

Bevezetés az algebrába és a számelméletbe II.

Dr. TÓTH LÁSZLÓ egyetemi docens
Pécsi Tudományegyetem

2007

Bevezetés

Ez az anyag tartalmazza a „Bevezetés az algebra és a számelméletbe II.” című tárgy 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 algebra: <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 **metsszete** 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 **hatványhalmaz**.

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 **transzítív**, 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 $x, y \in A$, $x\rho y$ és $y\rho x$ esetén $x = y$ ($\forall x, y \in A : x\rho y \wedge y\rho x \Rightarrow x = y$), 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, transzítív és szimmetrikus;

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

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

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

- 3) A $\mathbb{Z}$ halmazon az $a \equiv b \pmod{n} \Leftrightarrow n|a-b$ kongruencia reláció ekvivalenciareláció.
- 4) Az $(A, A, A \times A)$ univerzális reláció ekvivalenciareláció.

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

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

1.B.5. Példa. • Az $A = \{1, 2, 3, 4, 4, 6\}$ 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 $A/\rho = \{\rho\langle x \rangle : x \in A\}$ 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 $R = \bigcup_{i \in I} (B_i \times B_i)$, azaz $x\rho y \Leftrightarrow \exists i \in I : x, y \in B_i$ (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 **értéktartománya**, jelölés $B = \text{codom } f$ (f kodoméniuma), az $f(A)$ metszet az f függvény **értékeinek halmaza** 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 $f(a) = \{b\}$ 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 $\rho(a) = \{1, 2\}$ 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 $\mathbf{1}_A = (A, A, \Delta_A)$ diagonális reláció egy függvény, ennek neve az A halmaz **identikus függvénye**: $\mathbf{1}_A : A \rightarrow A$, $\mathbf{1}_A(a) = a$ 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.

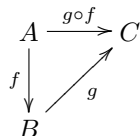
• A $g : [0, \infty) \rightarrow \mathbb{R}, g(x) = x^2$ függvény injektív és nem szürjektív,
 $h : [0, \infty) \rightarrow [0, \infty), h(x) = x^2$ pedig injektív és szürjektív, tehát bijektív.

• Bármely A halmaz esetén az $\mathbf{1}_A$ 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 $(x_1^2 + x_2/2)^2 + 3x_2^2/4 + 1 \neq 0$, 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 $x > 1$.

▼ 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 halmazon,

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. $\square$

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 $(S, \circ), (S, \Delta)$, 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** nevezünk, 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 $\mathcal{M}_2(\mathbb{Z})$ 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 zárójelezéstől, 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 tényezős 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. • $(\mathbb{Z}, +)$ -ban $e = 0$ semleges elem, $(\mathbb{R}, \cdot)$ -ban $e = 1$ semleges elem,

• 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 félcsoporthat sok szerző **monoid**nak nevezi.

2.D.4. Feladat. ▼ 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. • $(\mathbb{Z}, +)$ -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 művelet táblája, 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 művelet tábla 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.

$$\begin{aligned} (y' * x') * (x * y) &= y' * (x' * x) * y = y' * e * y = y' * y = e, \\ (x * y) * (y' * x') &= x * (y * y') * x' = x * e * x' = x * x' = e. \quad \square \end{aligned}$$

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 félcsoporthoz

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

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

(a ρ szerinti kongruenciák összesorozhatók).

2.G.1. Példa. • $(\mathbb{R}, \cdot)$ félcsoporthoz és az " $\equiv$ " 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 $\forall x, x', y, y' \in S : x\rho x', y\rho y'$. 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 $xy\rho z, x'y'\rho z \Rightarrow xy\rho x'y'$. $\square$

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

$\forall x, x', y \in G : x\rho x' \Rightarrow xy\rho x'y, yx\rho yx'$ (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 $yx\rho yx'$. $\star$

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

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

$\blacktriangledown$ 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.

$\blacktriangledown$ 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 $(x, y), (z, w) \in \mathbb{Z} \times \mathbb{Z}$.

$\blacktriangledown$ 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 $a = 1/2, b = 1$.

$\blacktriangledown$ 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?

$\blacktriangledown$ 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: $n^{(n-1)^2+1}$)

$\blacktriangledown$ 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 félcsoportot **csoportnak** nevezzük, ha minden $x \in G$ elem invertálható. A $(G, \cdot)$ struktúra tehát csoport, ha G -n értelmezett egy (multiplikatív) művelet, az ún. **csoportszorzás**, 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. Példa. • $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ Abel-csoportok,

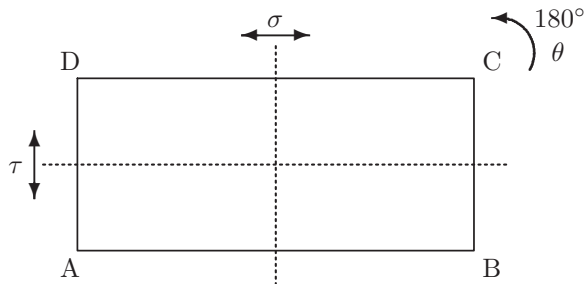
• $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ nem csoportok, csak egységelemes félcsoportok, de $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ Abel-csoportok.

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 $(\text{mod } n)$. Ekkor $(\mathbb{Z}_n, +)$ Abel-csoport, a **maradékosztályok (additív) csoportja** $(\text{mod } n)$, 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 egyenlő 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 „ $\circ$ ”-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 $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $\mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \in \mathcal{M}_2(\mathbb{C})$ és $Q = \{\pm \mathbf{1}, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$. Akkor $(Q, \cdot)$ nem kommutatív csoport.

Valóban, az adott mátrixok szorzásával látható, hogy $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ és $\mathbf{ij} = \mathbf{k}, \mathbf{jk} = \mathbf{i}, \mathbf{ki} = \mathbf{j}, \mathbf{ji} = -\mathbf{k}, \mathbf{kj} = -\mathbf{i}, \mathbf{ik} = -\mathbf{j}$. Q így is megadható: $Q = \{1, \mathbf{i}, \mathbf{i}^2, \mathbf{i}^3, \mathbf{j}, \mathbf{ij}, \mathbf{i}^2\mathbf{j}, \mathbf{i}^3\mathbf{j}\}$. 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: $(g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2 h_2)$. 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) $S_M = \{f : M \rightarrow M | f \text{ bijektív}\}$ 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 $f \circ \mathbf{1}_M = \mathbf{1}_M \circ f = f$, hiszen $(f \circ \mathbf{1}_M)(x) = f(\mathbf{1}_M(x)) = f(x)$, $(\mathbf{1}_M \circ f)(x) = \mathbf{1}_M(f(x)) = f(x)$ minden $x \in M$ -re.

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

Ha $f \in U(\mathcal{F}(M))$, akkor f invertálható, azaz létezik olyan $f' : M \rightarrow M$ függvény, amelyre $f \circ f' = f' \circ f = \mathbf{1}_M$, $f(f'(x)) = f'(f(x)) = x, \forall x \in M$. Kérdés, hogy f bijektív-e, azaz tetszőleges $y \in M$ -re létezik-e egy

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 $(\mathcal{F}(M), \circ)$ 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 pontosan egyszer. Ez az egyszerűsítési szabály miatt van így (vizsgáljuk meg a 3.B. szakasz műveletábráit).

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.

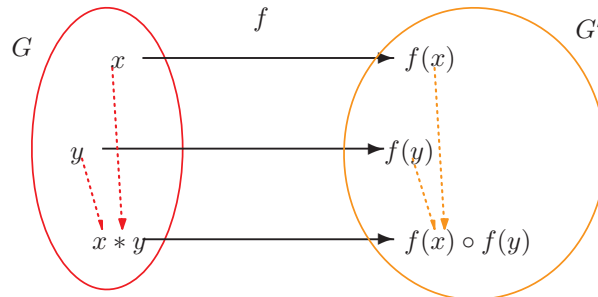
$\blacktriangledown$ 2. A $(G, \cdot)$ csoportban $x^2 = e, \forall x \in G$ (e az egységelem). Igazoljuk, hogy G kommutatív csoport.

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 ekvivalencia-reláció 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 $f(2) = f(1) + f(1) = 2f(1)$, $f(3) = f(1) + f(2) = 3f(1), \dots, f(n) = nf(1), \forall n \in \mathbb{N}$, 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 előbbiekből 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 $f(\widehat{0}) = 0, f(\widehat{2}) = 2f(\widehat{1}), \dots, f(\widehat{k}) = kf(\widehat{1}), 0 \leq k \leq n$. 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 **alcsoporthja**), 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 részcsoporthjai a $H = \{e\}$ és $H = G$, ezeket **triviális részcsoporthoknak** nevezzük. Ha $H \leq G$ és $H \neq \{e\}, H \neq G$, akkor H -t **valódi részcsoporthnak** 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 részcsoporthja, lásd 3.F.2. Feladat, jelölés $H = \langle x \rangle$, ennek neve az x **elem által generált részcsoporth**.

• 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 részcsoporthjai.

• 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 részcsoporthja.

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. ▼ Részcsoporthját 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 részcsoporthjának metszete is részcsoporth:
 $\forall H_1, H_2 \leq G \Rightarrow H_1 \cap H_2 \leq G$. Általánosabban, részcsoporthok tetszőleges rendszerének a metszete is részcsoporth:

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

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

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. $\blacktriangledown$ 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.

$\blacktriangledown$ 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 $Z(G) = G$.

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

- $H_1 \cup H_2 \leq G \Leftrightarrow H_1 \leq H_2$ vagy $H_2 \leq H_1$,
- $H_1 \cup H_2 = G \Leftrightarrow H_1 = G$ vagy $H_2 = G$,
- $H_3 \subseteq H_1 \cup H_2 \Leftrightarrow H_3 \leq H_1$ 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. $\bullet$ 1. Minden csoportban $o(x) = 1 \Leftrightarrow x = e$.

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

$\bullet$ 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.

$\star$ 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. $\bullet$ 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. $\blacktriangledown$ 1. Igazoljuk, hogy $U = \{z \in \mathbb{C} : \exists n \in \mathbb{N} : z^n = 1\}$ (végtelen) csoport a szorzásra nézve. $\star$

$\blacktriangledown$ 2. Határozzuk meg a következő x elemek rendjét a megadott csoportokban:

- $x = 1, x = 2, x = -3$ a $(\mathbb{Z}, +)$ csoportban,
- $x = -1, x = i, x = 2i$ a $(\mathbb{C}^*, \cdot)$ csoportban,
- $x = \hat{1}, x = \hat{2}, x = \hat{4}$ a $(\mathbb{Z}_5, +)$ csoportban,
- $x = \hat{1}, x = \hat{2}, x = \hat{4}$ 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: $g_1g_2 \cdot \dots \cdot g_n = (xg_1)(xg_2) \cdot \dots \cdot (xg_n)$, innen a kommutativitást alkalmazva: $g_1g_2 \cdot \dots \cdot g_n = x^n g_1g_2 \cdot \dots \cdot g_n$, 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. Feladatok. $\blacktriangledown$ 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 prímrendű 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 **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: $\mathbb{Z}_n = \langle \hat{1} \rangle$,

$\bullet$ 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.

★ **3.H.4. Feladat.** ▼ 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 $n \mid (kr - 1)$. Ha $d \mid r$ és $d \mid n$, akkor következik, hogy $d \mid 1$, 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 $x = (x^r)^u, x^2 = (x^r)^{2u}, \dots$ ★

★ 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. ▼ 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 szükségeség 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 szükségeség 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) $A(\frac{x}{2x-1})$.

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

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

Megoldás. b) A 3.E.5/4 Feladat megoldását követve, következik, hogy $\text{Hom}(\mathbb{Z}, A) = \{f_a : \mathbb{Z} \rightarrow A | f_a(x) = ax, a \in A\}$, 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 $z = f(x) = f(n \cdot \frac{x}{n}) = nf(\frac{x}{n})$ 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

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

Megoldás. a) A korábbi feladatokhoz hasonlóan:

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

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

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

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 $d = (n, m)$ ltko., 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 $\psi : (\mathbb{Z}_m)_n \rightarrow \mathbb{Z}_d, \psi(\widehat{\frac{jm}{d}}) = \widehat{j}$ 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. ★