

4. Részcsoporthok

4.A. Csoport részhalmazainak félcsoporthja

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

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

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

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

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

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

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

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

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

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

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

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

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

4.B. Részcsoporthok jellemzése

A részcsoporth fogalmát a 3.F. szakaszban definiáltuk.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- a) ha $H \leq G$, akkor $f(H) = \{f(h) : h \in H\} \leq G'$,
- b) $f(G) \leq G'$, tehát csoport homomorf képe csoport,
- c) ha $H' \leq G'$, akkor $f^{-1}(H') = \{g \in G : f(g) \in H'\} \leq G$.

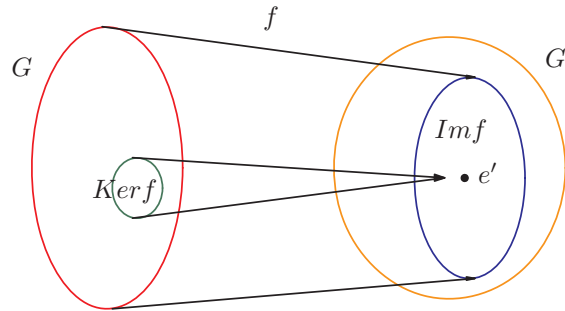
Bizonyítás. Használjuk a részcsoportok jellemzési tételét: elég belátni, hogy

- a) $e \in H$ miatt $f(e) = e' \in f(H) \neq \emptyset$, továbbá $\forall x, y \in H : f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(H)$.
- b) az előző speciális esete: $H = G$.
- c) $e \in f^{-1}(H') \neq \emptyset$, mert $f(e) = e' \in H'$, továbbá $\forall x, y \in f^{-1}(H') : f(x), f(y) \in H'$ és $f(xy^{-1}) = f(x)f(y)^{-1} \in H'$, ezért $xy^{-1} \in f^{-1}(H')$. □

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

4.C. Csoportmorfizmus magja és képe

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



3. ábra

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

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

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

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

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

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

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

4.D. Ciklikus csoportok részcsoportjai

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.E. Generált részcsoport

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

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

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

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

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

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

Az alábbi állítások következnek a definíciókból:

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

- $\langle X \rangle \leq G$, $X \subseteq \langle X \rangle$,
- ha $X \subseteq H$ és $H \leq G$, akkor $\langle X \rangle \leq H$,
- legyen $H \subseteq G$, akkor $H \leq G \Leftrightarrow \langle H \rangle = H$. □

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

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

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

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

★ **Bizonyítás.** (részletesen) Legyen

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

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

$$\forall x = x_1 x_2 \dots x_n, y = y_1 y_2 \dots y_m \in K \Rightarrow xy^{-1} = x_1 x_2 \dots x_n (y_1 y_2 \dots y_m)^{-1} =$$

$$= x_1 x_2 \dots x_n y_m^{-1} y_{m-1}^{-1} \dots y_1^{-1} \in K.$$

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

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

A fentiek szerint $\langle X \rangle = K$. $\square \star$

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

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

Additív jelöléssel:

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

Az $X = \{x\}$ esetben az x elem által generált részcsoporthoz: $\langle x \rangle = \{x^k : k \in \mathbb{Z}\}$, amit már láttunk.

Additív jelöléssel a tétel a következő:

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

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

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

Bizonyítás. Ha $HK = KH$, akkor $HK \leq G$, lásd 4.B.5. $H = He \subseteq HK, K = eK \subseteq HK$, innen $H \cup K \subseteq HK$, s mivel HK részcsoporthoz tartozik, ezért $\langle H \cup K \rangle \leq HK$. Továbbá, $\forall hk \in HK \Rightarrow hk \in \langle H \cup K \rangle$, innen $HK \leq \langle H \cup K \rangle$. Kapjuk, hogy $\langle H \cup K \rangle = HK$. $\square \star$

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

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

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

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

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

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

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

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

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

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

4.F. Elemek és részcsoporthoz tartozásuk konjugáltjai

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

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

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

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

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

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

ii) " $\Rightarrow$ " Feltételezzük, hogy $\tilde{x} = \{x\}$. Kérdés, hogy $x \in Z(G) \Leftrightarrow \forall y \in G : xy = yx \Leftrightarrow \forall y \in G : x = yxy^{-1}$?

Legyen $yxy^{-1} = z \Rightarrow z \sim x \Rightarrow z = x$ a feltételből, kész.

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

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

4.F.2. Tétel. Legyen G egy csoport.

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

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

Bizonyítás. a) Minden τ_g morfizmus, mert $\tau_g(x_1x_2) = g(x_1x_2)g^{-1} = (gx_1g^{-1})(gx_2g^{-1}) = \tau_g(x_1)\tau_g(x_2)$, $\forall x_1, x_2 \in G$. Továbbá ha $y = gxg^{-1}$, akkor $x = g^{-1}yg$, ahonnan kapjuk, hogy τ_g bijektív és inverze éppen $\tau_{g^{-1}}$.

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

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

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

★ 4.G. Abel csoport részcsoportjainak direkt összege

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

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

1) a következő állítások egyenértékűek:

- i) $A = B \oplus C$,
- ii) $A = B + C$ és $B \cap C = \{0\}$,
- iii) $f : B \times C \rightarrow A$, $f((b, c)) = b + c$ izomorfizmus,

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

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

4.G.3. Feladatok. $\blacktriangledown$ 1. Igazoljuk a 4.G.1. és 4.G.2. állításokat.

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

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

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

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

4.H. Cayley tétele

A következő tétel a szimmetrikus csoport fontosságát mutatja:

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

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

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

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

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

★ 4.I. Részcsoportok megfeleltetési tétele

Szükségünk lesz a következő tulajdonságra:

4.I.1. Tétel. (részcsoportok megfeleltetési tétele) Legyen $f : G \rightarrow G'$ egy szürjektív csoportmorfizmus. Akkor minden $K \leq G'$ esetén létezik egy és csak egy $H \leq G$ úgy, hogy $\text{Ker } f \leq H$ és $f(H) = K$, nevezetesen

$H = f^{-1}(K)$. Tehát $H \mapsto f(H)$ bijektív megfeleltetés G -nek a $\text{Ker } f$ -et tartalmazó részcsoportjai és G' részcsoportjai között.

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

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

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

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

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

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

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

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

b) Alkalmazzuk a 4.I.1. Tételt. $\star$

4.J. Feladatok

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

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

▼ 2. Egy végtelen csoportnak végtelen sok részcsoportja van.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. Mellékosztályok, Lagrange tétele

5.A. Bal oldali és jobb oldali mellékosztályok

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.B. Bal oldali és jobb oldali kongruenciarelációk

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

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

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

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

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

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

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

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

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

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

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

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

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

5.C. A mellékosztályok számossága

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.D. Lagrange tétele, elem rendjének tulajdonságai

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

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

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

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

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

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

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

Az előbbieket szerint $|G| = n = k\ell$, ahonnan $x^n = (x^k)^\ell = e$, kész. □

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

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

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

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

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

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

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

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

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

Ellenkező esetben $o(x) = o(y) = o(z) = 2$, mert az elem rendje a csoport rendjének osztója. Akkor $xy = x \Rightarrow y = e$ nem lehet, $xy = y \Rightarrow x = e$ nem lehet, $xy = e \Rightarrow x = x^{-1} = y$ nem lehet, tehát $xy = z$ és $G = \{e, x, y, xy\}$ és $yx = y^{-1}x^{-1} = (xy)^{-1} = z^{-1} = z = xy$, a csoport kommutatív (készítsünk műveletábrát). Itt x, y, z közül

bármely kettő szorzata egyenlő a harmadikkal és $x^2 = y^2 = e$, ez a Klein-csoport, lásd 3.B. szakasz és 3.E.5/1. Feladat. $\square$

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

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

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

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

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

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

b) azonnali a) alapján. $\square$

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

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

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

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

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

★ 5.E. Megjegyzések

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

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

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

5.F. Feladatok

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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