvény, melynek eredménye nem függ az első változója értékétől. Továbbá $g^{\mathcal{D}}$ -t értelmeznünk kell a teljes $\mathbb{N}^2$ -en, ehhez alkalmazzuk a szokásos $0^0 = 1$ konvenciót.

Klasszikus esetekben használjuk a szokásos jelöléseket is. Például $f^{\mathcal{A}}(x, y)$ helyett írhatunk $x + y$ -t is.

1.4. Példa (További példák). Általános algebrák még pl. a félcsoporthok, a csoportok és a gyűrűk. Ezért minden, amit ebben a fejezetben megismerünk, érvényes lesz félcsoporthokra, csoportokra, gyűrűkre, és még sokminden másra is.

Ebben a felépítésben a testek nem algebrák, mert a 0-nak nincs reciproka, emiatt az $x \mapsto x^{-1}$ leképezés nem az egész testen értelmezett művelet. A testeket speciális gyűrűkként kezelhetjük: a testek olyan gyűrűk, melyekben minden nem-nulla elemnek van reciproka, de a reciprokképzés nem művelet (nincs is neve neki a hasonlósági típusban).

A vektorterek viszont beleférnek ebbe a fogalomba. Legyen W vektortér a K test felett, legyen V a vektorok halmaza. Minden $\lambda \in K$ -ra legyen

$$f_{\lambda}(v) = \lambda \cdot v.$$

Ekkor a

$$\langle V, +, 0, f_{\lambda} \rangle_{\lambda \in K}$$

algebra azonosítható a W vektortérrel.

- Egyrészt itt F -nek (a műveletek neveinek) is van szerkezete: a műveletnevek egy testet alkotnak.
- Másrészt itt F végtelen is lehet, pl. $\mathbb{R}$ feletti vektorterekben $|\mathbb{R}| = \text{kontínuum}$ darab művelet van. Figyeljük meg, hogy általában is: az 1.2 Definícióban semmiféle előírás nincs F méretére (F akár üres is lehet, vagy lehet véges, vagy lehet akár tetszőlegesen nagy végtelen halmaz).

1.1. Termek és azonosságok

1.5. Definíció (Term). Legyen $\langle F, \varrho \rangle$ hasonlósági típus, X pedig a változók halmaza. A t szimbólumsorozat $\langle F, \varrho \rangle$ típusú term X felett, ha

- $t \in X$ változó, vagy $t \in F$ és $\varrho(t) = 0$ (konstansszimbólum);
- $t = f(t_1, \dots, t_{\varrho(f)})$, ahol $f \in F$, és $t_1, \dots, t_{\varrho(f)}$ termek;
- minden term az előző két szabály véges sok alkalmazásával áll elő.

Az, hogy egy t szimbólumsorozat adott típusú term, nem több és nem kevesebb annál, mint hogy t a fenti szabályokkal előállítható.

A termek jelentés nélküli jelsorozatokat. Jelentést akkor kapnak, ha megfelelő kontextusba helyezzük őket. Egy ilyen kontextus

- egy, a term típusával megegyező típusú algebra (ez mondja meg, hogy a termben szereplő műveletnevek milyen műveleteket neveznek meg) és
- egy behelyettesítés (mely azt adja meg, hogy a termben szereplő változók az alaphalmaz mely elemeit jelölik).

Ha t_1, t_2 termek, akkor a $t_1 = t_2$ kifejezés egy *azonosság*.

1.6. Definíció (Azonosság teljesülése). Legyen $\mathcal{A}$ egy $\langle F, \varrho \rangle$ típusú algebra. A

$$\mathcal{A} \models t_1 = t_2$$

jelölés azt jelenti, hogy az azonosság igaz $\mathcal{A}$ -ban: a változók helyére bárhogyan írunk $\mathcal{A}$ -beli elemeket, a két oldal értéke egyenlő lesz.

1.7. Példa. Az 1.3 Példában megadott algebrákra, a $+$ és $\cdot$ jelöléseket rendre az f és g műveletnevekre használva:

$$\mathcal{A} \models x(y + z) = xy + xz,$$

$$\mathcal{B} \models x(y + z) = xy + xz,$$

$$\mathcal{C} \not\models x(y + z) = xy + xz \text{ (mert itt } xy \text{ jelöli } x \text{ és } y \text{ összegét, továbbá } x + y \text{ jelöli } x \text{ és } y \text{ szorzatát),}$$

$$\mathcal{D} \not\models x \cdot y = y \cdot x.$$

1.2. Algebrák konstrukciói: Reduktumképzés

1.8. Definíció (Reduktum). Legyenek $\langle F, \varrho \rangle$ és $\langle G, \sigma \rangle$ olyan hasonlósági típusok, melyekre $G \subseteq F$ és $\sigma = \varrho|_G$. Legyen

$$\mathcal{A} = \langle A, f^{\mathcal{A}} \rangle_{f \in F}$$

$\langle F, \varrho \rangle$ típusú algebra. Ekkor

$$\mathcal{B} = \langle A, f^{\mathcal{A}} \rangle_{f \in G}$$

az $\mathcal{A}$ algebra $\langle G, \sigma \rangle$ típusú *reduktuma*.

Reduktum-képzésnél tehát az algebra alaphalmaza nem változik, csak a műveletei közül hagyunk el („felejtünk el”) néhányat.

1.9. Példa. Minden csoportnak van félcsoport-reduktuma, és minden gyűrűnek van Abel-csoport-reduktuma.

1.3. Algebrák konstrukciói: Részalgebrák

1.10. Definíció. [Részalgebra] Legyen

$$\mathcal{A} = \langle A, f^{\mathcal{A}} \rangle_{f \in F}, \quad \mathcal{B} = \langle B, f^{\mathcal{B}} \rangle_{f \in F}$$

két $\langle F, \varrho \rangle$ típusú algebra. Ekkor $\mathcal{B}$ *részalgebrája* $\mathcal{A}$ -nak (jelölés: $\mathcal{B} \leq \mathcal{A}$), ha

- $B \subseteq A$;
- minden $f \in F$ esetén

$$f^{\mathcal{B}} = f^{\mathcal{A}}|_B.$$

1.11. Példa. A szokásos $\mathbb{Z}$ gyűrű részalgebrája a szokásos $\mathbb{Q}$ gyűrűnek:

$$\mathbb{Z} \leq \mathbb{Q}.$$

1.12. Definíció (Generált részalgebra). Legyen $X \subseteq A$. Ekkor a $\mathcal{B} \leq \mathcal{A}$ részalgebra az X által generált részalgebra, ha

- $X \subseteq B$;
- minden $\mathcal{C} \leq \mathcal{A}$ esetén $X \subseteq \mathcal{C} \implies \mathcal{B} \leq \mathcal{C}$.

Azaz $\mathcal{B}$ a legkisebb X -et tartalmazó $\mathcal{A}$ -beli részalgebra (abban az értelemben, hogy egyrészt X részhalmaza $\mathcal{B}$ alaphalmazának, másrészt, ha X részhalmaza valamely $\mathcal{C} \leq \mathcal{A}$ alaphalmazának, akkor $\mathcal{B} \leq \mathcal{C}$). Jelölés:

$$\mathcal{B} = \langle X \rangle, \quad \text{esetleg} \quad \mathcal{B} = \langle X \rangle^{\mathcal{A}}.$$

Az X halmaz nem feltétlenül zárt az $\mathcal{A}$ -beli műveletekre, ezért lehetséges, hogy $X \subsetneq B$ (sőt, ez a tipikus eset).

1.13. Tétel (A generált részalgebra létezése). *Minden nemüres $X \subseteq A$ -ra létezik $\langle X \rangle \leq \mathcal{A}$.*

Első bizonyítás. Legyen

$$\mathcal{H} = \{\mathcal{C} \leq \mathcal{A} : X \subseteq \mathcal{C}\}.$$

Ez nem üres, hiszen például $\mathcal{A} \in \mathcal{H}$. Legyen

$$B = \bigcap_{\mathcal{C} \in \mathcal{H}} \mathcal{C}.$$

Egyrészt $X \subseteq B$.

Másrészt azt állítjuk, hogy, B zárt a műveletekre. Ez a következők miatt van így. Legyen $f \in F$ tetszőleges, és legyenek $a_1, \dots, a_{\ell(f)} \in B$. Ekkor minden $\mathcal{C} \in \mathcal{H}$ esetén

$$a_1, \dots, a_{\ell(f)} \in \mathcal{C}.$$

Továbbá mindegyik $\mathcal{C}$ zárt a műveletekre (hiszen mindegyik $\mathcal{C}$ részalgebra). Ezért

$$(\forall \mathcal{C} \in \mathcal{H}) \quad f^{\mathcal{A}}(a_1, \dots, a_{\ell(f)}) \in \mathcal{C}.$$

Tehát

$$f^{\mathcal{A}}(a_1, \dots, a_{\ell(f)}) \in \bigcap_{\mathcal{C} \in \mathcal{H}} \mathcal{C} = B.$$

Értelmezzük B -n a műveleteket az $\mathcal{A}$ műveleteinek megszorításaként. Ezzel elértük, hogy $\mathcal{B} \leq \mathcal{A}$ egy X -et tartalmazó részalgebra.

Harmadrészt a metszet definíciójából nyilvánvaló, hogy $\mathcal{B}$ a legkisebb X -t tartalmazó részalgebra: $\mathcal{B} \leq \mathcal{C}$ teljesül minden $\mathcal{C} \in \mathcal{H}$ -ra. $\square$

Arra a feltételre, hogy a generáló X halmaz nemüres, azért volt szükség, mert az 1.2 Definíció értelmében egy algebra alaphalmaza sosem lehet üres. Ha a hasonlósági típus tartalmaz konstansszimbólumot, akkor ez önmagában garantálja, hogy – az előző bizonyítás jelöléseit használva – $\bigcap_{\mathcal{C} \in \mathcal{H}} \mathcal{C} \neq \emptyset$, mert mindegyik $\mathcal{C}$

tartalmazza az összes konstans (= 0-változós művelet eredményét). Ezért ha hasonlósági típusunkban van legalább 1 darab konstansszimbólum (=nulla-változós függvénytípus), akkor az $X \neq \emptyset$ feltétel elhagyható.

Második bizonyítás. Az ötlet: vegyük az összes olyan elemet, amit úgy kapunk, hogy egy tetszőleges termet X -beli elemeken kiértékelünk. Ez lesz a keresett B . Formálisan, legyen

$$B = \{t^A(a_1, \dots, a_n) : n \in \mathbb{N}, t \text{ egy } n\text{-változós term, } a_1, \dots, a_n \in X\}.$$

(1) Állítjuk, hogy $X \subseteq B$.

Ez teljesül, mert X minden eleme előáll úgy, hogy x -be, mint egyetlen változóból álló termbe behelyettesítjük X elemeit. Tehát minden $a \in X$ -re teljesül, hogy $a \in B$.

(2) Állítjuk, hogy $B \subseteq \langle X \rangle$.

Ez a következők miatt van így. Legyen $\mathcal{C} \leq \mathcal{A}$ tetszőleges, melyre $X \subseteq \mathcal{C}$. Az 1.5 Definíciót követve, a termék összetettsége szerinti indukcióval belátjuk, hogy minden n -változós t termre és minden $a_1, \dots, a_n \in X \subseteq \mathcal{C}$ esetén $t^A(a_1, \dots, a_n) \in \mathcal{C}$:

- **alaplépés:** ha t változó vagy konstansszimbólum, akkor ez triviális;
- **indukciós lépés:** ha $t = f(t_1, \dots, t_{\varrho(f)})$, akkor az indukciós feltevés szerint $t_i^A(a_1, \dots, a_n) \in \mathcal{C}$ minden i -re, és mivel $\mathcal{C}$ zárt f^A -ra, az eredmény is $\mathcal{C}$ -ben van.

Az indukció kész, beláttuk, hogy $\mathcal{C}$ minden termre zárt.

Mivel az előző bekezdés minden X -et tartalmazó $\mathcal{C} \leq \mathcal{A}$ algebrára igaz, ezért, ha $\langle X \rangle$ létezik egyáltalán, akkor (2)-nek teljesülnie kell.

(3) Állítjuk, hogy $\mathcal{B} \leq \mathcal{A}$ (azaz B zárt a műveletekre).

Ennek igazolásához legyen $f \in F$ és legyenek $b_1, \dots, b_{\varrho(f)} \in B$. Ekkor B definíciója szerint minden $i = 1, \dots, \varrho(f)$ -hez létezik egy t_i (mondjuk k_i változós) term és egy $\bar{a}_i \in X^{k_i}$ sorozat úgy, hogy $b_i = t_i^A(\bar{a}_i)$. Feltehetjük, hogy a t_i termék változóinak halmaza páronként diszjunkt. Ekkor

$$f^A(b_1, \dots, b_{\varrho(f)}) = f^A(t_1^A(\bar{a}_1), \dots, t_{\varrho(f)}^A(\bar{a}_n)) = \left(f(t_1, \dots, t_{\varrho(f)})\right)^A(\bar{a}_1, \dots, \bar{a}_n) \in B.$$

Ez pontosan azt jelenti, hogy B zárt f^A -ra; mivel $f \in F$ tetszőleges volt, (3) teljesül, azaz $\mathcal{B} \leq \mathcal{A}$.

Összefoglalva: $X \subseteq B \leq \mathcal{A}$ (1) és (3) miatt, és $B \subseteq \langle X \rangle$ (2) miatt. De $\langle X \rangle$ definíció szerint a legkisebb X -et tartalmazó részalgebra, tehát $\langle X \rangle \subseteq B$ is fennáll (hiszen $\mathcal{B}$ maga is egy X -et tartalmazó részalgebra). Így

$$\mathcal{B} = \langle X \rangle,$$

ami éppen a bizonyítandó állítás. □

1.4. Algebrák konstrukciói: Faktoralgebrák, homomorf kép

1.14. Definíció (Izomorfizmus és homomorfizmus). Legyen $\mathcal{A} = \langle A, f^A \rangle_{f \in F}$ és $\mathcal{B} = \langle B, f^B \rangle_{f \in F}$ két $\langle F, \varrho \rangle$ típusú struktúra, és $\varphi: A \rightarrow B$ egy leképezés. Azt mondjuk, hogy φ egy izomorfizmus, ha

- (1) φ bijekció;
- (2) φ művelettartó, azaz minden $f \in F$ és minden $a_1, \dots, a_{\varrho(f)} \in A$ esetén

$$\varphi(f^A(a_1, \dots, a_{\varrho(f)})) = f^B(\varphi(a_1), \dots, \varphi(a_{\varrho(f)})).$$

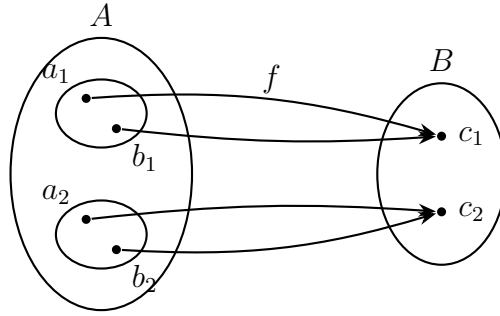
Azt mondjuk, hogy $\mathcal{A}$ izomorf $\mathcal{B}$ -vel, ha van köztük izomorfizmus. Emellett használjuk még a következő elnevezéseket is.

- Ha (2) teljesül (azaz φ művelettartó), akkor φ *homomorfizmus*;
- Ha (1) és (2) is teljesül, akkor φ *izomorfizmus*;
- Ha (2) teljesül és $\mathcal{A} = \mathcal{B}$, akkor φ *endomorfizmus*;
- Ha (1) és (2) is teljesül és $\mathcal{A} = \mathcal{B}$, akkor φ *automorfizmus*.

1.15. Definíció (Egy függvény magja). Legyen $f: A \rightarrow B$ tetszőleges függvény. Ekkor

$$\ker(f) = \ker^A(f) = \{\langle a, b \rangle \in A \times A : f(a) = f(b)\}$$

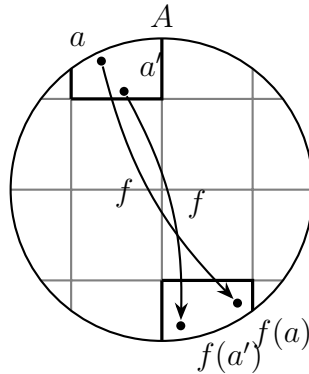
az f *magja*. Ez nem a lineáris algebrában használt magfogalom: itt egy relációt adunk meg, ezt – szükség esetén – $\ker^A(f)$ -ben a kitevőbe írt A -val is hangsúlyozzuk (A -val itt az „Algebrai” szóra utalunk). Később, ??-ban visszatérünk még a lineáris algebrából ismert *ker*-el való kapcsolatra.



1.16. Definíció (Kongruenciareláció). Legyen $\mathcal{A} = \langle A, f^A \rangle_{f \in F}$ algebra, és Θ ekvivalenciareláció A -n. A Θ reláció *kongruenciareláció*, ha minden művelettel kompatibilis, azaz ha minden $f \in F$ és minden $a_1, \dots, a_{\varrho(f)}, a'_1, \dots, a'_{\varrho(f)} \in A$ esetén

$$\left. \begin{array}{l} \langle a_1, a'_1 \rangle \in \Theta, \\ \vdots \\ \langle a_{\varrho(f)}, a'_{\varrho(f)} \rangle \in \Theta \end{array} \right\} \implies \langle f^A(a_1, \dots, a_{\varrho(f)}), f^A(a'_1, \dots, a'_{\varrho(f)}) \rangle \in \Theta.$$

Szavakkal: Azonos kongruencia-osztályban lévő elempárokat minden $\mathcal{A}$ -beli művelet azonos osztályba képez.



1.17. Definíció (Faktoralgebra). Az $\mathcal{A}$ algebra kongruenciáinak halmazát $\text{Con}(\mathcal{A})$ -val jelöljük. Ha $\Theta \in \text{Con}(\mathcal{A})$, akkor $\mathcal{A}/\Theta$ az $\mathcal{A}$ algebra Θ szerinti *faktoralgebrája*, amit a következő módon definiálunk:

- $\mathcal{A}/\Theta$ alaphalmaza a Θ ekvivalenciaosztályainak halmaza:

$$A/\Theta = \{a/\Theta : a \in A\};$$

- $\mathcal{A}/\Theta$ műveletei: ha $f \in F$ és $a_1/\Theta, \dots, a_{\varrho(f)}/\Theta \in A/\Theta$, akkor

$$f^{\mathcal{A}/\Theta}(a_1/\Theta, \dots, a_{\varrho(f)}/\Theta) = f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)})/\Theta.$$

Az $f^{\mathcal{A}/\Theta}$ művelet tehát a Θ ekvivalenciaosztályain van értelmezve. Az előző definícióban úgy vettük fel Θ néhány ekvivalenciaosztályát, hogy reprezentánsokat választottunk belőlük: a_1/Θ -ből a_1 -et, ..., $a_{\varrho(f)}/\Theta$ -ből $a_{\varrho(f)}$ -et. Ha

$$a'_1 \in a_1/\Theta, \dots, a'_{\varrho(f)} \in a_{\varrho(f)}/\Theta,$$

akkor mindegyik a_i/Θ ekvivalenciaosztályt megnevezhetjük volna a'_i/Θ -val is, hiszen ekkor $a_i/\Theta = a'_i/\Theta$. Ezért

$$(*) \quad f^{\mathcal{A}/\Theta}(a_1/\Theta, \dots, a_{\varrho}/\Theta) = f^{\mathcal{A}/\Theta}(a'_1/\Theta, \dots, a'_{\varrho}/\Theta),$$

mert a két oldalon az $f^{\mathcal{A}/\Theta}$ argumentumában szereplő ekvivalenciaosztályok páronként rendre egyenlők. Tehát, amikor $f^{\mathcal{A}/\Theta}$ eredményét definiáljuk, akkor az 1.17 Definíció 2. pontjának baloldalait különböző módon is megnevezhetjük! Ugyanakkor a definíció jobboldalán használtuk, hogy Θ egyes ekvivalenciaosztályaiból melyik reprezentánst választottuk (azaz használtuk, hogy Θ egyes ekvivalenciaosztályait milyen konkrét módon neveztük meg). Ezért felmerül a kérdés, hogy

vajon $f^{\mathcal{A}/\Theta}$ jóldefiniált-e abban az értelemben, hogy a definíció jobboldala nem függ-e a reprezentánsok megválasztásától. Ahhoz, hogy a fenti definíció értelmes legyen, szükséges, hogy ha ugyanazt a baloldali objektumot különböző módon neveztük meg (azaz, ha $(*)$ fennáll), akkor a jobboldalnak is egyenlőknek kell lenniük:

$$(**) \quad f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)})/\Theta = f^{\mathcal{A}}(a'_1, \dots, a'_{\varrho(f)})/\Theta,$$

vagyis, ha az argumentumokból másképp választunk reprezentánsokat, akkor a két reprezentációsrendszer mellett számított eredménynek legalább az ekvivalenciaosztálya azonos kell, hogy maradjon. Ha ez nem teljesülne, akkor a fenti 1.17 Definíció szerint $f^{\mathcal{A}/\Theta}$ nem lenne függvény: értelmezési tartománya elemeihez esetleg több különböző eredményt is hozzárendeltünk volna.

Ez a probléma a faktoralgebrák definíciójában nem lép fel, mert kongruenciareláció szerint faktorizáltunk (valójában ez indokolja meg a kongruenciarelációk 1.16-beli definícióját). Formálisabban, ahhoz, hogy a fenti 1.17-ben értelmes módon definiáljuk az $f^{\mathcal{A}/\Theta}$ műveletet, pont arra van szükségünk, hogy ha minden $i = 1, \dots, \varrho(f)$ -re $\langle a_i, a'_i \rangle \in \Theta$, akkor

$$\langle f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)}), f^{\mathcal{A}}(a'_1, \dots, a'_{\varrho(f)}) \rangle \in \Theta,$$

vagyis Θ kongruenciareláció legyen. Így $f^{\mathcal{A}}$ eredményeinek ekvivalenciaosztálya nem függ a reprezentánsok megválasztásától és ezért $f^{\mathcal{A}}$ jóldefiniált.

1.18. Tétel (Mag, természetes homomorfizmus és homomorfizmustétel).

Legyen $\varphi: \mathcal{A} \rightarrow \mathcal{B}$ homomorfizmus, és $\Theta \in \text{Con}(\mathcal{A})$. Ekkor:

(1) $\ker(\varphi) \in \text{Con}(\mathcal{A})$.

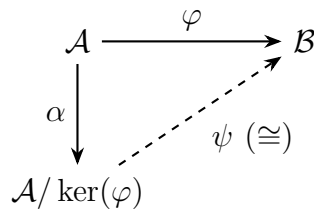
(2) Az

$$\alpha: A \longrightarrow A/\Theta, \quad \alpha(b) = b/\Theta$$

leképezés homomorfizmus; ez a Θ -hoz tartozó természetes homomorfizmus.

(3) **Homomorfizmustétel:** ha φ szürjektív, akkor

$$\mathcal{B} \cong \mathcal{A}/\ker(\varphi).$$



Bizonyítás. **(1)** Világos, hogy $\ker(\varphi)$ ekvivalenciareláció. Azt kell még igazolni, hogy a műveletekkel kompatibilis. Legyen $f \in F$, és tegyük fel, hogy

$$a_1, \dots, a_{\varrho(f)}, a'_1, \dots, a'_{\varrho(f)} \in A$$

úgy, hogy minden $i = 1, \dots, \varrho(f)$ -re $\langle a_i, a'_i \rangle \in \ker(\varphi)$. Ez azt jelenti, hogy

$$(\forall i \leq \varrho(f)) \quad \varphi(a_i) = \varphi(a'_i).$$

A cél:

$$\langle f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)}), f^{\mathcal{A}}(a'_1, \dots, a'_{\varrho(f)}) \rangle \in \ker(\varphi),$$

azaz

$$\varphi(f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)})) = \varphi(f^{\mathcal{A}}(a'_1, \dots, a'_{\varrho(f)})).$$

Ez következik abból, hogy φ egy homomorfizmus:

$$\begin{aligned} \varphi(f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)})) &= f^{\mathcal{B}}(\varphi(a_1), \dots, \varphi(a_{\varrho(f)})) \\ &= f^{\mathcal{B}}(\varphi(a'_1), \dots, \varphi(a'_{\varrho(f)})) \\ &= \varphi(f^{\mathcal{A}}(a'_1, \dots, a'_{\varrho(f)})). \end{aligned}$$

(2) Legyen $f \in F$, és legyen $a_1, \dots, a_{\varrho(f)} \in A$. Azt kell ellenőrizni, hogy

$$\alpha(f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)})) = f^{\mathcal{A}/\Theta}(\alpha(a_1), \dots, \alpha(a_{\varrho(f)})).$$

Azaz az kell, hogy

$$f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)})/\Theta = f^{\mathcal{A}/\Theta}(a_1/\Theta, \dots, a_{\varrho(f)}/\Theta).$$

De ez a faktoralgebra műveleteinek definíciója szerint igaz:

$$\begin{aligned} f^{\mathcal{A}/\Theta}(\alpha(a_1), \dots, \alpha(a_{\varrho(f)})) &= f^{\mathcal{A}/\Theta}(a_1/\Theta, \dots, a_{\varrho(f)}/\Theta) \\ &= f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)})/\Theta. \end{aligned}$$

(3) Tegyük fel, hogy φ szürjektív. Defináljuk a következő leképezést:

$$\psi: \mathcal{A}/\ker(\varphi) \longrightarrow \mathcal{B}, \quad \psi(a/\ker(\varphi)) = \varphi(a).$$

Ez jóldefiniált, mert

$$a/\ker(\varphi) = a'/\ker(\varphi) \iff \langle a, a' \rangle \in \ker(\varphi) \iff \varphi(a) = \varphi(a').$$

Azt kell igazolni, hogy ψ izomorfizmus.

• *Injektivitás.* Ha $a/\ker(\varphi) \neq b/\ker(\varphi)$, akkor $\varphi(a) \neq \varphi(b)$. Ezért

$$\psi(a/\ker(\varphi)) = \varphi(a) \neq \varphi(b) = \psi(b/\ker(\varphi)).$$

• *Szürjektivitás.* Ha $y \in B$, akkor φ szürjektivitása miatt létezik $a \in A$, amelyre $\varphi(a) = y$. Ekkor

$$\psi(a/\ker(\varphi)) = \varphi(a) = y.$$

• *Művelettartás.* Legyen $f \in F$, és

$$a_1/\ker(\varphi), \dots, a_{\varrho(f)}/\ker(\varphi) \in A/\ker(\varphi).$$

A bizonyítandó egyenlőség

$$\psi(f^{\mathcal{A}/\ker(\varphi)}(a_1/\ker(\varphi), \dots, a_{\varrho(f)}/\ker(\varphi))) = f^{\mathcal{B}}(\psi(a_1/\ker(\varphi)), \dots, \psi(a_{\varrho(f)}/\ker(\varphi))).$$

Ez teljesül, mert,

$$\begin{aligned} f^{\mathcal{B}}(\psi(a_1/\ker(\varphi)), \dots, \psi(a_{\varrho(f)}/\ker(\varphi))) &= f^{\mathcal{B}}(\varphi(a_1), \dots, \varphi(a_{\varrho(f)})) \\ &= \varphi(f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)})) \\ &= \psi(f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)})/\ker(\varphi)) \\ &= \psi(f^{\mathcal{A}/\ker(\varphi)}(a_1/\ker(\varphi), \dots, a_{\varrho(f)}/\ker(\varphi))). \end{aligned}$$

Tehát ψ bijektív és művelettartó, vagyis izomorfizmus. $\square$

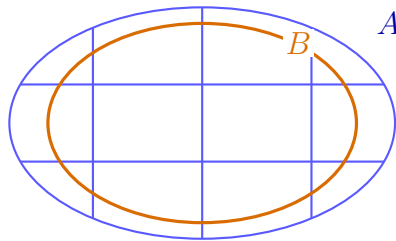
Izomorfia-tételek

1.19. Tétel (1. izomorfizmus-tétel). *Legyen $\mathcal{A}$ egy $\langle F, \varrho \rangle$ típusú algebra, $\mathcal{B} \leq \mathcal{A}$ és $\Theta \in \text{Con}(\mathcal{A})$. Ekkor:*

(1) $\Theta_B = \Theta \cap (B \times B) \in \text{Con}(\mathcal{B})$.

(2) Ha $\forall a \in A \exists b \in B : \langle a, b \rangle \in \Theta$, akkor

$$\mathcal{A}/\Theta \cong \mathcal{B}/\Theta_B.$$



A rács cellái a Θ -osztályok;
a B -vel vett nem üres metszeteik a Θ_B -osztályok.

Bizonyítás.

(1) A Θ_B reláció ekvivalenciareláció B -n, hiszen Θ ekvivalenciareláció A -n. A műveletekkel való kompatibilitás ellenőrzéséhez legyen $f \in F$, és legyen $a_1, \dots, a_{\varrho(f)}, a'_1, \dots, a'_{\varrho(f)} \in B$ úgy, hogy $\langle a_i, a'_i \rangle \in \Theta_B$ minden $i = 1, \dots, \varrho(f)$ esetén. Mivel $\Theta_B \subseteq \Theta$ és Θ kongruencia,

$$\langle f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)}), f^{\mathcal{A}}(a'_1, \dots, a'_{\varrho(f)}) \rangle \in \Theta.$$

Másrészt $\mathcal{B} \leq \mathcal{A}$, így a két műveletérték B -beli, és megegyezik a megfelelő $\mathcal{B}$ -beli műveletértékkel. Tehát

$$\langle f^{\mathcal{B}}(a_1, \dots, a_{\varrho(f)}), f^{\mathcal{B}}(a'_1, \dots, a'_{\varrho(f)}) \rangle \in \Theta \cap (B \times B) = \Theta_B.$$

(2) Definiáljuk a

$$\varphi : \mathcal{B}/\Theta_B \longrightarrow \mathcal{A}/\Theta, \quad \varphi(b/\Theta_B) = b/\Theta$$

leképezést. Ez jóldefiniált: ha $\langle b, b' \rangle \in \Theta_B$, akkor $\langle b, b' \rangle \in \Theta$, ezért

$$\varphi(b/\Theta_B) = b/\Theta = b'/\Theta = \varphi(b'/\Theta_B).$$

- **Injektív:** ha $a, b \in B$ és $a/\Theta_B \neq b/\Theta_B$, akkor $\langle a, b \rangle \notin \Theta_B \rightsquigarrow \langle a, b \rangle \notin \Theta$. Ebből

$$\varphi(a/\Theta_B) = a/\Theta \neq b/\Theta = \varphi(b/\Theta_B).$$

- **Szürjektív:** minden $a \in A$ -hoz van olyan $b \in B$, amelyre $\langle a, b \rangle \in \Theta$. Így

$$a/\Theta = b/\Theta = \varphi(b/\Theta_B).$$

- **Művelettartó:** legyen $f \in F$ és $a_1, \dots, a_{\varrho(f)} \in B$. Azt kell ellenőrizni, hogy

$$\varphi(f^{\mathcal{B}/\Theta_B}(a_1/\Theta_B, \dots, a_{\varrho(f)}/\Theta_B)) = f^{\mathcal{A}/\Theta}(\varphi(a_1/\Theta_B), \dots, \varphi(a_{\varrho(f)}/\Theta_B)).$$

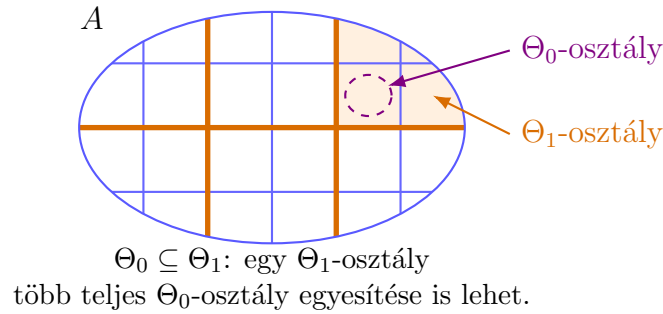
A jobboldalról kiindulva:

$$\begin{aligned} & f^{\mathcal{A}/\Theta}(\varphi(a_1/\Theta_B), \dots, \varphi(a_{\varrho(f)}/\Theta_B)) \\ &= f^{\mathcal{A}/\Theta}(a_1/\Theta, \dots, a_{\varrho(f)}/\Theta) \\ &= f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)})/\Theta \\ &= \varphi(f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)}))/\Theta_B \\ &= \varphi(f^{\mathcal{B}}(a_1, \dots, a_{\varrho(f)}))/\Theta_B \\ &= \varphi(f^{\mathcal{B}/\Theta_B}(a_1/\Theta_B, \dots, a_{\varrho(f)}/\Theta_B)). \end{aligned}$$

Tehát φ bijektív homomorfizmus, azaz izomorfizmus. □

1.20. Definíció. Legyen $\mathcal{A} = \langle A, f^{\mathcal{A}} \rangle_{f \in F}$ egy $\langle F, \varrho \rangle$ típusú algebra, és $\Theta_0, \Theta_1 \in \text{Con}(\mathcal{A})$, $\Theta_0 \subseteq \Theta_1$. Az A/Θ_0 halmazon értelmezett **faktorreláció**:

$$\Theta_1/\Theta_0 = \{ \langle a/\Theta_0, b/\Theta_0 \rangle : a, b \in A, \langle a, b \rangle \in \Theta_1 \}.$$



1.21. Tétel (2. izomorfizmus-tétel). Legyen $\mathcal{A}$ egy $\langle F, \varrho \rangle$ típusú algebra, $\Theta_0, \Theta_1 \in \text{Con}(\mathcal{A})$, $\Theta_0 \subseteq \Theta_1$. Ekkor:

- (1) $\Theta_1/\Theta_0 \in \text{Con}(\mathcal{A}/\Theta_0)$.
- (2) Legyen $M = \{ \eta \in \text{Con}(\mathcal{A}) : \Theta_0 \subseteq \eta \}$ az $\mathcal{A}$ algebra Θ_0 -nál bővebb kongruenciáinak halmaza. Ekkor

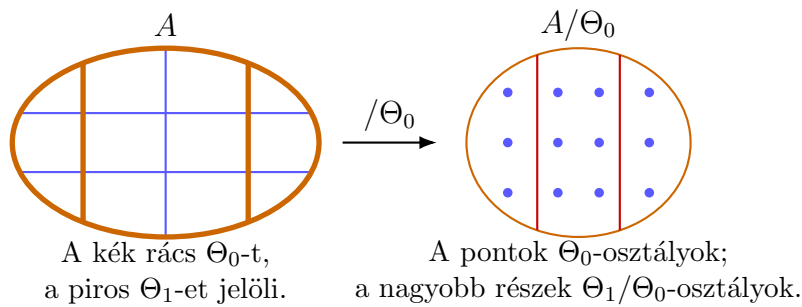
$$\mu : M \longrightarrow \text{Con}(\mathcal{A}/\Theta_0), \quad \mu(\eta) = \eta/\Theta_0$$

leképezés bijekció és rendezéstartó:

$$(\forall \eta_0, \eta_1 \in M) \quad \eta_0 \subseteq \eta_1 \implies \mu(\eta_0) \subseteq \mu(\eta_1),$$

(sőt valójában μ hálózomorfizmus, de ennek jelentését most nem részletezzük).

- (3) $\mathcal{A}/\Theta_1 \cong (\mathcal{A}/\Theta_0)/(\Theta_1/\Theta_0)$.



Bizonyításvázlat. A bizonyítás egyes részleteit feladatok formájában megbeszéltük a 2. gyakorlaton, de a teljesség kedvéért ide is beillesztem.

(1)-hez először azt látjuk be, hogy Θ_1/Θ_0 egy ekvivalenciareláció A/Θ_0 -on. Ehhez megadunk egy φ függvényt, melyre $\Theta_1/\Theta_0 = \ker(\varphi)$.

Legyen $\varphi : A/\Theta_0 \rightarrow A/\Theta_1$, $\varphi(a/\Theta_0) = a/\Theta_1$. Ez jóldefiniált, mert

$$a/\Theta_0 = b/\Theta_0 \rightsquigarrow \langle a, b \rangle \in \Theta_0 \subseteq \Theta_1 \rightsquigarrow a/\Theta_1 = b/\Theta_1.$$

Világos, hogy $\ker(\varphi) = \Theta_1/\Theta_0$, ezért ez utóbbi egy ekvivalenciareláció $D(\varphi) = A/\Theta_0$ -n. (1)-hez be kell még látni, hogy Θ_1/Θ_0 kompatibilis a műveletekkel. Ehhez legyenek

$$f \in F, \quad a_1, \dots, a_{\varrho(f)}, a'_1, \dots, a'_{\varrho(f)} \in A$$

úgy hogy minden $1 \leq i \leq \varrho(f)$ -re $\langle a_i/\Theta_0, a'_i/\Theta_0 \rangle \in \Theta_1/\Theta_0$. Ekkor minden $1 \leq i \leq \varrho(f)$ -re $\langle a_i, a'_i \rangle \in \Theta_1$ is teljesül, továbbá

$$f^A(a_1, \dots, a_{\varrho(f)})/\Theta_1 \stackrel{\Theta_1 \in \text{Con}(\mathcal{A})}{=} f^A(a'_1, \dots, a'_{\varrho(f)})/\Theta_1$$

és ezért Θ_1/Θ_0 definíciója szerint

$$\underbrace{\langle f^A(a_1, \dots, a_{\varrho(f)})/\Theta_0, f^A(a'_1, \dots, a'_{\varrho(f)})/\Theta_0 \rangle}_{f^{A/\Theta_0}(a_1/\Theta_0, \dots, a_{\varrho(f)}/\Theta_0)} \in \Theta_1/\Theta_0.$$

(2)-höz a rendezéstartást közvetlenül a faktorreláció definíciójából kapjuk. Legyen $\eta_0, \eta_1 \in \text{Con}(\mathcal{A})$ úgy, hogy $\Theta_0 \subseteq \eta_0 \subseteq \eta_1$. Ekkor minden $a, b \in A$ -ra

$$\begin{aligned} \langle a/\Theta_0, b/\Theta_0 \rangle \in \mu(\eta_0) &\iff \langle a, b \rangle \in \eta_0 \\ &\implies \langle a, b \rangle \in \eta_1 \\ &\iff \langle a/\Theta_0, b/\Theta_0 \rangle \in \mu(\eta_1). \end{aligned}$$

Tehát $\mu(\eta_0) \subseteq \mu(\eta_1)$.

• **μ injektív:** ha $\eta_0 \neq \eta_1$, akkor valamelyik (mondjuk η_0) nem részhalmaza a másiknak, azaz van $\langle a, b \rangle \in \eta_0 - \eta_1$. De akkor $\langle a/\Theta_0, b/\Theta_0 \rangle \in \eta_0/\Theta_0 = \mu(\eta_0)$, és $\langle a/\Theta_0, b/\Theta_0 \rangle \notin \eta_1/\Theta_0 = \mu(\eta_1)$, tehát $\mu(\eta_0) \neq \mu(\eta_1)$.

• **μ szürjektív:** legyen $\eta \in \text{Con}(\mathcal{A}/\Theta_0)$, legyenek

$$\alpha : \mathcal{A}/\Theta_0 \rightarrow \mathcal{A}/\eta, \quad \alpha(a/\Theta_0) = (a/\Theta_0)/\eta \quad \text{és} \quad \beta : \mathcal{A} \rightarrow \mathcal{A}/\Theta_0, \quad \beta(a) = a/\Theta_0$$

a természetes homomorfizmusok. Homomorfizmusok kompozíciója homomorfizmus (ha nem világos, gondold meg), így $\alpha \circ \beta$ homomorfizmus $\mathcal{A}$ -ból $\mathcal{A}/\eta$ -ba. Ezért $\Theta_1 = \ker(\alpha \circ \beta)$ kongruenciája $\mathcal{A}$ -nak. A kompozícióképzés miatt $\Theta_0 = \ker(\beta) \subseteq \Theta_1$ és ezért $\Theta_1 \in M$. Végül $\eta = \mu(\Theta_1)$ mert tetszőleges $a, b \in A$ -ra

$$\begin{aligned} \langle a/\Theta_0, b/\Theta_0 \rangle \in \mu(\Theta_1) &\iff \langle a/\Theta_0, b/\Theta_0 \rangle \in \Theta_1/\Theta_0 \iff \langle a, b \rangle \in \Theta_1 \iff \\ &\iff \langle a, b \rangle \in \ker(\alpha \circ \beta) \iff \langle a/\Theta_0, b/\Theta_0 \rangle \in \ker(\alpha) = \eta. \end{aligned}$$

Ezzel (2) igazolásával készen vagyunk. (3) igazolásához legyen

$$\varphi : (\mathcal{A}/\Theta_0)/(\Theta_1/\Theta_0) \longrightarrow \mathcal{A}/\Theta_1, \quad \varphi((a/\Theta_0)/(\Theta_1/\Theta_0)) = a/\Theta_1.$$

Könnyen ellenőrizhető, hogy ez jóldefiniált, bijektív és művelettartó, tehát izomorfizmus. $\square$

1.5. Algebrák konstrukciói: Direktszorzat

1.22. Definíció. Legyen minden $i \in I$ -re $\mathcal{A}_i$ egy $\langle F, \varrho \rangle$ típusú algebra. Ezek $\prod_{i \in I} \mathcal{A}_i$ **direktszorzata** az az algebra, melynek alaphalmaza az $(A_i)_{i \in I}$ család kiválasztási függvényeinek halmaza:

$$\prod_{i \in I} A_i = \{s : s \text{ egy függvény, } D(s) = I, (\forall i \in I) s(i) \in A_i\}.$$

Ha $f \in F$ és $s_1, \dots, s_{\varrho(f)} \in \prod_{i \in I} A_i$, akkor

$$f^{\prod_{i \in I} \mathcal{A}_i}(s_1, \dots, s_{\varrho(f)}) = \langle f^{\mathcal{A}_i}(s_1(i), \dots, s_{\varrho(f)}(i)) : i \in I \rangle.$$

Vagyis a műveleteket **koordinátánként** végezzük:

$$(f^{\prod_{i \in I} \mathcal{A}_i}(s_1, \dots, s_{\varrho(f)}))(i) = f^{\mathcal{A}_i}(s_1(i), \dots, s_{\varrho(f)}(i)).$$

1.23. Tétel. Legyen $\mathcal{A}$ egy $\langle F, \varrho \rangle$ típusú algebra és $I \subseteq \text{Con}(\mathcal{A})$ olyan **szeparáló rendszer**, amelyre

$$\forall a, b \in A, \quad a \neq b \implies \exists \Theta \in I : \langle a, b \rangle \notin \Theta.$$

Ekkor $\mathcal{A}$ beágyazható a $\prod_{\Theta \in I} \mathcal{A}/\Theta$ direktszorzatba.

Bizonyítás. Minden $\Theta \in I$ -re legyen

$$\alpha_\Theta : A \longrightarrow A/\Theta, \quad \alpha_\Theta(a) = a/\Theta$$

a természetes homomorfizmus. Definiáljuk a

$$\varphi : \mathcal{A} \longrightarrow \prod_{\Theta \in I} \mathcal{A}/\Theta, \quad \varphi(a) = \langle \alpha_\Theta(a) : \Theta \in I \rangle$$

leképezést. Azt állítjuk, hogy φ injektív homomorfizmus.

Injektivitás. Ha $a \neq b$, akkor van $\Theta \in I$, amelyre $\langle a, b \rangle \notin \Theta$. Ezért

$$\alpha_\Theta(a) = a/\Theta \neq b/\Theta = \alpha_\Theta(b),$$

tehát a Θ -nak megfelelő koordináták eltérnek, ezért $\varphi(a) \neq \varphi(b)$.

Művelettartás. Legyen $f \in F$ és $a_1, \dots, a_{\varrho(f)} \in A$. Azt kell ellenőrizni, hogy

$$\varphi(f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)})) = f^{\prod_{\Theta \in I} \mathcal{A}/\Theta}(\varphi(a_1), \dots, \varphi(a_{\varrho(f)})).$$

A jobboldalból kiindulva, a direktszorzat definíciójából

$$\begin{aligned}
& f^{\prod_{\Theta \in I} \mathcal{A}/\Theta}(\varphi(a_1), \dots, \varphi(a_{\varrho(f)})) \\
&= f^{\prod_{\Theta \in I} \mathcal{A}/\Theta}(\langle \alpha_{\Theta}(a_1) : \Theta \in I \rangle, \dots, \langle \alpha_{\Theta}(a_{\varrho(f)}) : \Theta \in I \rangle) \\
&= \langle f^{\mathcal{A}/\Theta}(\alpha_{\Theta}(a_1), \dots, \alpha_{\Theta}(a_{\varrho(f)})) : \Theta \in I \rangle \\
&= \langle f^{\mathcal{A}/\Theta}(a_1/\Theta, \dots, a_{\varrho(f)}/\Theta) : \Theta \in I \rangle \\
&= \langle f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)})/\Theta : \Theta \in I \rangle \\
&= \varphi(f^{\mathcal{A}}(a_1, \dots, a_{\varrho(f)})).
\end{aligned}$$

Így φ valóban beágyazás.

□

$$\begin{array}{ccc}
\mathcal{A} & \xrightarrow{\varphi \text{ (beágyazás)}} & \prod_{\Theta \in I} \mathcal{A}/\Theta \\
& \searrow \alpha_{\Theta} & \downarrow \pi_{\Theta} \\
& & \mathcal{A}/\Theta
\end{array}$$

$$a \mapsto \langle a/\Theta : \Theta \in I \rangle, \quad \pi_{\Theta} \circ \varphi = \alpha_{\Theta}.$$

1.6. Összefoglalás

Ez az összefoglalás nem hangzott el előadáson, de úgy gondolom, sokat segít az eddigiek áttekintésében, ezért később (a szorgalmi időszak végéig) ideírom.

2. Félcsoportok

2.1. Definíció. Az $\mathcal{A} = \langle A, \cdot \rangle$ algebra **félcsoport**, ha a kétváltozós $\cdot$ művelet asszociatív, azaz

$$(\forall a, b, c \in A) \quad (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

- $e \in A$ **balegység**, ha minden $a \in A$ -ra $e \cdot a = a$;
- $f \in A$ **jobbegység**, ha minden $a \in A$ -ra $a \cdot f = a$;
- egy elem **egységelem**, ha balegység és jobbegység is.

Az egységelemes félcsoportot **monoidnak** nevezzük; jelölése $\langle A; e, \cdot \rangle$.

Legyen e egységelem és $a, b \in A$. Ha $ab = e$, akkor a a b **balinverze**, b pedig az a **jobbinverze**. Ha $ab = ba = e$, akkor a és b egymás **inverzei**.

2.2. Tétel (Általános asszociativitás). *Legyen $\langle A, \cdot \rangle$ félcsoport és $a_1, \dots, a_n \in A$. Az $a_1 \cdots a_n$ szorzat értéke minden zárójelezés mellett ugyanaz, ha a tényezők sorrendjét megtartjuk.*

2.3. Példa.

$$((a_1 a_2) a_3) (a_4 a_5) = (a_1 ((a_2 a_3) a_4)) a_5 = ((a_1 a_2) (a_3 a_4)) a_5.$$

Bizonyítás. Azt látjuk be, hogy minden zárójelezés eredménye a balra zárójelezett

$$(((a_1 a_2) a_3) \cdots a_{n-1}) a_n$$

szorzattal egyezik meg. Ehhez n szerinti teljes indukciót alkalmazunk; $n = 1, 2$ esetén az állítás triviális; $n = 3$ esetén éppen az asszociativitás adja: $(a_1 a_2) a_3 = a_1 (a_2 a_3)$.

Tegyük fel, hogy minden n -nél rövidebb szorzatra igaz az állítás. Egy tetszőleges zárójelezés a legkülső műveletnél

$$\underbrace{(a_1 \cdots a_k)}_{\alpha} \underbrace{(a_{k+1} \cdots a_n)}_{\beta}, \quad 1 \leq k < n$$

alakú. Itt α egy k -tényezős ($1 \leq k \leq n-1$), β pedig egy $(n-k)$ -tényezős szorzat. Az indukciós feltevés miatt β megegyezik az utolsó $n-k$ tényezőből álló szorzat balra zárójelezett alakjával:

$$\beta = (((a_{k+1} a_{k+2}) a_{k+3}) \cdots a_{n-1}) a_n.$$

Legyen $\gamma = (((a_{k+1} a_{k+2}) a_{k+3}) \cdots a_{n-1})$ a β első $(n-1)$ elemének szorzata. Így

$$\alpha \beta = \alpha (((a_{k+1} a_{k+2}) a_{k+3}) \cdots a_{n-1}) a_n = \alpha (\gamma a_n).$$

Az asszociativitást alkalmazva azt kapjuk, hogy

$$\alpha\beta = (\alpha\gamma)a_n = (\alpha(a_{k+1}((a_{k+2}a_{k+3})\cdots a_{n-1})))a_n.$$

Végül az indukciós feltevést alkalmazzuk $\alpha\gamma = (\alpha(a_{k+1}((a_{k+2}a_{k+3})\cdots a_{n-1})))$ -re (ami $n-1$ tényezős), így

$$\alpha\beta = (((a_1a_2)a_3)\cdots a_{n-1})a_n.$$

Ezzel az indukciós lépést beláttuk, tehát minden zárójelezés eredménye megegyezik a balra zárójelezett szorzattal. $\square$

2.4. Tétel (Egységelem és inverz). *Legyen $\langle A, \cdot \rangle$ félcsoport.*

- (1) *Ha e balegység és f jobbegység, akkor $e = f$.*
- (2) *A -ban legfeljebb egy egységelem van.*
- (3) *Ha $a \in A$ -nak van bal- és jobbinverze az e egységelemre nézve, akkor ezek megegyeznek. Ekkor a -nak pontosan egy inverze van.*
- (4) *Ha minden $a \in A$ -nak van balinverze az e egységelemre nézve, akkor minden elemnek van jobbinverze is.*
- (4') *Ha minden $a \in A$ -nak van jobbinverze az e egységelemre nézve, akkor minden elemnek van balinverze is.*

Bizonyítás.

(1) Ha e balegység és f jobbegység, akkor

$$f \stackrel{e \text{ balegység}}{=} ef \stackrel{f \text{ jobbegység}}{=} e.$$

Tehát $e = f$.

(2) Ha e és f egységelemek, akkor e balegység, f jobbegység, ezért az előző (1) szerint $e = f$.

(4) Minden $a \in A$ -hoz válasszunk egy a_b balinverzet: $a_b a = e$. Az a_b -nek is van balinverze, jelöljük $(a_b)_b$ -vel. Ekkor a_b egyúttal jobbinverze is a -nak, mert

$$\begin{aligned} aa_b &= e(aa_b) \\ &= ((a_b)_b a_b)(aa_b) \\ &= (a_b)_b (a_b a) a_b \\ &= (a_b)_b e a_b = (a_b)_b a_b = e. \end{aligned}$$

(4') Hasonlóan, a szorzások sorrendjének megfordításával.

(3) Tegyük fel, hogy a_b az a balinverze, a_j pedig az a jobbinverze. Ekkor

$$a_j = ea_j = (a_b a) a_j = a_b (aa_j) = a_b e = a_b.$$

Ha a'_b egy másik balinverz, akkor ugyanígy $a'_b = a_j = a_b$; a jobbinverz egyértelműsége is hasonlóan adódik. $\square$

2.5. Megjegyzés.

1. Mátrixszorzásnál láttuk: egy négyzetes mátrix balinverze egyúttal jobbinverze is. Ez erősebb az előző állításnál.
2. Az előző tétel 3. és 4. pontjából együtt következik: ha egy monoid minden elemének van balinverze, akkor minden elemnek pontosan egy inverze van.
3. Megtörténhet, hogy egy monoidban egy elemnek nincs pl. jobbinverze, de végtelen sok balinverze van. Erre ad példát az alábbi konstrukció.

2.6. Példa (Függvények félcsoportha, egyoldali inverzek). Legyen

$$A = \{f : \mathbb{N} \longrightarrow \mathbb{N}\},$$

a művelet pedig a függvénykompozíció. Itt $\mathbb{N} = \{0, 1, 2, \dots\}$, és

$$(f \circ g)(a) = f(g(a)).$$

Érdemes megjegyezni, hogy a függvények kompozíciója általában is asszociatív művelet. Ezt gyorsan belátjuk, hogy igazoljuk: $\langle A, \circ \rangle$ egy félcsoportha. Legyen tehát $f, g, h \in A$ és $a \in \mathbb{N}$ tetszőleges. Ekkor

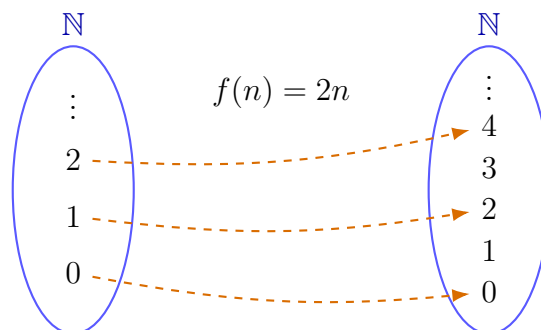
$$\begin{aligned} (f \circ (g \circ h))(a) &= f((g \circ h)(a)) = f(g(h(a))), \\ ((f \circ g) \circ h)(a) &= (f \circ g)(h(a)) = f(g(h(a))). \end{aligned}$$

Tehát $f \circ (g \circ h) = (f \circ g) \circ h$ (mert mint függvényeknek, minden pontban azonos a helyettesítési értékük). Sőt monoidot kapunk, mert az $\text{id}(x) = x$ identikus függvény egységelem.

Tekintsük az

$$f : \mathbb{N} \longrightarrow \mathbb{N}, \quad f(n) = 2n$$

függvényt.



f -nek nincs jobbinverze. Tetszőleges $g : \mathbb{N} \rightarrow \mathbb{N}$ esetén

$$R(f \circ g) \subseteq R(f) = \{0, 2, 4, \dots\}.$$

Így például $3 \notin R(f \circ g)$, ezért $f \circ g \neq \text{id}$. Tehát nem létezik g , amelyre $f \circ g = \text{id}$ teljesülne.

f -nek végtelen sok (pontosabban kontínuum sok) balinverze van. Legyen $g : \mathbb{N} \rightarrow \mathbb{N}$ olyan függvény, amelyre

$$g(n) = \begin{cases} n/2, & \text{ha } n \text{ páros,} \\ \text{tetszőleges } \mathbb{N}\text{-beli érték,} & \text{ha } n \text{ páratlan.} \end{cases}$$

A páratlan helyeken egymástól függetlenül, tetszőlegesen választhatjuk az értékeket. Minden ilyen g balinverze f -nek, ugyanis

$$(g \circ f)(n) = g(f(n)) = g(2n) = n \quad (n \in \mathbb{N}),$$

tehát $g \circ f = \text{id}$.

2.7. Megjegyzés. Az előző példában függvények alkotják a félcsoportot, és a művelet a kompozíció. Később a ?? tételben látni fogjuk: izomorfia erejéig minden félcsoport ilyen alakban is megadható.

3. Csoportok

3.1. Definíció. A $\mathcal{G} = \langle G, \cdot, ^{-1}, e \rangle$ algebra **csoport**, ha $\langle G, \cdot, e \rangle$ monoid, és minden $x \in G$ esetén $x^{-1}x = e$, vagyis x^{-1} az x balinverze.

3.2. Megjegyzés. A 2.4 Tétel (4) illetve (3) pontjai szerint, ha egy monoid minden elemének van balinverze, akkor a balinverz jobbinverz (tehát inverz) is, és ez az inverz egyértelmű. Csoportban tehát $x^{-1}x = xx^{-1} = e$.

A $\mathcal{G}$ csoport **Abel-csoport**, ha $\mathcal{G} \models xy = yx$.

Példák

1. $\langle \mathbb{Z}, +, -, 0 \rangle$;
2. $\langle \mathbb{Q}, +, -, 0 \rangle$;
3. $\langle \mathbb{R}, +, -, 0 \rangle$;
4. $\langle \mathbb{C}, +, -, 0 \rangle$.

Az első négy példa Abel-csoport. Abel-csoportok esetében gyakran alkalmaznak additív jelölést: a kétváltozós csoport-művelet jele $+$, az inverzé $-$, az egységelem pedig 0 .

5. Rögzített $m \geq 1$ esetén a modulo m maradékosztályok az összeadással: $\langle \mathbb{Z}_m, +, -, \bar{0} \rangle$.
6. A **kvaterniócsoport**:

$$Q_8 = \{1, i, j, k, -1, -i, -j, -k\}.$$

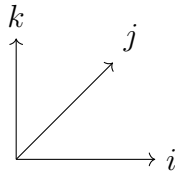
A szorzótábla $1, i, j, k$ elemekhez tartozó része:

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

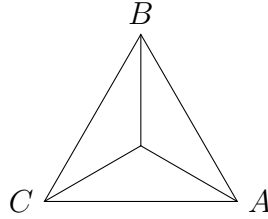
A további szorzatokat a szokásos előjelszabályok adják: pl.

$$(-1)a = a(-1) = -a.$$

Első ránézésre az sem világos, hogy ez csoport. Erre a ?? pontban visszatérünk. Az viszont világos, hogy ez a szorzás nem kommutatív, például $ij = k$, de $ji = -k$, stb. A fenti szorzótábla-részletet a térvektorok vektori szorzására gondolva lehet könnyen megjegyezni:



7. A **Diéder-csoport**: $n \geq 3$ esetén D_n a szabályos n -szög szimmetriáinak (önmagába vivő egybevágóságainak) csoportja. A művelet a kompozíció. Például D_3 a szabályos háromszög szimmetriacsoportja.



Az egybevágóságokat a csúcsok képeivel adjuk meg:

$$\text{identitás: } \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix};$$

$$\text{tükrözések: } \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}, \quad \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}, \quad \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix};$$

$$\text{nemtriviális forgatások: } \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}, \quad \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}.$$

Ezek a csúcsok 6 különböző permutációját adják. De 3 csúcsnak összesen 6 permutációja van, ezért $|D_3| = 3! = 6$, és $D_3 \cong \text{Sym}([3])$, ahol $[n] = \{1, \dots, n\}$. Általában $|D_n| = 2n$, míg $|\text{Sym}([n])| = n!$; $n \geq 4$ esetén nem izomorfak.

8. Tetszőleges A halmaz önmagába menő bijekciói a kompozícióval és a függvényinverzrel csoportot alkotnak. Ez a **szimmetrikus csoport**, jelölése $\text{Sym}(A)$. Véges A esetén ezeket a bijekciókat permutációknak is nevezzük (illetve végtelen halmaz sajátmagára vett bijekcióit is nevezhetjük permutációknak).
9. Rögzített $n \geq 1$ esetén az $\mathbb{R}^{n \times n}$ ortogonális mátrixai a mátrixszorzással és mátrixinvertálással csoportot alkotnak. Ezek is speciális egybevágóságok.
10. Egy adott struktúra (például gráf vagy algebra) automorfizmusai a kompozícióval és függvényinverzrel csoportot alkotnak. Ezek az egybevágóságok mintájára (a távolság megtartása helyett) él-tartóak, illetve művelet-tartóak.

Mit fogunk vizsgálni?

1. Csoportok felismerése más matematikai területeken: ahol szimmetria van, ott általában csoport is megjelenik.

2. A csoportok leírása, osztályozása.
3. A csoportelmélet önmaga által felvetett kérdései.

3.1. Részcsoportok

Legyen $\mathcal{G} = \langle G, \cdot, {}^{-1}, e \rangle$ csoport. Az 1.10 Definíció csoportokra vonatkozó speciális esete szerint a $\mathcal{H}$ csoport $\mathcal{G}$ részcsoporthja, ha $H \subseteq G$ és $\mathcal{H}$ műveletei $\mathcal{G}$ műveleteiből öröklődnek. Csoportok esetében is, $\mathcal{H} \leq \mathcal{G}$ azt jelöli, hogy $\mathcal{H}$ részcsoporthja (=részalgebrája) $\mathcal{G}$ -nek.

Ha a H részhalmaz zárt $\mathcal{G}$ műveleteire, akkor $\mathcal{G}$ műveletei H -ra vett megszorításaival $\mathcal{G}$ egy részcsoporthját kapjuk. Csoportok esetében a műveletekre való zártság vizsgálatára kínálkozik egy kényelmes mód; ennek ismertetésével folytatjuk.

3.3. Definíció. [Komplexusok] A G csoport részhalmazait **komplexusoknak** nevezzük; ezek összessége a $\mathcal{P}(G)$ hatványhalmaz. Ha $K, K_1, K_2 \subseteq G$, akkor

$$K^{-1} = \{a^{-1} : a \in K\}, \quad K_1 K_2 = \{ab : a \in K_1, b \in K_2\}.$$

$\mathcal{P}(G)$ a halmazszorzással monoidot alkot, egységeleme $\{e\}$.

3.4. Tétel (Részcsoporthkritériumok). *Legyen G csoport és $\emptyset \neq H \subseteq G$. A következő állítások ekvivalensek:*

- (1) $H \leq G$;
- (2) $HH = H$ és $H^{-1} = H$;
- (3) $H^{-1}H \subseteq H$;
- (4) minden $a, b \in H$ esetén $a^{-1}b \in H$.

Bizonyítás.

(1) $\Rightarrow$ (2): A szorzásra való zártság miatt $HH \subseteq H$. Mivel $e \in H$, ezért

$$H = H\{e\} \subseteq HH,$$

az előző két tartalmazás miatt tehát $HH = H$. Továbbá, az inverzképzésre való zártság miatt $H^{-1} \subseteq H$. Fordítva, ha $h \in H$, akkor $h^{-1} \in H$, így $h = (h^{-1})^{-1} \in H^{-1}$. Ez mutatja, hogy $H \subseteq H^{-1}$, amiből $H^{-1} = H$.

(2) $\Rightarrow$ (3): $H^{-1}H \stackrel{(2)}{=} HH \stackrel{(2)}{=} H \subseteq H$.

(3) $\Rightarrow$ (4): Ha $a, b \in H$, akkor $a^{-1}b \in H^{-1}H \subseteq H$.

(4) $\Rightarrow$ (1): A nemüresség miatt választható $a \in H$, így $e = a^{-1}a \in H$. Minden $a \in H$ esetén $a^{-1} = a^{-1}e \in H$, tehát H inverzképzésre zárt. Ha $a, b \in H$, akkor $a^{-1} \in H$, ezért $(a^{-1})^{-1}b = ab \in H$. Így H részcsoporth. $\square$

3.2. Mellékosztályok, Lagrange tétele

3.5. Definíció. Legyen $H \leq G$. Ekkor H

- bal oldali mellékosztályai az $aH = \{ah : h \in H\}$,
- jobb oldali mellékosztályai a $Ha = \{ha : h \in H\}$

alakú komplexusok, ahol $a \in G$.

3.6. Megjegyzés. A bal és jobb oldali mellékosztályok általában különböznek, erre láttunk példát a 3. gyakorlatra szánt feladatlap 4. feladatában.

A 3.3 Tétel (4) pontjában megjelenő feltétel szoros kapcsolatban áll a mellékosztályokkal is, ennek bemutatásával folytatjuk.

3.7. Tétel. Legyen $H \leq G$, és legyen

$$\varrho = \{\langle a, b \rangle \in G \times G : a^{-1}b \in H\}.$$

Ekkor:

- (1) ϱ ekvivalenciareláció;
- (2) $\langle a, b \rangle \in \varrho \iff aH = bH$;
- (3) minden $a \in G$ esetén a $\varphi_a : H \rightarrow aH$, $\varphi_a(x) = ax$ leképezés bijekció;
- (4) minden $a \in G$ esetén a $\psi_a : H \rightarrow Ha$, $\psi_a(x) = xa$ leképezés bijekció;
- (5) minden $a, b \in G$ esetén $|aH| = |H| = |Hb|$.

Bizonyítás.

(1) ϱ reflexív, mert $a^{-1}a = e \in H$. Ha $\langle a, b \rangle \in \varrho$, akkor $a^{-1}b \in H$, így mivel H zárt az inverzképzésre $(a^{-1}b)^{-1} = b^{-1}a \in H$; ezért ϱ szimmetrikus. Végül, ha $\langle a, b \rangle, \langle b, c \rangle \in \varrho$, akkor $(a^{-1}b) \in H$ és $(b^{-1}c) \in H$; mivel H zárt a szorzásra:

$$(a^{-1}b)(b^{-1}c) = a^{-1}c \in H,$$

vagyis $\langle a, c \rangle \in \varrho$; ezért ϱ tranzitív.

(2) Ha $\langle a, b \rangle \in \varrho$, akkor $a^{-1}b \in H$. Legyen $h_0 = a^{-1}b$. Ekkor $b = ah_0$, ezért minden $h \in H$ esetén

$$bh = a(h_0h) \in aH,$$

hiszen $h_0h \in H$. Tehát $bH \subseteq aH$. Az 1. pontban bizonyított szimmetria miatt $(b, a) \in \varrho$, így ugyanezzel az érveléssel $aH \subseteq bH$. Következésképpen $aH = bH$.

(3) A φ_a szürjektív az aH definíciója miatt. Injektív is, mert $ax = ay$ esetén $x = y$.

(4) Hasonlóan: ψ_a szürjektív a Ha definíciója miatt, és $xa = ya$ esetén $x = y$, tehát injektív.

(5) A 3. és 4. pont bijekcióiból következik. □

Ciklikus csoportok

3.8. Definíció. A G csoport **ciklikus**, ha egyetlen eleme generálja, azaz ha létezik $a \in G$, amelyre $\langle a \rangle = G$, ahol $\langle a \rangle$ az a által generált részcsoport. Az a elemet generátorelemnek nevezzük.

3.9. Példa. Az additív $\mathbb{Z}$ csoport ciklikus: $\langle 1 \rangle = \mathbb{Z}$. Jelölje $\mathbb{Z}_m$ az m szerinti maradékosztályok szokásos összeadásukkal vett csoportját. Rögzített $m \geq 1$ esetén $\mathbb{Z}_m$ is ciklikus. A következő tételben belátjuk, hogy nincs is más ciklikus csoport.

3.10. Tétel.

- (1) Ha G ciklikus, akkor $G \cong \mathbb{Z}$ vagy $G \cong \mathbb{Z}_m$ valamely $m \geq 1$ esetén.
- (2) Minden ciklikus csoport Abel-csoport.

Bizonyítás.

(1) Legyen $G = \langle a \rangle$ és $B = \{a^j : j \in \mathbb{Z}\}$. Ez a B tartalmazza a -t és e -t, továbbá zárt a szorzásra és inverzképzésre. Másrészt minden a -t tartalmazó részcsoport tartalmazza B -t, így $G = \langle a \rangle = B$.

Ha B végtelen, akkor a hatványok páronként különbözők. Ugyanis $a^i = a^j$, $i < j$ esetén $a^{j-i} = e$, így minden hatvány az $e, a, \dots, a^{j-i-1}$ elemek valamelyike lenne. Ezért a $\mathbb{Z} \rightarrow G$, $j \mapsto a^j$ leképezés bijektív, és $a^{i+j} = a^i a^j$ miatt izomorfizmus.

Ha B véges, akkor léteznek $i < j$ kitevők, amelyekre $a^i = a^j$, tehát $a^{j-i} = e$. Legyen k a legkisebb pozitív egész, amelyre $a^k = e$ és legyen $C = \{e, a, a^2, \dots, a^{k-1}\}$. Állítjuk, hogy

$$G = \langle a \rangle = C.$$

C inverzképzésre zárt: $e^{-1} = e$, és $1 \leq j < k$ esetén $(a^j)^{-1} = a^{k-j} \in C$. Szorzásra is zárt: ha $1 \leq i, j \leq (k-1)$, akkor osszuk $(i+j)$ -t maradékosan k -val $\rightsquigarrow$ van $q, r \in \mathbb{N}$, hogy $i+j = qk + r$, $0 \leq r < k$. Ekkor

$$a^i a^j = a^{i+j} = (a^k)^q a^r = a^r \in C.$$

Így C részcsoport, és tartalmazza a -t, tehát $\langle a \rangle \subseteq C$. A fordított tartalmazás nyilvánvaló, ezért $G = C$.

A felsorolt elemek páronként különbözők, mert $a^i = a^j$ és $0 \leq i < j < k$ esetén $a^{j-i} = e$ ellentmondana k minimalitásának. Így a $\varphi : \mathbb{Z}_k \rightarrow G$, $\varphi(j) = a^j$ leképezés bijektív és $a^{i+j} = a^i a^j$ miatt φ izomorfizmus.

(2) Az 1. pontból következik, hiszen az additív $\mathbb{Z}$ és $\mathbb{Z}_m$ csoportok kommutatívak. □

Elemrend és csoportrend

3.11. Definíció. Legyen G csoport és $a \in G$. Az a elem **rendje**

$$|a| = \begin{cases} \min\{k \in \mathbb{N}_{>0} : a^k = e\}, & \text{ha létezik ilyen } k, \\ \infty, & \text{különben.} \end{cases}$$

A G csoport **rendje** az alaphalmaz száma: $|G|$.

3.12. Tétel. Ha G véges csoport, akkor minden $a \in G$ elem rendje véges, és

$$|a| = |\langle a \rangle|.$$

Bizonyítás. Mivel $\langle a \rangle \leq G$, az $\langle a \rangle$ ciklikus csoport véges. Az előző, 3.10 Tétel bizonyításában láttuk, hogy ekkor létezik legkisebb $k > 0$, amelyre $a^k = e$, és

$$\langle a \rangle = \{e, a, \dots, a^{k-1}\}.$$

Ezek az elemek páronként különbözők, ezért $|\langle a \rangle| = k = |a|$. □

3.13. Tétel (Lagrange). Legyen G véges csoport.

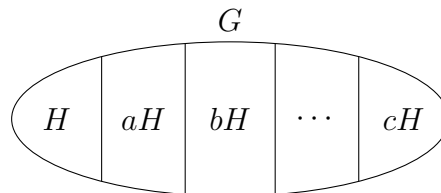
- (1) Ha $H \leq G$, akkor $|H| \mid |G|$.
- (2) Ha $a \in G$, akkor $|a| \mid |G|$.

Bizonyítás.

(1) A $\varrho = \{\langle a, b \rangle \in G \times G : a^{-1}b \in H\}$ reláció ekvivalenciareláció, és az a elem osztálya $a/\varrho = aH$. Legyen $T \subseteq G$ a ϱ egy reprezentánsrendszere: minden ekvivalencia-osztályból pontosan egy elemet tartalmazzon. Ekkor

$$|G| = \sum_{a \in T} |a/\varrho| = \sum_{a \in T} |aH| \stackrel{3.7(5) \text{ Tétel}}{=} \sum_{a \in T} |H| = |H| |T|,$$

tehát $|H| \mid |G|$.



(2) Egyrészt a 3.12 Tétel szerint $|a| = |\langle a \rangle|$. Másrészt, az előző (1) miatt $|\langle a \rangle| \mid |G|$. Tehát $|a| \mid |G|$. □

3.14. Definíció. Legyen G csoport, és legyen $H \leq G$. Ekkor a H részcsoporthoz G -beli **indexe** a H baloldali mellékosztályainak száma. Jelölése: $[G : H]$.

3.15. Megjegyzés. A 3.13 Tétel bizonyításának jelöléseivel $[G : H] = |T|$, így

$$|G| = |H| [G : H].$$

Eddig baloldali mellékosztályokra fókuszáltunk; ez az asszimetria zavaró lehet. Jobboldali mellékosztályokra ugyanezek az állítások érvényesek; azok száma is $[G : H]$. A jobboldali és baloldali mellékosztályok kapcsolatával sokat fogunk még foglalkozni, ??-ban megadunk egy módszert, amivel könnyen, és szinte automatikusan át lehet vinni állításainkat baloldali mellékosztályokról jobboldaliakra, illetve jobboldali mellékosztályokról baloldaliakra.

A Lagrange-tétel megfordítása

Felmerül a kérdés, hogy Lagrange tétele (a 3.13 Tétel) megfordítható-e: véges G és pozitív egész k esetén igaz-e, hogy:

$$k \mid |G| \stackrel{?}{\implies} \exists a \in G : |a| = k.$$

Ez általában nem igaz. A 3.2 megjegyzés alatti 7. példában láttuk, hogy a D_3 Diéder-csoport rendje 6, de nincsen neki 6-os rendű eleme:

- Az identitás rendje 1,
- a tükrözéseké 2,
- a nemtriviális forgatásoké 3.

Tehát $6 \mid |D_3|$ ellenére sincs 6-os rendű elem.

Prím osztókra viszont igaz a következő állítás.

3.16. Tétel (Cauchy). *Ha a p prímszám osztja a véges G csoport rendjét, akkor G -ben van p rendű elem.*

Cauchy előbbi tételét be fogjuk bizonyítani, de csak később, ???-ben.