

Absztrakt algebra I.

Csoportelmélet

Dr. TÓTH LÁSZLÓ egyetemi docens
Pécsi Tudományegyetem

2006

Bevezetés

Ez az anyag tartalmazza az „Algebra és számelmélet” című tárgy 4. féléves részének kötelező elméleti anyagát és a feldolgozandó feladatoknak a nagy részét. Tartalmaz továbbá olyan kiegészítő részeket is, amelyek nem kötelezőek, ezek ★ ★ jelek között szerepelnek. A feladatok előtt ▼ jel áll. A nehezebb feladatokat ▼▼ jelöli.

Az első, „Halmazok, relációk, függvények” című fejezetben azoknak a korábbiakban tanult algebrai alapfogalmaknak az áttekintése szerepel, amelyeket használni fogunk. Használni fogjuk továbbá a következő fogalmakat és az ezekre vonatkozó alaptulajdonságokat: logikai műveletek, számhalmazok, komplex számok, egész számok oszthatósága, legnagyobb közös osztó, legkisebb közös többszörös, maradékosztályok (mod n), Euler-függvény, mátrix, determináns.

A tételek, állítások és bizonyítások végét a □ jel mutatja.

Felhívom a figyelmet

- a definíciók pontos ismeretére (a fogalmak nevei **kövér betűkkel** szedettek),
- az egyes fogalmakra adott példákra (ezek általában • jel után szerepelnek); adjanak, keressenek további példákat az anyag jobb megértése érdekében,
- a Tételek pontos megfogalmazására és a bizonyításokra,
- a kitűzött feladatok megoldására.

További irodalom

1. Szendrei János, Algebra és számelmélet, Nemzeti Tankönyvkiadó, Budapest, 1996.
2. Szendrei Ágnes, Diszkrét matematika, Polygon, Szeged, 2000.
3. Fried Ervin, Általános algebra, Tankönyvkiadó, Budapest, 1981.
4. Fuchs László, Algebra, Tankönyvkiadó, Budapest, 1980.
5. Környei Imre, Algebra (Turán Pál előadásai alapján), Tankönyvkiadó, Budapest, 1974.

Feladatgyűjtemények

1. Varga Árpád, Absztrakt algebra feladatgyűjtemény, Tankönyvkiadó, Budapest, 1983.
2. Varga Árpád, Elemi matematika II. (feladatgyűjtemény), Algebrai struktúrák, PTE, 2000.
3. Bálintné Szendrei Mária, Czédli Gábor, Szendrei Ágnes, Absztrakt algebrai feladatok, Tankönyvkiadó, Budapest, 1988.

Online jegyzetek

1. Kiss E., Bevezetés az absztrakt algebraiba:
<http://www.cs.elte.hu/~ewkiss/bboard/algebrabook>
2. Marcus A., Algebra jegyzet:
http://math.ubbcluj.ro/~marcus/for_students/marcus_algebra.pdf
3. Pelikán J., Algebra:
<http://www.cs.elte.hu/~pelikan/algebra.html>

1. Halmazok, relációk, függvények

1.A. Halmazok

A **halmaz** bizonyos jól meghatározott dolgok (tárgyak, fogalmak), a halmaz **elemeinek** az összessége. Azt, hogy az a elem **hozzátartozik** az A halmazhoz így jelöljük: $a \in A$ (a eleme A -nak); $b \notin A$ jelentése: b nem eleme A -nak.

Egy halmazt egyértelműen meghatároznak az elemei. Egy halmazt megadhatunk úgy, hogy felsoroljuk az elemeit, pl. $A = \{1, 2, 3, 4\}$, $B = \{x, y, z\}$ vagy úgy, hogy megadunk egy, a halmaz x elemeire jellemző $T(x)$ tulajdonságot: $A = \{x | T(x)\} = \{x : T(x)\}$, pl. $A = \{x | x \in \mathbb{R} \text{ és } 0 \leq x \leq 3\}$.

Itt és a továbbiakban a számhalmazokra az alábbi jelöléseket használjuk:

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$ a természetes számok halmaza, $\mathbb{N}^* = \{1, 2, 3, \dots\} = \mathbb{N} \setminus \{0\}$ a nullától különböző természetes számok halmaza, $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ az egész számok halmaza, $\mathbb{Q} = \{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\}$ a racionális számok halmaza, $\mathbb{R}$ a valós számok halmaza, $\mathbb{C}$ a komplex számok halmaza. Továbbá $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, $2\mathbb{Z}$ a páros egészek halmaza, $2\mathbb{Z} + 1$ a páratlan egészek halmaza.

Az üres halmaz (egyetlen eleme sincs) jele: $\emptyset$. Az A és B halmazokat egyenlőknek nevezzük, ha ugyanazok az elemei, azaz $\forall x : x \in A \Leftrightarrow x \in B$, jel. $A = B$.

Az A halmaz **részhalmaza** a B halmaznak, ha A minden eleme B -nek is eleme, azaz $\forall x : x \in A \Rightarrow x \in B$, jel. $A \subseteq B$.

Jegyezzük meg, hogy $A = B$ akkor és csak akkor teljesül, ha $A \subseteq B$ és $B \subseteq A$.

Műveletek halmazokkal. Az A és B halmazok **metszete** a közös elemek összessége: $A \cap B = \{x | x \in A \text{ és } x \in B\}$. Ha $A \cap B = \emptyset$, akkor azt mondjuk, hogy A és B **diszjunkt** vagy **idegen halmazok**.

Az A és B halmazok **egyesítése** vagy **uniója** azoknak az elemeknek az összessége, melyek hozzátartoznak legalább az egyik halmazhoz: $A \cup B = \{x | x \in A \vee x \in B\}$.

Itt $\vee$ a "logikai vagy" művelet, $\wedge$ pedig a "logikai és" művelet.

Az $A \setminus B$ **különbség**halmaz az A olyan elemeinek a halmaza, melyek nem tartoznak a B -hez: $A \setminus B = \{x | x \in A \wedge x \notin B\}$.

Ha $A \subseteq E$, akkor $E \setminus A$ -t az A halmaz E -re vonatkozó **kiegészítő** vagy **komplementer halmazának** nevezzük, jelölés: $\complement_E(A)$. Ha E , neve **alaphalmaz**, rögzített, akkor a $\complement(A)$ vagy $\bar{A}$ jelöléseket is használjuk.

Az A és B halmazok **szimmetrikus különbsége** az $A \Delta B = (A \setminus B) \cup (B \setminus A)$ halmaz.

1.A.1. Tétel. Ha $A, B, C \subseteq E$ tetszőleges halmazok, akkor

- 1) $(A \cap B) \cap C = A \cap (B \cap C)$, $(A \cup B) \cup C = A \cup (B \cup C)$ (asszociativitás),
- 2) $A \cap B = B \cap A$, $A \cup B = B \cup A$ (kommutativitás),
- 3) $A \cap (A \cup B) = A$, $A \cup (A \cap B) = A$ (abszorbcio),
- 4) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (disztributivitás),
- 5) $A \cup \complement_E(A) = E$, $A \cap \complement_E(A) = \emptyset$,
- 6) $\complement(A \cap B) = \complement(A) \cup \complement(B)$, $\complement(A \cup B) = \complement(A) \cap \complement(B)$ (de Morgan képletek),
- 7) $A \cap A = A$, $A \cup A = A$,
- 8) $\complement(\complement(A)) = A$, $A \setminus B = A \cap \complement(B)$,
- 9) $A \Delta B = (A \cup B) \setminus (A \cap B)$,
- 10) $A \Delta B = B \Delta A$, $A \Delta \emptyset = A$, $A \Delta A = \emptyset$
- 11) $(A \Delta B) \Delta C = A \Delta (B \Delta C)$,
- 12) $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$. $\square$

Az A és B halmazok **Descartes-szorzatának** nevezzük az

$A \times B = \{(x, y) : x \in A \wedge y \in B\}$ halmazt. Itt (x, y) **rendezett elempárt** jelöl, ahol lényeges az elemek sorrendje: $(x, y) = (z, t)$ akkor és csak akkor, ha $x = z$ és $y = t$.

Ha A és B elemeinek a száma m , illetve n ($m, n \in \mathbb{N}^*$), akkor $A \times B$ elemeinek a száma mn .

1.A.2. Példa. • $A = \{1, 2, 3\}$, $B = \{a, b\}$ esetén $A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$.

Általánosan, az $A_1, A_2, \dots, A_n$ halmazok **Descartes-szorzata**: $A_1 \times A_2 \times \dots \times A_n = \{(x_1, x_2, \dots, x_n) : x_1 \in A_1 \wedge x_2 \in A_2 \wedge \dots \wedge x_n \in A_n\}$, ahol $(x_1, x_2, \dots, x_n)$ ún. **rendezett elem n -es**. Ha $A_1 = A_2 = \dots = A_n = A$, akkor jelölés: $A \times A \times \dots \times A = A^n$.

Például, $\mathbb{R}^2$ és $\mathbb{R}^3$ azonosítható a sík, illetve a tér pontjainak halmazával.

Az A halmaz részhalmazainak az összességét $\mathcal{P}(A)$ -val jelöljük: $\mathcal{P}(A) = \{B : B \subseteq A\}$, ez az A **hatványhalmaza**.

Ha A elemeinek a száma n ($n \in \mathbb{N}^*$), akkor a részhalmazok száma 2^n , azaz a hatványhalmaz 2^n elemből áll.

1.A.3. Feladatok. ▼ 1. Milyen A és B halmazokra igaz, hogy $A \setminus B = B \setminus A$?

▼ 2. Ha $A \cap C = \emptyset$, akkor igazoljuk, hogy $A \setminus (B \setminus C) = (A \setminus B) \setminus C$.

▼ 3. Határozzuk meg a következő halmaz elemeit:

$$A = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x^2 - (y + 1)^2 = 12\}.$$

▼ 4. Határozzuk meg a következő halmaz elemeit:

$$B = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x^2 + 2y^2 = 5\}.$$

▼ 5. Igazoljuk, hogy ha $A \cap C = B \cap C$ és $A \cup C = B \cup C$, akkor $A = B$.

▼ 6. Igazoljuk, hogy ha A, B, C, D tetszőleges halmazok, akkor:

a) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.

b) Az $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D)$ állítás nem igaz általában.

c) $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

d) $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$.

1.B. Relációk

Legyenek A és B tetszőleges halmazok. **Bináris relációnak**, röviden **relációnak** nevezzük a $\rho = (A, B, R)$ rendszert, ahol $R \subseteq A \times B$.

Itt az R halmaz a ρ **grafikonja**, jelölés: $(a, b) \in R \Leftrightarrow a\rho b$, olvasd: a ρ relációban van b -vel. Ellenkező esetben (a nincs ρ relációban b -vel) a jelölés: $(a, b) \notin R \Leftrightarrow a \not\rho b$.

Azt mondjuk, hogy ρ **homogén reláció**, ha $A = B$; ρ az **üres reláció**, ha $R = \emptyset$; ρ az **univerzális reláció**, ha $R = A \times B$.

Az A halmazon értelmezett **diagonális relációnak** nevezzük az $1_A = (A, A, \Delta_A)$, $\Delta_A = \{(a, a) : a \in A\}$ relációt. Itt $a1_A b \Leftrightarrow a = b$.

A ρ relációt gyakran azonosítjuk R grafikonjával, így $A \times B$ az univerzális reláció, $\emptyset$ az üres reláció, Δ_A pedig a diagonális reláció.

1.B.1. Példák. • 1) Legyen $A = \{a, b, c, d\}$, $B = \{1, 2\}$ és $\rho = (A, B, R)$, ahol $R = \{(a, 1), (a, 2), (b, 2), (c, 1)\}$. Itt például $a\rho 1$, $a\rho 2$ és $c \not\rho 2$.

• 2) Egy sík háromszögeinek A halmazában a hasonlósági reláció grafikonja $A \times A$ -nak az a részhalmaza, mely az egymással hasonló háromszögpárokból áll.

• 3) Az egész számok $\mathbb{Z}$ halmazán értelmezett oszthatósági reláció a következő homogén reláció: $\rho = (\mathbb{Z}, \mathbb{Z}, R)$, ahol $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a|b\} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : \exists c \in \mathbb{Z} : b = ac\}$.

★ • 4) Ha $A = \emptyset$ vagy $B = \emptyset$, akkor csak egy $\rho = (A, B, R)$ reláció értelmezhető, s ez az üres reláció, melynek grafikonja $R = \emptyset$. ★

Legyen $\rho = (A, B, R)$ egy reláció és $X \subseteq A$. A $\rho(X) = \{b \in B \mid \exists x \in X : x\rho b\}$ halmazt a ρ **reláció X részhalmazra vonatkozó metszetének** nevezzük. Itt $\rho(X) \subseteq B$. Ha $X = \{x\}$ egy egyelemű halmaz, akkor jelölés: $\rho(\{x\}) = \rho\langle x \rangle = \{b \in B : x\rho b\}$.

1.B.2. Példa. • Az 1.B.1/1. Példában adott relációra $\rho(\{a, b\}) = \{1, 2\}$, $\rho(\{c, d\}) = \{1\}$, $\rho\langle a \rangle = \{1, 2\}$, $\rho\langle d \rangle = \emptyset$.

A következő tulajdonságoknak kizárólag homogén relációk esetén van értelmük.

Legyen $\rho = (A, A, R)$ egy homogén reláció. Ekkor azt mondjuk, hogy ρ egy reláció az A halmazon és

a) ρ **reflexív**, ha minden $x \in A$ esetén $x\rho x$ ($\forall x \in A \Rightarrow x\rho x$), azaz „minden elem relációban van önmagával”;

b) ρ **transzitív**, ha minden $x, y, z \in A$, $x\rho y$ és $y\rho z$ esetén $x\rho z$ ($\forall x, y, z \in A : x\rho y \wedge y\rho z \Rightarrow x\rho z$), azaz „valahányszor, ha egy elem relációban van egy másik elemmel és ez utóbbi elem relációban van egy harmadikkal, akkor az első is relációban van a harmadikkal”;

c) ρ **szimmetrikus**, ha minden $x, y \in A$, $x\rho y$ esetén $y\rho x$ ($\forall x, y \in A : x\rho y \Rightarrow y\rho x$), azaz „valahányszor, ha egy elem relációban van egy másik elemmel, akkor ez utóbbi elem is relációban van az első elemmel”;

d) ρ **antiszimmetrikus**, ha minden $x, y \in A$, xpy és ypx esetén $x = y$ ($\forall x, y \in A : xpy \wedge ypx \Rightarrow x = y$), azaz „valahányszor, ha egy elem relációban van egy másik elemmel és ha ez utóbbi elem is relációban van az elsővel, akkor a két elem egyenlő”;

e) ρ **ekvivalenciareláció**, ha ρ reflexív, tranzitív és szimmetrikus;

f) ρ **rendezési reláció**, ha ρ reflexív, tranzitív és antiszimmetrikus. Ekkor (A, ρ) neve **rendezett halmaz**.

1.B.3. Példák. • 1) Az egész számok $\mathbb{Z}$ halmazán az oszthatósági reláció reflexív és tranzitív, de nem szimmetrikus és nem antiszimmetrikus, mert például $3 \mid -3$ és $-3 \mid 3$, de $-3 \nmid 3$.

• 2) Az $\mathbb{N}^*$ halmazon az oszthatóság rendezési reláció és $(\mathbb{N}^*, \mid)$ rendezett halmaz.

• 3) A $\mathbb{Z}$ halmazon az $a \equiv b \pmod{n} \Leftrightarrow n \mid a - b$ kongruencia reláció ekvivalenciareláció.

• 4) Az $(A, A, A \times A)$ univerzális reláció ekvivalenciareláció.

Ha ρ ekvivalenciareláció az A halmazon, akkor a $\rho(x) = \{y \in A : xpy\}$ metszeteket, ahol $x \in A$, **ekvivalenciaosztályoknak** nevezzük. Egy rögzített ekvivalenciaosztályba tartoznak az egymással relációban lévő elemek. Az ekvivalenciaosztályok egy-egy tetszőleges elemét **reprezentánsoknak** nevezzük. Azt mondjuk, hogy a kiválasztott elem **reprezentálja** a megfelelő ekvivalenciaosztályt. Az ekvivalenciaosztályok halmazát a ρ -hoz rendelt **faktorhalmaznak** nevezzük: $A/\rho = \{\rho(x) : x \in A\}$.

1.B.4. Példák. • 1) A $\mathbb{Z}$ halmazon az előbbi, $a \equiv b \pmod{n}$ kongruencia relációhoz rendelt faktorhalmaz: $\mathbb{Z}/\rho = \{\widehat{0}, \widehat{1}, \widehat{2}, \dots, \widehat{n-1}\}$, ahol $\widehat{k} = \{x \in \mathbb{Z} : x \equiv k \pmod{n}\} = \{\dots, k-2n, k-n, k, k+n, k+2n, \dots\}$.

2) Ha $n = 6$, akkor a $(\text{mod } 6)$ kongruencia relációhoz tartozó ekvivalenciaosztályok: $\widehat{0}, \widehat{1}, \widehat{2}, \widehat{3}, \widehat{4}, \widehat{5}$. A faktorhalmaz $\{\widehat{0}, \widehat{1}, \widehat{2}, \widehat{3}, \widehat{4}, \widehat{5}\}$. Az $\widehat{1}$ osztálynak például 1 egy reprezentánsa, de 7, 13, -5 is reprezentánsak.

3) $A/1_A = \{\{x\} : x \in A\}$ és $A/(A \times A) = \{A\}$.

Legyen A egy nemüres halmaz és legyen $(B_i)_{i \in I}$ az A részhalmazainak egy rendszere (itt I egy ún. indexhalmaz): $B_i \subseteq A$ minden $i \in I$ -re. Azt mondjuk, hogy $(B_i)_{i \in I}$ egy **osztályfelbontása** vagy **osztályozása** A -nak, ha

a) $B_i \neq \emptyset, \forall i \in I$,

b) $B_i \cap B_j = \emptyset, \forall i, j \in I, i \neq j$, azaz bármely két különböző részhalmaz diszjunkt,

c) $A = \cup_{i \in I} B_i$, azaz a $(B_i)_{i \in I}$ -beli részhalmazok uniója az adott A halmaz.

1.B.5. Példa. • Az $A = \{1, 2, 3, 4, 6\}$ halmaznak a $B_1 = \{1, 2\}, B_2 = \{3, 4\}, B_3 = \{5\}, B_4 = \{6\}$ részhalmazok egy osztályfelbontását adják.

A következő tétel azt mutatja, hogy az ekvivalenciarelációk és az osztályfelbontások kölcsönösen meghatározzák egymást. Ha ugyanis adott egy ekvivalenciareláció, akkor gyűjtsük össze az egymással relációban levő elemeket és egy osztályfelbontást kapunk. Ha pedig adott egy osztályfelbontás, akkor képezzük azt a relációt, mely szerint két elem relációban van, ha ugyanahhoz az osztályhoz tartoznak. Ez ekvivalenciareláció lesz. Pontosabban,

1.B.6. Tétel. Legyen A egy nemüres halmaz.

1) Ha ρ egy ekvivalenciareláció az A -n, akkor az $A/\rho = \{\rho(x) : x \in A\}$ faktorhalmaz egy osztályfelbontása A -nak.

2) Legyen $(B_i)_{i \in I}$ egy osztályfelbontása A -nak és értelmezzük a következő relációt: $\rho = (A, A, R)$, ahol $R = \cup_{i \in I} (B_i \times B_i)$, azaz $xpy \Leftrightarrow \exists i \in I : x, y \in B_i$ (x és y ugyanahhoz a B_i -hez tartoznak). Akkor ρ ekvivalenciareláció az A -n. $\square$

1.B.7. Feladatok. ▼ 1) Legyen $A = \{1, 2, 3, 4\}$.

a) Ha $\rho = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 1), (3, 2), (2, 3), (1, 3), (3, 1)\}$, határozzuk meg a megfelelő osztályfelbontást.

b) Ha $\pi = \{\{1, 2\}, \{3\}, \{4\}\}$, határozzuk meg a megfelelő ekvivalenciarelációt.

▼ 2. Az $\mathbb{N} \times \mathbb{N}$ halmazon a ρ relációt így definiáljuk: $(a, b) \rho (c, d) \Leftrightarrow a + d = b + c$.

Igazoljuk, hogy ρ ekvivalenciareláció.

▼ 3. A komplex számok halmazán tekintsük a ρ_1 és ρ_2 relációkat, ahol $z\rho_1 w \Leftrightarrow |z| = |w|$ és $z\rho_2 w \Leftrightarrow z = w = 0$ vagy $\arg z = \arg w$. Igazoljuk, hogy ρ_1 és ρ_2 ekvivalenciarelációk és ábrázoljuk grafikusan a $\mathbb{C}/\rho_1$ és $\mathbb{C}/\rho_2$ osztályokat.

▼ 4. Adjuk meg az összes ekvivalenciarelációt az $A = \{1, 2, 3\}$ halmazon.

▼ 5. Az A halmazon értelmezett ρ homogén reláció neve cirkuláris reláció, ha $\forall x, y, z \in A, x\rho y, y\rho z \Rightarrow z\rho x$. Igazoljuk, hogy ρ akkor és csak akkor ekvivalenciareláció, ha ρ reflexív és cirkuláris.

Útmutatás. Ha ρ reflexív és cirkuláris, akkor szimmetrikus, mert ha $x\rho y$, akkor $x\rho y, y\rho y$ (reflexivitás miatt) $\Rightarrow y\rho x$ és tranzitív, mert $x\rho y, y\rho z \Rightarrow z\rho x \Rightarrow x\rho z$ (szimmetria).

▼ 6. Hol a hiba a következőben? „Minden szimmetrikus és tranzitív ρ reláció reflexív. Bizonyítás: ha $x\rho y$, akkor a szimmetria miatt $y\rho x$, innen $x\rho y$ és $y\rho x$, tehát $x\rho x$, mert a reláció tranzitív.”

Útmutatás. Az állítás nem igaz. Adjunk ellenpéldát. A „bizonyításban” ott a hiba, hogy feltételeztük, hogy adott x -hez van olyan y , hogy relációban legyenek, ilyen y nem biztos, hogy létezik.

1.C. Függvények

Az $f = (A, B, F), F \subseteq A \times B$ relációt **függvénynek** (vagy leképezésnek) nevezzük, ha minden $a \in A$ esetén az $f\langle a \rangle$ metszet egyelemű részhalmaza B -nek. Ez azt jelenti, hogy az f függvény az A halmaz minden elemének megfelelteti a B halmaz egy és csak egy elemét.

Ha $f = (A, B, F)$ egy függvény, akkor A -t az f **értelmezési halmazának** vagy **értelmezési tartományának** nevezzük, jelölés $A = \text{dom } f$ (f doméniuma). A B halmaz az f **értékkészlete**, jelölés $B = \text{codom } f$ (f kodoméniuma), az $f(A)$ metszet az f függvény **értéktartománya** vagy **képe**, jelölés $f(A) = \text{Im } f$, F pedig a függvény grafikonja.

Ha $f = (A, B, F)$ egy függvény, akkor a következő jelöléseket használjuk:

$f : A \rightarrow B$ vagy $A \xrightarrow{f} B$. Ha $a \in A$, akkor az $f\langle a \rangle = \{b\}$ egyenlőséggel meghatározott $b \in B$ elem jelölése $b = f(a)$ vagy $a \mapsto b = f(a)$.

Megjegyzések. a) Az $f : A \rightarrow B$ és $f' : A' \rightarrow B'$ függvények akkor és csak akkor egyenlőek ($f = f'$), ha $A = A', B = B'$ és $f(a) = f'(a')$ minden $a \in A$ esetén.

b) Ha $f : A \rightarrow B$ egy függvény és $X \subseteq A, Y \subseteq B, y \in Y$, akkor $f(X) = \{b \in B \mid \exists x \in X : f(x) = b\} = \{f(x) : x \in X\}$ az X **részhalmaz képe** az f függvényben, $f^{-1}(Y) = \{a \in A \mid \exists y \in Y : f(a) = y\} = \{a \in A : f(a) \in Y\}$ az Y **inverz képe** f -ben, $Y = \{y\}$ esetén $f^{-1}(\{y\}) = f^{-1}(y) = \{a \in A : f(a) = y\}$, a függvény grafikonja pedig $F = \{(a, f(a)) : a \in A\}$.

1.C.1. Példák. • 1) A fenti 1. Példában szereplő reláció nem függvény, mert például $\rho\langle a \rangle = \{1, 2\}$ kételemű halmaz. A $\rho' = (A, B, R'), A = \{a, b, c, d\}, B = \{1, 2\}, R' = \{(a, 1), (b, 1), (c, 2), (d, 2)\}$ reláció függvény.

2) Bármely A halmaz esetén az $1_A = (A, A, \Delta_A)$ diagonális reláció egy függvény, ennek neve az A halmaz **identikus függvénye**: $1_A : A \rightarrow A, 1_A(a) = a$ minden $a \in A$ esetén.

Injektív, szürjektív és bijektív függvények. Legyen $f : A \rightarrow B$ egy függvény. Azt mondjuk, hogy

f **injektív**, ha A különböző elemeinek különböző képelemek felelnek meg, azaz, ha $\forall x_1, x_2 \in A, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$. Ez egyenértékű a következő állítással: $\forall x_1, x_2 \in A, f(x_1) = f(x_2) \Rightarrow x_1 = x_2$;

f **szürjektív**, ha B -nek minden eleme képelem, azaz, ha $\forall y \in B \exists x \in A : f(x) = y$. Ez a feltétel így is írható: $f(A) = B$;

f **bijektív**, ha injektív és szürjektív, azaz, ha $\forall y \in B \exists! x \in A$ (létezik egy és csak egy $x \in A$): $f(x) = y$.

1.C.2. Példák. • Az $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^2$ függvény nem injektív, mert pl. $-1 \neq 1$ és $f(-1) = f(1) = 1$ és nem is szürjektív, mert pl. $y = -1 \in \mathbb{R}$ esetén nem létezik $x \in \mathbb{R}$ úgy, hogy $f(x) = x^2 = -1$ legyen.

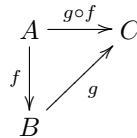
• A $g : [0, \infty) \rightarrow \mathbb{R}, g(x) = x^2$ függvény injektív és nem szürjektív,
 $h : [0, \infty) \rightarrow [0, \infty), h(x) = x^2$ pedig injektív és szürjektív, tehát bijektív.

• Bármely A halmaz esetén az 1_A identikus függvény bijektív.

Az $f : A \rightarrow B$ és a $g : B \rightarrow C$ függvényeknek ilyen sorrendben vett **összetétele** (vagy **kompozíciója** vagy **szorzata**) az a $g \circ f : A \rightarrow C$ függvény, amelyre $(g \circ f)(a) = g(f(a))$ minden $a \in A$ -ra. Ez az a leképezés, amelyet előbb az f majd a g leképezés egymásutáni végrehajtása révén kapunk.

A $g(f(x))$ függvényben a g -t külső, az f -et pedig belső függvénynek nevezzük.

Diagrammal szemléltetve:



1.C.3. Tétel. a) Ha $f : A \rightarrow B, g : B \rightarrow C, h : C \rightarrow D$ tetszőleges függvények, akkor

$$(h \circ g) \circ f = h \circ (g \circ f),$$

azaz a függvények szorzása asszociatív.

b) Minden $f : A \rightarrow B$ függvényre

$$f \circ \mathbf{1}_A = \mathbf{1}_B \circ f = f.$$

c) A függvények szorzása nem kommutatív.

Bizonyítás. a) A definíció alapján $(h \circ g) \circ f : A \rightarrow D$ és $h \circ (g \circ f) : A \rightarrow D$, tehát mindkét esetben A az értelmezési halmaz és D az értékkészlet, továbbá minden $a \in A$ -ra $((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$ és $(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$.

c) Legyen például $f, g : \mathbb{R} \rightarrow \mathbb{R}, f(x) = x + 3$ és $g(x) = x^2$. Akkor $(g \circ f)(x) = g(f(x)) = g(x + 3) = (x + 3)^2$ és $(f \circ g)(x) = f(g(x)) = f(x^2) = x^2 + 3$, ahonnan következik, hogy $g \circ f \neq f \circ g$. $\square$

Ha $f : A \rightarrow B$ egy bijektív függvény, akkor az f **inverz függvénye** az $f^{-1} : B \rightarrow A, f^{-1}(b) = a \Leftrightarrow f(a) = b$ függvény. Ekkor az f^{-1} függvény is bijektív és f^{-1} inverze az eredeti f függvény : $(f^{-1})^{-1} = f$. Igaz továbbá, hogy

$$f^{-1} \circ f = \mathbf{1}_A, \quad f \circ f^{-1} = \mathbf{1}_B.$$

1.C.4. Feladatok. ▼ 1. Határozzuk meg mindazokat az $f : \mathbb{R} \rightarrow \mathbb{R}$ függvényeket, amelyekre $2f(x) + 3f(1 - x) = 4x - 1, \forall x \in \mathbb{R}$.

Megoldás. x helyett $(1 - x)$ -et írva: $3f(x) + 2f(1 - x) = -4x + 3$, az eredetivel együtt ez egy egyenletrendszer. Kapjuk, hogy: $f(x) = -4x + 11/5$.

▼ 2. Határozzuk meg mindazokat az $f : \mathbb{R} \rightarrow \mathbb{R}$ függvényeket, amelyekre $f(x) - f(-x) = x^2, \forall x \in \mathbb{R}$.

Megoldás. $x = 1$ -re: $f(1) - f(-1) = 1, x = -1$ -re: $f(-1) - f(1) = 1$, ellentmondás, nincs ilyen függvény.

▼ 3. Igazoljuk, hogy $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = 2x^4 + 3x^3 + 4$ nem injektív függvény, $g : \mathbb{R} \rightarrow \mathbb{R}, g(x) = x^3 + x + 2$ pedig injektív függvény.

Megoldás. $f(x) = x^3(2x + 3) + 4$, itt $x^3(2x + 3) = 0$, ha $x = 0$ vagy $x = -3/2$, tehát $f(0) = f(-3/2) = 4$, f nem injektív.

Ha $g(x_1) = g(x_2)$, akkor $x_1^3 + x_1 = x_2^3 + x_2, (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2 + 1) = 0$, ahol a második zárójel $(x_1^2 + x_2^2)/2 + 3x_1x_2/4 + 1 \neq 0$, tehát $x_1 = x_2, g$ injektív.

▼ 4. Injektívek-e, szürjektívek-e, illetve bijektívek-e a következő függvények:

- a) $f : \{1, 2, 3\} \rightarrow \{a, b, c\}, f(1) = b, f(2) = c, f(3) = a;$
- b) $f : \mathbb{Z} \rightarrow \mathbb{Z}, f(x) = 2x + 1,$ c) $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = 2x + 1,$
- d) $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = 3x^2 + 4,$ e) $f : \mathbb{Z} \rightarrow \mathbb{Z}, f(x) = -x^2 + 4x.$
- f) $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^4 - 2x^2 + 3.$

▼ 5. Legyenek A és B egyenlő számosságú véges halmazok és legyen $f : A \rightarrow B$ egy függvény. Igazoljuk, hogy a következő állítások egyenértékűek:

- i) f injektív, ii) f szürjektív, iii) f bijektív.

▼ 6. Határozzuk meg az $f \circ g$ és $g \circ f$ összetett függvényeket, ahol

- a) $f, g : \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^2 + 1, g(x) = 3x + 1,$ b) $f, g : \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^3 - 2, g(x) = 1 - 2x,$
- c) $f, g : \mathbb{R} \rightarrow \mathbb{R}, f(x) = 2x - 1$ és $g(x) = x$, ha $x \leq 1, g(x) = x + 2$, ha $x > 0$.

▼ 7. A következő függvények közül melyeknek van inverze? Ha létezik inverz, adjuk meg!

- a) $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = x + 1,$ b) $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = 4x + 2,$

c) $f : \mathbb{N} \rightarrow \mathbb{N}$, $f(x) = 4x + 2$, d) $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^2 + 3$.

▼ 8. Legyen $f : A \rightarrow B$ egy függvény. Az A halmazon az $a_1 \rho a_2 \Leftrightarrow f(a_1) = f(a_2)$ előírással értelmezett ρ relációt az f **magjának** nevezzük, jelölés: $\rho = \ker f$.

Igazoljuk, hogy a) $\ker f$ egy ekvivalenciareláció az A hamazon,

b) f injektív $\Leftrightarrow \ker f = \mathbf{1}_A$,

Útmutatás. a) Azonnali, hogy a $\ker f$ reláció reflexív, szimmetrikus és tranzitív, mert az " $=$ " reláció is az.

b) Ha $f : A \rightarrow B$ egy tetszőleges függvény, akkor $\forall a_1, a_2 \in A : a_1 \mathbf{1}_A a_2 \Rightarrow a_1 = a_2 \Rightarrow f(a_1) = f(a_2) \Rightarrow a_1 \ker f a_2$. Továbbá, ha f injektív és $a_1 \ker f a_2$, akkor $f(a_1) = f(a_2)$, ahonnan $a_1 = a_2$, azaz $a_1 \ker f a_2$. Fordítva, ha $\forall a_1, a_2 \in A : a_1 \ker f a_2 \Rightarrow a_1 \mathbf{1}_A a_2$, akkor $\forall a_1, a_2 \in A : f(a_1) = f(a_2) \Rightarrow a_1 = a_2$ és következik, hogy f injektív.

▼ 9. Legyen $f : A \rightarrow B$ és $g : B \rightarrow C$ két függvény. Igazoljuk, hogy:

a) Ha f és g injektív (szürjektív), akkor $g \circ f$ is injektív (szürjektív).

b) Ha $g \circ f$ injektív (szürjektív), akkor f injektív (g szürjektív).

c) Ha $g \circ f$ injektív és f szürjektív, akkor g injektív.

d) Ha $g \circ f$ szürjektív és g injektív, akkor f szürjektív.

1.D. Halmazok számossága

Az A és B halmazokat **ekvivalens halmazoknak** nevezzük, ha létezik egy $f : A \rightarrow B$ bijektív függvény. Jelölés: $A \sim B$. Ez egy, a halmazokra vonatkozó reláció.

1.D.1. Tétel. $A \sim$ reláció egy ekvivalenciareláció.

Bizonyítás. Ha A egy tetszőleges halmaz, akkor az $\mathbf{1}_A : A \rightarrow A$, $\mathbf{1}_A(a) = a$ függvény bijektív, tehát $\sim$ reflexív. Ha $A \sim B$ és $B \sim C$, akkor léteznek az $f : A \rightarrow B$ és $g : B \rightarrow C$ bijektív függvények. Mivel $g \circ f : A \rightarrow C$ is bijektív, következik, hogy $A \sim C$, tehát $\sim$ tranzitív. Ha $f : A \rightarrow B$ bijektív, akkor $f^{-1} : B \rightarrow A$ is bijektív, tehát $\sim$ szimmetrikus. □

Az A halmaz ekvivalenciaosztályát az A **számosságának** vagy **kardinális számának** nevezzük. Jelölés: $|A| = \{B : A \sim B\}$.

Bármely halmazt összehasonlíthatunk olyan halmazokkal, amelyek elemei természetes számok. Azt mondjuk, hogy az A halmaz **véges** és n számosságú, ahol $n \in \mathbb{N}^*$, ha A ekvivalens az $\{1, 2, 3, \dots, n\}$ halmazzal: $A \sim \{1, 2, 3, \dots, n\}$, vagy ha $A = \emptyset$. Jelölés: $|A| = n, n \in \mathbb{N}^*, |\emptyset| = 0$. Egy halmaz **végtelen**, ha nem véges.

Az $\mathbb{N}$ halmaz végtelen, számossága $|\mathbb{N}| = \aleph_0$ (alef null), itt $\aleph$ a héber ábécé első betűje.

Az $\aleph_0$ számosságú halmazokat **megszámlálhatóan végtelen halmazoknak** nevezzük. Így egy A halmaz akkor és csak akkor megszámlálhatóan végtelen, ha létezik egy $f : \mathbb{N} \rightarrow A$ bijektív függvény. Ez azt jelenti, hogy az A halmaz elemei egy végtelen sorozatba rendezhetők, amelyben nincs ismétlődés, azaz A felírható $A = \{a_1, a_2, \dots, a_n, \dots\}$ alakban.

Például az egész számok $\mathbb{Z}$ halmaza megszámlálható, mert $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, 4, -4, \dots\}$, itt

$$f : \mathbb{N} \rightarrow \mathbb{Z}, \quad f(n) = \begin{cases} 0, & \text{ha } n = 0, \\ \frac{n+1}{2}, & \text{ha } n \text{ páratlan,} \\ -\frac{n}{2}, & \text{ha } n \text{ páros,} \end{cases}$$

bijektív függvény.

A racionális számok $\mathbb{Q}$ halmaza is megszámlálható. A valós számok $\mathbb{R}$ halmaza nem megszámlálható.

1.D.2. Tétel. Legyen A egy véges halmaz és $f : A \rightarrow A$ egy függvény. Akkor egyenértékűek a következő állítások:

1) f injektív,

2) f szürjektív,

3) f bijektív.

Bizonyítás. A definíciók alapján azonnali, hogy 3) $\Rightarrow$ 1) és 3) $\Rightarrow$ 2).

1) $\Rightarrow$ 3) A véges halmaz, legyen $A = \{a_1, a_2, \dots, a_n\}$. Az f függvény injektív, ezért $f(A) = \{f(a_1), f(a_2), \dots, f(a_n)\}$, ahol $f(a_i) \neq f(a_j)$ ha $i \neq j$. Így az $f(A)$ halmaz n -elemű és mivel $f(A) \subseteq A$ következik, hogy $f(A) = A$, azaz f szürjektív, tehát bijektív.

2) $\Rightarrow$ 3) Legyen $A = \{a_1, a_2, \dots, a_n\}$. Az f függvény szürjektív, ezért $f(A) = A$, innen $|f(A)| = |A| = n$. Ha az $f(a_1), f(a_2), \dots, f(a_n)$ elemek nem lennének páronként különbözőek, akkor az $f(A) = \{f(x) : x \in A\}$ halmaz elemeinek a száma n -nél kisebb lenne: $|f(A)| < n$, ami ellentmond az $|f(A)| = n$ feltételnek. $\square$

1.D.3. Feladatok. ▼ 1. Határozzuk meg a következő halmaz elemeinek a számát:

$$C = \{(x, y) \in \mathbb{N}^* \times \mathbb{N}^* \mid 2x + 3y = 2000\}.$$

▼ 2. Ha A, B, C tetszőleges véges halmazok, akkor

a) $|A \cup B| = |A| + |B| - |A \cap B|,$

b) $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$

Általánosítás.

▼ 3. Legyenek A és B véges halmazok, $|A| = k$, $|B| = n$.

a) Hány $f : A \rightarrow B$ függvény van ?

b) Hány $f : A \rightarrow B$ injektív függvény van ?

c) Ha $k = n$, akkor hány bijektív függvény van ?

Megoldás. a) n^k , b) ha $k \leq n$, akkor $n(n-1)(n-2) \cdots (n-k+1)$, c) $n! = n(n-1)(n-2) \cdots 2 \cdot 1$.

▼ 4. Mutassuk meg, hogy $\mathbb{N}^* \times \mathbb{N}^* \sim \mathbb{N}^*$.

Útmutatás. Tekintsük az $f : \mathbb{N}^* \times \mathbb{N}^* \rightarrow \mathbb{N}^*$, $f(m, n) = 2^{m-1}(2n-1)$ függvényt. Igazoljuk, hogy f bijektív.

2. Algebrai műveletek

2.A. Algebrai műveletek

Legyen S egy nemüres halmaz és $\varphi : S \times S \rightarrow S$, $(x, y) \mapsto \varphi(x, y)$ egy függvény. φ -t az S halmazon értelmezett **(algebrai) műveletnek** nevezzük és azt mondjuk, hogy (S, φ) egy **grupoid**. Jelölés: $\varphi(x, y) = x * y$ (vagy $x \circ y$, $x \Delta y$, stb.), a grupoid pedig $(S, *)$ (vagy $(S, \circ)$, (S, Δ) , stb.).

2.A.1. Példák. • $(\mathbb{Z}, +)$, $(\mathbb{R}, \cdot)$, $(2\mathbb{Z}, +)$ grupoidok, ahol "+" és "." a szokásos összeadás, illetve szorzás,

• $(\mathbb{N}, -)$ és $(2\mathbb{Z} + 1, +)$ nem grupoidok, itt "-" nem művelet az $\mathbb{N}$ halmazon, mert pl. $3 - 7 = -4 \notin \mathbb{N}$.

Ha egy halmazon legalább egy algebrai műveletet értelmezünk, akkor **algebrai struktúráról** beszélünk. Pl. a grupoid, a félcsoport és a csoport egyműveletes algebrai struktúrák, a gyűrű és a test kétműveletes algebrai struktúrák.

Ha $\varphi(x, y) = x * y$ egy tetszőleges művelet, akkor ezt gyakran **multiplikatív írásmóddal** jelöljük: $\varphi(x, y) = x \cdot y = xy$, amelyet az x és y **szorzatának** nevezzük, itt x és y a szorzat **tényezői**.

Használatos az **additív írásmód** is: $\varphi(x, y) = x + y$ és ezt az x és y **összegének** nevezzük, itt x és y az összeg **tagjai**.

2.A.2. Feladat. ▼ Algebrai struktúrát alkot-e

i) $\mathbb{N}$ a szorzásra nézve ii) $\{2n + 1 : n \in \mathbb{N}\}$ az összeadásra nézve

iii) $2\mathbb{Z}$ az összeadásra nézve iv) $\mathbb{R}^*$ az osztásra nézve.

v) $\mathbb{Z}$ az $x * y = \frac{x-1}{y^2+1}$ megfeleltetéssel.

2.B. Asszociativitás, kommutativitás, félcsoport. Az S halmazon értelmezett $*$ művelet **asszociatív**, ha minden $x, y, z \in S$ esetén $(x * y) * z = x * (y * z)$. Ekkor $(S, *)$ neve **félcsoport**.

2.B.1. Példák. • $(\mathbb{Z}, +)$, $(\mathbb{R}, \cdot)$ félcsoportok,

• $\mathbb{Z}$ -n a kivonás művelet: $\forall x, y \in \mathbb{Z} : x - y \in \mathbb{Z}$, de "-" nem asszociatív, mert pl. $(3 - 7) - 1 = -5 \neq -3 = 3 - (7 - 1)$.

Az S halmazon értelmezett $*$ művelet **kommutatív**, ha minden $x, y \in S$ esetén $x * y = y * x$. Ha az S -en értelmezett $*$ művelet kommutatív, akkor $(S, *)$ neve **kommutatív grupoid**. Ha az S -en értelmezett $*$ művelet asszociatív és kommutatív, akkor $(S, *)$ neve **kommutatív félcsoport**.

2.B.2. Példák. • $(\mathbb{Z}, +)$, $(\mathbb{R}, \cdot)$ kommutatív félcsoportok,

• nem kommutatív műveletek pl. a mátrixok szorzása és a függvények összetétele (kompozíciója), pontosabban pl. a 2×2 -es $\mathbb{Z}$ -beli elemekből álló mátrixok $\mathcal{M}_{\in}(\mathbb{Z})$ halmazán a szorzás nem kommutatív, de speciális mátrixhalmazokon a szorzás lehet kommutatív, lásd 2.B.3/ 1. Feladat.

2.B.3. Feladatok. ▼ 1. Igazoljuk, hogy az

$$S = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \in \mathbb{Z} \right\},$$

halmaz a mátrixok szorzásával kommutatív félcsoport.

▼ 2. Mutassuk meg, hogy

a) az $\mathbb{N}^*$ halmazon az $x * y = x^y$ művelet nem kommutatív és nem asszociatív,

b) az $S = [0, \infty)$ halmazon az $x * y = \frac{x+y}{2}$ művelet nem asszociatív, de kommutatív,

c) az $S = (0, \infty)$ halmazon az $x * y = x^{\ln y}$ művelet kommutatív és asszociatív.

2.C. Általánosított asszociativitás és kommutativitás. A következő két tételben a multiplikatív írásmódot használjuk.

2.C.1. Tétel. (általánosított asszociativitás) Ha "." egy, az S halmazon értelmezett asszociatív művelet, $n \in \mathbb{N}$, $n \geq 1$ és $a_1, a_2, \dots, a_n \in S$, akkor az $a_1 a_2 \dots a_n$ szorzat értéke nem függ a zárójelvezéstől, csak a tényezők sorrendjétől függ.

★ **Bizonyítás.** Azt mutatjuk meg, hogy minden szorzat egyenlő a

$$b = (\dots((a_1 a_2) a_3) a_4 \dots) a_n$$

szorzattal.

n -szerinti indukcióval bizonyítunk. Ha $n = 1$ vagy $n = 2$, akkor ez evidens, $n = 3$ -ra pedig következik az asszociativitásból. Tegyük fel, hogy $n \geq 4$, s hogy ez a tulajdonság igaz minden k tényező szorzatra, ahol $k < n$.

Egy tetszőleges szorzat $b_1 b_2$ alakú, ahol b_1 az $a_1, a_2, \dots, a_m$ elemeknek ebben a sorrendben vett szorzata, b_2 pedig az $a_{m+1}, a_{m+2}, \dots, a_n$ elemeknek ebben a sorrendben vett szorzata valamely m -re, ahol $1 \leq m \leq n-1$. Például, ha $n = 4$, akkor $(a_1 a_2)(a_3 a_4)$ esetén $m = 2$, $(a_1(a_2 a_3))a_4$ esetén pedig $m = 3$.

Ha $m = n-1$, akkor az indukciós feltétel miatt

$$b_1 = (\dots((a_1 a_2) a_3) \dots) a_{n-1}, \quad b_2 = a_n, \quad b_1 b_2 = b.$$

Ha $1 \leq m \leq n-2$, akkor b_1 -re és b_2 -re is alkalmazzuk az indukciós feltételt, majd az asszociativitást:

$$\begin{aligned} b_1 b_2 &= ((\dots((a_1 a_2) a_3) \dots) a_m) ((\dots((a_{m+1} a_{m+2}) a_{m+3}) \dots) a_n) = \\ &= (((\dots((a_1 a_2) a_3) \dots) a_m) ((\dots((a_{m+1} a_{m+2}) a_{m+3}) \dots) a_{n-1})) a_n. \end{aligned}$$

Most az a_n előtti tényezőkre használva ismét a feltételt ($k = n-1$), kapjuk, hogy

$$b_1 b_2 = (\dots((a_1 a_2) a_3) \dots) a_n = b,$$

azaz a tulajdonság igaz $k = n$ -re. $\square \star$

2.C.2. Tétel. (általánosított kommutativitás) Ha „ $\cdot$ ” egy, az S halmazon értelmezett asszociatív és kommutatív művelet, $n \in \mathbb{N}, n \geq 1$ és $a_1, a_2, \dots, a_n \in S$, akkor az $a_1 a_2 \dots a_n$ szorzat értéke nem függ a tényezők sorrendjétől.

Bizonyítás. Ezt is indukcióval lehet bizonyítani. Itt csak arra hivatkozunk, hogy egy adott szorzatból kiindulva a tényezők tetszőleges sorrendjéhez (permutációjához) eljuthatunk szomszédos elemek cseréjének egymás utáni alkalmazásával, s használva az általánosított asszociativitást. Pl. $n = 4$ -re

$$a_1 a_2 a_3 a_4 = a_1 (a_2 a_3) a_4 = a_1 (a_3 a_2) a_4 = (a_1 a_3) a_2 a_4 = (a_3 a_1) a_2 a_4 = a_3 a_1 a_2 a_4 = \dots \square$$

2.D. Semleges elem

Legyen $(S, *)$ egy grupoid. Az $e_b \in S$ elem **bal oldali semleges elem**, ha minden $x \in S$ esetén $e_b * x = x$. Az $e_j \in S$ elem **jobb oldali semleges elem**, ha minden $x \in S$ esetén $x * e_j = x$. Továbbá $e \in S$ elem **(kétoldali) semleges elem** vagy **neutrális elem**, ha minden $x \in S$ esetén $e * x = x * e = x$.

2.D.1. Példák. $\bullet$ $(\mathbb{Z}, +)$ -ban $e = 0$ semleges elem, $(\mathbb{R}, \cdot)$ -ban $e = 1$ semleges elem,

$\bullet$ Legyen $S = \{a, b, c, d\}$ és $x * y = x$, $\forall x, y \in S$, itt S minden eleme jobb oldali semleges elem és bal oldali semleges elem nem létezik.

2.D.2. Tétel. Ha $(S, *)$ egy grupoid és létezik egy $e_b \in S$ bal oldali semleges elem és létezik egy $e_j \in S$ jobb oldali semleges elem, akkor $e_b = e_j = e$ semleges elem.

Bizonyítás. Feltétel szerint minden $x \in S$ -re $e_b * x = x$ és minden $y \in S$ -re $y * e_j = y$. Legyen $x = e_j$ és $y = e_b$, akkor $e_b * e_j = e_j$, $e_b * e_j = e_b$, ahonnan $e_b = e_j$. $\square$

Innen azonnali, hogy

2.D.3. Következmény. Ha egy grupoidban létezik semleges elem, akkor az egyértelműen meghatározott (ezért ekkor „ e ” semleges elemről beszélünk). $\square$

Multiplikatív írásmód esetén a semleges elem neve **egységelem**, ezt e -vel vagy 1-gyel jelöljük, additív írásmód esetén a semleges elem neve **zéruselem**, ennek jelölése 0.

Az egységelemes félcsoporthot sok szerző **monoidnak** nevezi.

2.D.4. Feladat. $\blacktriangledown$ Az $\mathbb{R}$ halmazon tekintsük az $x * y = x + y + xy$ műveletet. Igazoljuk, hogy ez a művelet asszociatív, kommutatív és rendelkezik semleges elemmel.

Igazoljuk, hogy „ $*$ ” művelet az $[-1, \infty)$ halmazon, azaz $\forall x, y \in [-1, \infty) \Rightarrow x * y \in [-1, \infty)$.

2.E. Szimmetrikus elem. Legyen $(S, *)$ egy egységelemes (semleges elemes) grupoid, az egységelem e . Az $x \in S$ elemnek $x'_b \in S$ **bal oldali szimmetrikusa**, ha $x'_b * x = e$, az $x \in S$ elemnek $x'_j \in S$ **jobb oldali szimmetrikusa**, ha $x * x'_j = e$ és x -nek $x' \in S$ **szimmetrikusa**, ha $x' * x = x * x' = e$. Ha x -nek létezik szimmetrikusa, akkor azt mondjuk, hogy x **szimmetrizálható**.

2.E.1. Példák. $\bullet$ $(\mathbb{Z}, +)$ -ban minden x szimmetrizálható és $x' = -x$, $(\mathbb{R}, \cdot)$ -ban az egységelem az $e = 1$ és minden $x \neq 0$ szimmetrizálható: $x' = x^{-1} = 1/x$, $x = 0$ nem szimmetrizálható,

- Ha $(S, *)$ egységelemes grupoid, akkor az e egységelem szimmetrizálható és szimmetrikusa önmaga: $e' = e$,
- Legyen $S = \{e, a, b\}$ és egy $*$ művelet, amelynek műveletábrája, ún. **Cayley-féle művelet-táblája**:

$*$	e	a	b
e	e	a	b
a	a	e	e
b	b	e	a

Itt e a semleges elem és a művelet kommutatív, mert a műveletábra szimmetrikus a főátlóra nézve, továbbá $a * a = e$, $a * b = b * a = e$, tehát a -nak a is és b is szimmetrikusa.

2.E.2. Tétel. Ha $(S, *)$ egy egységelemes félcsoporthoz (a művelet asszociatív) és az $x \in S$ elemnek létezik x'_b bal oldali szimmetrikusa és létezik x'_j jobb oldali szimmetrikusa, akkor $x'_b = x'_j = x'$ az x szimmetrikusa.

Bizonyítás. Feltétel szerint

$$x'_b = x'_b * e = x'_b * (x * x'_j) = (x'_b * x) * x'_j = e * x'_j = x'_j. \quad \square$$

2.E.3. Következmény. Ha egy egységelemes félcsoporthoz egy elemnek létezik szimmetrikusa, akkor az egyértelműen meghatározott. $\square$

Multiplikatív írásmód esetén a szimmetrikus elem neve **inverz elem**, ezt x^{-1} -nel jelöljük, s azt mondjuk, hogy x **invertálható**, additív írásmód esetén a szimmetrikus elem neve **ellentett elem**, ennek jelölése $-x$.

Az előbbi példában a művelet nem asszociatív, pl. $(b * b) * a = a * a = e$ és $b * (b * a) = b * e = b$, ezért fordulhat elő, hogy egy adott elemnek két szimmetrikusa is van.

2.E.4. Tétel. Ha $(S, *)$ egy egységelemes félcsoporthoz és $x, y \in S$ invertálhatók, akkor az $x * y$ elem is invertálható és $(x * y)' = y' * x'$, továbbá $(x')' = x$.

Bizonyítás.

$$(y' * x') * (x * y) = y' * (x' * x) * y = y' * e * y = y' * y = e,$$

$$(x * y) * (y' * x') = x * (y * y') * x' = x * e * x' = x * x' = e. \quad \square$$

Multiplikatív írásmóddal: $(xy)^{-1} = y^{-1}x^{-1}$, $(x^{-1})^{-1} = x$. Ha kommutatív a művelet, akkor $(xy)' = x'y'$, de nem kommutatív esetben lényeges a sorrend.

2.E.5. Feladat. ▼ Legyen $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Igazoljuk, hogy $(\mathbb{Z}[i], \cdot)$ kommutatív egységelemes félcsoporthoz. Melyek az invertálható elemek?

Válasz: $\pm 1, \pm i$, mert ha $z = a + bi \in \mathbb{Z}[i]$, akkor $z^{-1} = \frac{1}{z} = \frac{1}{a+bi} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$, itt $a, b \neq 0$ esetén $|a| < a^2 + b^2$, $|b| < a^2 + b^2$ és ekkor $z^{-1} \notin \mathbb{Z}[i]$. Ha $a = 0$, akkor $z^{-1} = -\frac{1}{b}i \in \mathbb{Z}[i]$ alapján $b = \pm 1$, hasonlóan, ha $b = 0$.)

2.F. Elem hatványai

Legyen $(S, \cdot)$ egy egységelemes félcsoporthoz és $x \in S$. Értelmezzük x **hatványait**:

$$x^1 = x, x^2 = x \cdot x, \dots, x^{n+1} = x^n \cdot x, \quad n \in \mathbb{N}, n \geq 1, \quad x^0 = e.$$

Azonnali, hogy $x^n x^m = x^{n+m}$ és $(x^n)^m = x^{nm}$ minden $n, m \in \mathbb{N}$ esetén.

2.F.1. Tétel. Ha az $(S, \cdot)$ egységelemes félcsoporthoz az $x \in S$ elem invertálható akkor x^n is invertálható minden $n \in \mathbb{N}$ -re és

$$(x^n)^{-1} = (x^{-1})^n.$$

Bizonyítás.

$$x^n (x^{-1})^n = \underbrace{xx \dots x}_n \underbrace{x^{-1} x^{-1} \dots x^{-1}}_n = \underbrace{xx \dots x}_{n-1} \underbrace{(xx^{-1})}_{=e} \underbrace{x^{-1} \dots x^{-1}}_{n-1} = \dots = e. \quad \square$$

Additív jelöléssel:

$$1x = x, 2x = x + x, \dots, (n+1)x = nx + x, \quad n \in \mathbb{N}, n \geq 1, \quad 0x = 0, \quad -(nx) = n(-x).$$

★ 2.G. Kongruenciareláció félcsoporthban

Legyen $(S, \cdot)$ egy félcsoporth és ρ egy ekvivalenciareláció S -en. Azt mondjuk, hogy ρ egy **kongruenciareláció** S -en, ha ρ kompatibilis a félcsoporthbeli művelettel, azaz

$$\forall x, x', y, y' \in S : \quad x\rho x', \quad y\rho y' \Rightarrow xy\rho x'y'$$

(a ρ szerinti kongruenciák összesorozhatók).

2.G.1. Példa. • $(\mathbb{R}, \cdot)$ félcsoporth és az „=” egy kongruenciareláció.

S -nek egy ρ kongruenciarelációhoz tartozó osztályozását, vagyis az S/ρ faktorhalmazt **kompatibilis osztályozásnak** nevezzük.

Ha $(S, \cdot)$ egy félcsoporth és $X, Y \subseteq S$, jelölje $XY = \{xy : x \in X, y \in Y\}$.

2.G.2. Tétel. Legyen ρ egy ekvivalenciareláció az S félcsoporthon. Akkor egyenértékűek a következő állítások:

- a) ρ kongruenciareláció,
- b) $\forall X, Y \in S/\rho \Rightarrow \exists Z \in S/\rho : XY \subseteq Z$.

Bizonyítás. A definíció alapján. Részletezve:

”a) $\Rightarrow$ b)” Legyenek tetszőleges $X, Y \in S/\rho$ és legyenek $x \in X, y \in Y$ tetszőleges reprezentánsok, azaz $X = \rho\langle x \rangle, Y = \rho\langle y \rangle$.

Legyen $Z = \rho\langle xy \rangle$ az xy osztálya. Akkor $\forall x' \in X, y' \in Y \Rightarrow x\rho x', y\rho y' \Rightarrow xy\rho x'y' \Rightarrow x'y' \in \rho\langle xy \rangle = Z$, azaz $XY \subseteq Z$.

”b) $\Rightarrow$ a)” Legyen $\forall x, x', y, y' \in S : \quad x\rho x', \quad y\rho y'$. Jelölje $X = \rho\langle x \rangle = \rho\langle x' \rangle$ és $Y = \rho\langle y \rangle = \rho\langle y' \rangle$. Feltétel szerint létezik $Z = \rho\langle z \rangle \in S/\rho$ úgy, hogy $XY \subseteq Z$.

Akkor $xy \in XY \subseteq Z, x'y' \in XY \subseteq Z$. Tehát $xy\rho z, x'y'\rho z \Rightarrow xy\rho x'y'$. □

2.G.3. Feladat. ▼ Ha $(S, \cdot)$ egy félcsoporth és ρ egy kongruenciareláció S -en, akkor

$\forall x, x', y \in G : x\rho x' \Rightarrow xy\rho x'y, \quad yx\rho yx'$ (egy kongruenciát lehet szorozni jobbról ill. balról egy tetszőleges elemmel).

Megoldás. Ha $x\rho x'$, akkor mivel $y\rho y$ (reflexivitás) következik, hogy $xy\rho x'y$ és $yx\rho yx'$. ★

A továbbiakban a grupoidokkal és félcsoporthokkal részletesebben nem foglalkozunk. A csoport fogalmát a következő szakaszban adjuk meg. A csoport már elég általános ahhoz, hogy a matematika legkülönbözőbb területein fellelhető legyen, másrészt elég speciális, hogy a csoportokról általában, vagy az egyes csoporttípusokról mélyreható eredmények legyenek levezethetők.

2.H. Feladatok

▼ 1. Adott $A = \{1, -1, i, -i\}$. Igazoljuk, hogy a szorzás művelet az A halmazon. Készítsük el a művelet táblát.

▼ 2. Legyen $E = \mathbb{R} \setminus \{1/\sqrt{3}, -1/\sqrt{3}\}$ és $F = \{f_1, f_2, f_3\}$, ahol $f_1, f_2, f_3 : E \rightarrow E$,

$$f_1(x) = x, \quad f_2(x) = \frac{x + \sqrt{3}}{1 - x\sqrt{3}}, \quad f_3(x) = \frac{x - \sqrt{3}}{1 + x\sqrt{3}}.$$

Igazoljuk, hogy $(F, \circ)$ egy algebrai struktúra. Készítsük el a művelet táblát.

▼ 3. Vizsgáljuk a következő műveletek tulajdonságait:

- i) $m * n = m^n$, ahol $m, n \in \mathbb{N}^*$,
- ii) $a * b = \sqrt{ab}$, ahol $a, b \in (0, \infty)$,
- iii) $x * y = xy - x - y + 2$, ahol $x, y \in \mathbb{R}$,
- iv) $x * y = \sqrt{x^2 + y^2}$, ahol $x, y \in [0, \infty)$,
- v) $(x, y) + (z, w) = (x + z, y + w)$, ahol $(x, y), (z, w) \in \mathbb{Z} \times \mathbb{Z}$.

▼ 4. Határozzuk meg $a, b \in \mathbb{R}$ értékét úgy, hogy az $x * y = xy + 2ax + by, x, y \in \mathbb{R}$ művelet kommutatív és asszociatív legyen.

Válasz. $a = b = 0$ vagy $a = 1/2, b = 1$.

▼ 5. A $\mathbb{Z} \times \mathbb{Z}$ halmazon legyen $(a, b) \circ (c, d) = (ac + bd, ad + bc)$. Igazoljuk, hogy $(\mathbb{Z} \times \mathbb{Z}, \circ)$ egy egységelemes félcsoporth. Melyek az invertálható elemek ?

▼ 6. Legyen S egy n elemű halmaz.

i) Hány művelet értelmezhető az S halmazon? (Válasz: n^{n^2})

ii) Ezek közül hány művelet kommutatív? (Válasz: $n^{n(n+1)/2}$)

iii) Hány műveletre nézve van semleges elem? (Válasz: $n^{(n-1)^2+1}$)

▼ 7. Ha $(S, *)$ és $(S', \circ)$ grupoidok és $f : S \rightarrow S'$ olyan függvény, amelyre $f(a * b) = f(a) \circ f(b)$, $\forall a, b \in S$, akkor f -et **művelettartó** függvénynek vagy **homomorfizmusnak** (**morfizmusnak**) nevezzük.

Igazoljuk, hogy ha $(S, *)$ félcsoporth, akkor $(f(S), \circ)$ is félcsoporth (félcsoporth homomorf képe félcsoporth).

3. Csoportok és morfizmusok

3.A. A csoport fogalma

A $(G, \cdot)$ egységelemes félcsoporthot **csoportnak** nevezzük, ha minden $x \in G$ elem invertálható. A $(G, \cdot)$ struktúra tehát csoport, ha G -n értelmezett egy (multiplikatív) művelet, az ún. **csoport-szorzás**, amelyre

(G_1) $(xy)z = x(yz)$ minden $x, y, z \in G$ -re, azaz a művelet asszociatív,

(G_2) létezik $e \in G$ úgy, hogy $xe = ex = x$ minden $x \in G$ -re, azaz létezik egységelem,

(G_3) minden $x \in G$ -re létezik $x^{-1} \in G$ úgy, hogy $xx^{-1} = x^{-1}x = e$, azaz minden elem invertálható.

Ha még teljesül

(G_4) $xy = yx$ minden $xy \in G$ -re, azaz a művelet kommutatív,

akkor **kommutatív csoportról** vagy **Abel-csoportról** beszélünk (Niels Henrik Abel, XIX. századi norvég matematikus).

Ha a G csoportban az x, y elemekre $xy = yx$, akkor azt mondjuk, hogy x és y **felcserélhető elemek**. Pl. az e egységelem minden más elemmel felcserélhető. A csoport akkor kommutatív, ha bármely két eleme felcserélhető.

Azt mondjuk, hogy $(G, \cdot)$ **véges csoport**, ha a G halmaz véges, ellenkező esetben **végtelen csoportról** beszélünk. Ha G halmaz n elemű: $|G| = n$, akkor n -et a G **csoport rendjének** nevezzük és azt mondjuk, hogy G egy n -edrendű csoport.

A továbbiakban a csoportokra a multiplikatív írásmódot használjuk. Megjegyezzük, hogy kommutatív csoportokra szokásos az additív írásmód is.

3.B. Példák csoportokra

3.B.1. Példák. • $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ Abel-csoportok,

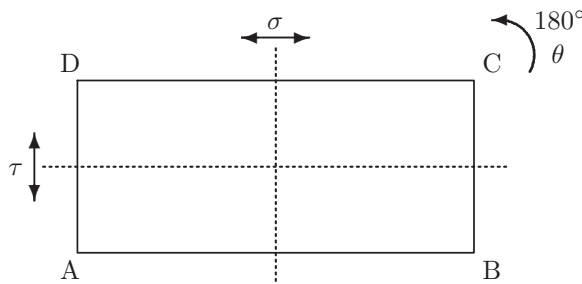
• $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ nem csoportok, csak egységelemes félcsoporthok, de $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ Abel-csoportok.

Az előbbi példák mind végtelen csoportok, véges csoportra példák következnek:

3.B.2. Példa. • Ha $n \in \mathbb{N}^*$, akkor $(U_n = \{z \in \mathbb{C} : z^n = 1\}, \cdot)$ kommutatív csoport. ▼ Igazoljuk ezt! U_n -et az n -edik **egységgyökök csoportjának** nevezzük, pl. $U_2 = \{-1, +1\}$, $U_4 = \{-1, +1, -i, +i\}$.

3.B.3. Példa. • Ha $n \in \mathbb{N}^*$, legyen $\mathbb{Z}_n = \{\widehat{0}, \widehat{1}, \dots, \widehat{n-1}\}$ a maradékosztályok halmaza (mod n). Ekkor $(\mathbb{Z}_n, +)$ Abel-csoport, a **maradékosztályok (additív) csoportja** (mod n), ahol $\widehat{x} + \widehat{y} = \widehat{x+y}$.

3.B.4. Példa. • Tekintsünk az $\mathcal{S}$ síkban egy olyan $ABCD$ téglalapot, amely nem négyzet és vizsgáljuk ennek az egybevágósági transzformációit, vagyis az olyan távolságtartó $f : \mathcal{S} \rightarrow \mathcal{S}$ függvényeket, amelyek a téglalapot önmagába viszik át. Ezek a következők, lásd 1. ábra:



1. ábra

- (1) az e identikus függvény, amelyre $e(A) = A$, $e(B) = B$, $e(C) = C$, $e(D) = D$,
- (2) a téglalap középpontja körüli 180° -os θ forgatás: $\theta(A) = C$, $\theta(B) = D$, $\theta(C) = A$, $\theta(D) = B$,
- (3) az AB oldal felezőmerőlegesére, mint szimmetriatengelyre való σ tükrözés: $\sigma(A) = B$, $\sigma(B) = A$, $\sigma(C) = D$, $\sigma(D) = C$,
- (4) a AD oldal felezőmerőlegesére, mint szimmetriatengelyre való τ tükrözés: $\tau(A) = D$, $\tau(B) = C$, $\tau(C) = B$, $\tau(D) = A$.

Legyen a művelet a transzformációk kompozíciója (egymásutáni elvégzése), szorzással jelölve, amely asszociatív. Figyeljük meg, hogy a θ, σ, τ közül bármely két különböző transzformáció szorzata a harmadikkal, pl. $\theta\sigma = \tau$, $\sigma\tau = \theta$, stb. és mindegyik négyzete egyenlő e -vel: $\theta^2 = \sigma^2 = \tau^2 = e$.

A művelet tábla:

$\cdot$	e	θ	σ	τ
e	e	θ	σ	τ
θ	θ	e	τ	σ
σ	σ	τ	e	θ
τ	τ	σ	θ	e

A művelet kommutatív, mert a művelet tábla szimmetrikus a főátlóra nézve. Az e egységelem és minden elemnek önmaga az inverze. $K = \{e, \theta, \sigma, \tau\}$ tehát Abel-csoport, ezt **Klein-csoport**nak nevezzük (Kleinsche Viergruppe).

3.B.5. Példa. • Legyen $n \in \mathbb{N}^*$ és tekintsük a $\sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ bijektív függvényeket. Ezeket n -edfokú permutációknak nevezzük, jelölés

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Az n -edfokú permutációk S_n halmaza csoport a függvényösszetétel (kompozíció) művelettel. Az $(S_n, \circ)$ csoport neve **n -edfokú szimmetrikus csoport** vagy **n -edfokú teljes permutációcsoport**, amelynek rendje $n!$ és amely nem kommutatív, ha $n \geq 3$.

A csoportműveletet itt gyakran „ $\cdot$ ”-tal jelöljük, $\sigma \circ \tau$ helyett tehát $\sigma\tau$ -t írunk és $\sigma^2 = \sigma \circ \sigma$, $\sigma^3 = \sigma^2 \circ \sigma$, stb. Az egységelem az e **identikus permutáció**, amelyre $e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$, és σ inverze $\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix}$.

3.B.6. Feladatok. ▼ 1. Legyen $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

- a) Igazoljuk, hogy S_3 megadható így: $S_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$, ahol $\sigma^3 = e$, $\tau^2 = e$, $\tau\sigma = \sigma^2\tau$.
b) Az előbbi összefüggések alapján töltsük ki a Cayley-táblázatot.

Megoldás.

$\cdot$	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
e	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	e	$\sigma\tau$	$\sigma^2\tau$	τ
σ^2	σ^2	e	σ	$\sigma^2\tau$	τ	$\sigma\tau$
τ	τ	$\sigma^2\tau$	$\sigma\tau$	e	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^2\tau$	σ	e	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	e

▼ 2. Igazoljuk, hogy $n \geq 3$ esetén az S_n csoport nem kommutatív.

Csoportstruktúrákra fontos példák a **mátrix-csoportok** is.

3.B.7. Példa. • Legyen

$$\mathcal{M}_n(\mathbb{C}) = \{A = (a_{ij})_{1 \leq i, j \leq n} : a_{ij} \in \mathbb{C}, \quad \forall i, j \in \mathbb{C}\}$$

az $n \times n$ -es komplex elemű mátrixok halmaza ($\mathbb{C}$ helyett vehető $\mathbb{R}$ vagy egy tetszőleges $(K, +, \cdot)$ kommutatív test). Ekkor $(\mathcal{M}_n(\mathbb{C}), +)$ Abel-csoport és $(\mathcal{M}_n(\mathbb{C}), \cdot)$ egységelemes félcsoport. Az invertálható mátrixok csoportot alkotnak a szorzásra nézve, ennek neve **általános lineáris csoport** (general linear group), jelölés: $(GL_n(\mathbb{C}), \cdot)$, ahol

$$GL_n(\mathbb{C}) = \{A \in \mathcal{M}_n(\mathbb{C}) : \exists A^{-1} \in \mathcal{M}_n(\mathbb{C})\} = \{A \in \mathcal{M}_n(\mathbb{C}) : \det A \neq 0\}.$$

A **speciális lineáris csoport** (special linear group) a következő: $(SL_n(\mathbb{C}), \cdot)$, ahol

$$SL_n(\mathbb{C}) = \{A \in \mathcal{M}_n(\mathbb{C}) : \det A = 1\}.$$

3.B.8. Példa. • **A kvaterniók csoportja.** Legyenek $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \in \mathcal{M}_2(\mathbb{C})$ és $Q = \{\pm 1, \pm i, \pm j, \pm k\}$. Akkor $(Q, \cdot)$ nem kommutatív csoport.

Valóban, az adott mátrixok szorzásával látható, hogy $i^2 = j^2 = k^2 = -1$ és $ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j$. Q így is megadható: $Q = \{1, i, i^2, i^3, j, ij, i^2j, i^3j\}$. A Cayley-táblázat a következő:

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

3.B.9. Példa. • Legyen $(G_1, \cdot)$ és $(G_2, \cdot)$ két csoport, két nem feltétlenül azonos, multiplikatív módon jelölt művelettel, e_1 és e_2 egységelemekkel. A $G_1 \times G_2$ halmazon definiáljuk a következő műveletet: $(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2)$. Ekkor $(G_1 \times G_2, \cdot)$ csoport, az adott csoportok ún. **direkt szorzata**. Ennek egységeleme (e_1, e_2) , (g, h) inverze pedig $(g, h)^{-1} = (g^{-1}, h^{-1})$. ▼ Igazoljuk ezt! Ez a konstrukció elvégezhető általánosabban is, ha $(G_i)_{i \in I}$ csoportok egy tetszőleges rendszere.

3.B.10. Feladatok. ▼ 1. Legyen $G = (0, \infty) \setminus \{1\}$ és $x * y = x^{\ln y}$. Igazoljuk, hogy $(G, *)$ Abel-csoport.

▼ 2. A $\mathbb{Z}$ halmazon értelmezzük az $x * y = x + y - 1$ műveletet. Igaz-e, hogy $(\mathbb{Z}, *)$ Abel-csoport?

▼ 3. Csoport-e az 2.H/2. Feladatban adott $(F, \circ)$ struktúra?

3.C. Félcsoport invertálható elemeinek csoportja

Egy egységelemes félcsoport invertálható elemei (egységei) csoportot alkotnak, lásd alábbi tételt, ez egy fontos eljárás csoportok szerkesztésére.

3.C.1. Tétel. Legyen $(S, \cdot)$ egy egységelemes félcsoport és $U(S) = \{x \in S : x \text{ invertálható}\}$. Akkor $(U(S), \cdot)$ csoport.

Bizonyítás. $U(S) \subseteq S$ és $U(S)$ zárt a műveletre nézve: $\forall x, y \in U(S) \Rightarrow xy \in U(S)$, mert ha x és y invertálható, akkor xy is invertálható (lásd 2.E.4). A művelet asszociatív $U(S)$ -en, mert S -en is asszociatív. S -nek az e egységeleme $U(S)$ -ben is egységelem, itt fontos, hogy $e \in U(S)$. Továbbá minden $x \in U(S)$ invertálható az $U(S)$ definíciója szerint, ahol $x^{-1} \in U(S)$, mert ha x invertálható, akkor x^{-1} is invertálható (lásd 2.E.4). □

3.C.2. Példák. • Az $(A, \cdot)$, $A = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ félcsoportok esetén $U(A) = A \setminus \{0\}$.

3.C.3. Feladat. ▼ $(\mathbb{Z}, \cdot)$ esetén mi lesz az $(U(\mathbb{Z}), \cdot)$ csoport?

3.C.4. Példák. • 1. Az $(\mathcal{M}_n(\mathbb{C}), \cdot)$ félcsoport esetén $U(\mathcal{M}_n(\mathbb{C})) = GL_n(\mathbb{C})$, lásd 3.B. szakasz.

• 2. $(\mathbb{Z}_n, \cdot)$ kommutatív egységelemes félcsoport, ahol $\widehat{x} \cdot \widehat{y} = \widehat{xy}$. Itt az invertálható elemek halmaza $U(\mathbb{Z}_n, \cdot) = \{\widehat{x} \in \mathbb{Z}_n : (x, n) = 1\}$, ▼ Igazoljuk!, amely csoport a szorzásra nézve és ennek rendje $\varphi(n)$ (Euler-függvény). Ha $n = p$ prímszám, akkor $(\mathbb{Z}_p^*, \cdot)$ egy $(p-1)$ -edrendű csoport.

Megoldás. Tegyük fel, hogy $\widehat{x}$ invertálható, akkor létezik $\widehat{y}$ úgy, hogy $\widehat{x}\widehat{y} = \widehat{xy} = \widehat{1}$, azaz $xy = 1 + nk, k \in \mathbb{Z}, xy - nk = 1$, s innen $(x, n) = 1$.

Fordítva, ha $(x, n) = 1$, akkor ismert, hogy létezik $k, \ell \in \mathbb{Z}$ úgy, hogy $kx + \ell n = 1$ és innen

$$\widehat{1} = \widehat{kx + \ell n} = \widehat{kx} + \widehat{\ell n} = \widehat{k}\widehat{x} + \widehat{\ell}\widehat{n} = \widehat{k}\widehat{x} + \widehat{\ell}\widehat{0} = \widehat{k}\widehat{x},$$

tehát $\widehat{x}$ invertálható és inverze $\widehat{k}$.

Egy további fontos példát ad a következő

3.C.5. Tétel. Legyen M egy tetszőleges nemüres halmaz és $\mathcal{F}(M) = \{f|f : M \rightarrow M \text{ függvény}\}$. Akkor

1) $(\mathcal{F}(M), \circ)$ egységelemes félcsoport a függvények összetételére nézve és $U(\mathcal{F}(M)) = \{f : M \rightarrow M | f \text{ bijektív}\}$.

2) $S_M = \{f : M \rightarrow M \mid f \text{ bijektív}\}$ csoport a függvények összetételére nézve, ennek neve az M halmazon értelmezett **szimmetrikus csoport**, más jelölések: $\text{Sym}(M)$, $\text{Perm}(M)$.

Bizonyítás. Értelmezés szerint, ha $f, g : M \rightarrow M$, akkor ezek összetétele $g \circ f : M \rightarrow M$, ahol $(g \circ f)(x) = g(f(x))$. Ez asszociatív művelet: ha $f, g, h : M \rightarrow M$ tetszőleges függvények, akkor $(h \circ g) \circ f = h \circ (g \circ f)$.

Minden $f : M \rightarrow M$ függvényre $f \circ 1_M = 1_M \circ f = f$, hiszen $(f \circ 1_M)(x) = f(1_M(x)) = f(x)$, $(1_M \circ f)(x) = 1_M(f(x)) = f(x)$ minden $x \in M$ -re.

Belátjuk, hogy $U(\mathcal{F}(\mathcal{M})) = \{\{ : \mathcal{M} \rightarrow \mathcal{M} \mid \{ \text{bijektív} \}\}$.

Ha $f \in U(\mathcal{F}(\mathcal{M}))$, akkor f invertálható, azaz létezik olyan $f' : M \rightarrow M$ függvény, amelyre $f \circ f' = f' \circ f = 1_M$, $f(f'(x)) = f'(f(x)) = x, \forall x \in M$. Kérdés, hogy f bijektív-e, azaz tetszőleges $y \in M$ -re létezik-e egy és csak egy $x \in M$ úgy, hogy $f(x) = y$? Legyen $f'(y) = a$, akkor $f(a) = f(f'(y)) = y$, tehát választható $x = a$. Ha $f(a) = f(b)$, akkor $a = f'(f(a)) = f'(f(b)) = b$, ezért $x = a$ egyértelmű.

Fordítva, ha f bijektív, értelmezzük az f' függvényt így: $\forall t \in M, f'(t) = u$, ha $f(u) = t$. Ekkor $f(f'(t)) = f(u) = t, \forall t \in M, f'(f(u)) = f'(t) = u, \forall u \in M$. $\square$

A 3.C.5. alapján például az összes $f : \mathbb{R} \rightarrow \mathbb{R}$ bijektív függvény csoportot alkot a kompozícióra nézve ($M = \mathbb{R}$). Ha $M = \{1, 2, \dots, n\}$, akkor $S_M = S_n$ az n -edfokú szimmetrikus csoport, lásd 3.B.5.

3.C.6. Feladat. $\blacktriangledown$ Ha M -nek van legalább két eleme, akkor az $(\mathcal{F}(\mathcal{M}), \circ)$ félcsoport nem kommutatív.

Megoldás. Legyen $a, b \in M, a \neq b$ és $f(x) = a, \forall x \in M$ és $g(x) = b, \forall x \in M$. Akkor $f(g(x)) = f(b) = a, g(f(x)) = g(a) = b, \forall x \in M$, ezért $g \circ f \neq f \circ g$.

3.D. Számítási szabályok csoportban

3.D.1. Tétel. (számítási szabályok csoportban) Ha $(G, \cdot)$ egy csoport, akkor

1) $ab = ac \Rightarrow b = c$ és $ba = ca \Rightarrow b = c, \forall a, b, c \in G$, azaz teljesülnek a balról illetve jobbról való egyszerűsítés szabályai,

2) $\forall a, b \in G$ esetén az $ax = b$ egyenlet egyetlen megoldása $x = a^{-1}b$ és az $ya = b$ egyenlet egyetlen megoldása $y = ba^{-1}$.

Bizonyítás. 1) Ha $ab = ac$, akkor akkor mindkét oldalt szorozva balról az a inverzával: $a^{-1}(ab) = a^{-1}(ac)b, (a^{-1}a)b = (a^{-1}a)c, eb = ec$, ahonnan $b = c$. Hasonlóan a másik.

2) Ha $ax = b$, akkor mindkét oldalt szorozva balról az a inverzával: $a^{-1}(ax) = a^{-1}b, (a^{-1}a)x = a^{-1}b, ex = a^{-1}b$, ahonnan $x = a^{-1}b$. Hasonlóan a másik. $\square$

Ha $(G, \cdot)$ egy csoport és $a \in G$, akkor a $t_a : G \rightarrow G, t_a(x) = ax$ és $t'_a : G \rightarrow G, t'_a(x) = xa$ függvényeket **bal oldali** illetve **jobb oldali translációknak** nevezzük. Ezek bijektívek 3.D.1. szerint.

Csoportban értelmezhetők az elemek egész kitevős hatványai:

$$x^0 = e, \quad x^{n+1} = x^n \cdot x, \quad n \in \mathbb{N}, \quad x^{-n} = (x^{-1})^n = (x^n)^{-1}.$$

Belátható, hogy $x^{m+n} = x^m x^n, (x^m)^n = x^{mn}, \forall m, n \in \mathbb{Z}$.

Megjegyezzük, hogy általában $(xy)^n \neq x^n y^n$, de ha $xy = yx$ (azaz ha x és y felcserélhetők, amelynek elégséges, de nem szükséges feltétele, hogy a csoport kommutatív legyen), akkor $(xy)^n = x^n y^n$.

Additív jelöléssel: $0x = 0, (n+1)x = nx + x, n \in \mathbb{N}, (-n)x = n(-x) = -(nx)$, s ekkor $(m+n)x = mx + nx, m(nx) = (mn)x, \forall m, n \in \mathbb{Z}$.

Bármely véges csoport Cayley-táblázatában minden sor és minden oszlop tartalmazza mindegyik elemet és pontosan egyszer. Ez az egyszerűsítési szabály miatt van így (vizsgáljuk meg a 3.B. szakasz művelet tábláit).

3.D.2. Feladatok. $\blacktriangledown$ 1. Legyen $(G, \cdot)$ egy olyan csoport, amelyben $(xy)^2 = x^2 y^2, \forall x, y \in G$. Igazoljuk, hogy G kommutatív csoport.

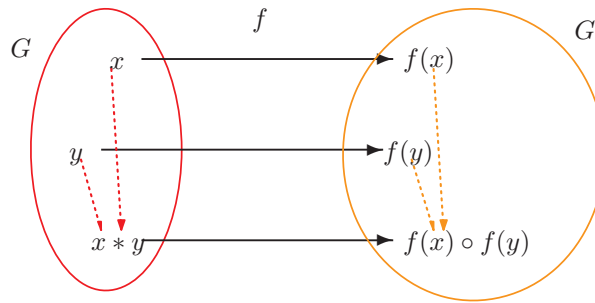
$\blacktriangledown$ 2. A $(G, \cdot)$ csoportban $x^2 = e, \forall x \in G$ (e az egységelem). Igazoljuk, hogy G kommutatív csoport.

3.E. Csoportmorfizmusok

Legyen $(G, *)$ és $(G', \circ)$ két csoport. Az $f : G \rightarrow G'$ függvényt **csoportmorfizmusnak** vagy **csoporthomomorfizmusnak** nevezzük, ha

$$f(x * y) = f(x) \circ f(y), \quad \forall x, y \in G,$$

azaz, ha bármely két elem G -beli összetételének a képe egyenlő a képelemek G' -beli összetételével (f művelettartó), lásd 2. ábra, jelölés: $f \in \text{Hom}(G, G')$.



2. ábra

Multiplikatív írásmóddal (a továbbiakban ezt használjuk):

$$f(xy) = f(x)f(y), \quad \forall x, y \in G,$$

azaz bármely két elem G -beli szorzatának a képe egyenlő a képelemek G' -beli szorzatával.

Az f csoportmorfizmus neve **csoportizomorfizmus**, ha f bijektív. Ekkor azt mondjuk, hogy a két csoport **izomorf** (algebrailag azonos), jelölés: $G \simeq G'$.

Ha $(G, \cdot) = (G', \cdot)$ azonos csoportok, akkor az $f \in \text{Hom}(G, G)$ homomorfizmus neve **endomorfizmus**, jelölés $f \in \text{End}(G)$, az $f : G \rightarrow G$ izomorfizmus pedig **automorfizmus**, jelölés $f \in \text{Aut}(G)$.

3.E.1. Tétel. (morfizmusok tulajdonságai) Legyen $f : G \rightarrow G'$ egy csoportmorfizmus. Akkor

- (i) $f(e) = e'$, ahol e a G egységeleme, e' pedig a G' egységeleme,
- (ii) $f(x^{-1}) = f(x)^{-1}$, $\forall x \in G$,
- (iii) $1_G : G \rightarrow G$, $1_G(x) = x$ morfizmus,
- (iv) ha $f' : G' \rightarrow G''$ egy további morfizmus, akkor $f' \circ f : G \rightarrow G''$ is morfizmus.
- (v) ha $f : G \rightarrow G'$ izomorfizmus, akkor $f^{-1} : G' \rightarrow G$ is izomorfizmus.

Bizonyítás. (i) $f(e) = f(ee) = f(e)f(e)$, ahonnan szorozva $f(e)^{-1}$ -nel: $f(e) = e'$,

(ii) $f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e'$ és $f(x^{-1})f(x) = f(x^{-1}x) = f(e) = e'$, ezért $f(x^{-1}) = f(x)^{-1}$,

(iii) $1_G(xy) = xy = 1_G(x)1_G(y)$, $\forall x, y \in G$,

(iv) $(f' \circ f)(xy) = f'(f(xy)) = f'(f(x)f(y)) = f'(f(x))f'(f(y)) = (f' \circ f)(x)(f' \circ f)(y)$, $\forall x, y \in G$.

(v) $\forall u, v \in G$: legyen $x = f^{-1}(u)$, $y = f^{-1}(v)$, akkor $f^{-1}(uv) = f^{-1}(f(x)f(y)) = f^{-1}(f(xy)) = xy = f^{-1}(u)f^{-1}(v)$. $\square$

3.E.2. Példák. • 1. Ha $a > 0, a \neq 1$, akkor $f : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \cdot)$, $f(x) = a^x$ izomorfizmus, tehát $(\mathbb{R}, +) \simeq (\mathbb{R}_+^*, \cdot)$, és $f^{-1}(x) = \log_a x$.

- 2. $f : (\mathbb{C}^*, \cdot) \rightarrow (\mathbb{R}_+^*, \cdot)$, $f(z) = |z|$ és $f : (\mathbb{C}, +) \rightarrow (\mathbb{R}, +)$, $f(z) = \text{Re } z$ morfizmusok.
- 3. $f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_n, +)$, $f(x) = \hat{x}$ morfizmus.
- 4. $f : GL_n(\mathbb{C}) \rightarrow \mathbb{C}^*$, $f(A) = \det A$ morfizmus.

3.E.3. Tétel. Ha $(G, \cdot)$ egy csoport, akkor $(\text{End}(G), \circ)$ egységelemes félcsoport és $U(\text{End}(G)) = \text{Aut}(G)$, tehát $(\text{Aut}(G), \circ)$ csoport, ez a G **automorfizmuscsoportja**. $\square$

3.E.4. Feladat. ▼ Igazoljuk a 3.E.3. Tételt.

A csoportok közötti izomorfizmus egy ekvivalenciareláció és a megfelelő ekvivalenciaosztályokat **csoporttípusoknak** nevezzük. A csoportelmélet a csoportoknak azokat a tulajdonságait tanulmányozza, amelyek ha igazak egy G csoportra, akkor igazak minden a G -vel izomorf csoportra is. Általában, az algebrai vizsgálatokban két algebrai struktúrát (csoport, gyűrű, test, stb.) azonosnak tekintünk, ha egymással izomorfak (kivéve, ha egy halmaz különböző részeiről van szó, ekkor ezek nem azonosíthatók). "Az algebra az izomorfizmusokkal szemben invariáns tulajdonságokat vizsgálja."

A csoportelmélet legfontosabb feladatai:

- 1) az összes létező csoporttípus leírása,
- 2) olyan eljárás keresése, amellyel két adott csoportról eldönthető, hogy izomorfak-e vagy sem.

Minden $n \geq 1$ -re létezik n -edrendű csoport. Valóban tekintsük pl. az n -edik egységgyökök $(U_n, \cdot)$ csoportját vagy a $(\mathbb{Z}_n, +)$ csoportot.

3.E.5. Feladatok. ▼ 1. Legyen $f_i : \mathbb{R}^* \rightarrow \mathbb{R}^*$, $f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = -x$, $f_4(x) = -\frac{1}{x}$. Igazoljuk, hogy $(G = \{f_1, f_2, f_3, f_4\}, \circ)$ Abel-csoport, amely izomorf a Klein-csoporttal (készítsünk Cayley-táblázatot).

▼ 2. Legyen $G = (-1, 1)$ és $x * y = \frac{x+y}{1+xy}$. Igazoljuk, hogy

a) $(G, *)$ Abel-csoport.

b) $f : (0, \infty) \rightarrow (-1, 1)$, $f(x) = \frac{x-1}{x+1}$ izomorfizmus a $((0, \infty), \cdot)$ és $(G, *)$ csoportok között.

c) Határozzuk meg: $\underbrace{x * x * \dots * x}_n$, ahol $n \in \mathbb{N}^*$.

Megoldás. c) $x * x = \frac{2x}{1+x^2}$, $x * x * x = \frac{3x+x^3}{1+3x^2}$, $x * x * x * x = \frac{4x+4x^3}{1+6x^2+x^4}$, innen nehezen található ki az eredmény.

A b) pontbeli f izomorfizmus inverze $f^{-1} : (-1, 1) \rightarrow (0, \infty)$, $f^{-1}(x) = \frac{1+x}{1-x}$ is izomorfizmus és $f^{-1}(x * y) = f^{-1}(x)f^{-1}(y)$, általánosabban: $f^{-1}(x_1 * \dots * x_n) = f^{-1}(x_1) \cdots f^{-1}(x_n)$, ahonnan $x_1 * \dots * x_n = f(f^{-1}(x_1) \cdots f^{-1}(x_n))$, $\forall x_i \in (-1, 1)$. Ha $x_1 = \dots = x_n = x$, akkor kapjuk, hogy

$$\underbrace{x * \dots * x}_n = \frac{(1+x)^n - (1-x)^n}{(1+x)^n + (1-x)^n}.$$

▼ 3. Igazoljuk, hogy

1) $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ izomorf a Klein-csoporttal,

2) $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$ izomorf a $(\mathbb{Z}_6, +)$ csoporttal.

▼ 4. i) Határozzuk meg $(\mathbb{Z}, +)$ endomorfizmusait és automorfizmusait. Igazoljuk, hogy $(\text{Aut}(\mathbb{Z}, +), \circ) \simeq (U_2, \cdot)$.

ii) Határozzuk meg $(\mathbb{Q}, +)$ endomorfizmusait és automorfizmusait. Igazoljuk, hogy $(\text{Aut}(\mathbb{Q}, +), \circ) \simeq (\mathbb{Q}^*, \cdot)$.

Megoldás. i) $f(x+y) = f(x) + f(y)$, $\forall x, y \in \mathbb{Z}$, ahonnan $x = 0$ -ra $f(0) = f(0) + f(0)$, $f(0) = 0$; $y = -x$ -re $0 = f(0) = f(x) + f(-x)$, $f(-x) = -f(x)$, $\forall x \in \mathbb{N}^*$. Továbbá $x = y = 1$ -re $f(2) = f(1) + f(1) = 2f(1)$, $f(3) = f(1) + f(2) = 3f(1)$, ..., $f(n) = nf(1)$, $\forall n \in \mathbb{N}$, és (*) miatt $f(x) = xf(1)$, $\forall x \in \mathbb{Z}$.

Tehát, ha $f : \mathbb{Z} \rightarrow \mathbb{Z}$ endomorfizmus, akkor $f(x) = ax$, $\forall x \in \mathbb{Z}$, ahol $a = f(1) \in \mathbb{Z}$ (a tetszőleges egész szám, amely csak f -től függ). Fordítva, azonnali, hogy ezek mind endomorfizmusok.

Az előbbieket közül csak $f_1(x) = x$ és $f_{-1} = -x$ bijektív: $\text{Aut}(\mathbb{Z}, +) = \{f_1, f_{-1}\}$. Legyen $\phi(f_1) = 1$, $\phi(f_{-1}) = -1$, ez izomorfizmus.

ii) itt $f(x+y) = f(x) + f(y)$, $\forall x, y \in \mathbb{Q}$, ahonnan az i) alapján $f(x) = xf(1)$, $\forall x \in \mathbb{Z}$, most $f(1) \in \mathbb{Q}$, továbbá $f(1) = f(n \cdot \frac{1}{n}) = nf(\frac{1}{n})$, $f(\frac{1}{n}) = \frac{1}{n}f(1)$, $\forall n \in \mathbb{N}^*$, $f(\frac{m}{n}) = mf(\frac{1}{n}) = \frac{m}{n}f(1)$, $\forall m, n \in \mathbb{N}^*$. Itt $f(-x) = -f(x)$, $\forall x \in \mathbb{Q}$ alapján kapjuk, hogy $f(x) = xf(1)$, $\forall x \in \mathbb{Q}$.

Tehát, ha $f : \mathbb{Q} \rightarrow \mathbb{Q}$ endomorfizmus, akkor $f(x) = rx$, $\forall x \in \mathbb{Q}$, ahol $r = f(1) \in \mathbb{Q}$ (r tetszőleges racionális szám, amely csak f -től függ). Ezek mind endomorfizmusok és $r = 0$ kivételével mind bijektívek, tehát automorfizmusok.

Legyen $\phi : (\text{Aut}(\mathbb{Q}, +), \circ) \rightarrow (\mathbb{Q}^*, \cdot)$, $\phi(f) = f(1) = r$, ez izomorfizmus.

▼ 5. Határozzuk meg az $f : (\mathbb{Z}_n, +) \rightarrow (\mathbb{Z}, +)$ csoportmorfizmusokat, ahol $n \in \mathbb{N}^*$.

Megoldás. $f(\widehat{x+y}) = f(\widehat{x}) + f(\widehat{y})$, $\forall \widehat{x}, \widehat{y} \in \mathbb{Z}_n$ alapján $f(\widehat{0}) = 0$, $f(\widehat{2}) = 2f(\widehat{1})$, ..., $f(\widehat{k}) = kf(\widehat{1})$, $0 \leq k \leq n$. Itt $f(\widehat{0}) = f(\widehat{n}) = 0$ miatt $f(\widehat{1}) = 0$ és válasz: $f(\widehat{x}) = 0$ az egyedüli morfizmus.

3.F. A részcsoporth fogalma, példák

Legyen $(G, \cdot)$ egy csoport és $H \subseteq G$. Azt mondjuk, hogy H a G **részcsoporthja** (vagy **alcsoportja**), ha a H elemei a G -beli műveletre nézve maguk is csoportot alkotnak, jelölés $H \leq G$, azaz

(i) $\forall x, y \in H : xy \in H$ (H zárt részhalmaz),

(ii) $(H, \cdot)$ csoport.

3.F.1. Példák. • 1. $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$, $(\mathbb{Q}^*, \cdot) \leq (\mathbb{R}^*, \cdot) \leq (\mathbb{C}^*, \cdot)$.

• 2. Ha $n \in \mathbb{Z}$, akkor $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\} \leq (\mathbb{Z}, +)$ (és minden részcsoporth ilyen alakú, lásd később), itt $(-n)\mathbb{Z} = n\mathbb{Z}$.

• 3. Minden $(G, \cdot)$ csoportnak részcsoportjai a $H = \{e\}$ és $H = G$, ezeket **triviális részcsoportoknak** nevezzük. Ha $H \leq G$ és $H \neq \{e\}$, $H \neq G$, akkor H -t **valódi részcsoportnak** nevezzük.

• 4. Ha $(G, \cdot)$ egy csoport és $x \in G$, akkor x egész kitevős hatványainak $H = \{x^k : k \in \mathbb{Z}\}$ halmaza a G kommutatív részcsoportja, lásd 3.F.2. Feladat, jelölés $H = \langle x \rangle$, ennek neve az x **elem által generált részcsoport**.

• 5. Ha $n \in \mathbb{N}^*$, akkor az n -edik egységgyökök U_n csoportjára $(U_n, \cdot) \leq (\mathbb{C}^*, \cdot)$.

• 6. A valós számsorozatok Abel-csoportot alkotnak az összeadásra nézve és a korlátos, illetve a konvergens sorozatok ennek részcsoportjai.

• 7. $(SL_n(\mathbb{C}), \cdot) \leq (GL_n(\mathbb{C}), \cdot)$.

3.F.2. Feladat. ▼ Legyen $(G, \cdot)$ egy csoport és $x \in G$. Akkor $H = \{x^k : k \in \mathbb{Z}\}$ a G kommutatív részcsoportja.

3.F.3. Tétel. Ha $H \leq G$, akkor H egységeleme a G egységeleme és minden elem H -beli inverze éppen a G -beli inverz.

Bizonyítás. H csoport, ezért H -ban létezik egy u egységelem legyen ez $u \in H$. Az $i : H \rightarrow G$, $i(x) = x, \forall x \in H$ függvény csoportmorfizmus, ezért $i(u) = e$ a G egységeleme (3.E.1. Tétel). De $i(u) = u$, ahonnan $u = e$.

Továbbá, jelölje $x' \in H$ az x H -beli inverzét és $x^{-1} \in G$ az x G -beli inverzét. Ekkor $i(x') = x^{-1}$ (3.E.1. Tétel), ahonnan $x' = x^{-1}$. □

3.F.4. Feladat. ▼ Részcsoportját alkotják-e az $(\mathbb{R}, +)$ csoportnak a következő halmazok: $\mathbb{N}$, $\mathbb{Z}$, $2\mathbb{Z}$, $2\mathbb{Z} + 1$, $\mathbb{Q}$, a negatív racionális számok, az irracionális számok?

3.F.5. Tétel. Egy csoport két részcsoportjának metszete is részcsoport:

$\forall H_1, H_2 \leq G \Rightarrow H_1 \cap H_2 \leq G$. Általánosabban, részcsoportok tetszőleges rendszerének a metszete is részcsoport:

$$\forall (H_i)_{i \in I}, \quad H_i \leq G \Rightarrow \bigcap_{i \in I} H_i \leq G.$$

Bizonyítás. Valóban, $\forall x, y \in \bigcap_{i \in I} H_i \Rightarrow x, y \in H_i, \forall i \in I \Rightarrow xy \in \bigcap_{i \in I} H_i$, továbbá $\bigcap_{i \in I} H_i$ -n a művelet asszociatív, $e \in H_i, \forall i \in I \Rightarrow e \in \bigcap_{i \in I} H_i$ és $\forall x \in \bigcap_{i \in I} H_i \Rightarrow x \in H_i, \forall i \in I \Rightarrow x^{-1} \in H_i, \forall i \in I \Rightarrow x^{-1} \in \bigcap_{i \in I} H_i$, tehát $\bigcap_{i \in I} H_i$ csoport. □

Egy csoport két részcsoportjának uniója általában nem részcsoport. Pl. $(\mathbb{Z}, +)$ -nak $(2\mathbb{Z}, +)$ és $(3\mathbb{Z}, +)$ részcsoportja, de $2\mathbb{Z} \cup 3\mathbb{Z}$ nem az, mert pl. $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, de $2+3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$ (ugyanakkor $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$ részcsoport).

3.F.6. Feladatok. ▼ 1. Tekintsük a $(G, *)$ Abel-csoportot, ahol $G = (0, \infty) \setminus \{1\}$ és $x*y = x^{\ln y}$, lásd 2.B.3/2 Feladat. Igazoljuk, hogy $H = \{e^x : x \in \mathbb{Q}, x > 0\}$ részcsoportja G -nek.

▼ 2. Legyen $(G, \cdot)$ egy csoport és $H = \{g \in G : gx = xg, \forall x \in G\}$ azoknak a G -beli elemeknek a halmaza, amelyek minden más elemmel felcserélhetők. Igazoljuk, hogy $H \leq G$ (itt H a G csoport centruma, jelölés $H = Z(G)$, G akkor és csak akkor kommutatív, ha $Z(G) = G$).

▼ 3. Legyen $(G, \cdot)$ egy csoport és $H_1, H_2, H_3 \leq G$. Igazoljuk, hogy

a) $H_1 \cup H_2 \leq G \Leftrightarrow H_1 \leq H_2$ vagy $H_2 \leq H_1$,

b) $H_1 \cup H_2 = G \Leftrightarrow H_1 = G$ vagy $H_2 = G$,

c) $H_3 \subseteq H_1 \cup H_2 \Leftrightarrow H_3 \leq H_1$ vagy $H_3 \leq H_2$.

3.G. Elem rendje

Legyen $(G, \cdot)$ egy csoport és $x \in G$. Tekintsük az $x, x^2, x^3, \dots \in G$ elemeket. Ha van olyan $k \in \mathbb{N}^*$ szám, amelyre $x^k = e$, akkor a legkisebb ilyen számot az x **elem G -re vonatkozó rendjének** nevezzük és azt mondjuk, hogy x **véges rendű**, jelölés: $o_G(x) = o(x) = \min\{k \in \mathbb{N}^* : x^k = e\}$. Ellenkező esetben (ha nincs ilyen szám), akkor azt mondjuk, hogy x **végtelen rendű**, jelölés: $o(x) = \infty$.

Additív írásmóddal x rendje az a legkisebb $k \in \mathbb{N}^*$, amelyre $kx = 0$.

3.G.1. Példák. • 1. Minden csoportban $o(x) = 1 \Leftrightarrow x = e$.

• 2. $(\mathbb{C}^*, \cdot)$ -ban $o(i) = 4, o(-1) = 2, o(3) = \infty$.

• 3. Az S_3 szimmetrikus csoportban legyen $\tau \in S_3, \tau(1) = 2, \tau(2) = 1, \tau(3) = 3$, amelyre jelölés: $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, ennek rendje 2: $o(\tau) = 2$, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ rendje 3: $o(\sigma) = 3$.

Ha x véges rendű, $o(x) = n$, akkor az $e, x, x^2, \dots, x^{n-1}$ elemek páronként különbözőek és minden x^k , $k \in \mathbb{Z}$ hatvány ezek egyikével egyenlő. Valóban, ha $x^i = x^j$, ahol $0 \leq i < j \leq n-1$, akkor $x^{j-i} = e$, $1 \leq j-i < n$, ellentmondás, továbbá $x^{n+1} = x^n x = ex = x$, $x^{n+2} = x^n x^2 = ex^2 = x^2, \dots$, általában, ha $k = nq + r$, $0 \leq r < n$ alakú, akkor $x^k = (x^n)^q x^r = x^r$. Innen következik, hogy

3.G.2. Tétel. Legyen $(G, \cdot)$ egy csoport, $x \in G$, $o(x) = n \in \mathbb{N}^*$. Ha $x^k = e$ valamilyen $k \in \mathbb{Z}$ -re, akkor $n|k$. $\square$

Ha $o(x) = \infty$, akkor az x^k , $k \in \mathbb{Z}$ hatványok mind különbözőek, mert ha létezne $i, j \in \mathbb{Z}$, $i < j$ úgy, hogy $x^i = x^j$, akkor $x^{j-i} = e$, $j-i > 0$, ellentmondás.

★ Ezért, ha $o(x) = \infty$, akkor G végtelen csoport. Következik, hogy ha G véges csoport, akkor minden x elemének a rendje véges. De vannak végtelen csoportok is, amelyekben minden elem rendje véges.

3.G.3. Példa. • Legyen $U = \{z \in \mathbb{C} : \exists n \in \mathbb{N}^* : z^n = 1\}$ a komplex egységgyökök halmaza. Ekkor $(U, \cdot)$ végtelen csoport, itt ha z_1 és z_2 n_1 -edik ill. n_2 -edik egységgyök, akkor $z_1 z_2$ $n_1 n_2$ -edik egységgyök, lásd 3.B.2., és ha z n -edik egységgyök, akkor $o(z) \leq n$ véges.

3.G.4. Feladatok. ▼ 1. Igazoljuk, hogy $U = \{z \in \mathbb{C} : \exists n \in \mathbb{N} : z^n = 1\}$ (végtelen) csoport a szorzásra nézve. ★

▼ 2. Határozzuk meg a következő x elemek rendjét a megadott csoportokban:

- a) $x = 1, x = 2, x = -3$ a $(\mathbb{Z}, +)$ csoportban,
- b) $x = -1, x = i, x = 2i$ a $(\mathbb{C}^*, \cdot)$ csoportban,
- c) $x = \hat{1}, x = \hat{2}, x = \hat{4}$ a $(\mathbb{Z}_5, +)$ csoportban,
- d) $x = \hat{1}, x = \hat{2}, x = \hat{4}$ a $(\mathbb{Z}_{12}, +)$ csoportban.

Ha $(G, \cdot)$ egy csoport és $x \in G$, akkor láttuk, hogy $H = \{x^k : k \in \mathbb{Z}\} = \langle x \rangle$ a G kommutatív részcsoportja (3.F. szakasz). Erre vonatkozik az alábbi

3.G.5. Tétel. Legyen $(G, \cdot)$ egy csoport, $x \in G$ és $H = \langle x \rangle \leq G$.

1) Ha $o(x) = \infty$, akkor H izomorf a $(\mathbb{Z}, +)$ csoporttal.

2) Ha $o(x) = n$, akkor $H = \{e, x, x^2, \dots, x^{n-1}\}$ és H izomorf a $(\mathbb{Z}_n, +)$ maradékosztálycsoporttal.

Bizonyítás. A fentieket használva, ha 1) $o(x) = \infty$, akkor $f : (\mathbb{Z}, +) \rightarrow (H, \cdot)$, $f(k) = x^k$ izomorfizmus, mert bijektív és művelettartó: $f(k + \ell) = x^{k+\ell} = x^k \cdot x^\ell = f(k)f(\ell)$ minden $k, \ell \in \mathbb{Z}$ esetén. Tehát $(H, \cdot) \simeq (\mathbb{Z}, +)$.

Hasonlóan, ha 2) $o(x) = n$, akkor $f : (\mathbb{Z}_n, +) \rightarrow (H, \cdot)$, $f(\hat{k}) = x^k$ izomorfizmus, mert bijektív és művelettartó, tehát $(H, \cdot) \simeq (\mathbb{Z}_n, +)$. $\square$

3.G.6. Tétel. Ha $(G, \cdot)$ egy véges n -edrendű Abel-csoport, akkor

- i) minden $x \in G$ elemre $x^n = e$,
- ii) minden $x \in G$ elem rendje osztója G rendjének: $o(x)|n$.

Bizonyítás. i) Legyen $G = \{g_1, g_2, \dots, g_n\}$ és legyen tetszőleges $x \in G$. Akkor az $xg_1, xg_2, \dots, xg_n$ elemek különbözőek és számuk n , tehát G elemeinek egy permutációját adják, ahonnan $G = \{xg_1, xg_2, \dots, xg_n\}$. Kapjuk, hogy: $g_1 g_2 \cdot \dots \cdot g_n = (xg_1)(xg_2) \cdot \dots \cdot (xg_n)$, innen a kommutativitást alkalmazva: $g_1 g_2 \cdot \dots \cdot g_n = x^n g_1 g_2 \cdot \dots \cdot g_n$, és $x^n = e$.

ii) azonnali i) és 3.G.2 alapján. $\square$

Látni fogjuk, hogy a 3.G.6 tulajdonságok, nemcsak Abel-csoportok, hanem tetszőleges véges csoportok esetén igazak.

A számelméletből ismert Euler-féle és Fermat-féle kongruenciátétel következik a 3.G.6 állításból.

3.G.7. Tétel. a) (Euler-tétel) Ha $n \in \mathbb{N}$, $n \geq 2$ és $a \in \mathbb{Z}$, $(a, n) = 1$, akkor

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

b) (Fermat-tétel) Ha p prímszám, $a \in \mathbb{Z}$ és $p \nmid a$, akkor

$$a^{p-1} \equiv 1 \pmod{p}.$$

Bizonyítás. a) Alkalmazzuk a 3.G.6. állítást az $(U(\mathbb{Z}_n), \cdot)$ Abel-csoportra, amely $\varphi(n)$ -edrendű, mert $U(\mathbb{Z}_n) = \{\hat{a} \in \mathbb{Z}_n : 1 \leq a \leq n, (a, n) = 1\}$ és következik, hogy

$$\hat{a}^{\varphi(n)} = \hat{1}, \quad \forall \hat{a} \in U(\mathbb{Z}_n).$$

b) Speciális esete a)-nak, ahol $n = p$ prímszám és $\varphi(p) = p - 1$. $\square$

3.G.8. Feladat. $\blacktriangledown$ 1. Legyen $(G, \cdot)$ egy csoport és $x, y \in G$. Akkor $o(x^{-1}) = o(x)$ és $o(xy) = o(yx)$.

Megoldás. $(x^{-1})^n = (x^n)^{-1}, \forall n \in \mathbb{N}^*$, ezért $(x^{-1})^n = e \Leftrightarrow x^n = e$, tehát $o(x^{-1}) = o(x)$. Minden $n \in \mathbb{N}^*$ esetén $(xy)^n = x \underbrace{(yx)(yx) \dots (yx)}_{n-1} y = x(yx)^{n-1}y$, ezért $(xy)^n = e \Leftrightarrow (yx)^{n-1} = x^{-1}y^{-1} =$

$(yx)^{-1} \Leftrightarrow (yx)^n = e$.

$\star \blacktriangledown$ 2. Ha egy csoportban az egységelemen kívül létezik végesrendű elem, akkor létezik prírendű elem.

Megoldás. Legyen $x \in G, x \neq e, o(x) = n$ véges. Ha n prím, akkor kész. Ha nem, akkor legyen $p|n$, p prím és $y = x^{n/p}$. Akkor $y \neq e$ és $o(y) = p$, mert $y^p = e$ és ha $k < p$, akkor $y^k \neq e$, mert $kn/p < n$. $\star$

3.H. Ciklikus csoportok

Ha $(G, \cdot)$ egy csoport és $x \in G$, akkor láttuk, hogy $\langle x \rangle = \{x^k : k \in \mathbb{Z}\} \leq G$. A G csoportot **ciklikus csoportnak** nevezzük, ha létezik olyan $x \in G$ elem, hogy $G = \langle x \rangle$. Ekkor G minden eleme x^k alakú, valamely $k \in \mathbb{Z}$ -re, itt x a G **generáló eleme**. Ha G ciklikus csoport, akkor kommutatív.

3.H.1. Példák. $\bullet$ 1. A $(\mathbb{Z}, +)$ csoport ciklikus: $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$,

$\bullet$ 2. A $(\mathbb{Z}_n, +)$ csoport ciklikus minden $n \in \mathbb{N}^*$ esetén: $\mathbb{Z}_n = \langle 1 \rangle$,

$\bullet$ 3. Az n -edrendű egységgyökök $U_n = \{z \in \mathbb{C} : z^n = 1\} = \{\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} : k \in \{0, 1, 2, \dots, n-1\}\}$ csoportja ciklikus csoport, mert $U_n = \langle \varepsilon_1 \rangle$.

$\star$ Azokat az ε_k számokat, amelyek U_n generáló elemei, azaz $\langle \varepsilon_k \rangle = U_n$, n -edik **primitív egységgyököknek** nevezzük. Itt ε_k akkor és csak akkor primitív egységgyök, ha $(k, n) = 1$, lásd 3.H.4. Feladat. $\star$

$\bullet$ 4. $(\mathbb{Q}, +)$ nem ciklikus csoport, lásd 3.H.2. Feladat.

3.H.2. Feladat. $\blacktriangledown$ Igazoljuk, hogy $(\mathbb{Q}, +)$ nem ciklikus csoport.

Megoldás. Tegyük fel, hogy $\exists q \in \mathbb{Q} : \mathbb{Q} = \langle q \rangle = \{nq : n \in \mathbb{Z}\}$. Akkor $\forall x \in \mathbb{Q} \Rightarrow \exists n \in \mathbb{Z} : x = nq$. Legyen $x = q/2$, akkor $q/2 = nq \Rightarrow n = 1/2$, ellentmondás.

A ciklikus csoportok a legegyszerűbb szerkezetű csoportok. A 3.G.5. Tétel alapján azonnali:

3.H.3. Tétel. (A ciklikus csoportok leírása) 1) Ha G végtelen ciklikus csoport, akkor G izomorf a $(\mathbb{Z}, +)$ csoporttal (a végtelen ciklikus csoportok tehát mind izomorfak egymással).

2) Ha G egy n -edrendű ciklikus csoport, akkor G izomorf a $(\mathbb{Z}_n, +)$ maradékosztály-csoporttal.

$\square$

A végtelen ciklikus csoport jelölése $C(\infty)$, az n -edrendű ciklikus csoporté pedig $C(n)$, ezekre gyakran a $\mathbb{Z}$, illetve $\mathbb{Z}_n$ additív csoportokkal hivatkozunk.

$\star$ 3.H.4. Feladat. $\blacktriangledown$ Legyen G egy n -edrendű ciklikus csoport, amelynek x generáló eleme. Igazoljuk, hogy x^r akkor és csak akkor generáló elem, ha $(r, n) = 1$.

Megoldás. Ha $G = \langle x^r \rangle$, akkor létezik k úgy, hogy $x = x^{kr}$, innen $kr \equiv 1 \pmod{n}$, azaz $n|(kr-1)$. Ha $d|r$ és $d|n$, akkor következik, hogy $d|1$, tehát $(r, n) = 1$.

Fordítva, ha $(r, n) = 1$, akkor $\exists u, v \in \mathbb{Z}$ úgy, hogy $ru + nv = 1$, innen $x^{ru} = x$ és kapjuk, hogy $x = (x^r)^u, x^2 = (x^r)^{2u}, \dots$ $\star$

$\star$ 3.I. Megjegyzések

A 3.A. szakaszban adott definíció H. Weber "Lehrbuch der Algebra", 1899 könyvében szerepel először.

A csoport fenti szokásos definíciója helyett elegendő a következőket megkövetelni: $(G, \cdot)$ egy félcsoport, amelyben létezik jobboldali e_j egységelem és minden elemnek létezik e_j -re vonatkozó jobboldali inverze, lásd 3.I.1/1,2 Feladatok.

A csoport egy másik, történetileg első definíciója (E. Cayley, 1854): A $(G, \cdot)$ nemüres félcsoportot csoportnak nevezzük, ha G -ben az $ax = b$ és $ya = b$ egyenleteknek vannak megoldásai, lásd 3.I.3. Feladat.

3.I.1. Feladatok. $\blacktriangledown$ 1. Legyen $(G, \cdot)$ egy félcsoport. Tegyük fel, hogy

i) létezik jobboldali egységelem: $\exists e \in G : xe = x, \forall x \in G$,

ii) minden elemnek létezik e -re vonatkozó jobboldali inverze:

$\forall x \in G \exists x' \in G : xx' = e$.

Igazoljuk, hogy ekkor G egy csoport.

Megoldás. $\forall x \in G \Rightarrow x' \in G \Rightarrow \exists (x')' = y : x'y = e$, innen $x'x = (x'x)e = (x'x)(x'y) = x'(xx')y = x'ey = x'y = e$, tehát $x'x = e$, továbbá $ex = (xx')x = x(x'x) = xe = x$, azaz $ex = x$. Következik, hogy e egységelem és x' az x inverze, tehát G csoport.

▼ 2. Adjunk példát egy olyan félcsoportra, amelyben létezik e_j jobb oldali egységelem, minden elemnek van e_j -re vonatkozó bal oldali inverze és amelyik nem csoport.

Megoldás. Legyen $S = \{a, b, c, d\}$ és $xy = x$, $\forall x, y \in S$, lásd 2.D.1, itt S minden z eleme jobb oldali egységelem, minden z -re és minden $x \in S$ -re $zx = z$, tehát x -nek z bal oldali inverze z -re nézve.

▼ 3. Legyen $(M, \cdot)$ egy (nemüres) félcsoport. Igazoljuk, hogy M akkor és csak akkor csoport, ha M -ben az $ax = b$ és $ya = b$ egyenleteknek vannak (egyértelmű) megoldásai. (Ez a feltétel úgy is megadható, hogy a $t_a, t'_a : M \rightarrow M$, $t_a(x) = ax$, $t'_a(x) = xa$ translációk szürjektívek minden $a \in M$ -re)

Megoldás. A szükségesség igaz (Tétel). Az elégségesség: legyen $a_0 \in M$, az $a_0x = a_0$ egyenletnek létezik $e \in M$ megoldása, amelyre $a_0e = a_0$. Igazoljuk, hogy $ae = a$, $\forall a \in M$.

Az $ya_0x = a$ egyenletnek létezik $y = y_0 \in M$ megoldása, amelyre $y_0a_0 = a$. Így $ae = (y_0a_0)e = y_0(a_0e) = y_0a_0 = a$, tehát e jobboldali egységelem.

$\forall x \in M \Rightarrow \exists x' \in M : xx' = e$ (az $xz = e$ egyenletnek van megoldása), tehát x' az x jobb oldali inverze.

Az előző feladat szerint így M csoport.

▼ 4. Legyen $(M, \cdot)$ egy (nemüres) véges félcsoport. Igazoljuk, hogy M akkor és csak akkor csoport, ha $\forall a, x, y \in M : ax = ay \Rightarrow x = y$ és $xa = ya \Rightarrow x = y$. (Ez a feltétel úgy is megadható, hogy a $t_a, t'_a : M \rightarrow M$, $t_a(x) = ax$, $t'_a(x) = xa$ translációk injektívek minden $a \in M$ -re)

Megoldás. A szükségesség igaz (egyszerűsítési szabály). Az elégségesség: feltétel szerint $t_a, t'_a : M \rightarrow M$ injektív, de mivel M véges, ezért t_a, t'_a szürjektív is, és használjuk az előző feladatot.

Minden síkidomhoz, ill. testhez hozzárendelhető a sík, ill. tér transzformációinak egy csoportja, amely azokból a transzformációkból áll, amelyek az síkidomot, ill. testet önmagába viszik át. Ilyen a 2.B.4. pontban definiált negyedrendű csoport és ilyenek az ún. diédercsoportok, lásd később.

Az olyan csoportokat, amelyekben minden elem végesrendű **torziócsoportoknak** nevezzük, ilyen minden véges csoport és például az egységgyökök U csoportja, amely végtelenrendű torziócsoport. Ha az egységelem kivételével minden elem végtelenrendű, akkor **torziómentes csoportról** beszélünk, ilyen például a pozitív racionális számok csoportja.

Ha a G csoportban léteznek olyan x, y elemek, amelyekre $o(x) = \infty$, $2 \leq o(y) < \infty$, akkor G neve **vegyes csoport**, például $(\mathbb{Q}^*, \cdot)$, ahol $o(-1) = 2$. ★

3.J. Feladatok

▼ 1. Legyen S egy tetszőleges halmaz, $(G, \cdot)$ egy csoport és $f : S \rightarrow G$ egy bijektív függvény. Igazoljuk, hogy $x * y = f^{-1}(f(x)f(y))$ egy csoportstruktúrát definiál az S halmazon.

▼ 2. Igazoljuk, hogy a $(\mathbb{Q}, +)$ és $(\mathbb{R}, +)$ csoportok nem izomorfak.

Megoldás. 1. mód. Ha izomorfak lennének, akkor $|\mathbb{Q}| = |\mathbb{R}|$ lenne, de tudjuk, hogy $\mathbb{Q}$ megszámlálható, $\mathbb{R}$ viszont nem.

2. mód. Közvetlenül: felt. létezik $f : \mathbb{Q} \rightarrow \mathbb{R}$ izomorfizmus, akkor $f(0) = 0$ és $\exists a \in \mathbb{Q}, a \neq 0 : f(a) = \sqrt{2}$, $\exists b \in \mathbb{Q}, b \neq 0 : f(b) = 1$. Legyen $\frac{a}{b} = \frac{m}{n} \in \mathbb{Q}$, akkor $na = mb$, $f(na) = f(mb)$, $nf(a) = mf(b)$, $n\sqrt{2} = m$, $\sqrt{2} = \frac{m}{n} \in \mathbb{Q}$, ellentmondás.

▼ 3. Legyenek M és N halmazok és $f : M \rightarrow N$ egy bijektív függvény. Mutassuk meg, hogy $(S_M, \circ) \simeq (S_N, \circ)$.

Megoldás. Legyen $F : S_M \rightarrow S_N$, $F(\varphi) = f \circ \varphi \circ f^{-1}$, $\forall \varphi \in S_M$. Ez izomorfizmus. Valóban, F morfizmus, mert $F(\varphi \circ \psi) = f \circ (\varphi \circ \psi) \circ f^{-1} = (f \circ \varphi \circ f^{-1}) \circ (f \circ \psi \circ f^{-1}) = F(\varphi) \circ F(\psi)$, és F bijektív, mert bijektív függvények összetétele.

★ ▼ 4. Legyen M egy halmaz és $(G, \cdot)$ egy csoport. A $G^M = \{f | f : M \rightarrow G\}$ halmazon értelmezzük a következő műveletet: $(fg)(x) = f(x)g(x)$, $\forall x \in M$. Igazoljuk, hogy $(G^M, \cdot)$ egy csoport és G beágyazható G^M -be, azaz létezik egy $\phi : G \rightarrow G^M$ injektív morfizmus.

Útmutatás. $\forall a \in G$ esetén legyen $\phi(a) = f_a$, ahol $f_a(x) = a$, $\forall x \in M$.

▼ 5. Igazoljuk, hogy $(\mathbb{Z} \times \mathbb{Z}, +)$ nem ciklikus csoport.

Megoldás. Tegyük fel, hogy $(\mathbb{Z} \times \mathbb{Z}, +)$ ciklikus, akkor - mivel végtelen - következik, hogy izomorf a $(\mathbb{Z}, +)$ csoporttal, tehát létezik egy $f : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ izomorfizmus. Legyen $f(1) = (a, b)$, akkor $f(2) = (2a, 2b)$, általában $f(x) = (xa, xb)$ minden $x \in \mathbb{Z}$ -re. Itt f szürjektív, ezért létezik $n \in \mathbb{Z}$ úgy, hogy $f(n) = (1, 1)$. Innen $(na, nb) = (1, 1)$, $na = nb = 1$, tehát $n = a = b = 1$ vagy $n = a = b = -1$. Első esetben $f(1) = (x, x), \forall x \in \mathbb{Z}$, második esetben $f(1) = (-x, -x), \forall x \in \mathbb{Z}$. De akkor pl. $(1, 0)$ nem képelem, ellentmondás. ★

▼ 6. Legyen

$$K = \left\{ A(x) = \begin{pmatrix} 1-x & 0 & x \\ 0 & 0 & 0 \\ x & 0 & 1-x \end{pmatrix} : x \in \mathbb{R} \setminus \left\{ \frac{1}{2} \right\} \right\}.$$

Igaz-e, hogy K csoport a mátrixok szorzására nézve ?

Megoldás. Igen ! Ugyanakkor a K -beli mátrixok szingulárisak, azaz nincs inverzük.

Megállapítható, hogy $(*) A(x)A(y) = A(x+y-2xy), \forall x, y \in \mathbb{R} \setminus \left\{ \frac{1}{2} \right\}$, ahol $x+y-2xy \neq \frac{1}{2}$, tehát K -n a szorzás művelet.

A mátrixok szorzása asszociatív és $(*)$ alapján K -n kommutatív is. $A(x)A(e) = A(x)$ -ből $e = 0$, tehát $A(0)$ semleges elem. $A(x)A(x') = A(0)$ -ből $x' = \frac{x}{2x-1}$, tehát $A(x)$ inverze (szimmetrikusa) $A\left(\frac{x}{2x-1}\right)$.

Következik, hogy $(K, \cdot)$ Abel-csoport.

★ ▼ 7. Legyen $(A, +)$ és $(B, +)$ két Abel-csoport. Ha $f, g \in \text{Hom}(A, B)$, legyen $f+g : A \rightarrow B, (f+g)(x) = f(x) + g(x), \forall x \in A$. Igazoljuk, hogy

- $(\text{Hom}(A, B), +)$ Abel-csoport,
- $(\text{Hom}(\mathbb{Z}, A), +) \simeq (A, +)$,
- $\text{Hom}(\mathbb{Q}, \mathbb{Z}) = \{0\}$.

Megoldás. b) A 3.E.5/4 Feladat megoldását követve, következik, hogy $\text{Hom}(\mathbb{Z}, A) = \{f_a : \mathbb{Z} \rightarrow A \mid f_a(x) = ax, a \in A\}$, továbbá $\phi : (\text{Hom}(\mathbb{Z}, A), +) \rightarrow (A, +), \phi(f_a) = a$ izomorfizmus.

Másképp: közvetlenül igazolható, hogy $\Gamma : (\text{Hom}(\mathbb{Z}, A), +) \rightarrow (A, +), \Gamma(f) = f(1)$ izomorfizmus.

c) Tegyük fel, hogy $f : (\mathbb{Q}, +) \rightarrow (\mathbb{Z}, +), f \neq 0$ egy morfizmus. Akkor létezik $x \in \mathbb{Q}$ úgy, hogy $f(x) = z \in \mathbb{Z}^*$. Innen $z = f(x) = f\left(n \cdot \frac{x}{n}\right) = nf\left(\frac{x}{n}\right)$ és következik, hogy $n|z$ minden $n \in \mathbb{N}^*$ számra, ellentmondás.

Másképp: $f(x) = xf(1), \forall x \in \mathbb{Q}$, ahol $f(1) \in \mathbb{Z}$, ez ugyanúgy adódik mint a 3.E.5/4-ben. Ha $f(1) \neq 0$, legyen $x = \frac{1}{2f(1)}$, innen $f(x) = \frac{1}{2} \notin \mathbb{Z}$, ellentmondás.

▼ 8. Legyen $(A, +)$ egy Abel-csoport és $m, n \geq 2$. Mutassuk meg, hogy

- $(\text{Hom}(\mathbb{Z}_n, A), +) \simeq (A_n, +)$, ahol $A_n = \{a \in A : na = 0\}$,
- $\text{Hom}(\mathbb{Z}_n, \mathbb{Z}) = \{0\}$,
- $(\text{Hom}(\mathbb{Z}_n, \mathbb{Z}_m), +) \simeq (\mathbb{Z}_{(n,m)}, +)$,
- $(\text{Aut}(\mathbb{Z}_n, +), \circ) \simeq (U(\mathbb{Z}_n), \cdot)$.

Megoldás. a) A korábbi feladatokhoz hasonlóan:

$$\text{Hom}(\mathbb{Z}_n, A) = \{f : \mathbb{Z}_n \rightarrow A : f(\widehat{x}) = xa, a = f(\widehat{1}) \in A_n\}.$$

Itt $a = f(\widehat{1}) \in A_n$, mert $0 = f(\widehat{0}) = f(\widehat{n}) = na$. Ekkor $\Gamma : (\text{Hom}(\mathbb{Z}_n, A), +) \rightarrow (A_n, +), \Gamma(f) = f(\widehat{1}) = a$ izomorfizmus.

b) Itt $A = \mathbb{Z}, (\mathbb{Z})_n = \{z \in \mathbb{Z} : nz = 0\} = \{0\}$ és az a) pont szerint $\text{Hom}(\mathbb{Z}_n, \mathbb{Z}) = \{f : \mathbb{Z}_n \rightarrow \mathbb{Z} : f(\widehat{x}) = xa, a = f(\widehat{1}) = 0\} = \{0\}$.

c) Most $A = \mathbb{Z}_m, (\mathbb{Z}_m)_n = \{\widehat{x} \in \mathbb{Z}_m : n\widehat{x} = \widehat{0}\}$ és a) szerint $(\text{Hom}(\mathbb{Z}_n, \mathbb{Z}_m), +) \simeq ((\mathbb{Z}_m)_n, +)$. Határozzuk meg $(\mathbb{Z}_m)_n$ elemeit. Ehhez megoldandó az $n\widehat{x} = \widehat{0}$ egyenlet, ahol $\widehat{x} \in \mathbb{Z}_m$. Itt $nx = mb, b \in \mathbb{Z}$ és legyen $x \in \{0, 1, \dots, m-1\}$. Legyen $d = (n, m)$ lnko., akkor $(n/d, m/d) = 1$ és $(n/d)x = (m/d)b$ alapján $(m/d)|x$ és

$$\widehat{x} = \widehat{0}, \widehat{\frac{m}{d}}, \widehat{\frac{2m}{d}}, \dots, \widehat{\frac{(d-1)m}{d}},$$

és ezek mind megoldások. Továbbá $\psi : (\mathbb{Z}_m)_n \rightarrow \mathbb{Z}_d, \psi\left(\widehat{\frac{jm}{d}}\right) = \widehat{j}$ izomorfizmus.

d) Az $A = \mathbb{Z}_n$ esetben $A_n = \mathbb{Z}_n$ és $\text{End}(\mathbb{Z}_n, +) = \{f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n : f(\widehat{x}) = x\widehat{a} = \widehat{xa}, \widehat{a} \in \mathbb{Z}_n\}$. Itt $f \in \text{End}(\mathbb{Z}_n, +)$ bijektív $\Leftrightarrow f$ szürjektív $\Leftrightarrow \exists \widehat{k} \in \mathbb{Z}_n : f(\widehat{k}) = \widehat{1} = \widehat{ka}$ (mivel $\mathbb{Z}_n$ ciklikus, $\widehat{1}$ generáló elem és f morfizmus) $\Leftrightarrow \widehat{a} \in U(\mathbb{Z}_n)$ (invertálható).

Továbbá következik, hogy $\Psi : (\text{Aut}(\mathbb{Z}_n, +), \circ) \rightarrow (U(\mathbb{Z}_n), \cdot)$, $\Psi(f) = f(\widehat{1})$ jól értelmezett izomorfizmus. ★

4. Részcsoporthok

4.A. Csoport részhalmazainak félcsoporthja

Legyen $(G, \cdot)$ egy csoport és tekintsük G részhalmazait. Ha $H, K \subseteq G$ ($H, K \in \mathcal{P}(G)$) definiáljuk ezek szorzatát így:

$$HK = \{hk : h \in H, k \in K\}.$$

Ha $H = \{h\}$ egy elemből áll, akkor jelölés:

$$hK = \{hk : k \in K\}.$$

Ha $H = \emptyset$ vagy $K = \emptyset$, akkor $HK = \emptyset$.

Ha G egy csoport, akkor $\forall g \in G : gG = Gg = G$ (mert $gG \subseteq G$ evidens és $\forall y \in G : y = g(g^{-1}y) \in gG$, tehát $G \subseteq gG$, ahonnan $G = gG$, hasonlóan a másik).

Additív jelöléssel, ha H és K a $(G, +)$ csoport részhalmazai és $h \in G$, akkor

$$H + K = \{h + k : h \in H, k \in K\}, \quad h + K = \{h + k : k \in K\}.$$

Ha $H_1, H_2, H_3 \subseteq G$, akkor $(H_1H_2)H_3 = H_1(H_2H_3)$, ez következménye az elemek szorzása asszociativitásának. Továbbá $eH = He = H$ minden $H \subseteq G$ -re. Eszerint $(\mathcal{P}(G), \cdot)$ egy egységelemes félcsoporth. Egy csoport részhalmazait régebbi könyvekben komplexusoknak is nevezik.

Ha $H \in \mathcal{P}(G)$, akkor jelölés: $H^{-1} = \{h^{-1} : h \in H\}$. Megjegyezzük, hogy ha $H, K \subseteq G$, akkor $(HK)^{-1} = K^{-1}H^{-1}$, mert $(HK)^{-1} = \{(hk)^{-1} : h \in H, k \in K\} = \{k^{-1}h^{-1} : h \in H, k \in K\} = K^{-1}H^{-1}$.

H^{-1} általában nem a H inverze a $(\mathcal{P}(G), \cdot)$ félcsoporthban. Ha $H = \{h\}$ egyelemű, akkor invertálható és inverze éppen $\{h^{-1}\} = H^{-1}$. Ha H legalább kételemű, akkor nem invertálható, lásd következő Feladat.

4.A.1. Feladatok. ▼ 1. Ha H legalább kételemű, akkor nem invertálható a $(\mathcal{P}(G), \cdot)$ félcsoporthban.

▼ 2. Ha G egy csoport és $H, K \subseteq G$, akkor $(H \cup K)^{-1} = H^{-1} \cup K^{-1}$ és $(H \cap K)^{-1} = H^{-1} \cap K^{-1}$.

4.B. Részcsoporthok jellemzése

A részcsoporth fogalmát a 3.F. szakaszban definiáltuk.

4.B.1. Tétel. (részcsoporthok jellemzése) Ha $(G, \cdot)$ egy csoport és $H \subseteq G$, akkor egyenértékűek a következő állítások:

- 1) $H \leq G$, azaz H részcsoporth,
- 2) $H \neq \emptyset$ és $\forall x, y \in H \Rightarrow xy \in H, x^{-1} \in H$,
- 3) $H \neq \emptyset$ és $\forall x, y \in H \Rightarrow xy^{-1} \in H$.

Bizonyítás. "1) $\Rightarrow$ 2)" Ha $H \leq G$, akkor $e \in H \neq \emptyset$ (Tétel) és definíció alapján $\forall x, y \in H : xy \in H$. Ugyanakkor $x^{-1} \in H, \forall x \in H$ (Tétel).

"2) $\Rightarrow$ 3)" a feltételek alapján $H \neq \emptyset$ evidens, továbbá $\forall x, y \in H : y^{-1} \in H$ és $xy^{-1} \in H$.

"3) $\Rightarrow$ 1)" $H \neq \emptyset$, ezért létezik $x_0 \in H$ és $e = x_0x_0^{-1} \in H$. Továbbá, $\forall x, y \in H : x^{-1} = ex^{-1} \in H$, $xy = x(y^{-1})^{-1} \in H$, ezért H zárt a műveletre nézve. A művelet asszociatív H -ban, mert G -ben az, létezik egységelem H -ban, mert $e \in H$, és minden H -beli x -nek van inverze: $x^{-1} \in H$. □

Megjegyzés. A Tétel 2) pontjában szereplő feltétel így is írható: $HH \subseteq H$ és $H^{-1} \subseteq H$, a 3) pontban pedig: $HH^{-1} \subseteq H$. Ezekben egyenlőség is írható, pontosabban igaz a következő

4.B.2. Tétel. (részcsoporthok jellemzése újra) Ha $(G, \cdot)$ egy csoport és $H \subseteq G$, akkor egyenértékűek a következő állítások:

- 1*) $H \leq G$, azaz H részcsoporth,
- 2*) $H \neq \emptyset$, $HH = H$ és $H^{-1} = H$,
- 3*) $H \neq \emptyset$ és $HH^{-1} = H$.

Bizonyítás. "1*) $\Rightarrow$ 2*)" Ha $H \leq G$, akkor az előző tétel szerint $H \neq \emptyset$, $HH \subseteq H$ és $H^{-1} \subseteq H$. Továbbá $\forall h \in H : h = he \in HH$, tehát $H \subseteq HH$. Ugyanakkor $H \subseteq H^{-1}$, mert $\forall h \in H : h = (h^{-1})^{-1} \in H^{-1}$, hiszen $H \leq G$ miatt $h^{-1} \in H$.

"2*) $\Rightarrow$ 3*)" Azonnali 2*) alapján: $HH^{-1} = HH = H$.

"3*) $\Rightarrow$ 1*)" $HH^{-1} = H \Rightarrow HH^{-1} \subseteq H$ és alkalmazzuk az előző tétel "3) $\Rightarrow$ 1)" implikációját. □

4.B.3. Példa. • Ha $(G, \cdot)$ egy csoport és $H = Z(G) = \{g \in G : gx = xg, \forall x \in G\}$, akkor $Z(G) \leq G$, $Z(G)$ a G csoport centruma, lásd 3.F.6. Feladat. G akkor és csak akkor kommutatív, ha $Z(G) = G$.

Belátjuk, hogy $Z(G) \leq G$. Valóban, alkalmazva a jellemzési tételt: $e \in Z(G) \neq \emptyset$, mert $\forall x \in G : ex = xe (= e)$; ha $g, h \in Z(G)$, akkor $\forall x \in G : (gh)x = g(hx) = g(xh) = (gx)h = (xg)h = x(gh) \Rightarrow gh \in Z(G)$ és ha $g \in G$, akkor $\forall x \in G : g^{-1}x = (x^{-1}g)^{-1} = (gx^{-1})^{-1} = xg^{-1}$, innen $g^{-1} \in Z(G)$.

4.B.4. Feladat. ▼ Legyen $(A, +)$ egy Abel-csoport és $B, C \leq A$. Igazoljuk, hogy a $B + C = \{b + c : b \in B, c \in C\}$ halmaz az A részcsoportja (ez a B és C összege). A $(\mathbb{Z}, +)$ csoportban mi lesz $2\mathbb{Z}$ és $3\mathbb{Z}$ (általánosabban $n\mathbb{Z}$ és $m\mathbb{Z}$) összege?

★ Mi annak a feltétele, hogy egy tetszőleges csoport két részcsoportjának szorzata részcsoport legyen? Erre ad választ a következő

4.B.5. Tétel. Legyen $(G, \cdot)$ egy csoport és $H, K \leq G$. Akkor $HK \leq G \Leftrightarrow HK = KH$.

Bizonyítás. Legyen $H, K \leq G$. Ha $HK \leq G$, akkor 4.B.2. szerint $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$. Ha pedig $HK = KH$, akkor $(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$ és $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$ és kapjuk, hogy $HK \leq G$. □

Ha G Abel-csoport, akkor a $HK = KH$ feltétel automatikusan teljesül és HK mindig részcsoport, ez az adott részcsoportok szorzata, lásd 4.B.4., ott additív az írásmód. ★

4.B.6. Tétel. Legyen $f : G \rightarrow G'$ egy csoportmorfizmus.

a) ha $H \leq G$, akkor $f(H) = \{f(h) : h \in H\} \leq G'$,

b) $f(G) \leq G'$, tehát csoport homomorf képe csoport,

b) ha $H' \leq G'$, akkor $f^{-1}(H') = \{g \in G : f(g) \in H'\} \leq G$.

Bizonyítás. Használjuk a részcsoportok jellemzési tételét: elég belátni, hogy

a) $e \in H$ miatt $f(e) = e' \in f(H) \neq \emptyset$, továbbá $\forall x, y \in H : f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(H)$.

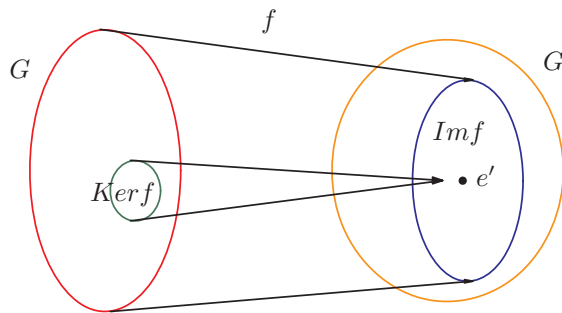
b) az előző speciális esete: $H = G$.

c) $e \in f^{-1}(H') \neq \emptyset$, mert $f(e) = e' \in H'$, továbbá $\forall x, y \in f^{-1}(H') : f(x), f(y) \in H'$ és $f(xy^{-1}) = f(x)f(y)^{-1} \in H'$, ezért $xy^{-1} \in f^{-1}(H')$. □

4.B.7. Feladat. Ha $(G, \cdot)$ egy csoport, akkor $(\text{Aut}(G), \circ) \leq (S_G, \circ)$.

4.C. Csoportmorfizmus magja és képe

Ha $f : G \rightarrow G'$ egy csoportmorfizmus, akkor a $\text{Ker}(f) = \{x \in G : f(x) = e'\}$ halmaz az f **magja**, $\text{Im } f = f(G) = \{f(x) : x \in G\}$ pedig az f **képhalmaza** vagy **képe**, lásd 3. ábra.



3. ábra

4.C.1. Tétel. Ha $f : G \rightarrow G'$ egy csoportmorfizmus, akkor

a) $\text{Ker } f \leq G$,

b) $\text{Im } f \leq G'$,

tehát minden csoportmorfizmus magja és képe (csoport homomorf képe) részcsoport.

Bizonyítás. A 4.B.6. következménye. Legyen $H = G$ és $H' = \{e'\}$, amelyre $\text{Ker } f = f^{-1}(\{e'\})$.

□

4.C.2. Feladat. Legyen $f : G \rightarrow G'$ egy csoportmorfizmus. f akkor és csak akkor injektív, ha $\text{Ker } f = \{e\}$.

Megoldás. " $\Rightarrow$ " $e \in \text{Ker } f$, mert $f(e) = e'$. Tegyük fel, hogy $x \in \text{Ker } f$, akkor $f(x) = e' = f(e)$, s mivel f injektív, következik, hogy $x = e$.

" $\Leftarrow$ " Legyen $x, y \in G$ úgy, hogy $f(x) = f(y)$. Akkor $f(x)f(y)^{-1} = e'$, $f(xy^{-1}) = e'$, ahonnan $xy^{-1} = e$, $x = y$, tehát f injektív.

4.D. Ciklikus csoportok részcsoportjai

Most igazoljuk, hogy egy ciklikus csoport minden részcsoportja ciklikus, pontosabban:

4.D.1. Tétel. (A ciklikus csoportok részcsoportjai) Egy ciklikus csoport minden részcsoportja ciklikus. Továbbá

1) Ha $G = \{x^k : k \in \mathbb{Z}\}$ végtelen ciklikus csoport, akkor G -nek végtelen sok részcsoportja van és ezek a következők: $H_m = \langle x^m \rangle = \{x^{km} : k \in \mathbb{Z}\}$, ahol $m \in \mathbb{N}$.

2) Ha $G = \{e, x, x^2, \dots, x^{n-1}\}$ egy n -edrendű ciklikus csoport, akkor G részcsoportjainak száma egyenlő n pozitív osztóinak számával és a részcsoportok a következők: $H_m = \langle x^m \rangle = \{e, x^m, x^{2m}, \dots, x^{n-m}\}$, ahol $m \in \mathbb{N}^*$, $m|n$, itt H_m rendje n/m .

Bizonyítás. Legyen $G = \langle x \rangle$ egy ciklikus csoport és legyen $H \leq G$. Ha $H = \{e\}$, akkor $H = \langle e \rangle$ ciklikus.

Ha $H \neq \{e\}$, akkor létezik $y \in H \setminus \{e\}$ és ez az elem előáll x valamilyen hatványaként: $\exists k \in \mathbb{Z} : y = x^k$, ahol $k \neq 0$, mert $x^0 = e$. Ekkor $x^{-k} = (x^{-1})^k \in H$, mert H részcsoport. A k és $-k$ közül az egyik pozitív, ezért $M = \{k \in \mathbb{N}^* : x^k \in H\}$ nemüres. Legyen $m = \min M$. Megmutatjuk, hogy $H = \langle x^m \rangle$, ami ciklikus.

Valóban, $x^m \in H \Rightarrow \langle x^m \rangle \subseteq H$. Fordítva, $\forall h \in H \Rightarrow h = x^\ell$, $\ell \in \mathbb{Z}$ és legyen $\ell = mq + r$, ahol $q, r \in \mathbb{Z}$, $0 \leq r < m$ (maradékos osztás tétele). Akkor $x^r = x^{\ell - mq} = x^\ell (x^m)^{-q} \in H$. De akkor m minimalitásából következik, hogy $r = 0$, ahonnan $h = (x^m)^q \in \langle x^m \rangle$.

★ 1) Ha G végtelen ciklikus csoport, akkor a $H_m = \langle x^m \rangle$, $m \in \mathbb{N}$ részcsoportok mind különbözőek. Itt $H_0 = \langle e \rangle = \{e\}$, $H_1 = \langle x \rangle = G$.

2) Ha $G = \{e, x, x^2, \dots, x^{n-1}\}$ véges ciklikus csoport, akkor $x^n = e \in H_m$ minden m -re, ezért $n = mk$ alakú, azaz $m|n$. H_m elemei tehát x^{um} , ahol $0 \leq u \leq n/m - 1$, mert $u = n/m$ -re $x^{(n/m)m} = x^n = e$. Ha $m|n$, akkor a H_m -ek különböző részcsoportok, itt $H_1 = \langle x \rangle = G$, $H_n = \langle x^n \rangle = \langle e \rangle = \{e\}$.

★ □

Megjegyzés. 4.D.1. 2)-ben H_m így is megadható: $H_m = \{g \in G : g^{n/m} = e\}$, ahol $m|n$.

4.D.2. Példák. • A $(\mathbb{Z}, +)$ ciklikus csoport részcsoportjai: $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$, ahol $n \in \mathbb{N}$, itt $0\mathbb{Z} = \{0\}$, $1\mathbb{Z} = \mathbb{Z}$.

• A $(\mathbb{Z}_n, +)$, $n \in \mathbb{N}^*$, ciklikus csoport részcsoportjai: $H_m = \{\widehat{0}, \widehat{m}, \widehat{2m}, \dots, \widehat{n-m}\}$, ahol $m|n$.

4.D.3. Feladat. ▼ Adjuk meg $(\mathbb{Z}_6, +)$ részcsoportjait.

Válasz. $H_1 = \{\widehat{0}, \widehat{1}, \widehat{2}, \widehat{3}, \widehat{4}, \widehat{5}\} = \mathbb{Z}_6$, $H_2 = \{\widehat{0}, \widehat{2}, \widehat{4}\}$, $H_3 = \{\widehat{0}, \widehat{3}\}$, $H_6 = \{\widehat{0}\}$.

4.E. Generált részcsoport

Ha $(G, \cdot)$ egy csoport és H_1, H_2 részcsoportok, akkor láttuk, hogy $H_1 \cup H_2$ általában nem részcsoport. Tekintsük ezért azt a legkisebb (a bennfoglalásra nézve) részcsoportot, amely tartalmazza H_1 -et és H_2 -t. Általánosabban, definiáljuk egy adott részhalmazt tartalmazó legkisebb részcsoportot a következőképpen:

Legyen $(G, \cdot)$ egy csoport és $X \subseteq G$. Akkor

$$\langle X \rangle = \cap \{H : H \leq G, X \subseteq H\}$$

részcsoportja G -nek 3.F.5. szerint, neve az X által **generált részcsoport**, X neve **generátorrendszer**. Ez az X -et tartalmazó összes H részcsoport metszete, tehát a legkisebb olyan részcsoport, amely tartalmazza X -et.

Ha $X = \{x\}$, akkor $\langle X \rangle = \langle x \rangle$ neve **ciklikus részcsoport** vagy az x elem által generált részcsoport, amit már korábban definiáltunk. Megjegyezzük, hogy $\langle \emptyset \rangle = \{e\}$.

Ha X véges halmaz, akkor $\langle X \rangle$ **végesen generált részcsoport**.

Az alábbi állítások következnek a definíciókból:

4.E.1. Tétel. (a generált részcsoport tulajdonságai) Ha $(G, \cdot)$ egy csoport és $X \subseteq G$, akkor

a) $\langle X \rangle \leq G$, $X \subseteq \langle X \rangle$,

b) ha $X \subseteq H$ és $H \leq G$, akkor $\langle X \rangle \leq H$,

c) legyen $H \subseteq G$, akkor $H \leq G \Leftrightarrow \langle H \rangle = H$. □

Fontos tudni hogyan kapjuk meg az X által generált részcsoportot, ha ismerjük az X elemeit. $\langle X \rangle$ tartalmaz minden $x \in X$ elemet, ezek inverzeit és véges sok $X \cup X^{-1}$ -beli elem szorzatát is. Ezek már G egy részcsoportját alkotják. Pontosabban:

4.E.2. Tétel. *Ha $(G, \cdot)$ egy csoport és $\emptyset \neq X \subseteq G$, akkor*

$$\langle X \rangle = \{x_1 x_2 \dots x_n \mid n \in \mathbb{N}^*, x_i \in X \cup X^{-1}, \forall 1 \leq i \leq n\},$$

ahol $X^{-1} = \{x^{-1} \mid x \in X\}$, azaz $\langle X \rangle$ az összes olyan véges sok tényező szorzatából áll, amelyeknek tényezői X -beli elemek vagy ezek inverzei (másképp: az X -beli elemek pozitív és negatív kitevős hatványainak szorzataiból áll).

★ **Bizonyítás.** (részletesen) Legyen

$$K = \{x_1 x_2 \dots x_n \mid n \in \mathbb{N}^*, x_i \in X \cup X^{-1}, \forall 1 \leq i \leq n\}.$$

Ez tartalmazza X -et: $X \subseteq K$, hiszen minden $x \in X$ -re x egytényezős szorzat ($n = 1$). Megmutatjuk, hogy $K \leq G$. Valóban, X -nek van legalább egy x eleme és $xx^{-1} = e \in K \neq \emptyset$, továbbá:

$$\begin{aligned} \forall x = x_1 x_2 \dots x_n, y = y_1 y_2 \dots y_m \in K &\Rightarrow xy^{-1} = x_1 x_2 \dots x_n (y_1 y_2 \dots y_m)^{-1} = \\ &= x_1 x_2 \dots x_n y_m^{-1} y_{m-1}^{-1} \dots y_1^{-1} \in K. \end{aligned}$$

(részcsoportok jellemzési tétele!) Ezért $\langle X \rangle = K \cap (\quad) \cap (\quad) \cap \dots$ és $\langle X \rangle \subseteq K$, pontosabban $\langle X \rangle \leq K$.

Belátjuk még, hogy K a legkisebb olyan részcsoport, amely tartalmazza X -et, azaz $\forall H \leq G, X \subseteq H$ esetén $K \subseteq H$. Valóban, ekkor $\forall y \in K \Rightarrow y = x_1 x_2 \dots x_n$ alakú, ahol $x_i \in X \cup X^{-1}$ és kapjuk, hogy $y \in H$, mert H részcsoport. Tehát $K \subseteq \langle X \rangle$.

A fentiek szerint $\langle X \rangle = K$. □★

Ha $x_1, \dots, x_n$ páronként felcserélhető elemek (speciálisan, ha a csoport kommutatív), akkor

$$\langle \{x_1, \dots, x_n\} \rangle \equiv \langle x_1, \dots, x_n \rangle = \{x_1^{k_1} \dots x_n^{k_n} : k_i \in \mathbb{Z}\}.$$

Additív jelöléssel:

$$\langle x_1, \dots, x_n \rangle = \{k_1 x_1 + \dots + k_n x_n : k_i \in \mathbb{Z}\}.$$

Az $X = \{x\}$ esetben az x elem által generált részcsoport: $\langle x \rangle = \{x^k : k \in \mathbb{Z}\}$, amit már láttunk. Additív jelöléssel a tétel a következő:

$$\langle X \rangle = \{x_1 + x_2 + \dots + x_n \mid n \in \mathbb{N}^*, x_i \in X \cup (-X), \forall 1 \leq i \leq n\},$$

ahol $-X = \{-x \mid x \in X\}$, továbbá $\langle x \rangle = \{kx : k \in \mathbb{Z}\}$.

★ **4.E.3. Tétel.** *Ha G egy csoport, $H, K \leq G$ és $HK = KH$, akkor $\langle H \cup K \rangle = HK$.*

Bizonyítás. Ha $HK = KH$, akkor $HK \leq G$, lásd 4.B.5. $H = He \subseteq HK, K = eK \subseteq HK$, innen $H \cup K \subseteq HK$, s mivel HK részcsoport, ezért $\langle H \cup K \rangle \leq HK$. Továbbá, $\forall h, k \in HK \Rightarrow hk \in \langle H \cup K \rangle$, innen $HK \leq \langle H \cup K \rangle$. Kapjuk, hogy $\langle H \cup K \rangle = HK$. □★

4.E.4. Feladatok. ▼ 1. a) Ha $f : G \rightarrow G'$ egy homomorfizmus és $X \subseteq G$, akkor $f(\langle X \rangle) = \langle f(X) \rangle$.

b) Ciklikus csoport homomorf képe is ciklikus, azaz ha $f : G \rightarrow G'$ egy homomorfizmus és G ciklikus, akkor $f(G)$ is ciklikus.

Megoldás. a) $X \subseteq \langle X \rangle$, ezért $f(X) \subseteq f(\langle X \rangle)$. Mivel $\langle X \rangle \leq G$ és f morfizmus következik, hogy $f(\langle X \rangle) \leq G'$. Kapjuk, hogy $\langle f(X) \rangle \subseteq f(\langle X \rangle)$.

Fordítva: igazoljuk, hogy $f(\langle X \rangle) \subseteq \langle f(X) \rangle$. Legyen $\forall g \in \langle X \rangle$ és kérdés, hogy $f(g) \in \langle f(X) \rangle$. Itt $g = x_1 \dots x_n$, ahol $x_i \in X \cup X^{-1}$ és $f(g) = f(x_1) \dots f(x_n)$, ahol $f(x_i) \in f(X)$ vagy $f(x_i) \in f(X^{-1}) = (f(X))^{-1}$, tehát $f(g) \in \langle f(X) \rangle$.

b) a fenti speciális esete: ha $G = \langle x \rangle$ ciklikus, akkor $f(G) = f(\langle x \rangle) = \langle f(x) \rangle$ ciklikus.

▼ 2. Igazoljuk, hogy $(\mathbb{Q}, +)$ nem végesen generált csoport.

Megoldás. Tegyük fel, hogy $\mathbb{Q} = \langle q_1, \dots, q_r \rangle = \{k_1 q_1 + \dots + k_r q_r : k_i \in \mathbb{Z}\}$, ahol $q_i = \frac{m_i}{n_i}$, $(m_i, n_i) = 1$, adott racionális számok.

Legyen $q = \frac{1}{2n_1 \dots n_r} \in Q$. Akkor $\exists k_i \in \mathbb{Z}$:

$$q = k_1 q_1 + \dots + k_r q_r = k_1 \frac{m_1}{n_1} + \dots + k_r \frac{m_r}{n_r} = \frac{k_1 m_1 n_2 \dots n_r + \dots + k_r m_r n_1 \dots n_{r-1}}{n_1 \dots n_r}.$$

Innen $\frac{1}{2} = k_1 m_1 n_2 \dots n_r + \dots + k_r m_r n_1 \dots n_{r-1} \in \mathbb{Z}$, ellentmondás.

4.F. Elemek és részcsoportok konjugáltjai

Legyen $(G, \cdot)$ egy csoport. Ha $x, y \in G$, akkor azt mondjuk, hogy x konjugált az y elemmel, jelölés $x \sim y$, ha $\exists g \in G : y = gxg^{-1}$. Ez egy ekvivalenciareláció a G -n és az $x \in G$ ekvivalenciaosztályának elemeit, azaz a gxg^{-1} elemeket, ahol $g \in G$, az x **elem konjugáltjainak** nevezzük, jelölés: ${}^g x = gxg^{-1}$.

4.F.1. Feladat. ▼ i) Igazoljuk, hogy " $\sim$ " ekvivalenciareláció G -n.

ii) Jelölje x ekvivalenciaosztályát $\tilde{x}$. Mutassuk meg, hogy $\tilde{x} = \{x\} \Leftrightarrow x \in Z(G)$.

Megoldás. i) reflexivitás: $x \sim x$, mert $\exists e \in G : x = exe^{-1}$,

szimmetria: ha $x \sim y$, akkor $\exists g \in G : y = gxg^{-1} \Rightarrow x = g^{-1}yg \Rightarrow y \sim x$,

transzitivitás: $x \sim y, y \sim z \Rightarrow \exists g, h \in G : y = gxg^{-1}, z = hyh^{-1} \Rightarrow z = h(gxg^{-1})h^{-1} = (hg)x(hg)^{-1} \Rightarrow x \sim z$.

ii) " $\Rightarrow$ " Feltételezzük, hogy $\hat{x} = \{x\}$. Kérdés, hogy $x \in Z(G) \Leftrightarrow \forall y \in G : xy = yx \Leftrightarrow \forall y \in G : x = yxy^{-1}$? Legyen $yxy^{-1} = z \Rightarrow z \sim x \Rightarrow z = x$ a feltételből, kész.

" $\Leftarrow$ " Legyen $\forall x \in Z(G)$. Akkor $x \in \hat{x} \Rightarrow \{x\} \subseteq \hat{x}$ (evidens). Kérdés: $\hat{x} \subseteq \{x\}$? $\forall y \in G : y \sim x \Rightarrow \exists g \in G : y = gxg^{-1} = xgx^{-1} = x$, használva, hogy $x \in Z(G)$. Innen $y = x \Rightarrow \hat{x} \subseteq \{x\}$.

Hasonlóan, ha $H \leq G$, akkor a H **részcsoporth konjugáltjai** a $gHg^{-1} = \{ghg^{-1} : h \in H\}$ részhalmazok, ahol $g \in G$, jelölés ${}^g H = gHg^{-1}$. A H részcsoporth konjugáltjai részcsoporthok, ez következik az alábbiakból.

4.F.2. Tétel. Legyen G egy csoport.

a) Ha $g \in G$, akkor $\tau_g : G \rightarrow G, \tau_g(x) = {}^g x = gxg^{-1}$ automorfizmusa G -nek (ennek neve belső automorfizmus),

b) Ha $H \leq G, g \in G$, akkor $gHg^{-1} \leq G$.

Bizonyítás. a) Minden τ_g morfizmus, mert $\tau_g(x_1 x_2) = g(x_1 x_2)g^{-1} = (gx_1 g^{-1})(gx_2 g^{-1}) = \tau_g(x_1)\tau_g(x_2), \forall x_1, x_2 \in G$. Továbbá ha $y = gxg^{-1}$, akkor $x = g^{-1}yg$, ahonnan kapjuk, hogy τ_g bijektív és inverze éppen $\tau_{g^{-1}}$.

b) $gHg^{-1} = \tau_g(H) \leq G$ a 4.B.6. alapján (csoport homomorf képe csoport). □

Azt mondjuk, hogy a H, K részcsoporthok **konjugált részcsoporthok**, jelölés $H \sim K$, ha $\exists g \in G : K = gHg^{-1}$.

4.F.3. Feladat. ▼ Igazoljuk, hogy " $\sim$ " ekvivalenciareláció a G részcsoporthjai halmazán.

★ 4.G. Abel csoport részcsoportjainak direkt összege

Legyen $(A, +)$ egy Abel-csoport és $B, C \leq A$. Akkor $B + C = \{b + c : b \in B, c \in C\} \leq A$, lásd 4.B.4. Azt mondjuk, hogy A **direkt összege** B -nek és C -nek, ha minden $a \in A$ elem egyértelműen felírható $a = b + c$ alakban, ahol $b \in B, c \in C$. Jelölés: $A = B \oplus C$ (multiplikatív írásmóddal $A = B \otimes C$, ekkor az elnevezés **direkt szorzat**).

4.G.1. Tétel. Legyen $(A, +)$ egy Abel-csoport és $B, C \leq A$. Akkor

1) a következő állítások egyenértékűek:

i) $A = B \oplus C$,

ii) $A = B + C$ és $B \cap C = \{0\}$,

iii) $f : B \times C \rightarrow A, f((b, c)) = b + c$ izomorfizmus,

2) ha $A = B \oplus C$ és A véges csoport, akkor $|A| = |B| \cdot |C|$.

4.G.2. Tétel. Ha G egy ciklikus csoport, $|G| = mn$, ahol $(m, n) = 1$, akkor G felbontható egy $G = H \otimes K$ direkt szorzatra, ahol H és K ciklikus részcsoporthok és $|H| = m, |K| = n$.

4.G.3. Feladatok. ▼ 1. Igazoljuk a 4.G.1. és 4.G.2. állításokat.

Megoldás. 4.G.2. igazolása: Legyen $G = \langle x \rangle$. Igazoljuk, hogy $G = \langle x^m \rangle \times \langle x^n \rangle$. Valóban, $(m, n) = 1$ miatt $\exists r, s \in \mathbb{Z} : 1 = rm + sn$ és minden t -re $x^t = x^{rtm+stn} = (x^m)^{rt}(x^n)^{st} \in \langle x^m \rangle \langle x^n \rangle$. Továbbá, ha $x^{km} = x^{\ell n} \in \langle x^m \rangle \cap \langle x^n \rangle$, akkor $x^{km-\ell n} = e, mn | km - \ell n$, innen $n | km$ és $(m, n) = 1$ miatt $n | k, k = nu$ és $x^{km} = x^{nmu} = e$. Tehát $H = \langle x^n \rangle, K = \langle x^m \rangle$.

▼ 2. i) Alkalmazzuk 4.G.2.-öt a $(\mathbb{Z}_{mn}, +)$ csoportra és mutassuk meg, hogy $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$, ahol $(m, n) = 1$.

ii) Mutassuk meg, hogy a $(\mathbb{Z}_{p^k}, +)$ csoport, ahol p prím, $k \in \mathbb{N}^*$, nem bontható fel két valódi részcsoport direkt szorzatára (ez minden prímhatalványrendű ciklikus csoportra is igaz).

Megoldás. ii) Tegyük fel, hogy $A = \mathbb{Z}_{p^k} = B \oplus C$, ahol $B, C \leq \mathbb{Z}_{p^k}$, $|B| = p^t$, $|C| = p^s$, ahol $1 < t, s < k$. Itt $p^k = |A| = |B| \cdot |C|$, lásd 4.G.1. Akkor B -ben minden elem rendje $\leq p^t$ (mi több, osztója p^t -nek), C -ben minden elem rendje $\leq p^s$ (osztója p^s -nek). Következik, hogy A minden a elemének rendje $\leq p^{\max(t,s)} = p^r$, ahol $r < k$. Valóban, minden $a \in A$ -ra $a = b + c$, ahol $b \in B, c \in C$ (egyértelműek) és $p^r a = p^r(b + c) = p^{r-t}(p^t b) + p^{r-s}(p^s c) = 0$, innen a rendje $\leq p^r$. Ez ellentmond annak, hogy $\mathbb{Z}_{p^k}$ ciklikus, azaz van p^k -adrendű eleme. ★

4.H. Cayley tétele

A következő tétel a szimmetrikus csoport fontosságát mutatja:

4.H.1. Tétel. (Cayley) Minden $(G, \cdot)$ csoport beágyazható egy szimmetrikus csoportba, pontosabban G izomorf az S_G szimmetrikus csoport egy részcsoportjával.

Bizonyítás. Ha $a \in G$, legyen $t_a : G \rightarrow G$, $t_a(x) = ax$ (bal oldali transláció), amely bijektív függvény, tehát $t_a \in S_G$. Legyen $\varphi : G \rightarrow S_G$, $\varphi(a) = t_a$.

Igazoljuk, hogy φ injektív morfizmus. Valóban, $\forall a, b \in G : \varphi(ab) = t_{ab}$, ahol $\forall x \in G : \varphi_{ab}(x) = t_{ab}(x) = (ab)x = a(bx) = t_a(t_b(x)) = (t_a \circ t_b)(x) = (\varphi(a) \circ \varphi(b))(x)$. Tehát $\varphi(ab) = \varphi(a) \circ \varphi(b)$

Továbbá, ha $\varphi(a) = 1_G$, akkor $\forall x \in G : t_a(x) = ax = x$, innen $a = e$, ezért $\text{Ker } \varphi = \{e\}$ és következik, hogy φ injektív.

Az előbbieket alapján G izomorf $\varphi(G)$ -vel, amely részcsoportja S_G -nek. □

★ 4.I. Részcsoportok megfeleltetési tétele

Szükségünk lesz a következő tulajdonságokra:

4.I.1. Tétel. (részcsoportok megfeleltetési tétele) Legyen $f : G \rightarrow G'$ egy szürjektív csoportmorfizmus. Akkor minden $K \leq G'$ esetén létezik egy és csak egy $H \leq G$ úgy, hogy $\text{Ker } f \leq H$ és $f(H) = K$, nevezetesen $H = f^{-1}(K)$. Tehát $H \mapsto f(H)$ bijektív megfeleltetés G -nek a $\text{Ker } f$ -et tartalmazó részcsoportjai és G' részcsoportjai között.

Bizonyítás. Tegyük fel, hogy adott $K \leq G'$ -re létezik olyan $H \leq G$, amelyre $\text{Ker } f \leq H$ és $f(H) = K$. Akkor ez csak $H = f^{-1}(K)$ lehet. Valóban, $\forall h \in H \Rightarrow f(h) \in f(H) = K \Rightarrow h \in f^{-1}(K) \Rightarrow H \leq f^{-1}(K)$. Fordítva, $\forall x \in f^{-1}(K) \Rightarrow f(x) \in K = f(H) \Rightarrow \exists h \in H : f(x) = f(h) \Rightarrow xh^{-1} \in \text{Ker } f \leq H$, innen $x = xh^{-1}h \in H$, $f^{-1}(K) \leq H$.

Legyen most $H = f^{-1}(K)$. Tudjuk, hogy ez részcsoportja G -nek és $\forall x \in \text{Ker } f \Rightarrow f(x) = e' \in K \Rightarrow x \in f^{-1}(K) = H$, tehát $\text{Ker } f \leq H$.

$f(H) = f(f^{-1}(K)) = K$ az f szürjektivitása miatt igaz: ha $x \in H$, akkor $f(x) \in K \Rightarrow f(H) \subseteq K$, és fordítva, $y \in K \Rightarrow \exists x \in G : f(x) = y$ (ide kell a szürjektivitás), innen $x \in f^{-1}(K)$ és $y = f(x) \in f(f^{-1}(K)) = f(H) \Rightarrow K \subseteq f(H)$. □

4.I.2. Feladat. a) Legyen $f : G \rightarrow G'$ egy csoportmorfizmus, $H \leq G$ és $N = \text{Ker } f$. Akkor $f^{-1}(f(H)) = NH = HN$.

b) Ha $f : G \rightarrow G'$ egy szürjektív csoportmorfizmus és $H' \leq G'$, akkor $f(f^{-1}(H')) = H'$.

Megoldás. a) $\forall x \in f^{-1}(f(H)) \Rightarrow f(x) \in f(H) \Rightarrow \exists h \in H : f(x) = f(h) \Rightarrow f(xh^{-1}) = e \Rightarrow xh^{-1} \in N \Rightarrow xh^{-1} = n \in N \Rightarrow x = nh \in NH$.

Fordítva, $\forall x = nh \in NH \Rightarrow f(x) = f(n)f(h) = f(h) \in f(H) \Rightarrow x \in f^{-1}(f(H))$, tehát $f^{-1}(f(H)) = NH$.

Továbbá, $f(H) \leq G' \Rightarrow f^{-1}(f(H)) \leq G$, lásd Tétel, ezért $NH \leq G$ és innen a 4.B.5. Tétel szerint $NH = HN$.

b) Alkalmazzuk a 4.I.1. Tételt. ★

4.J. Feladatok

▼ 1. Legyen G csoport, $H \subseteq G$ nemüres és véges. Igazoljuk, hogy H akkor és csak akkor részcsoportja G -nek, ha $\forall x, y \in H \Rightarrow xy \in H$ (azaz H zárt részhalmaz).

Megoldás. A szükségesség evidens. Az elégségesség: mivel H véges, ezért minden $x \in H$ elem H -ra vonatkozó rendje véges, legyen $o_H(x) = n$, ekkor $x^n = e$ és $x^{-1} = x^{n-1} \in H$.

▼ 2. Egy végtelen csoportnak végtelen sok részcsoportja van.

Megoldás. Legyen G egy végtelen csoport. Ha $\exists x \in G, o(x) = \infty$, akkor $\langle x \rangle \simeq (\mathbb{Z}, +)$ és ennek végtelen sok részcsoportja van. Ellenkező esetben $\forall x \in G : o(x) < \infty$, ekkor $\{\langle x \rangle : x \in G\}$ részcsoportok végtelen halmaza.

▼ 3. Ha $f : G \rightarrow G'$ egy izomorfizmus, akkor $f(Z(G)) = Z(G')$.

Megoldás. " $\subseteq$ " $\forall y \in f(Z(G)) \Rightarrow \exists x \in Z(G) : y = f(x)$. Kérdés: $y \in Z(G')$, azaz $\forall z \in G' : yz = zy$? $\exists g \in G : z = f(g)$ és $yz = f(x)f(g) = f(xg) = f(gx) = f(g)f(x) = zy$. Hasonlóan fordítva.

★ ▼ 4. Legyen G egy csoport és $H \leq G$, $H \neq G$. Igazoljuk, hogy $\langle G \setminus H \rangle = G$.

Megoldás. Legyen $K \leq G$ és $G \setminus H \subseteq K$. Akkor $K \cup H = G$, ahol $K, H \leq G$. Következik, hogy $K = G$ vagy $H = G$, lásd 3.F.6/3. Feladat, itt $H = G$ kizárt, ezért $K = G$, kész. ★

▼ 5. Legyen G egy véges Abel-csoport és P a G elemeinek szorzata: $P = \prod_{x \in G} x$. Igazoljuk, hogy:

i) $P^2 = e$, $P = \prod_{x \in G, x=x^{-1}} x$,

ii) Alkalmazás: ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$ (Wilson-tétel),

iii) Ha $|G|$ páros, akkor $\exists x \in G, x \neq e : o(x) = 2$,

★ iv) Legyen G ciklikus. Ha $|G|$ páratlan, akkor $P = e$, ha G páros, akkor $P \neq e$. ★

Megoldás. i) Minden $x \in G, x \neq e$ elemet állítsunk párba az x^{-1} inverzzel. Itt $x = x^{-1} \Leftrightarrow x^2 = e \Leftrightarrow o(x) = 2$ és $P = \prod_{x \in G} x = \prod_{x \neq x^{-1}} (xx^{-1}) \prod_{x=x^{-1}} x = \prod_{x^2=e} x$, $P^2 = \prod_{x^2=e} x^2 = e$.

ii) Legyen $p > 2$ és tekintsük a $(\mathbb{Z}_p^*, \cdot)$ csoportot. Itt $\widehat{x^2} = \widehat{1 \Leftrightarrow p | (x^2 - 1)} = (x-1)(x+1) \Leftrightarrow p | (x-1)$ vagy $p | (x+1) \Leftrightarrow \widehat{x} = \widehat{1}$ vagy $\widehat{x} = \widehat{p-1}$. i)-et alkalmazva: $\widehat{1 \cdot 2 \cdots p-1} = \widehat{p-1}$, innen $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$.

iii) Az i)-beli párosítással, most $|G \setminus \{e\}|$ páratlan, tehát $\exists x \in G, x \neq e : o(x) = 2$.

★ iv) Legyen $G = \langle x \rangle = \{e, x, x^2, \dots, x^{n-1}\}$, $o(x) = |G| = n$. Akkor $P = \prod_{x \in G} x = x^{1+2+\dots+n-1} = x^{n(n-1)/2}$. Ha $|G| = n = 2k+1$ páratlan, $a = x^{k(2k+1)} = (x^{2k+1})^k = e^k = e$, ha $|G| = n = 2k$ páros, $P = x^{k(2k-1)} = x^{2k^2} x^{-k} = (x^{2k})^k x^{-k} = x^{-k} \neq e$. (Másképp: $o(x^k) = \frac{o(x)}{(o(x), k)} = 2 \Leftrightarrow (o(x), k) = \frac{o(x)}{2} \Leftrightarrow k = \frac{o(x)}{2}$, stb., lásd később a képletet). ★

★ ▼ 6. Minden $m, n \in \mathbb{N}^*$ esetén

i) $m\mathbb{Z} \subseteq n\mathbb{Z} \Leftrightarrow n|m$, ii) $m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z}$,

iii) $\langle \{m, n\} \rangle = m\mathbb{Z} + n\mathbb{Z} = (m, n)\mathbb{Z}$, ahol $m\mathbb{Z} + n\mathbb{Z}$ részcsoportok összege, $[m, n]$ és (m, n) az m és n legkisebb közös többszöröse, illetve legnagyobb közös osztója.

Megoldás. i) " $\Rightarrow$ " $m\mathbb{Z} \subseteq n\mathbb{Z} \Rightarrow m \in n\mathbb{Z} \Rightarrow \exists j \in \mathbb{Z} : m = nj \Rightarrow n|m$,

" $\Leftarrow$ " $n|m \Rightarrow \exists j \in \mathbb{Z} : m = nj \Rightarrow \forall mk \in m\mathbb{Z} : mk = njk \in n\mathbb{Z}$.

ii) $m\mathbb{Z} \cap n\mathbb{Z} = k\mathbb{Z}$, mert két részcsoport metszete is részcsoport és minden részcsoport ilyen alakú.

Kérdés: $k = [m, n]$?

$k\mathbb{Z} \subseteq m\mathbb{Z}$ miatt i) alapján $m|k$ és hasonlóan $k\mathbb{Z} \subseteq n\mathbb{Z}$ miatt szintén i) alapján $n|k$, tehát k közös többszöröse m -nek és n -nek.

Legyen ℓ egy tetszőleges közös többszörös: $m|\ell, n|\ell$. Akkor i) szerint $\ell\mathbb{Z} \subseteq m\mathbb{Z}, \ell\mathbb{Z} \subseteq n\mathbb{Z}$, innen $\ell\mathbb{Z} \subseteq m\mathbb{Z} \cap n\mathbb{Z} = k\mathbb{Z}$, ahonnan újra i)-ből $k|\ell$ adódik, ezért k a legkisebb közös többszörös.

iii) Tétel alapján $\langle \{m, n\} \rangle = \{mk + nl : k, l \in \mathbb{Z}\} = m\mathbb{Z} + n\mathbb{Z}$, ez részcsoport, tehát $d\mathbb{Z}$ alakú. Megmutatjuk, hogy itt $d = (m, n)$. $m\mathbb{Z} \subseteq d\mathbb{Z}$ miatt i)-ből $d|m$ és hasonlóan $d|n$, tehát d közös osztó.

Legyen δ egy tetszőleges közös osztó: $\delta|m, \delta|n$. Akkor i) szerint $m\mathbb{Z} \subseteq \delta\mathbb{Z}, n\mathbb{Z} \subseteq \delta\mathbb{Z}$, innen $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z} \subseteq \delta\mathbb{Z}$, ahonnan újra i)-ből $\delta|d$, azaz d a legnagyobb közös osztó. ★

5. Mellékosztályok, Lagrange tétele

5.A. Bal oldali és jobb oldali mellékosztályok

Legyen $(G, \cdot)$ egy csoport, $H \leq G$ egy adott részcsoport és $x \in G$. Az

$$xH = \{xh : h \in H\} \quad \text{és} \quad Hx = \{hx : h \in H\}$$

részalmazokat az x elem H szerinti **bal oldali**, illetve **jobb oldali mellékosztályainak** nevezzük.

Azonnali, hogy ha a csoport kommutatív, akkor $xH = Hx$ minden $x \in G$ -re.

5.A.1 Feladat. ▽ Ha $x \in H$, akkor $xH = Hx = H$.

5.A.2. Tétel. Legyen $(G, \cdot)$ egy csoport és $H \leq G$.

i) Ha $x, y \in G$ és $y \in xH$, akkor $xH = yH$.

ii) Ha xH, yH két bal oldali mellékosztály, akkor $xH = yH$ vagy $xH \cap yH = \emptyset$. (hasonló igaz a jobb oldali mellékosztályokra is).

Bizonyítás. i) $y = xh \in xH \Rightarrow yH = (xh)H = x(hH) = xH$.

ii) Belátjuk, hogy ha $xH \cap yH \neq \emptyset$, akkor $xH = yH$. Valóban, ha $z \in xH \cap yH$, akkor i) alapján $zH = xH$ és $zH = yH$, tehát $xH = yH$. $\square$

5.A.3. Következmény. A különböző bal oldali (illetve jobb oldali) mellékosztályok a G egy osztályozását adják.

Egy bal oldali (jobb oldali) mellékosztály elemeit az adott mellékosztály **reprezentánsainak** nevezzük.

5.A.4. Példák. • Ha a $(G, \cdot)$ csoportban $H = \{e\}$, akkor $xH = Hx = \{x\}$ minden $x \in G$ -re és olyan osztályozást kapunk, amely G -t egyelemű részalmazokra bontja. Ha $H = G$, akkor $xG = Gx = G$ minden $x \in G$ -re és egyetlen osztály van, maga a G .

• A $(\mathbb{Z}, +)$ additív csoport $H = n\mathbb{Z}$ részcsoportjára nézve (most additív a jelölés!): $x + n\mathbb{Z} = \{x + nk : k \in \mathbb{Z}\}$, amit $\hat{x}$ -szel jelölünk és ez éppen egy $(\text{mod } n)$ maradékosztály. A mellékosztály fogalma tehát a maradékosztály $(\text{mod } n)$ fogalmának általánosítása.

5.B. Bal oldali és jobb oldali kongruenciarelációk

A bal oldali (illetve jobb oldali) mellékosztályok által meghatározott osztályozásoknak a következő ekvivalenciarelációk felelnek meg:

Ha $(G, \cdot)$ egy csoport és $H \leq G$, akkor legyen $\rho_H = \rho_{H,b}$ és $\rho'_H = \rho_{H,j}$ így értelmezett:

$$\forall x, y \in G : \quad x\rho_H y \Leftrightarrow x^{-1}y \in H, \quad x\rho'_H y \Leftrightarrow xy^{-1} \in H,$$

ezeket a H -szerinti **bal oldali**, illetve **jobb oldali kongruenciarelációknak** nevezzük.

5.B.1. Példák. • Ha a $(G, \cdot)$ csoportban $H = \{e\}$, akkor $x\rho_H y \Leftrightarrow x^{-1}y \in H \Leftrightarrow x^{-1}y = e \Leftrightarrow x = y$ és hasonlóan $x\rho'_H y \Leftrightarrow xy^{-1} \in H \Leftrightarrow xy^{-1} = e \Leftrightarrow x = y$, tehát mindkettő az egyenlőségi (diagonális) reláció: $\rho = \rho' = 1_G$. Ha $H = G$, akkor $x\rho_G y$ és $x\rho'_G y$ igaz tetszőleges $x, y \in G$ -re (univerzális reláció).

• A $(\mathbb{Z}, +)$ additív csoport $H = n\mathbb{Z}$ részcsoportjára nézve $x\rho'_H y \Leftrightarrow x - y \in n\mathbb{Z} \Leftrightarrow n|(x - y)$, ez a számelméleti kongruenciareláció $(\text{mod } n)$, jelölés: $x \equiv y \pmod{n}$. A ρ_H reláció ugyanezt adja: $x\rho_H y \Leftrightarrow -x + y \in n\mathbb{Z} \Leftrightarrow n|(-x + y) \Leftrightarrow n|(x - y)$.

5.B.2. Tétel. Ha $(G, \cdot)$ egy csoport és $H \leq G$, akkor a H szerinti bal oldali, illetve jobb oldali mellékosztályok által meghatározott osztályozásoknak a ρ_H , illetve a ρ'_H ekvivalenciarelációk felelnek meg.

Bizonyítás. A bal oldali mellékosztályokra nézve azt kell belátnunk, hogy $\forall y, z \in G$: $(\exists x \in G : y, z \in xH \Leftrightarrow y^{-1}z \in H)$. Valóban, ha $y, z \in xH$, akkor 5.A.2. szerint $yH = xH = zH$, innen $yH = zH$, $z = ze \in zH = yH$, tehát létezik $h \in H$ úgy, hogy $z = yh$, innen $y^{-1}z = h \in H$. Fordítva, ha $y^{-1}z \in H$, akkor létezik $h \in H$ úgy, hogy $z = yh$, $z \in yH$, innen $yH = zH$, tehát $y, z \in yH$ (vehető $x = y$). $\square$

5.B.3. Feladat. Adjunk közvetlen bizonyítást arra, hogy ρ_H és ρ'_H ekvivalenciarelációk.

Megoldás. ρ_H reflexív, mert $\forall x \in G : x\rho_H x \Leftrightarrow x^{-1}x = e \in H$ igaz,

ρ_H szimmetrikus: tegyük fel, hogy $x\rho_H y$, azaz $x^{-1}y \in H$, akkor $y^{-1}x = (x^{-1}y)^{-1} \in H$, tehát $y\rho_H x$ teljesül,

ρ_H tranzitív: tegyük fel, hogy $x\rho_H y$ és $y\rho_H z$, azaz $x^{-1}y \in H, y^{-1}z \in H$, akkor $(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$, tehát $x\rho_H z$.

Kapjuk, hogy ρ_H ekvivalenciareláció, hasonlóképpen ρ'_H is ekvivalenciareláció.

5.C. A mellékosztályok számossága

Az x elem H szerinti bal oldali és jobb oldali mellékosztályai általában különböznek, tehát $xH \neq Hx$, de bijektív megfeleltetés létesíthető közöttük. Továbbá a G/ρ_H és G/ρ'_H faktorhalmazok között is bijekció létesíthető, pontosabban

5.C.1. Tétel. Ha $(G, \cdot)$ egy csoport és $H \leq G$, akkor

a) $\forall x \in G : |xH| = |Hx| = |H|$, vagyis az x elem H szerinti bal oldali és jobb oldali mellékosztályai egyenlő számosságúak és ez egyenlő a H számosságával,

b) $|G/\rho_H| = |G/\rho'_H|$.

Bizonyítás. a) Minden $x \in G$ -re $f : H \rightarrow xH$, $f(h) = xh$ és $g : H \rightarrow Hx$, $g(h) = hx$ bijektív függvények, ezek éppen a 3.D szakaszban definiált translációk.

★ b) Legyen $\forall M \in G/\rho_H$, akkor $M = xH$, $x \in G$ és $M^{-1} = (xH)^{-1} = H^{-1}x^{-1} = Hx^{-1} \in G/\rho'_H$, mert $H^{-1} = H$, hiszen $H \leq G$. Hasonlóan, ha $N = Hx \in G/\rho'_H$, akkor $N^{-1} = x^{-1}H \in G/\rho_H$. Ezért értelmezhetők a következő függvények:

$$\varphi : G/\rho_H \rightarrow G/\rho'_H, \quad \varphi(xH) = Hx^{-1},$$

$$\psi : G/\rho'_H \rightarrow G/\rho_H, \quad \psi(Hx) = x^{-1}H,$$

Továbbá $\psi(\varphi(xH)) = \psi(Hx^{-1}) = (x^{-1})^{-1}H = xH = \mathbf{1}_{G/\rho_H}(xH)$ és hasonlóan

$\varphi(\psi(Hx)) = Hx = \mathbf{1}_{G/\rho'_H}(Hx)$, tehát az adott függvények egymás inverzei, s így mindkettő bijektív.

★ □

A $|G/\rho_H| = |G/\rho'_H|$ számot $[G : H]$ -val jelöljük és a H részcsoport G -beli **indexének** nevezzük. Az index tehát a különböző bal oldali (illetve jobb oldali) mellékosztályok száma.

5.C.2. Példa. • ha $n \in \mathbb{N}^*$, akkor $n\mathbb{Z}$ -nek $(\mathbb{Z}, +)$ -beli indexe $[\mathbb{Z} : \mathbb{Z}_n] = n$,

• ha G egy csoport, akkor $[G : G] = 1$, $[G : \{e\}] = |G|$.

Véges csoportban az index véges, de végtelen csoportban is lehet egy részcsoport indexe véges, pl. $[\mathbb{Z} : n\mathbb{Z}] = n$.

5.D. Lagrange tétele, elem rendjének tulajdonságai

5.D.1. Tétel. (Lagrange tétele) Ha $(G, \cdot)$ egy véges csoport és $H \leq G$, akkor

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

Tehát $|G|$ osztható $|H|$ -val és $[G : H]$ -val, azaz a csoport rendje osztható bármely részcsoportjának rendjével és a részcsoport indexével.

Bizonyítás. Az 5.C.1. Tétel szerint minden $xH \in G/\rho_H$ baloldali mellékosztály azonos számosságú és számossága $|H|$, és mivel G/ρ_H egy osztályozása (partíciója) G -nek, ezért $|G| = |H|k$, ahol k az osztályok száma: $k = |G/\rho_H| = [G : H]$. □

A Lagrange tétel a csoportelmélet egyik alapvető tétele, amelyből következik, hogy például egy 6-odrendű csoportnak nem lehetnek 4-edrendű részcsoportjai. További következmények, lásd 3.G.6. Tétel.

5.D.2. Következmény. Legyen G egy véges n -edrendű csoport. Akkor minden $x \in G$ elem rendje osztója G rendjének és $x^n = e$.

Bizonyítás. a) Legyen $o(x) = k$. Tudjuk, hogy $H = \langle x \rangle = \{e, x, x^2, \dots, x^{k-1}\}$, ahol $|H| = k$. A Lagrange-tétel szerint $|G| = |H|[G : H] = k[G : H]$, s innen k osztója $|G| = n$ -nek.

b) A a) pont szerint $|G| = n = k\ell$, ahonnan $x^n = (x^k)^\ell = e$, kész. □

5.D.3. Példa. • Ha p prím, akkor egy p rendű csoport minden $x \neq e$ elemének rendje p .

5.D.4. Tétel. Minden p -edrendű csoport, ahol p prím, ciklikus és bármely két p -edrendű csoport izomorf.

Bizonyítás. Legyen $x \in G$, $x \neq e$, akkor 5.D.3. alapján $o(x) = p$, ezért $\langle x \rangle = G$, tehát G ciklikus. □

5.D.5. Feladat. Határozzuk meg azokat a csoportokat, amelyeknek nincs valódi részcsoportjuk.

Megoldás. Biztosan ilyen a $G = \{e\}$ egyelemű csoport és minden $|G| = p$ prímrendű csoport, lásd Lagrange tétel.

Legyen G ilyen csoport és $x \in G, x \neq e$, akkor $\langle x \rangle \leq G$, amelynek 1-nél több eleme van, ezért $\langle x \rangle = G$ kell legyen. G tehát ciklikus és $|G| = o(x)$ nem lehet végtelen vagy összetett, mert ha $o(x) = st, s, t > 1$, akkor $\langle x^s \rangle = \{x^s, x^{2s}, \dots, x^{ts} = x^{o(x)} = e\}$ valódi részcsoport, ha $o(x) = \infty$, akkor $\langle x^2 \rangle = \{x^{2k} : k \in \mathbb{Z}\}$ valódi részcsoport (másképp: használjuk a ciklikus csoportok részcsoportjaira vonatkozó Tetelt).

Tehát a válasz: az egyelemű csoport és a prímrendű (ciklikus) csoportok.

5.D.6. Tétel. (A 4-edrendű csoportok leírása) Ha G egy csoport, $|G| = 4$, akkor vagy G ciklikus, azaz izomorf $\mathbb{Z}_4$ -gyel, vagy G izomorf a Klein csoporttal (G mindkét esetben kommutatív).

Bizonyítás. Legyen $G = \{e, x, y, z\}$. Ha létezik negyedrendű elem, pl. $o(x) = 4$, akkor G ciklikus, $G = \langle x \rangle$. Ilyen pl. a $(\mathbb{Z}_4, +)$ csoport.

Ellenkező esetben $o(x) = o(y) = o(z) = 2$, mert az elem rendje a csoport rendjének osztója. Akkor $xy = x \Rightarrow y = e$ nem lehet, $xy = y \Rightarrow x = e$ nem lehet, $xy = e \Rightarrow x = x^{-1} = y$ nem lehet, tehát $xy = z$ és $G = \{e, x, y, xy\}$ és $yx = y^{-1}x^{-1} = (xy)^{-1} = z^{-1} = z = xy$, a csoport kommutatív (készítsünk műveletábrát). Itt x, y, z közül bármely kettő szorzata egyenlő a harmadikkal és $x^2 = y^2 = e$, ez a Klein-csoport, lásd 3.B. szakasz és 3.E.5/1. Feladat. $\square$

Hasonlóképpen adható meg a 6-odrendű csoportok leírása: ha $|G| = 6$, akkor G vagy ciklikus: $G \simeq (\mathbb{Z}_6, +)$, vagy $G \simeq (S_3, \circ)$ a harmadfokú permutációcsoport, ez nem kommutatív. Ennek levezetése azonban így módon hosszadalmas, lásd később a struktúratételeket.

★ Jelölje $\nu(n)$ az n -edrendű csoporttípusok számát. Akkor $\nu(p) = 1$, $\nu(4) = \nu(6) = 2$, stb., a Cayley-tételből következik, hogy $\nu(n) \leq 2^{n!}$, mert $|S_n| = n!$ és $|\mathcal{P}(S_n)| = 2^{n!}$, de ez nagyon pontatlan becslés. ★

★ **5.D.7. Tétel.** Legyen $(G, \cdot)$ egy csoport és $x \in G, o(x) = n \in \mathbb{N}^*$. Akkor

a) minden $k \in \mathbb{Z}$ esetén $o(x^k) = \frac{n}{(k, n)}$,

b) ha $k|n$, akkor $o(x^k) = n/k$.

Bizonyítás. a) Legyen $(k, n) = d, k = dk_1, n = dn_1$, ahol $(k_1, n_1) = 1$. Legyen $o(x^k) = m$. Kérdés: $m = n_1$? Valóban, $(x^k)^{n_1} = x^{dk_1 n_1} = (x^n)^{k_1} = e$, innen $m|n_1$ és $e = (x^k)^m = x^{km}$ alapján $n|km, dn_1|dk_1 m, n_1|k_1 m$, ahonnan $n_1|m$, mert $(k_1, n_1) = 1$.

b) azonnali a) alapján. $\square$

5.D.8. Feladat. Legyen $(G, \cdot)$ egy csoport, $x \in G, o(x) = n \in \mathbb{N}^*$ és $k \in \mathbb{Z}$. Igazoljuk, hogy

a) $\langle x^k \rangle = \langle x^d \rangle$, ahol $d = (n, k)$,

b) $\langle x^k \rangle = \langle x \rangle \Leftrightarrow (n, k) = 1$.

Megoldás. a) Az 5.D.7. jelöléseivel $x^k = (x^d)^{k_1} \in \langle x^d \rangle$, innen $\langle x^k \rangle \subseteq \langle x^d \rangle$. Fordítva, $\exists u, v \in \mathbb{Z} : d = ku + nv, x^d = x^{ku+nv} = (x^k)^u \in \langle x^k \rangle$, tehát $\langle x^d \rangle \subseteq \langle x^k \rangle$.

b) Ha $d = 1$, akkor $\langle x^k \rangle = \langle x \rangle$. Fordítva, ha $x \in \langle x^k \rangle$, akkor $\exists u \in \mathbb{Z} : x = x^{ku}, x^{ku-1} = e$, innen $n|ku - 1, \exists v \in \mathbb{Z} : ku - 1 = nv, ku - nv = 1$, ezért $(n, k) = 1$. ★

★ 5.E. Megjegyzések

Ha $(G, \cdot)$ egy csoport és $x \in G$, akkor az $f : (\mathbb{Z}, +) \rightarrow (G, \cdot), f(k) = x^k$ függvény homomorfizmus, mert $f(k + \ell) = x^{k+\ell} = x^k x^\ell = f(k)f(\ell)$ és $\text{Im } f = \langle x \rangle$.

A 4.C.1. Tétel szerint $\text{Ker } f \leq \mathbb{Z}$. De tudjuk, hogy $(\mathbb{Z}, +)$ minden részcsoportja $n\mathbb{Z}$ alakú, ezért $\text{Ker } f = n\mathbb{Z}$, valamilyen $n \in \mathbb{N}$ -re. Ha $n = 0$, akkor $\text{Ker } f = \{0\}$, f injektív, azaz $x^k \neq x^\ell, \forall k, \ell \in \mathbb{Z}, k \neq \ell$ és x végtelen rendű. Ha $n \geq 1$, akkor f nem injektív és éppen ez az n lesz x rendje.

Igazolható a következő tulajdonság: Ha G egy véges csoport, $H \leq G$, akkor megadható a G elemeinek egy olyan rendszere, amely H -szerinti jobb oldali és bal oldali reprezentánsrendszer is. ★

5.F. Feladatok

▼ 1. Legyen $(G, \cdot)$ egy csoport és $\emptyset \neq H \subseteq G$ egy zárt részhalmaz. Ha minden H -beli elem végesrendű, akkor H részcsoport (Speciálisan, ha H véges, akkor $H \leq G$, lásd 4.J/1. Feladat).

Megoldás. $\forall x \in H : o(x) = n \in \mathbb{N}^* \Rightarrow x^n = e \Rightarrow x^{-1} = x^{n-1} \in H$, mert H zárt. Ha H véges, akkor H minden x eleme végesrendű, mert ellenkező esetben $x, x^2, x^3, \dots \in H$ végtelen sok különböző elem, ellentmondás.

▼ 2. Legyen $f : G \rightarrow G'$ egy csoportmorfizmus és $x \in G$. Igazoljuk, hogy

a) $o(f(x)) | o(x)$,

b) ha f injektív, akkor $o(f(x)) = o(x)$,

c) ha f izomorfizmus, akkor minden $n \in \mathbb{N}^*$ -ra $|\{x \in G : o(x) = n\}| = |\{y \in G' : o(y) = n\}|$,

d) alkalmazás: $(\mathbb{Q}, +) \not\cong (\mathbb{Q}^*, \cdot)$, $(\mathbb{R}, +) \not\cong (\mathbb{R}^*, \cdot)$, $(\mathbb{C}, +) \not\cong (\mathbb{C}^*, \cdot)$, $(\mathbb{R}^*, \cdot) \not\cong (\mathbb{C}^*, \cdot)$.

Megoldás. a) Legyen $o(x) = n$, akkor $(f(x))^n = f(x^n) = f(e) = e'$, ezért $o(f(x)) | n = o(x)$.

b) Kérdés: $o(x) | o(f(x))$? Legyen $o(f(x)) = m$, akkor $e' = (f(x))^m = f(x^m)$, $e' = f(e)$ és mivel f injektív következik, hogy $x^m = e$, innen $o(x) = n | m = o(f(x))$.

c) A b) alapján $F : \{x \in G : o(x) = n\} \rightarrow \{y \in G' : o(y) = n\}$, $F(x) = f(x)$ jól értelmezett és izomorfizmus (f leszűkítése).

d) Pl. $(\mathbb{R}, +)$ -ban nincs másodrendű elem ($2x = 0 \Leftrightarrow x = 0$, de $o(0) = 1$), $(\mathbb{R}^*, \cdot)$ -ban $x = -1$ másodrendű elem ($x^2 = 1 \Leftrightarrow x = \pm 1$, $o(-1) = 2$, $o(1) = 1$).

$(\mathbb{R}^*, \cdot)$ -ban nincs negyedrendű elem ($x^4 = 1 \Leftrightarrow x = \pm 1$, de $o(1) = 1$, $o(-1) = 2$), $(\mathbb{C}^*, \cdot)$ -ban $x = \pm i$ negyedrendű elemek ($x^4 = 1 \Leftrightarrow x = \pm 1, \pm i$).

★ ▼ 3. Legyen $(G, \cdot)$ egy csoport és $x, y \in G$ úgy, hogy $xy = yx$, $o(x) = m$, $o(y) = n$. Igazoljuk, hogy:

a) $o(xy) | [m, n]$,

b) Ha $\langle x \rangle \cap \langle y \rangle = \{e\}$, akkor $o(xy) = [m, n]$,

c) Ha $(m, n) = 1$, akkor $o(xy) = mn$ és $\langle xy \rangle = \langle \{x, y\} \rangle$,

d) Létezik $g \in G$ úgy, hogy $o(g) = [m, n]$.

Megoldás. a) $(xy)^{[m, n]} = x^{[m, n]} y^{[m, n]} = (x^m)^{[m, n]/m} (y^n)^{[m, n]/n} = e$, ezért $o(xy) | [m, n]$.

b) Legyen $o(xy) = \ell$, akkor $(xy)^\ell = e \Rightarrow x^\ell = y^{-\ell} \in \langle x \rangle \cap \langle y \rangle = \{e\} \Rightarrow x^\ell = y^\ell = e$, innen $m | \ell$, $n | \ell$ és $[m, n] | \ell$.

c) Ha $(m, n) = 1$, akkor $[m, n] = mn$. Továbbá $\langle x \rangle \cap \langle y \rangle = \{e\}$, valóban: legyen $H = \langle x \rangle \cap \langle y \rangle$, akkor $H \leq \langle x \rangle$, innen $|H| | |\langle x \rangle| = m$ (Lagrange-tétel), hasonlóan $|H| | n$ és $(m, n) = 1$ miatt $|H| = 1$, $H = \{e\}$.

Azonnali, hogy $\langle xy \rangle \leq \langle \{x, y\} \rangle$, továbbá $(m, n) = 1$ miatt $\exists u, v \in \mathbb{Z} : mu + nv = 1$, innen $y = y^{mu+nv} = y^{mu} = (xy)^{mu} \in \langle xy \rangle$, hasonlóan $x \in \langle xy \rangle$, tehát $\langle \{x, y\} \rangle \leq \langle xy \rangle$.

d) Legyen pl. $o(x) = m = 2^2 \cdot 3^3 \cdot 5$, $o(y) = n = 2 \cdot 3^2 \cdot 5^4$, akkor $[m, n] = 2^2 \cdot 3^3 \cdot 5^4 = m'n'$, ahol $m' = 2^2 \cdot 3^3$ (itt m kitevői a nagyobbak), $n' = 5^4$ (n kitevői a nagyobbak). Legyen $m'' = 2 \cdot 3^2$, $n'' = 5$ (itt a kitevők fordítva), akkor $o(x^{n''}) = o(x^5) = 2^2 \cdot 3^3 = m'$, $o(y^{m''}) = o(y^{2 \cdot 3^2}) = 5^4 = n'$. Mivel $(m', n') = 1$ következik, hogy $o(x^{n''} y^{m''}) = [m, n]$. Hasonlóan általánosan.

▼ 4. Ha G egy csoport és $K \leq H \leq G$, akkor igazoljuk, hogy $[G : K] = [G : H][H : K]$.

Megoldás. Legyen $G = \cup_{i \in I} x_i H$, ahol $x_i H \cap x_j H = \emptyset, \forall i, j \in I, i \neq j$. Azt mondjuk, hogy $\{x_i : i \in I\} \subseteq G$ egy H szerinti bal oldali reprezentánsrendszer.

Legyen továbbá $\{y_j : j \in J\} \subseteq H$ egy K szerinti bal oldali reprezentánsrendszer. Elég igazolni, hogy $\{x_i y_j : (i, j) \in I \times J\} \subseteq G$ egy K szerinti bal oldali reprezentánsrendszer.

Valóban, $\cup_{(i, j) \in I \times J} x_i y_j K = \cup_{i \in I} x_i (\cup_{j \in J} y_j K) = \cup_{i \in I} x_i H = G$.

Továbbá, legyen $(i, j) \neq (i', j')$. Ha $i \neq i'$, akkor $x_i y_j K \cap x_{i'} y_{j'} K \subseteq x_i H \cap x_{i'} H = \emptyset$. Ha $i = i'$ és $j \neq j'$, akkor $x_i y_j K \cap x_{i'} y_{j'} K = x_i (y_j K \cap y_{j'} K) = \emptyset$. ★

6. Normálrészcsoporthok

6.A. Normálrészcsoporthok és jellemzésük

A $(G, \cdot)$ csoport egy H részcsoporthját **normálrészcsoporthnak** (**normális részcsoporthnak** vagy **normálosztónak** vagy **invariáns részcsoporthnak**) nevezzük, ha minden $x \in G$ -re $xH = Hx$, azaz ha minden $x \in G$ elem H szerinti bal oldali és jobb oldali mellékosztályai egyenlőek, jelölés: $H \trianglelefteq G$.

Kommutatív csoport esetén minden $H \leq G$ -re és minden $x \in G$ -re $xH = Hx$, tehát kommutatív csoport minden részcsoporthja normálrészcsoporth, de nem kommutatív csoport esetén is megtörténhet ez valamely H részcsoporthra.

6.A.1. Tétel. (normálrészcsoporthok jellemzése) Legyen $(G, \cdot)$ egy csoport és $H \leq G$. Egyenértékűek a következő állítások:

- 1) H normálrészcsoporth,
- 2) $\forall x \in G, \forall h \in H : xhx^{-1} \in H$, azaz $\forall x \in G : xHx^{-1} \subseteq H$,
- 3) $\rho_H = \rho'_H$ (a H szerinti jobb oldali és bal oldali kongruenciarelációk egyenlőek).

Bizonyítás. "1) $\Rightarrow$ 2)" $\forall x \in G, \forall h \in H : xh \in xH = Hx \Rightarrow \exists h' \in H : xh = h'x \Rightarrow xhx^{-1} = h' \in H$.

"2) $\Rightarrow$ 3)" $\forall x, y \in G : x\rho_H y \Leftrightarrow x^{-1}y \in H \Leftrightarrow x(x^{-1}y)x^{-1} \in H$ (a feltétel alapján, ahol ha $x(x^{-1}y)x^{-1} \in H$, akkor szorozva balról x^{-1} -gyel és jobbról $(x^{-1})^{-1} = x$ -szel következik, hogy $x^{-1}y \in H$) $\Leftrightarrow yx^{-1} \in H \Leftrightarrow y\rho'_H x \Leftrightarrow x\rho'_H y$, tehát $\rho_H = \rho'_H$.

"3) $\Rightarrow$ 1)" $\rho_H = \rho'_H \Rightarrow \forall x \in G : \rho_H \langle x \rangle = \rho'_H \langle x \rangle$, tehát $xH = Hx$. $\square$

6.A.2. Feladat. Legyen $H \leq G$. Igazoljuk, hogy egyenértékűek a következő állítások:

- 1) H normálrészcsoporth,
- 2') $\forall x \in G : xHx^{-1} = H$,
- 3') $\forall x \in G : x^{-1}Hx = H$.

Tehát H akkor és csak akkor normálrészcsoporth, ha H minden konjugáltja egyenlő H -val, lásd 4.F. szakasz.

Ha H normálrészcsoporthja G -nek, akkor a következő jelölést használjuk: $G/\rho_H = G/\rho'_H = G/H$ és gyakran H helyett N -et írunk.

6.B. Példák normálrészcsoporthokra

6.B.1. Példák. • Minden G csoport esetén $\{e\}$ és G normálrészcsoporthok.

• Legyen $H = \{e, \tau\} \leq S_3$ részcsoporth, ahol $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ és $\tau\tau = e$. Ha $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, akkor $\sigma H = \left\{ \sigma, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \neq \left\{ \sigma, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\} = H\sigma$, tehát H nem normálosztó S_3 -ban.

• Egy csoport minden 2 indexű részcsoporthja normálrészcsoporth: ha $H \leq G$ és $[G : H] = 2$, akkor $H \trianglelefteq G$. Valóban, $G/\rho_H = \{H, G \setminus H\} = G/\rho_j$, mert ez osztályozás kell legyen és H az egyik osztály. További fontos példákat ad a következő Tétel.

6.B.2. Tétel. 1) Ha $f : G \rightarrow G'$ egy csoportmorfizmus, akkor ennek magja normálrészcsoporthja G -nek: $\text{Ker } f \trianglelefteq G$.

Ha $(G, \cdot)$ egy csoport, akkor a $Z(G) = \{g \in G : gx = xg, \forall x \in G\}$ centrum normálrészcsoporthja G -nek: $Z(G) \trianglelefteq G$.

Bizonyítás. 1) Valóban, $\forall x \in G, \forall h \in \text{Ker } f \Rightarrow f(xhx^{-1}) = f(x)f(h)f(x^{-1}) = f(x)e'f(x)^{-1} = e'$, ahonnan $xhx^{-1} \in \text{Ker } f$.

2) Tudjuk, hogy $Z(G) \leq G$, továbbá $Z(G)$ normálrészcsoporth, mert $\forall x \in G : xZ(G) = \{xg : g \in Z(G)\} = \{gx : g \in Z(G)\} = Z(G)x$. $\square$

A G csoportot **egyszerű csoportnak** nevezzük, ha $\{e\}$ és G az egyedüli normálrészcsoporthok G -ben, azaz G -nek nincs valódi normálosztója.

6.B.3. Példák. • $(\mathbb{Z}_p, +)$, ahol p prím, egyszerű csoport, általánosabban minden $(G, \cdot)$ prímrendű csoport egyszerű, mert a Lagrange tétel szerint ekkor G -nek nincs valódi részcsoporthja, tehát nincs valódi normálosztója sem.

• $(\mathbb{Z}, +)$ nem egyszerű csoport, mert $n\mathbb{Z} \trianglelefteq \mathbb{Z}, n > 1$ valódi normálosztó.

★ **6.B.4. Feladat.** ▼ Vizsgáljuk az S_3 permutációcsoport részcsoporthjait. Melyek a normálrészcsoporthok? (lásd 3.B.6/1 Feladat)

Megoldás. S_3 részcsoportjai: ha $H \leq S_3$, akkor a Lagrange-tétel szerint $|H| = 1, 2, 3$, vagy 6 .
 $|H| = 1 \Leftrightarrow H = H_1 := \{e\}$. $|H| = 2 \Leftrightarrow H = \{e, x\}$, ahol $x^2 = e$ és kapjuk, hogy $H_2 := \{e, \tau\}$, $H_3 := \{e, \sigma\tau\}$, $H_4 := \{e, \sigma^2\tau\}$, a műveletábra szerint. Továbbá $|H| = 3 \Leftrightarrow H = \{e, x, x^2\}$, ahol $x^3 = e$ és következik, hogy $H = H_5 := \{e, \sigma, \sigma^2\} = A_3$. $|H| = 6 \Leftrightarrow H = H_6 := S_3$.

$H_1, H_5, H_6 \leq S_3$ (itt $[S_3 : H_5] = 2$), de H_2, H_3, H_4 nem normálrészcsoportok, lásd 6.B.1. ★

6.C. Normálrészcsoportok metszete

6.C.1. Tétel. Két normálrészcsoport metszete is normálrészcsoport. Általánosabban, ha $(G, \cdot)$ egy csoport és $(N_i)_{i \in I}$ normálrészcsoportok tetszőleges rendszere, akkor

$$\bigcap_{i \in I} N_i \leq G, \quad \langle \bigcup_{i \in I} N_i \rangle \leq G.$$

Bizonyítás. Tudjuk, hogy $\cap_{i \in I} N_i \leq G$, $\langle \cup_{i \in I} N_i \rangle \leq G$ részcsoportok. Továbbá,

$$\begin{aligned} \forall x \in G: \quad \forall n \in \cap_{i \in I} N_i &\Rightarrow n \in N_i, \forall i \in I \Rightarrow xnx^{-1} \in N_i, \forall i \in I \Rightarrow \\ &\Rightarrow xnx^{-1} \in \cap_{i \in I} N_i. \end{aligned}$$

★ A 4.E.2. Tétel szerint $\forall n \in \langle \cup_{i \in I} N_i \rangle \Rightarrow n = n_1 n_2 \dots n_r$ alakú, ahol minden $j \in \{1, 2, \dots, r\}$ esetén vagy $n_j \in \cup_{i \in I} N_i$, vagy $n_j^{-1} \in \cup_{i \in I} N_i$. Következik, hogy $\forall j \in \{1, 2, \dots, r\}$ -re $\exists i_j \in I : n_j = n_{i_j}$ úgy, hogy vagy $n_{i_j} \in N_{i_j}$, vagy $n_{i_j}^{-1} \in N_{i_j}$, de ez utóbbi esetben is $n_{i_j} \in N_{i_j}$, mivel N_{i_j} részcsoport. Kapjuk, hogy $n = n_{i_1} n_{i_2} \dots n_{i_r}$ és kihasználva, hogy minden N_{i_j} normálrészcsoport, $\forall x \in G$:

$$xnx^{-1} = xn_{i_1} n_{i_2} \dots n_{i_r} x^{-1} = \underbrace{(xn_{i_1} x^{-1})}_{\in N_{i_1}} \underbrace{(xn_{i_2} x^{-1})}_{\in N_{i_2}} \dots \underbrace{(xn_{i_r} x^{-1})}_{\in N_{i_r}} \in \langle \cup_{i \in I} N_i \rangle. \quad \square \star$$

6.D. Kongruenciareláció csoportban

Legyen $(G, \cdot)$ egy csoport és ρ egy ekvivalenciareláció G -n. Azt mondjuk, hogy ρ **kongruenciareláció**, ha

$$\forall x, x', y, y' \in G: \quad x\rho x', \quad y\rho y' \Rightarrow x\rho y \Rightarrow xy' \rho yy'$$

(a ρ szerinti kongruenciák összesorozhatók), lásd 2.G. szakasz.

G -nek egy ρ kongruenciarelációhoz tartozó osztályozását, vagyis a G/ρ faktorhalmazt **kompatibilis osztályozásnak** nevezzük.

6.D.1. Példa. • Tekintsük a $(\mathbb{Z}, +)$ csoportot és a számelméleti kongruenciarelációt $(\text{mod } n)$. Ez ilyen tulajdonságú:

$$\forall x, y, x', y' \in \mathbb{Z}: \quad x \equiv x' \pmod{n}, \quad y \equiv y' \pmod{n} \Rightarrow x + y \equiv x' + y' \pmod{n}.$$

$\mathbb{Z}$ -nek a $(\text{mod } n)$ maradékosztályok halmazaira való bontása egy kompatibilis osztályozás.

★ **6.D.2. Feladat.** Ha G egy csoport és ρ egy kongruenciareláció, akkor igazoljuk, hogy

1) $\forall x, x' \in G: x\rho x' \Rightarrow x^{-1}\rho(x')^{-1}$, azaz ha két elem egy osztályban van, akkor az inverzeik is azonos osztályban vannak,

2) $\forall X \in G/\rho \Rightarrow \exists Y \in G/\rho: X^{-1} \subseteq Y$.

Megoldás. 1) Ha $x\rho x'$, akkor x^{-1} -nel szorozva (lásd 2.G.3. Feladat): $e = xx^{-1}\rho x'x^{-1}$, most $(x')^{-1}$ -gyel szorozva: $(x')^{-1}\rho(x')^{-1}x'x^{-1} = x^{-1}$.

2) $\forall X \in G/\rho$ -re legyen $X = \langle x \rangle$ és legyen $Y = \langle x^{-1} \rangle$ az x^{-1} osztálya.

$\forall (x')^{-1} \in X^{-1} \Rightarrow x' \in X \Rightarrow x\rho x'$, ahonnan 1) alapján $x^{-1}\rho(x')^{-1} \Rightarrow (x')^{-1} \in Y$, tehát $X^{-1} \subseteq Y$.

□★

6.D.3. Tétel. (normálrészcsoportok és kongruenciarelációk kapcsolata) Legyen G egy csoport.

a) Ha $N \leq G$, akkor ρ_N kongruenciareláció (tehát a normális részcsoportok szerinti mellékosztályok a csoport egy kompatibilis osztályozását adják),

b) Ha ρ egy kongruenciareláció, akkor $G/\rho = \{xN : x \in G\}$, ahol $N = \rho\langle e \rangle \leq G$ (minden kompatibilis osztályozás osztályai valamely normális részcsoport szerinti mellékosztályok).

Bizonyítás. a) Láttuk már, hogy ρ_N ekvivalenciareláció. Továbbá:

$$\begin{aligned} \forall x, x', y, y' \in G : \quad x\rho_N x', y\rho_N y' &\Rightarrow x^{-1}x' \in N, y^{-1}y' \in N \Rightarrow \\ &\Rightarrow (xy)^{-1}(x'y') = y^{-1}x^{-1}x'y' = \underbrace{(y^{-1} \underbrace{x^{-1}x'}_{\in N} y)}_{\in N} \underbrace{(y^{-1}y')}_{\in N} \in N, \end{aligned}$$

tehát $xy\rho_N x'y'$.

★ b) $N = \rho\langle e \rangle \neq \emptyset$, mert $e\rho e$. Továbbá $\forall x, y \in N \Rightarrow e\rho x, e\rho y$. De $e\rho y$ és $y^{-1}\rho y^{-1}$ miatt (ez utóbbi a reflexivitásból) $ey^{-1}\rho yy^{-1} \Rightarrow y^{-1}\rho e$, tehát $N \leq G$.

Megmutatjuk, hogy $\forall x \in G \Rightarrow xN = Nx = \rho\langle x \rangle$. Valóban, $xN \subseteq \rho\langle x \rangle$, mert $\forall xn \in xN \Rightarrow n\rho e, x\rho x \Rightarrow nx\rho x$. Fordítva, $\rho\langle x \rangle \subseteq xN$, mert $\forall y \in \rho\langle x \rangle \Rightarrow y\rho x, x^{-1}\rho x^{-1}$ (reflexivitás) $\Rightarrow x^{-1}y\rho e \Rightarrow x^{-1}y \in N$, tehát $y = x(x^{-1}y) \in xN$. Hasonlóan $Nx = \rho\langle x \rangle$. Tehát $xN = Nx$, azaz $N \trianglelefteq G$.

Ezzel azt is igazoltuk, hogy minden $x \in G$ -re $\rho\langle x \rangle = xN$, tehát az osztályok az N szerinti mellékosztályok. ★ □

★ 6.E. Normálrészcsoportok megfeleltetési tétele

6.E.1. Tétel. (normálrészcsoportok megfeleltetési tétele) Legyen $f : G \rightarrow G'$ egy csoportmorfizmus. Akkor

- 1) minden $K \trianglelefteq G'$ esetén $f^{-1}(K) \trianglelefteq G$,
- 2) ha f szürjektív és $H \trianglelefteq G$, akkor $f(H) \trianglelefteq G'$,
- 3) ha f szürjektív, akkor $H \mapsto f(H)$ bijektív megfeleltetés G -nek a $\text{Ker } f$ -et tartalmazó normálrészcsoportjai és G' normálrészcsoportjai között.

Bizonyítás. 1) A 4.B.6. Tétel szerint $f^{-1}(K) \leq G$ és $\forall x \in G, \forall h \in f^{-1}(K) \Rightarrow f(h) \in K, f(xhx^{-1}) = f(x)f(h)f(x)^{-1} \in K$, mert $K \trianglelefteq G'$. Tehát $f^{-1}(K) \trianglelefteq G$.

2) $f(H) \leq G'$ (lásd ua. a Tétel) és $\forall y \in G', \forall k \in f(H) \Rightarrow \exists x \in G : y = f(x)$, mert f szürjektív, és $\exists h \in H : k = f(h)$, innen $yky^{-1} = f(x)f(h)f(x)^{-1} = f(xhx^{-1}) \in f(H)$, mert $xhx^{-1} \in H$. Tehát $f(H) \trianglelefteq G'$.

3) Következik 1) és 2)-ből valamint a részcsoportok megfeleltetési tételéből (4.I.1. Tétel). □

6.E.2. Következmény. Ha $f : G \rightarrow G'$ csoportmorfizmus, akkor $\text{Ker } f = f^{-1}(\{e'\}) \trianglelefteq G$, mert $\{e'\} \trianglelefteq G'$. $\text{Ker } f$ tehát normálrészcsoport, ezt már láttuk közvetlen ellenőrzéssel. ★

★ 6.F. Megjegyzések

Bemutatjuk a 6.D.3. tétel első részének egy más bizonyítását részhalmazok (komplexusok) segítségével. Bizonyos esetekben ezek használata lerövidíti, átláthatóbbá teszi csoportelméleti tulajdonságok megfogalmazását és bizonyítását.

a) Ha $N \trianglelefteq G$, akkor az $xN = Nx$ mellékosztályok (a G/ρ faktorhalmaz elemei) páronként diszjunktak, tehát egy osztályozást adnak. Legyen xN, yN két mellékosztály, akkor $(xN)(yN) = x(Ny)N = x(yN)N = (xy)(NN) = (xy)N$ ismét egy N szerinti mellékosztály(ban van), tehát kompatibilis osztályozás a 2.G.2. Tétel szerint.

b) Fordítva, ha adott egy kompatibilis osztályozás, legyen N az e -t tartalmazó osztály: $N = \rho\langle e \rangle$.

Belátjuk, hogy $NN \subseteq N$ és $N^{-1} \subseteq N$. Valóban, $\forall xy \in NN \Rightarrow x\rho e, y\rho e \Rightarrow xy\rho ee = e \Rightarrow xy \in N$ (másképp: NN része egy osztálynak, lásd 2.G. szakasz, és $e \in NN$, ezért ez az osztály csak az N lehet: $NN \subseteq N$), továbbá $\forall x^{-1} \in N^{-1} \Rightarrow x \in N \Rightarrow x\rho e, x^{-1}\rho x^{-1}$ (reflexivitás) $\Rightarrow xx^{-1}\rho ex^{-1} \Rightarrow e\rho x^{-1} \Rightarrow x^{-1} \in N$ (másképp: N^{-1} része egy osztálynak, lásd 6.D.2. Feladat, és $e \in N^{-1}$ miatt ez csak az N lehet: $N^{-1} \subseteq N$). Tehát $N \leq G$. □★

★ 6.G. Feladatok

▼ 1. Legyen $(G, \cdot)$ egy csoport.

a) Egy $N \leq G$ részcsoport akkor és csak akkor normálosztó, ha minden K komplexus esetén $KN = NK$.

b) Ha $H \leq G$ és $N \trianglelefteq G$, akkor $HN = NH \leq G$ és ez éppen a H és N által generált részcsoport: $\langle H \cup N \rangle = HN = NH$.

Megoldás. a) Ha $N \trianglelefteq G$ és K komplexus, akkor $KN = \cup_{x \in K} xN = \cup_{x \in K} Nx = NK$. Fordítva, ha $KN = NK$ minden K komplexusra, akkor legyen $K = \{x\}, x \in G$ és kapjuk, hogy $xN = Nx$, $\forall x \in G$, ahonnan $N \trianglelefteq G$.

b) $HN = NH$ az a) pont szerint és innen $HN \leq G$ következik, lásd 4.B.5 Tétel. Továbbá: $\langle H \cup N \rangle = HN$, lásd 4.E.3. Tétel.

▼ 2. Legyen G egy csoport, $N \trianglelefteq G$ egy ciklikus normális részcsoport és $H \leq N$. Akkor $H \trianglelefteq G$.

Megoldás. Legyen $N = \langle x \rangle$ és $H = \langle x^m \rangle$, $m \geq 1$. Kérdés: $\forall g \in G, \forall x^{km} \in H \Rightarrow gx^{km}g^{-1} \in H$? Mivel $N \trianglelefteq G$ következik, hogy $gxg^{-1} = x^n \in N$, innen $gx^{km}g^{-1} = gxg^{-1}gxg^{-1} \dots gxg^{-1} = (gxg^{-1})^{km} = x^{knm} \in H$.

▼ 3. Vizsgáljuk a Q kvaterniócsoport részcsoportjait, lásd 3.B.8. Igazoljuk, hogy Q minden részcsoportja normálrészcsoport. Adjuk meg Q centrumát és faktorcsoportjait.

Megoldás. Q részcsoportjai: ha $H \leq Q$, akkor a Lagrange-tétel szerint $|H| = 1, 2, 4$, vagy 8 . $|H| = 1 \Leftrightarrow H = H_1 := \{1\}$. $|H| = 2 \Leftrightarrow H = H_2 := \{\pm 1\} = \langle -1 \rangle$, a táblázat szerint ez az egyedüli 2 elemű részcsoport. $|H| = 4 \Leftrightarrow H = H_3 := \{\pm 1, \pm i\} = \langle i \rangle$, vagy $H = H_4 := \{\pm 1, \pm j\} = \langle j \rangle$, vagy $H = H_5 := \{\pm 1, \pm k\} = \langle k \rangle$ ciklikus részcsoportok. (1)-ben csak egy másodrendű elem van, az i^2 , ezért Klein-féle 4 elemű részcsoport nincs. $|H| = 8 \Leftrightarrow H = H_6 := Q$.

Q nem kommutatív, de Q -nak minden részcsoportja normálrészcsoport. Valóban, a 4-edrendű részcsoportok ilyenek, mert indexük 2, lásd 6.B. szakasz, H_2 -re pedig $xH_2 = H_2x = \{x, -x\}, \forall x \in Q$ (Másképp: H_2 az egyedüli másodrendű részcsoport, ezért normálrészcsoport, lásd későbbi Tétel).

Q centruma $Z(Q) = \{1, -1\}$.

A $H_i, 1 \leq i \leq 6$ részcsoportok szerinti faktorcsoporthoz:

$$Q/H_1 = \{\{1\}, \{-1\}, \{i\}, \{-i\}, \{j\}, \{-j\}, \{k\}, \{-k\}\},$$

$$Q/H_2 = \{\{\pm 1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}\},$$

$$Q/H_3 = \{\{\pm 1, \pm i\}, \{\pm j, \pm k\}\},$$

$$Q/H_4 = \{\{\pm 1, \pm j\}, \{\pm i, \pm k\}\},$$

$$Q/H_5 = \{\{\pm 1, \pm k\}, \{\pm i, \pm j\}\},$$

$$Q/H_6 = \{\{\pm 1, \pm i, \pm j, \pm k\}\}.$$

Itt a $H_2 = N$ szerinti mellékosztályok: $N, iN = \{\pm i\}, jN = \{\pm j\}, kN = \{\pm k\}$ és a Q/N faktorcsoporthoz (lásd 7. szakasz) izomorf a Klein-csoporttal. ★

7. Faktorcsoporthok és a homomorfizmus-tétel

7.A. Faktorcsoporth

Legyen $(G, \cdot)$ egy csoport és $N \trianglelefteq G$ egy normálosztó. Láttuk, hogy ekkor $\rho_N = \rho'_N$ és G/N -nel jelöltük a $G/\rho_N = G/\rho'_N$ faktorhalmazt, ahol $G/N = \{xN : x \in G\}$, ennek elemei az $xN = \{xn : n \in N\} = Nx$ mellékosztályok.

Az xN mellékosztályok szorzása művelet a G/N halmazon. Valóban, két tetszőleges N szerinti mellékosztály szorzata: $(xN)(yN) = x(Ny)N = x(yN)N = (xy)NN = (xy)N$ ismét egy N szerinti mellékosztály, ahol használtuk, hogy $NN = N$, lásd 4.B.2. Tétel.

7.A.1. Tétel. Ha G egy csoport és $N \trianglelefteq G$, akkor a G/N halmazon az $(xN)(yN) = (xy)N$ művelet egy csoportstruktúrát határoz meg, ennek neve G -nek N szerinti **faktorcsoporthja**, jelölés $(G/N, \cdot)$.

Ha G véges csoport, akkor

$$|G/N| = \frac{|G|}{|N|}.$$

Bizonyítás. A művelet asszociatív, $eN = N$ az egységelem és xN inverze $(xN)^{-1} = x^{-1}N$, mert $(xN)(x^{-1}N) = (xx^{-1})N = eN = N$ és hasonlóan $(x^{-1}N)(xN) = N$.

Ha G véges, akkor $|G/N| = [G : N] = |G|/|N|$, a Lagrange tétel szerint. $\square$

Ha G kommutatív, akkor minden faktorcsoporthja is kommutatív.

7.A.2. Példa. • Határozzuk meg a $(\mathbb{Z}, +)$ csoport faktorcsoporthjait.

Tudjuk, hogy a $(\mathbb{Z}, +)$ részcsoportjai az $(n\mathbb{Z}, +)$ csoportok, ahol $n \in \mathbb{N}$, ezek mind normálrészcsoportok a kommutativitás miatt. Jelölés: $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, a megfelelő faktorcsoporthok. Ha $n = 0$, akkor $0\mathbb{Z} = \{0\}$ és $\mathbb{Z}_0 = \mathbb{Z}/\{0\} = \{x + \{0\} : x \in \mathbb{Z}\} = \{\{x\} : x \in \mathbb{Z}\} \simeq \mathbb{Z}$. Ha $n = 1$, akkor $1\mathbb{Z} = \mathbb{Z}$ és $\mathbb{Z}_1 = \mathbb{Z}/\mathbb{Z} = \{x + \mathbb{Z} : x \in \mathbb{Z}\} = \{\mathbb{Z}\}$.

Ha $n \geq 2$, akkor $\mathbb{Z}_n = \{x + n\mathbb{Z} : x \in \mathbb{Z}\} = \{\widehat{x} : x \in \mathbb{Z}\} = \{\widehat{0}, \widehat{1}, \dots, \widehat{n-1}\}$, ahol $x + n\mathbb{Z} = \widehat{x}$ jelölés.

★ Ha $N \trianglelefteq G$, akkor a $p_N : G \rightarrow G/N$, $p_N(x) = xN$ leképezést **kanonikus projekciónak** nevezzük. Ez a fentiek szerint homomorfizmus, szürjektív és ennek magja éppen az N : $\text{Ker } p_N = N$. Valóban, $\text{Ker } p_N = \{x \in G : xN = N\} = N$. Tehát minden normálrészcsoport egy homomorfizmus magja.

Az is igaz, hogy ha $N \trianglelefteq G$, akkor a G/N faktorhalmazon egyetlen csoportstruktúra létezik úgy, hogy a $p_N : G \rightarrow G/N$ kanonikus projekció homomorfizmus legyen. Egyértelműség: ha p_N homomorfizmus, akkor $p_N(xy) = p_N(x)p_N(y) \Leftrightarrow (xy)N = (xN)(yN), \forall x, y \in G$. ★

7.B. Homomorfizmus-tétel

7.B.1. Tétel. (homomorfizmus-tétel) Ha $f : G \rightarrow G'$ egy csoportmorfizmus, akkor az

$$\bar{f} : G/\text{Ker } f \rightarrow \text{Im } f, \quad \bar{f}(x \text{ Ker } f) = f(x)$$

függvény csoportizomorfizmus, tehát $G/\text{Ker } f \simeq \text{Im } f$.

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ p \downarrow & & \uparrow i \\ G/\text{Ker } f & \xrightarrow{\bar{f}} & \text{Im } f \end{array}$$

4.ábra

Bizonyítás. Ha $x \text{ Ker } f = x' \text{ Ker } f$, akkor $x\rho_{\text{Ker } f}x'$, ahonnan értelmezés szerint $x(x')^{-1} \in \text{Ker } f$, $f(x(x')^{-1}) = e'$, $f(x)f(x')^{-1} = e'$, $f(x) = f(x')$, tehát $\bar{f}$ helyesen értelmezett (nem függ a reprezentánsoktól).

$\bar{f}$ csoportmorfizmus, mert $\forall x \text{ Ker } f, y \text{ Ker } f \in G/\text{Ker } f \Rightarrow \bar{f}((x \text{ Ker } f)(y \text{ Ker } f)) = \bar{f}((xy) \text{ Ker } f) = f(xy) = f(x)f(y) = \bar{f}(x \text{ Ker } f)\bar{f}(y \text{ Ker } f)$.

$\bar{f}$ szürjektív, mert $\forall z \in \text{Im } f \Rightarrow \exists x \in G : z = f(x)$ és így $\bar{f}(x \text{ Ker } f) = f(x) = z$. Továbbá $\bar{f}$ injektív, mert $\bar{f}(x \text{ Ker } f) = \bar{f}(y \text{ Ker } f) \Rightarrow f(x) = f(y) \Rightarrow f(xy^{-1}) = e' \Rightarrow xy^{-1} \in \text{Ker } f \Rightarrow x \text{ Ker } f = y \text{ Ker } f$. $\square$

Ha $f : G \rightarrow G'$ egy csoportmorfizmus legyen $i : \text{Im } f \rightarrow G'$, $i(y) = y$ az ún. **kanonikus injekció** és $p = p_{\text{Ker } f} : G \rightarrow G/\text{Ker } f$, $p(x) = x \text{ Ker } f$ a $\text{Ker } f$ szerinti kanonikus projekció. Akkor az homomorfizmus-tétel szerint $i \circ \bar{f} \circ p = f$, azaz a 4. ábrán lévő diagram kommutatív.

7.C. Feladatok

▼ 1. Legyenek $a, b \in \mathbb{R}$, $a \neq 0$ és $f_{a,b} : \mathbb{R} \rightarrow \mathbb{R}$, $f_{a,b}(x) = ax + b$.

i) Igazoljuk, hogy $G = \{f_{a,b} : a \in \mathbb{R}^*, b \in \mathbb{R}\}$ csoport a függvénykompozícióra nézve és $H = \{f_{a,0} : a \in \mathbb{R}^*\}$, valamint $N = \{f_{1,b} : b \in \mathbb{R}\}$ ennek részcsoportjai.

ii) Igazoljuk, hogy H részcsoportja G -nek, N normálrészcsoportja G -nek és $(G/N, \circ) \simeq (\mathbb{R}^*, \cdot)$.

iii) H normálrészcsoportja-e G -nek?

Megoldás. i)-ii) Használjuk a részcsoportok jellemzési tételét. G csoport, mert részcsoportja az összes $f : \mathbb{R} \rightarrow \mathbb{R}$ bijektív függvény csoportjának. Valóban, $\forall f_{a,b}, f_{c,d} \in G$: $f_{a,b} \circ f_{c,d} = f_{ac,ad+b} \in G$, $f_{a,b}$ inverze $f_{1/a,-b/a} \in G$. Ugyanígy $H, N \leq G$ és $H \trianglelefteq G$, mert $\forall f_{a,b} \in G, f_{1,d} \in N$: $f_{a,b} \circ f_{1,d} \circ f_{1/a,-b/a} = f_{a,ad+b} \circ f_{1/a,-b/a} = f_{1,1+ad} \in N$.

iii) H nem normálosztó.

▼ 2. Legyen $(G, \cdot)$ egy csoport és $\Delta(G) = \{(g, g) : g \in G\}$. Igazoljuk, hogy

i) $\Delta(G) \leq G \times G$, $\Delta(G) \simeq G$,

ii) $\Delta(G)$ akkor és csak akkor normálrészcsoport, ha G kommutatív,

iii) Ha G kommutatív, akkor $(G \times G)/\Delta(G) \simeq G$.

Megoldás. i) $f : \Delta(G) \rightarrow G$, $f((g, g)) = g$ izomorfizmus.

ii) $\Delta(G)$ normális $G \times G$ -ben $\Leftrightarrow (x, y)(g, g)(x, y)^{-1} = (xgx^{-1}, ygy^{-1}) \in \Delta(G)$, $\forall (x, y) \in G \times G$, $\forall (g, g) \in \Delta(G) \Leftrightarrow (*) xgx^{-1} = ygy^{-1}$, $\forall (x, y) \in G \times G$, $\forall (g, g) \in \Delta(G)$. Ez ekvivalens azzal, hogy G kommutatív. Valóban, ha G kommutatív, akkor a fenti (*) egyenlőség: $g = g$ igaz, ha pedig (*) igaz, akkor legyen ebben $g = y$ és kapjuk, hogy $xy = yx$.

iii) Ha G kommutatív, legyen $F : G \times G \rightarrow G$, $F((g, h)) = gh^{-1}$. Ez izomorfizmus, $\text{Ker } F = \Delta(G)$ és alkalmazzuk a homomorfizmustételt.

★ ▼ 3. Legyen $H = \{z \in \mathbb{C} : |z| = 1\}$ és $U = \{z \in \mathbb{C} \mid \exists n \in \mathbb{N}^* : z^n = 1\}$, ahol $(H, \cdot)$ és $(U, \cdot)$ csoportok, U az egységgyökök csoportja. Igazoljuk, hogy

a) $(\mathbb{C}/\mathbb{R}, +) \simeq (\mathbb{R}, +)$,

b) $(\mathbb{C}^*/H, +) \simeq (\mathbb{R}_+^*, \cdot)$,

c) $(\mathbb{C}^*/\mathbb{R}_+^*, \cdot) \simeq (H, \cdot)$,

d) $(\mathbb{R}/\mathbb{Z}, +) \simeq (H, \cdot)$,

e) $(\mathbb{Q}/\mathbb{Z}, +) \simeq (U, \cdot)$.

Megoldás. Alkalmazzuk a homomorfizmus-tételt a következő homomorfizmusokra:

a) $f : \mathbb{C} \rightarrow \mathbb{R}$, $f(z) = \text{Im } z$, b) $f : \mathbb{C}^* \rightarrow \mathbb{R}^*$, $f(z) = |z|$, c) $f : \mathbb{C}^* \rightarrow \mathbb{C}^*$, $f(z) = \frac{z}{|z|}$, d) $f : \mathbb{R} \rightarrow \mathbb{C}^*$, $f(x) = \cos(2\pi x) + i \sin(2\pi x)$, e) $f : \mathbb{Q} \rightarrow \mathbb{C}^*$, $f(m/n) = \cos(2\pi m/n) + i \sin(2\pi m/n)$. ★

8. Permutációcsoportok

8.A. Inverzió, előjel, alternáló csoport

Az n -edfokú szimmetrikus csoportot vagy teljes permutációcsoportot, jelölése S_n , 3.B.5-ben definiáltuk. Itt $|S_n| = n!$. Ha $\sigma \in S_n$, akkor az (i, j) elempár **inverziója** σ -nak, ha $i < j$ és $\sigma(i) > \sigma(j)$. A σ permutáció inverzióinak számát $\text{Inv}(\sigma)$ jelöli.

$\text{sgn}(\sigma) = (-1)^{\text{Inv}(\sigma)}$ a σ permutáció **előjele**, σ **páros permutáció**, ha $\text{sgn}(\sigma) = +1$ és σ **páratlan permutáció**, ha $\text{sgn}(\sigma) = -1$.

Az (i, j) , $i < j$ párok száma $\binom{n}{2}$, ezért $0 \leq \text{Inv}(\sigma) \leq \binom{n}{2}$. Itt $\text{Inv}(\sigma) = 0 \Leftrightarrow \sigma = e$ az identikus permutáció. Továbbá $\text{Inv}(\sigma) = \binom{n}{2} \Leftrightarrow \sigma(i) = n - i + 1, \forall 1 \leq i \leq n$, azaz

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ n & n-1 & \dots & 1 \end{pmatrix}$$

Ha $n \geq 2$ és $j < k$, akkor a $\tau_{jk} \in S_n$,

$$\tau_{jk}(i) = \begin{cases} k, & i = j, \\ j, & i = k, \\ i, & i \neq j, k \end{cases}$$

permutációt **transzpozíciónak** nevezzük, itt

$$\tau_{jk} = \begin{pmatrix} 1 & \dots & j-1 & j & j+1 & \dots & k-1 & k & k+1 & \dots & n \\ 1 & \dots & j-1 & k & j+1 & \dots & k-1 & j & k+1 & \dots & n \end{pmatrix}$$

Itt $j(k-j)$ inverziót alkot, $j+1, j+2, \dots, k-1$ mindegyike 1 inverziót alkot és más inverzió nincs, tehát $\text{Inv}(\tau_{jk}) = (k-j) + (k-j-1) = 2(k-j) - 1$, ezért τ_{jk} páratlan permutáció.

8.A.1. Tétel. a) Minden $\sigma \in S_n$ esetén

$$\text{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

b) $\text{sgn} : S_n \rightarrow \{-1, +1\}$, $\text{sgn}(\sigma) = (-1)^{\text{Inv}(\sigma)}$ szürjektív csoportmorfizmus,

c) A_n részcsoportja S_n -nek, mi több: $A_n = \text{Ker } \text{sgn} \trianglelefteq S_n$, A_n neve n -edfokú **alternáló csoport** és $|A_n| = n!/2$.

Bizonyítás. a) σ bijektív, ezért $\forall i, j \in \{1, 2, \dots, n\}, i < j \Rightarrow \exists k, \ell \in \{1, 2, \dots, n\} : \sigma(k) = i, \sigma(\ell) = j$ és $k > \ell \Leftrightarrow (i, j)$ inverziója σ -nak. Következik, hogy a

$$\prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

szorzat egyszerűsíthető és a -1 tényezők száma éppen az inverziók száma.

b) ha $\sigma, \tau \in S_n$, akkor

$$\begin{aligned} \text{sgn}(\sigma \circ \tau) &= \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} = \\ &= \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \prod_{1 \leq i < j \leq n} \frac{\tau(j) - \tau(i)}{j - i} = \text{sgn}(\sigma) \text{sgn}(\tau), \end{aligned}$$

itt a $\tau(1), \tau(2), \dots, \tau(n)$ számok megadják az $1, 2, \dots, n$ számokat τ bijektivitása miatt.

sgn szürjektív, mert $\text{sgn}(e) = 1$ és $\text{sgn}(\tau_{jk}) = -1$, ahol τ_{jk} egy transzpozíció.

c) $e \in A_n$, továbbá, ha $\sigma, \tau \in A_n$, akkor mivel sgn morfizmus: $\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau) = 1 \cdot 1 = 1$, tehát $\sigma\tau \in A_n$; ha $\sigma \in A_n$, akkor $\text{sgn}(\sigma^{-1}) = (\text{sgn}(\sigma))^{-1} = 1^{-1} = 1$, ahonnan $\sigma^{-1} \in A_n$. Következik, hogy $A_n \leq S_n$.

Legyen $\tau \in S_n$ egy rögzített transzpozíció. Mivel sgn morfizmus, következik, hogy $\phi : A_n \rightarrow S_n \setminus A_n$, $\phi(\sigma) = \sigma\tau$ egy jól értelmezett bijektív függvény. Innen kapjuk, hogy $|A_n| = |S_n \setminus A_n| = \frac{n!}{2}$. Ugyanakkor $A_n \trianglelefteq S_n$, mert az előzőek szerint $[S_n : A_n] = 2$.

Másképp: A homomorfizmus-tételből $S_n/A_n \simeq U_2 = \{-1, +1\}$, innen $|S_n/A_n| = [S_n : A_n] = 2$ és $|S_n| = [S_n : A_n]|A_n|$, ahonnan $n! = 2|A_n|$ és $|A_n| = n!/2$. $\square$

8.A.2. Feladat. $\blacktriangledown$ Határozzuk meg az S_n -beli transzpozíciók számát.

Válasz. $\binom{n}{2}$.

8.B. Diszjunkt permutációk, orbitok, ciklus

A σ és τ permutációkat **diszjunkt permutációknak** nevezzük, ha minden $i \in \{1, 2, \dots, n\}$ esetén $a \sigma(i) = i$ vagy $a \tau(i) = i$ egyenlőségek közül legalább az egyik fennáll.

8.B.1. Példa. $\bullet$ A

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 4 & 1 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 2 & 5 & 6 \end{pmatrix} \in S_6$$

permutációk diszjunktak.

8.B.2. Tétel. Ha σ és τ diszjunkt permutációk, akkor $\sigma\tau = \tau\sigma$.

Bizonyítás. Legyen $\forall i \in \{1, 2, \dots, n\}$. Ha $\sigma(i) = \tau(i) = i$, akkor $\sigma(\tau(i)) = \sigma(i) = i = \tau(\sigma(i))$.

Ha $\sigma(i) = j \neq i$, akkor $\sigma(j) \neq j$ és $\tau(i) = i, \tau(j) = j$. Következik, hogy $\sigma(\tau(i)) = \sigma(i) = j$ és $\tau(\sigma(i)) = \tau(j) = j$. Hasonlóan, ha $\tau(i) \neq i$. $\square$

Legyen $\sigma \in S_n$ rögzített és tekintsük a következő relációt: $i \sim^\sigma j \Leftrightarrow \exists p \in \mathbb{Z} : \sigma^p(i) = j$.

8.B.3. Példa. $\bullet$ A

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix} \in S_6$$

permutációra pl. $1 \sim^\sigma 3$ és $4 \sim^\sigma 6$, mert $\sigma(1) = 3, \sigma^2(4) = 6$, de $1 \not\sim^\sigma 4$.

8.B.4. Tétel. Minden $\sigma \in S_n$ esetén $\sim^\sigma$ egy ekvivalenciareláció.

Bizonyítás. $i \sim^\sigma i$, mert $\sigma^0(i) = e(i) = i$. Ha $i \sim^\sigma j$, akkor $\exists p \in \mathbb{Z} : \sigma^p(i) = j \Rightarrow \sigma^{-p}(j) = i \Rightarrow j \sim^\sigma i$. Ha $i \sim^\sigma j, j \sim^\sigma k$, akkor $\exists p \in \mathbb{Z} : \sigma^p(i) = j, \exists q \in \mathbb{Z} : \sigma^q(j) = k \Rightarrow \sigma^{p+q}(i) = k \Rightarrow i \sim^\sigma k$. $\square$

Tekintsük a $\sim^\sigma$ reláció szerinti $\{1, 2, \dots, n\} / \sim^\sigma = \{O_1, O_2, \dots, O_r\}$ faktorhalmazt, ennek véges sok eleme van, hiszen S_n is véges. Itt $O_1, O_2, \dots, O_r$ -et a σ **permutáció pályáinak** vagy **orbitjainak** nevezzük.

8.B.5. Példa. $\bullet$ Az előbbi példában $O_1 = \{1, 3\}, O_2 = \{2\}, O_3 = \{4, 5, 6\}$ (ugyanahhoz az orbithoz tartoznak, azaz relációban vannak azok a számok, amelyek között „kapcsolat”, „átjárás” van alkalmazva a σ -t).

Ha $i \in \{1, 2, \dots, n\}$ tetszőleges, akkor az i -t tartalmazó orbit, jelölés O_{j_i} , megadható így: $O_{j_i} = \{\sigma^p(i) : p \in \mathbb{Z}\} = \{\dots, \sigma^{-1}(i), i, \sigma(i), \sigma^2(i), \dots\}$, de ez véges sok elemből áll, hiszen részhalmaza az $\{1, 2, \dots, n\}$ halmaznak, ezért a $\sigma^p(i)$ elemek nem lehetnek mind különbözőek. Létezik olyan $k, \ell, k > \ell$, amelyekre $\sigma^k(i) = \sigma^\ell(i)$, innen $\sigma^{k-\ell}(i) = \sigma^0(i) = i$, tehát van olyan pozitív p kitevő, amelyre $\sigma^p(i) = i$ (Másképp: az S_n csoportban $\sigma^{n!} = e$ (lásd 5.D.2), innen $\sigma^{n!}(i) = e(i) = i$ és következik, hogy van olyan pozitív p kitevő, amelyre $\sigma^p(i) = i$). Legyen ℓ_i a legkisebb ilyen pozitív kitevő: $\ell_i = \min\{k \in \mathbb{N}^* : \sigma^k(i) = i\}$. Így $O_{j_i} = \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{\ell_i-1}(i)\}$ és az O_{j_i} elemeinek száma $|O_{j_i}| = \ell_i$, ezt az **orbit hosszának** nevezzük.

A σ permutációt **ciklusnak** nevezzük, ha legfeljebb egy olyan orbitja van, amely 1-nél hosszabb. Ez azt jelenti, hogy $\sigma \in S_n$ egy ciklus, ha léteznek olyan $i_1, i_2, \dots, i_\ell \in \{1, 2, \dots, n\}$ különböző számok, ahol $1 \leq \ell \leq n$, hogy $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{\ell-1}) = i_\ell, \sigma(i_\ell) = i_1$ és $\sigma(i) = i$, ha $i \notin \{i_1, i_2, \dots, i_\ell\}$. Azt mondjuk, hogy ekkor σ egy ℓ -hosszúságú ciklus, jelölés $\sigma = (i_1 i_2 \dots i_\ell)$ és az $O_\sigma = \{i_1, i_2, \dots, i_\ell\}$ halmazt a σ **pályájának** vagy **orbitjának** nevezzük.

8.B.6. Példák. $\bullet$ A

$$\gamma = (1536) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 6 & 4 & 3 & 1 & 7 & 8 \end{pmatrix} \in S_8$$

permutáció egy 4 hosszúságú ciklus,

• A

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix} \in S_6$$

permutáció, lásd 8.B.3., nem ciklus, de felbontható ciklusok szorzatára:

$$\sigma = (1\ 3)(2)(4\ 5\ 6).$$

• Minden transzpozíció egy 2 hosszúságú ciklus: $\tau_{ij} = (i\ j)$.

A γ ciklus hossza akkor és csak akkor 1, ha $\gamma = e$ az identikus permutáció. Ha γ egy ciklus, akkor minden $i \in O_\gamma$ esetén $\gamma = (i\ \gamma(i)\ \gamma^2(i) \dots \gamma^{\ell-1}(i))$ és $\gamma^\ell(i) = i$.

8.B.7. Tétel. Egy ℓ hosszúságú ciklus felbontható $\ell - 1$ transzpozíció szorzatára, így előjele $(-1)^{\ell-1}$.

Bizonyítás. Azonnali, hogy $\sigma = (i_1\ i_2 \dots i_\ell) = (i_1\ i_\ell)(i_1\ i_{\ell-1}) \dots (i_1\ i_2)$. Mivel $\text{sgn}(\tau_{ij}) = \text{sgn}(i\ j) = -1$, következik, hogy $\text{sgn}(\sigma) = (-1)^{\ell-1}$. $\square$

A $\gamma = (i_1\ i_2 \dots i_\ell)$ és $\delta = (j_1\ j_2 \dots j_m)$ ciklusok akkor és csak akkor diszjunktak, ha orbitjaik diszjunktak, azaz ha $\{i_1, i_2, \dots, i_\ell\} \cap \{j_1, j_2, \dots, j_m\} = \emptyset$.

8.B.8. Feladat. $\blacktriangledown$ Határozzuk meg az S_n -beli ℓ hosszúságú ciklusok számát.

Válasz. $(\ell - 1)! \binom{n}{\ell}$.

8.C. Felbontási tétel

8.C.1. Tétel. Minden n -edfokú permutáció felírható diszjunkt ciklusok szorzataként és ez a felírás egyértelmű, eltekintve a ciklusok sorrendjétől.

8.C.2. Példa. • A

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 6 & 5 & 9 & 1 & 8 & 7 & 4 \end{pmatrix} \in S_9$$

permutáció orbitjai $O_1 = \{1, 3, 6\}$, $O_2 = \{2\}$, $O_3 = \{4, 5, 9\}$, $O_4 = \{7, 8\}$ és $\sigma = (1\ 3\ 6)(2)(4\ 5\ 9)(7\ 8) = (7\ 8)(1\ 3\ 6)(4\ 5\ 9)$, ahol az 1 hosszúságú ciklus elhagyható.

Ennek a permutációnak a típusa $(1, 1, 2, 0, 0, 0, 0, 0)$.

Általában, azt mondjuk, hogy a $\sigma \in S_n$ **permutáció típusa** $(k_1, k_2, \dots, k_n)$, ha σ felbontható k_1 számú 1 hosszúságú, k_2 számú 2 hosszúságú, ..., k_n számú n hosszúságú diszjunkt ciklus szorzatára, ahol $k_1 + 2k_2 + \dots + nk_n = n$.

8.C.3. Következmény. A transzpozíciók halmaza generálja S_n -et, azaz minden n -edfokú permutáció felírható transzpozíciók szorzataként, de ez a felbontás nem egyértelmű.

Bizonyítás. Az előző Tétel alapján elegendő belátni, hogy minden nemtriviális (nem 1 hosszúságú) ciklus előállítható transzpozíciók szorzataként, de ez következik a 8.B.7-ből. Ez a felbontás nem egyértelmű, mert például $(1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(1\ 3)(2\ 3)(1\ 2)$. $\square$

Ha egy σ permutáció páros (páratlan), akkor σ -nak bármely transzpozíciók szorzataként való felírásában a tényezők száma páros (páratlan).

8.D. Feladatok

$\blacktriangledown$ 1. Ha $n \geq 3$, akkor S_n nem kommutatív csoport, mi több, S_n centruma $Z(S_n) = \{e\}$. Ha $n \geq 4$, akkor $Z(A_n) = \{e\}$.

Megoldás. Tegyük fel, hogy $\exists \sigma \in Z(S_n) : \sigma \neq e \Rightarrow \exists i : j = \sigma(i) \neq i$. Mivel $n \geq 3$, következik, hogy $\exists k \neq i, k \neq j$, és tekintsük a $\tau = (j\ k)$ transzpozíciót. Akkor $(\sigma\tau)(i) = \sigma(\tau(i)) = \sigma(i) = j$ és $(\tau\sigma)(i) = \tau(\sigma(i)) = \tau(j) = k$, ellentmondás.

★ Ha $\exists \sigma \in Z(A_n) : \sigma \neq e \Rightarrow \exists i : j = \sigma(i) \neq i$. Mivel $n \geq 4$, következik, hogy $\exists k, \ell$ úgy, hogy i, j, k, ℓ páronként különbözők, s legyen $\tau = (j\ k\ \ell) \in A_n$. Akkor $(\sigma\tau)(i) = \sigma(\tau(i)) = \sigma(i) = j$ és $(\tau\sigma)(i) = \tau(\sigma(i)) = \tau(j) = k$, ellentmondás. ★

$\blacktriangledown$ 2. Mutassuk meg, hogy a következő halmazok generálják A_n -et:

a) a 3 hosszúságú ciklusok,

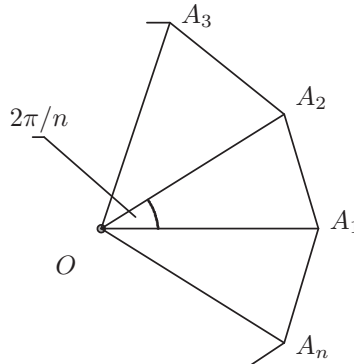
★ b) $\{(1\ 2\ 3), (1\ 2\ 4), \dots, (1\ 2\ n)\}$. ★

Megoldás. a) Ha a, b, c különbözőek, akkor $(ab)(b\ c) = (abc)$, $(a\ b)(c\ d) = (cad)(abc)$, ezért bármely 2 transzpozíció szorzata felírható 3-ciklusok szorzataként, és használjuk, hogy minden páros permutáció páros számú transzpozíció szorzata.

9. Struktúratételek

9.A. A diédercsoport

Legyen $n \in \mathbb{N}$, $n \geq 3$ és legyen P_n egy szabályos n -szög az $\mathcal{S}$ síkban. Tekintsük a P_n egybevágósági transzformációit, vagyis az olyan távolságtartó $f : \mathcal{S} \rightarrow \mathcal{S}$ függvényeket, amelyek a P_n sokszöget önmagába viszik át.



5. ábra

A P_n egybevágósági transzformációi a kompozíció művelettel egy $2n$ -edrendű nemkommutatív csoportot alkotnak, amelyet n -edfokú **diédercsoport**nak nevezünk. Jelölés: $(D_n, \circ)$ vagy $(D_n, \cdot)$.

Valóban, legyen O a P_n középpontja és legyenek $A_1, A_2, \dots, A_n$ a csúcsai, lásd 5. ábra. Minden ilyen f transzformációt meghatározza az, hogy hova kerül két csúcs, pl. A_1 és A_2 , tehát f -et meghatározza $f(A_1)$ és $f(A_2)$.

Jelölje $\rho = \rho_{2\pi/n}$ a O körüli $2\pi/n$ szöggel való rotációt (tehát $\rho(A_1) = A_2, \rho(A_2) = A_3$) és jelölje σ az OA_1 egyenesre való tükrözést ($\sigma(A_1) = A_1, \sigma(A_2) = A_n$).

Akkor $\rho^k = \rho_{2k\pi/n}$ a $2k\pi/n$ szöggel való rotáció, ahol $1 \leq k \leq n-1$ (itt $\rho^k(A_1) = A_{k+1}, \rho^k(A_2) = A_{k+2}$, ahol konvenció: $A_{n+1} = A_1$) és $\rho^n = \rho_0 = e$ az identikus transzformáció. Továbbá $\sigma^2 = e$ és $e, \rho, \dots, \rho^{n-1}, \sigma, \rho\sigma, \dots, \rho^{n-1}\sigma$ különböző transzformációk. Valóban, ha $0 \leq k \leq n-1$, akkor $(\rho^k\sigma)(A_1) = \rho^k(\sigma(A_1)) = \rho^k(A_1) = A_{k+1}$ és $(\rho^k\sigma)(A_2) = \rho^k(\sigma(A_2)) = \rho^k(A_n) = A_k$.

Ha most f egy tetszőleges egybevágósági transzformáció és $f(A_1) = A_{j+1}$, ahol $0 \leq j \leq n-1$, akkor $f(A_2)$ -re két lehetőség van: $f(A_2) = A_j$ vagy $f(A_2) = A_{j+2}$, ahol konvenció: $A_0 = A_n, A_{n+1} = A_1$. Tehát f vagy a ρ^j rotáció vagy a $\rho^j\sigma$ transzformáció. Tehát $f = \rho^j$ vagy $f = \rho^j\sigma$.

Ezzel igazoltuk, hogy az n -edfokú D_n diédercsoportra $|D_n| = 2n$ és

$$D_n = \{e, \rho, \rho^2, \dots, \rho^{n-1}, \sigma, \rho\sigma, \rho^2\sigma, \dots, \rho^{n-1}\sigma\},$$

ahol ρ és σ az előbbieken definiált transzformációk.

Megjegyzések: 1. Itt $\rho^k\sigma$ egy t szimmetriatengelyre való tükrözés. Ha $k = 2m-1$ páratlan, akkor t az $A_m A_{m+1}$ szakasz felezőmerőlegese, ha pedig $k = 2m$ páros, akkor t az OA_{m+1} egyenes.

2. Igazoljuk, hogy $\sigma\rho = \rho^{n-1}\sigma = \rho^{-1}\sigma$. Valóban, $(\sigma\rho)(A_1) = \sigma(\rho(A_1)) = \sigma(A_2) = A_n$, $(\rho^{n-1}\sigma)(A_1) = \rho^{n-1}(\sigma(A_1)) = \rho^{n-1}(A_1) = A_n$ és $(\sigma\rho)(A_2) = \sigma(\rho(A_2)) = \sigma(A_3) = A_{n-1}$, $(\rho^{n-1}\sigma)(A_2) = \rho^{n-1}(\sigma(A_2)) = \rho^{n-1}(A_n) = A_{n-1}$. A második egyenlőség pedig $\rho^n = e$ miatt igaz.

3. A $\rho^n = e, \sigma^2 = e$ és $\sigma\rho = \rho^{n-1}\sigma$ összefüggések meghatározzák D_n művelet tábláját.

4. Ugyanakkor $\rho^k\sigma$ inverze önmaga: $(\rho^k\sigma)^{-1} = \rho^k\sigma$, azaz $(\rho^k\sigma)^2 = e$, $0 \leq k < n$. Ez következik abból, hogy $\rho^k\sigma$ egy szimmetriatengelyre való tükrözés, lásd fennebb, és számolással is igazolható: $(\rho^k\sigma)^2 = \rho^k\sigma\rho^k\sigma = \rho^k(\sigma\rho)\rho^{k-1}\sigma = \rho^k(\rho^{-1}\sigma)\rho^{k-1}\sigma = \rho^{k-1}\sigma\rho^{k-1}\sigma = \dots = \rho\sigma\rho\sigma = \rho(\sigma\rho)\sigma = \rho(\rho^{-1}\sigma)\sigma = \sigma^2 = e$.

5. A D_n diédercsoport absztrakt definíciója a következő:

$$D_n = \{e, x, x^2, \dots, x^{n-1}, y, xy, x^2y, \dots, x^{n-1}y\},$$

ahol $x^n = y^2 = e, yx = x^{n-1}y$. Másképp:

$$D_n = \langle x, y | x^n = y^2 = e, yx = x^{n-1}y \rangle.$$

Itt x és y a generálóelemek és rájuk a fenti definiáló relációk vonatkoznak.

6. Ha a P_n sokszög csúcsait $1, 2, \dots, n$ -nel jelöljük, akkor minden f transzformáció egy S_n -beli permutáció. Így D_n azonosítható S_n egy részcsoportjával (izomorf vele).

7. Ha $n = 3$, akkor mivel $D_3 \leq S_3$ és $|D_3| = 6$, következik, hogy $D_3 = S_3$, pontosabban $D_3 \simeq S_3$.

Definiálhatjuk a D_2 és D_1 csoportokat is. D_2 az olyan téglalap transzformációs csoportja, amely nem négyzet, ez éppen a Klein-csoport: $D_2 = \langle x, y | x^2 = y^2 = e, yx = xy \rangle$, $|D_2| = 4$.

Továbbá D_1 az egyenlőszárú (nem szabályos) háromszög transzformációs csoportja. Ez két transzformációból áll: az e identikus (0° -kal való rotáció) és az alap felezőmerőlegesére vett s szimmetria, ahol $s^2 = e$. Itt $D_1 = \{e, s\}$, $|D_1| = 2$.

9.A.2. Feladat. ▼ a) Készítsük el D_4 műveletábráját.

★ b) Határozzuk meg D_4 részcsoportjait és normálosztóit.

Megoldás. a)

$$D_4 = \{e, \rho, \rho^2, \rho^3, \sigma, \rho\sigma, \rho^2\sigma, \rho^3\sigma\},$$

ahol $\rho^4 = e, \sigma^2 = e, \sigma\rho = \rho^3\sigma$.

★ b) D_4 részcsoportjainak rendje 1, 2, 4, 8 lehet. Ezek $H_1 = \{e\}$, a másodrendű részcsoportok $H = \{e, x\}$ alakúak, ahol $x^2 = e$. Öt ilyen találunk: $H_2 = \{e, \sigma\}$, $H_3 = \{e, \rho\sigma\}$, $H_4 = \{e, \rho^2\sigma\}$, $H_5 = \{e, \rho^3\sigma\}$, $H_6 = \{e, \rho^2\}$.

A negyedrendű részcsoportok $H = \{e, x, x^2, x^3\}$, $x^4 = e$ alakú ciklikusak vagy Klein-félék: $H = \{1, x, y, xy\}$, ahol $x^2 = y^2 = e, xy = yx$. Egy ciklikus részcsoport van: $H_7 = \{e, \rho, \rho^2, \rho^3\}$ és 2 Klein-féle: $H_8 = \{e, \rho^2, \sigma, \rho^2\sigma\}$ és $H_9 = \{e, \rho^2, \rho\sigma, \rho^3\sigma\}$.

Van még a $H_{10} = D_4$ részcsoport.

A fenti 10 részcsoportból 6 normálrészcsoport: H_1, H_{10} a triviálisak, H_7, H_8, H_9 indexe 2, H_6 pedig két normálrészcsoport metszete: $H_6 = H_7 \cap H_8$. A többi 4, tehát H_2, H_3, H_4, H_5 nem normálrészcsoport, mert pl. $\rho\sigma\rho^{-1} = \rho\sigma\rho^3 = \rho(\sigma\rho)\rho^2 = \rho(\rho^3\sigma)\rho^2 = \rho^4\sigma\rho^2 = \sigma\rho^2 = \rho^3\sigma\rho = \rho^2\sigma \notin H_2$.

Megjegyzés: $\{e, \sigma\} \trianglelefteq \{e, \rho^2, \sigma, \rho^2\sigma\} \trianglelefteq D_4$ (rendre 2 indexűek), de $\{e, \sigma\} \not\trianglelefteq D_4$. ★

9.B. A $2p$ rendű csoportok

A csoportelmélet egyik fontos feladata az összes létező csoporttípus leírása. Láttuk már, hogy csak egyfajta prímszámrendű csoport létezik. Tehát egy-egy olyan csoport van, amelynek rendje $2, 3, 5, 7, 11, 13, 17, 19, \dots$, ezek ciklikusak (és kommutatívak).

Nézzük most a $2p$ rendű csoportokat, ahol p prímszám. Szükségünk van a következő eredményre:

9.B.1. Tétel. Legyen $(G, \cdot)$ egy véges csoport úgy, hogy $\forall x \in G : x^2 = e$. Akkor G kommutatív és létezik $k \in \mathbb{N}$ úgy, hogy $|G| = 2^k$.

Bizonyítás. $\forall x, y \in G : e = (xy)^2 = xyxy, e = ee = x^2y^2 = xyxy \Rightarrow xy = yx$.

A második állítást $|G| = n$ -szerinti indukcióval bizonyítjuk. Ha $|G| = 1$ vagy $|G| = 2$, akkor az állítás igaz. Tegyük fel, hogy az állítás igaz minden n -nél kisebbrendű csoportra és legyen $|G| = n$. Legyen $x \in G, x \neq e$ és $N = \langle x \rangle$ az x által generált részcsoport, $N = \{e, x\}$, hiszen $x^2 = e$. Továbbá G kommutatív, ezért $N \trianglelefteq G$ és $G/N = |G|/2 = n/2 < n$ és $\forall yN \in G/N : (yN)^2 = y^2N = eN = N$, ami a G/N faktorcsoport egységeleme.

Így G/N -re alkalmazva az indukciós feltételt: $|G| = 2^k$, ahonnan $|G| = |G/N||N| = 2^{k+1}$. □

A következő tétel a diéderscsoport fontosságára is rávilágít.

9.B.2. Tétel. Ha a G csoport rendje $|G| = 2p$, ahol $p \geq 2$ prímszám, akkor $G \simeq (\mathbb{Z}_{2p}, +)$ vagy $G \simeq (D_p, \circ)$.

★ **Bizonyítás.** Minden $x \in G$ elem rendje osztója a csoport rendjének (Tétel), azaz $\forall x \in G : o(x) = 1, 2, p$ vagy $2p$. Ha $\exists x \in G : o(x) = 2p$, akkor G ciklikus: $G = \langle x \rangle \simeq (\mathbb{Z}_{2p}, +)$.

Ellenkező esetben $\forall x \in G, x \neq e : o(x) = 2$ vagy $o(x) = p$. Ha $p = 2$, akkor $\forall x \in G, x \neq e : o(x) = 2$ és a műveletábra elemzésével a $D_2 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ Klein-féle csoportot kapjuk.

Ha $p \geq 3$, akkor $|G| \neq 2^k$ és az előző Tétel alapján következik, hogy létezik $x \in G : o(x) = p$ és legyen $N = \langle x \rangle = \{e, x, x^2, \dots, x^{p-1}\}$. Mivel $|N| = p$, ezért $|G/N| = 2$, azaz N egy 2 indexű részcsoport, ezért $N \trianglelefteq G$, lásd 6. szakasz, és $\forall y \in G \setminus N : G/N = \{N, yN\}$, $yN = Ny$, $(yN)^2 = N$ (mert $(yN)^2 = yN \Rightarrow yN = N$, nem lehet) és $(yN)^p = yN$ (p páratlan). Ugyanakkor $yx \in yN \Rightarrow yN = (yx)N$. Tehát $y^p \neq e$, $(yx)^p \neq p$, s mivel minden elem rendje 2 vagy p , következik, hogy $o(y) = o(yx) = 2$.

Továbbá, $yx \in yN = Ny \Rightarrow \exists k \in \{1, 2, \dots, p-1\} : yx = x^k y$, itt $k \neq 0$, mert $k = 0$ -ra $yx = y \Rightarrow x = e$, ellentmondás. Itt $e = (yx)^2 = yxyx = x^k y^2 x = x^{k+1}$, tehát $o(x) = p = k+1 \Rightarrow k = p-1$, $yx = x^{p-1} y$.

Így $G = N \cup Ny = \{e, x, x^2, \dots, x^{p-1}, y, xy, \dots, x^{p-1}y\}$, ahol $o(x) = p$, $o(y) = 2$ és $yx = x^{p-1}y$, tehát $G \simeq D_p$, a diédercsoport. $\square \star$

Tehát két-két olyan csoport van, amelynek rendje $4, 6, 10, 14, 22, \dots$, ezek egyike ciklikus, a másik a diédercsoport.

9.C. A p^2 rendű csoportok

Igazolható továbbá:

9.C.1. Tétel. Ha a G csoport rendje $|G| = p^2$, ahol $p \geq 2$ prímszám, akkor G kommutatív és $G \simeq (\mathbb{Z}_{p^2}, +)$ vagy $G \simeq (\mathbb{Z}_p \times \mathbb{Z}_p, +)$. $\square$

Tehát két-két olyan csoport van, amelynek rendje $4, 9, 25, \dots$, ezek kommutatívak, az egyik ciklikus, a másik két ciklikus csoport direkt szorzata.

A legkisebb rendű csoport, amely nem szerepel a fentiekben, a 8-adrendű. Igazolható, hogy a G kommutatív esetben 3 lehetőség van: $G \simeq (\mathbb{Z}_8, +)$ ciklikus, vagy $G \simeq (\mathbb{Z}_2 \times \mathbb{Z}_4, +)$ vagy $G \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, +)$. Ha G nem kommutatív, akkor 2 eset van: $G \simeq D_4$ a diédercsoport vagy $G \simeq Q$ a kvaterniócsoport.

Továbbá a 12 elemű csoportok száma 5, 15 elemű csoport egyféle van, a ciklikus csoport, a 16 elemű csoportok száma pedig 14. Ezek meghatározása több előismeretet és több számolást igényel.

2006. ápr. 4.