

6. Normálrészcsoporthok

6.A. Normálrészcsoporthok és jellemzésük

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

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

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

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

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

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

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

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

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

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

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

6.B. Példák normálrészcsoporthokra

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

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

• Egy csoport minden 2 indexű részcsoporthja normálrészcsoporth: ha $H \leq G$ és $[G : H] = 2$, akkor $H \trianglelefteq G$. Valóban, $G/\rho_H = \{H, G \setminus H\} = G/\rho'_H$, mert ez osztályozás kell legyen és H az egyik osztály.

További fontos példákat ad a következő Tétel.

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

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

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

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

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

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

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

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

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

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

6.C. Normálrészcsoportok metszete

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

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

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

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

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

$$xnx^{-1} = xn_{i_1} n_{i_2} \dots n_{i_r} x^{-1} = \underbrace{(xn_{i_1} x^{-1})}_{\in N_{i_1}} \underbrace{(xn_{i_2} x^{-1})}_{\in N_{i_2}} \dots \underbrace{(xn_{i_r} x^{-1})}_{\in N_{i_r}} \in \langle \bigcup_{i \in I} N_i \rangle. \quad \square \star$$

6.D. Kongruenciareláció csoportban

Legyen $(G, \cdot)$ egy csoport és ρ egy ekvivalenciareláció G -n. Azt mondjuk, hogy ρ **kongruenciareláció**, ha

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

(a ρ szerinti kongruenciák összesorozhatók), lásd 2.G. szakasz.

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

6.D.1. Példa. • Tekintsük a $(\mathbb{Z}, +)$ csoportot és a számelméleti kongruenciarelációt $(\text{mod } n)$. Ez ilyen tulajdonságú:

$$\forall x, y, x', y' \in \mathbb{Z} : \quad x \equiv x' \pmod{n}, \quad y \equiv y' \pmod{n} \Rightarrow x + y \equiv x' + y' \pmod{n}.$$

$\mathbb{Z}$ -nek a $(\text{mod } n)$ maradékosztályok halmazaira való bontása egy kompatibilis osztályozás.

★ **6.D.2. Feladat.** Ha G egy csoport és ρ egy kongruenciareláció, akkor igazoljuk, hogy

1) $\forall x, x' \in G : x \rho x' \Rightarrow x^{-1} \rho (x')^{-1}$, azaz ha két elem egy osztályban van, akkor az inverzeik is azonos osztályban vannak,

2) $\forall X \in G/\rho \Rightarrow \exists Y \in G/\rho : X^{-1} \subseteq Y$.

Megoldás. 1) Ha $x \rho x'$, akkor x^{-1} -nel szorozva (lásd 2.G.3. Feladat): $e = x x^{-1} \rho x' x^{-1}$, most $(x')^{-1}$ -gyel szorozva: $(x')^{-1} \rho (x')^{-1} x' x^{-1} = x^{-1}$.

2) $\forall X \in G/\rho$ -re legyen $X = \langle x \rangle$ és legyen $Y = \langle x^{-1} \rangle$ az x^{-1} osztálya.

$\forall (x')^{-1} \in X^{-1} \Rightarrow x' \in X \Rightarrow x \rho x'$, ahonnan 1) alapján $x^{-1} \rho (x')^{-1} \Rightarrow (x')^{-1} \in Y$, tehát $X^{-1} \subseteq Y$. $\square \star$

6.D.3. Tétel. (normálrészcsoportok és kongruenciarelációk kapcsolata) Legyen G egy csoport.

a) Ha $N \trianglelefteq G$, akkor ρ_N kongruenciareláció (tehát a normális részcsoportok szerinti mellékosztályok a csoport egy kompatibilis osztályozását adják),

b) Ha ρ egy kongruenciareláció, akkor $G/\rho = \{xN : x \in G\}$, ahol $N = \rho(e) \trianglelefteq G$ (minden kompatibilis osztályozás osztályai valamely normális részcsoport szerinti mellékosztályok).

Bizonyítás. a) Láttuk már, hogy ρ_N ekvivalenciareláció. Továbbá:

$$\begin{aligned} \forall x, x', y, y' \in G : \quad x \rho_N x', y \rho_N y' &\Rightarrow x^{-1} x' \in N, y^{-1} y' \in N \Rightarrow \\ \Rightarrow (xy)^{-1} (x' y') &= y^{-1} x^{-1} x' y' = \underbrace{(y^{-1} x^{-1} x' y)}_{\in N} \underbrace{(y^{-1} y')}_{\in N} \in N, \end{aligned}$$

tehát $xy\rho_N x'y'$.

★ b) $N = \rho\langle e \rangle \neq \emptyset$, mert $e\rho e$. Továbbá $\forall x, y \in N \Rightarrow e\rho x, e\rho y$. De $e\rho y$ és $y^{-1}\rho y^{-1}$ miatt (ez utóbbi a reflexivitásból) $ey^{-1}\rho yy^{-1} \Rightarrow y^{-1}\rho e$, tehát $N \leq G$.

Megmutatjuk, hogy $\forall x \in G \Rightarrow xN = Nx = \rho\langle x \rangle$. Valóban, $xN \subseteq \rho\langle x \rangle$, mert $\forall xn \in xN \Rightarrow n\rho e, x\rho x \Rightarrow nx\rho x$. Fordítva, $\rho\langle x \rangle \subseteq xN$, mert $\forall y \in \rho\langle x \rangle \Rightarrow y\rho x, x^{-1}\rho x^{-1}$ (reflexivitás) $\Rightarrow x^{-1}y\rho e \Rightarrow x^{-1}y \in N$, tehát $y = x(x^{-1}y) \in xN$. Hasonlóan $Nx = \rho\langle x \rangle$. Tehát $xN = Nx$, azaz $N \trianglelefteq G$.

Ezzel azt is igazoltuk, hogy minden $x \in G$ -re $\rho\langle x \rangle = xN$, tehát az osztályok az N szerinti mellékosztályok.

★ □

★ 6.E. Normálrészcsoportok megfeleltetési tétele

6.E.1. Tétel. (normálrészcsoportok megfeleltetési tétele) Legyen $f : G \rightarrow G'$ egy csoportmorfizmus. Akkor

1) minden $K \trianglelefteq G'$ esetén $f^{-1}(K) \trianglelefteq G$,

2) ha f szürjektív és $H \trianglelefteq G$, akkor $f(H) \trianglelefteq G'$,

3) ha f szürjektív, akkor $H \mapsto f(H)$ bijektív megfeleltetés G -nek a $\text{Ker } f$ -et tartalmazó normálrészcsoportjai és G' normálrészcsoportjai között.

Bizonyítás. 1) A 4.B.6. Tétel szerint $f^{-1}(K) \leq G$ és $\forall x \in G, \forall h \in f^{-1}(K) \Rightarrow f(h) \in K, f(xhx^{-1}) = f(x)f(h)f(x)^{-1} \in K$, mert $K \trianglelefteq G'$. Tehát $f^{-1}(K) \trianglelefteq G$.

2) $f(H) \leq G'$ (lásd ua. a Tétel) és $\forall y \in G', \forall k \in f(H) \Rightarrow \exists x \in G : y = f(x)$, mert f szürjektív, és $\exists h \in H : k = f(h)$, innen $yky^{-1} = f(x)f(h)f(x)^{-1} = f(xhx^{-1}) \in f(H)$, mert $xhx^{-1} \in H$. Tehát $f(H) \trianglelefteq G'$.

3) Következik 1) és 2)-ből valamint a részcsoportok megfeleltetési tételéből (4.I.1. Tétel). □

6.E.2. Következmény. Ha $f : G \rightarrow G'$ csoportmorfizmus, akkor $\text{Ker } f = f^{-1}(\{e'\}) \trianglelefteq G$, mert $\{e'\} \trianglelefteq G'$. $\text{Ker } f$ tehát normálrészcsoport, ezt már láttuk közvetlen ellenőrzéssel. ★

★ 6.F. Megjegyzések

Bemutatjuk a 6.D.3. tétel első részének egy más bizonyítását részhalmazok (komplexusok) segítségével. Bizonyos esetekben ezek használata lerövidíti, átláthatóbbá teszi csoportelméleti tulajdonságok megfogalmazását és bizonyítását.

a) Ha $N \trianglelefteq G$, akkor az $xN = Nx$ mellékosztályok (a G/ρ faktorhalmaz elemei) páronként diszjunktak, tehát egy osztályozást adnak. Legyen xN, yN két mellékosztály, akkor $(xN)(yN) = x(Ny)N = x(yN)N = (xy)(NN) = (xy)N$ ismét egy N szerinti mellékosztály(ban van), tehát kompatibilis osztályozás a 2.G.2. Tétel szerint.

b) Fordítva, ha adott egy kompatibilis osztályozás, legyen N az e -t tartalmazó osztály: $N = \rho\langle e \rangle$.

Belátjuk, hogy $NN \subseteq N$ és $N^{-1} \subseteq N$. Valóban, $\forall xy \in NN \Rightarrow x\rho e, y\rho e \Rightarrow xy\rho ee = e \Rightarrow xy \in N$ (másképp: NN része egy osztálynak, lásd 2.G. szakasz, és $e \in NN$, ezért ez az osztály csak az N lehet: $NN \subseteq N$), továbbá $\forall x^{-1} \in N^{-1} \Rightarrow x \in N \Rightarrow x\rho e, x^{-1}\rho x^{-1}$ (reflexivitás) $\Rightarrow xx^{-1}\rho e \Rightarrow ex^{-1} \Rightarrow x^{-1} \in N$ (másképp: N^{-1} része egy osztálynak, lásd 6.D.2. Feladat, és $e \in N^{-1}$ miatt ez csak az N lehet: $N^{-1} \subseteq N$). Tehát $N \leq G$. □★

★ 6.G. Feladatok

▼ 1. Legyen $(G, \cdot)$ egy csoport.

a) Egy $N \leq G$ részcsoport akkor és csak akkor normálosztó, ha minden K komplexus esetén $KN = NK$.

b) Ha $H \leq G$ és $N \trianglelefteq G$, akkor $HN = NH \leq G$ és ez éppen a H és N által generált részcsoport: $\langle H \cup N \rangle = HN = NH$.

Megoldás. a) Ha $N \trianglelefteq G$ és K komplexus, akkor $KN = \cup_{x \in K} xN = \cup_{x \in K} Nx = NK$. Fordítva, ha $KN = NK$ minden K komplexusra, akkor legyen $K = \{x\}, x \in G$ és kapjuk, hogy $xN = Nx, \forall x \in G$, ahonnan $N \trianglelefteq G$.

b) $HN = NH$ az a) pont szerint és innen $HN \leq G$ következik, lásd 4.B.5 Tétel. Továbbá: $\langle H \cup N \rangle = HN$, lásd 4.E.3. Tétel.

▼ 2. Legyen G egy csoport, $N \trianglelefteq G$ egy ciklikus normális részcsoport és $H \leq N$. Akkor $H \trianglelefteq G$.

Megoldás. Legyen $N = \langle x \rangle$ és $H = \langle x^m \rangle, m \geq 1$. Kérdés: $\forall g \in G, \forall x^{km} \in H \Rightarrow gx^{km}g^{-1} \in H$? Mivel $N \trianglelefteq G$ következik, hogy $gxx^{-1} = x \in N$, innen $gx^{km}g^{-1} = gxx^{-1}gxg^{-1} \dots gxg^{-1} = (gxg^{-1})^{km} = x^{knm} \in H$.

▼ 3. Vizsgáljuk a Q kvaterniócsoport részcsoportjait, lásd 3.B.8. Igazoljuk, hogy Q minden részcsoportja normálrészcsoport. Adjuk meg Q centrumát és faktorcsoportjait.

Megoldás. Q részcsoportjai: ha $H \leq Q$, akkor a Lagrange-tétel szerint $|H| = 1, 2, 4$, vagy 8 . $|H| = 1 \Leftrightarrow H = H_1 := \{1\}$. $|H| = 2 \Leftrightarrow H = H_2 := \{\pm 1\} = \langle -1 \rangle$, a táblázat szerint ez az egyedüli 2 elemű részcsoport. $|H| = 4 \Leftrightarrow H = H_3 := \{\pm 1, \pm i\} = \langle i \rangle$, vagy $H = H_4 := \{\pm 1, \pm j\} = \langle j \rangle$, vagy $H = H_5 := \{\pm 1, \pm k\} = \langle k \rangle$

ciklikus részcsoporthok. (1)-ben csak egy másodrendű elem van, az $\mathbf{i}^2$, ezért Klein-féle 4 elemű részcsoporth nincs. $|H| = 8 \Leftrightarrow H = H_6 := Q$.

Q nem kommutatív, de Q -nak minden részcsoporthja normálrészcsoporth. Valóban, a 4-edrendű részcsoporthok ilyenek, mert indexük 2, lásd 6.B. szakasz, H_2 -re pedig $xH_2 = H_2x = \{x, -x\}, \forall x \in Q$ (Másképp: H_2 az egyedüli másodrendű részcsoporth, ezért normálrészcsoporth, lásd későbbi Tétel).

Q centruma $Z(Q) = \{\mathbf{1}, -\mathbf{1}\}$.

A $H_i, 1 \leq i \leq 6$ részcsoporthok szerinti faktorcsoporthok:

$$Q/H_1 = \{\{\mathbf{1}\}, \{-\mathbf{1}\}, \{\mathbf{i}\}, \{-\mathbf{i}\}, \{\mathbf{j}\}, \{-\mathbf{j}\}, \{\mathbf{k}\}, \{-\mathbf{k}\}\},$$

$$Q/H_2 = \{\{\pm\mathbf{1}\}, \{\pm\mathbf{i}\}, \{\pm\mathbf{j}\}, \{\pm\mathbf{k}\}\},$$

$$Q/H_3 = \{\{\pm\mathbf{1}, \pm\mathbf{i}\}, \{\pm\mathbf{j}, \pm\mathbf{k}\}\},$$

$$Q/H_4 = \{\{\pm\mathbf{1}, \pm\mathbf{j}\}, \{\pm\mathbf{i}, \pm\mathbf{k}\}\},$$

$$Q/H_5 = \{\{\pm\mathbf{1}, \pm\mathbf{k}\}, \{\pm\mathbf{i}, \pm\mathbf{j}\}\},$$

$$Q/H_6 = \{\{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}\}.$$

Itt a $H_2 = N$ szerinti mellékosztályok: $N, \mathbf{i}N = \{\pm\mathbf{i}\}, \mathbf{j}N = \{\pm\mathbf{j}\}, \mathbf{k}N = \{\pm\mathbf{k}\}$ és a Q/N faktorcsoporth (lásd 7. szakasz) izomorf a Klein-csoporttal. ★

7. Faktorcsoporthok és a homomorfizmus-tétel

7.A. Faktorcsoporth

Legyen $(G, \cdot)$ egy csoport és $N \trianglelefteq G$ egy normálosztó. Láttuk, hogy ekkor $\rho_N = \rho'_N$ és G/N -nel jelöltük a $G/\rho_N = G/\rho'_N$ faktorhalmazt, ahol $G/N = \{xN : x \in G\}$, ennek elemei az $xN = \{xn : n \in N\} = Nx$ mellékosztályok.

Az xN mellékosztályok szorzása művelet a G/N halmazon. Valóban, két tetszőleges N szerinti mellékosztály szorzata: $(xN)(yN) = x(Ny)N = x(yN)N = (xy)NN = (xy)N$ ismét egy N szerinti mellékosztály, ahol használtuk, hogy $NN = N$, lásd 4.B.2. Tétel.

7.A.1. Tétel. Ha G egy csoport és $N \trianglelefteq G$, akkor a G/N halmazon az $(xN)(yN) = (xy)N$ művelet egy csoportstruktúrát határoz meg, ennek neve G -nek N szerinti **faktorcsoporthja**, jelölés $(G/N, \cdot)$.

Ha G véges csoport, akkor

$$|G/N| = \frac{|G|}{|N|}.$$

Bizonyítás. A művelet asszociatív, $eN = N$ az egységelem és xN inverze $(xN)^{-1} = x^{-1}N$, mert $(xN)(x^{-1}N) = (xx^{-1})N = eN = N$ és hasonlóan $(x^{-1}N)(xN) = N$.

Ha G véges, akkor $|G/N| = [G : N] = |G|/|N|$, a Lagrange tétel szerint. $\square$

Ha G kommutatív, akkor minden faktorcsoporthja is kommutatív.

7.A.2. Példa. • Határozzuk meg a $(\mathbb{Z}, +)$ csoport faktorcsoporthjait.

Tudjuk, hogy a $(\mathbb{Z}, +)$ részcsoportjai az $(n\mathbb{Z}, +)$ csoportok, ahol $n \in \mathbb{N}$, ezek mind normálrészcsoportok a kommutativitás miatt. Jelölés: $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, a megfelelő faktorcsoporthok. Ha $n = 0$, akkor $0\mathbb{Z} = \{0\}$ és $\mathbb{Z}_0 = \mathbb{Z}/\{0\} = \{x + \{0\} : x \in \mathbb{Z}\} = \{\{x\} : x \in \mathbb{Z}\} \simeq \mathbb{Z}$. Ha $n = 1$, akkor $1\mathbb{Z} = \mathbb{Z}$ és $\mathbb{Z}_1 = \mathbb{Z}/\mathbb{Z} = \{x + \mathbb{Z} : x \in \mathbb{Z}\} = \{\mathbb{Z}\}$.

Ha $n \geq 2$, akkor $\mathbb{Z}_n = \{x + n\mathbb{Z} : x \in \mathbb{Z}\} = \{\hat{x} : x \in \mathbb{Z}\} = \{\hat{0}, \hat{1}, \dots, \widehat{n-1}\}$, ahol $x + n\mathbb{Z} = \hat{x}$ jelölés.

★ Ha $N \trianglelefteq G$, akkor a $p_N : G \rightarrow G/N$, $p_N(x) = xN$ leképezést **kanonikus projekciónak** nevezzük. Ez a fentiek szerint homomorfizmus, szürjektív és ennek magja éppen az N : $\text{Ker } p_N = N$. Valóban, $\text{Ker } p_N = \{x \in G : xN = N\} = N$. Tehát minden normálrészcsoport egy homomorfizmus magja.

Az is igaz, hogy ha $N \trianglelefteq G$, akkor a G/N faktorhalmazon egyetlen csoportstruktúra létezik úgy, hogy a $p_N : G \rightarrow G/N$ kanonikus projekció homomorfizmus legyen. Egyértelműség: ha p_N homomorfizmus, akkor $p_N(xy) = p_N(x)p_N(y) \Leftrightarrow (xy)N = (xN)(yN), \forall x, y \in G$. ★

7.B. Homomorfizmus-tétel

7.B.1. Tétel. (homomorfizmus-tétel) Ha $f : G \rightarrow G'$ egy csoportmorfizmus, akkor az

$$\bar{f} : G/\text{Ker } f \rightarrow \text{Im } f, \quad \bar{f}(x \text{Ker } f) = f(x)$$

függvény csoportizomorfizmus, tehát $G/\text{Ker } f \simeq \text{Im } f$.

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ p \downarrow & & \uparrow i \\ G/\text{Ker } f & \xrightarrow{\bar{f}} & \text{Im } f \end{array}$$

4.ábra

Bizonyítás. Ha $x \text{Ker } f = x' \text{Ker } f$, akkor $x\rho_{\text{Ker } f}x'$, ahonnan értelmezés szerint $x(x')^{-1} \in \text{Ker } f$, $f(x(x')^{-1}) = e'$, $f(x)f(x')^{-1} = e'$, $f(x) = f(x')$, tehát $\bar{f}$ helyesen értelmezett (nem függ a reprezentánsoktól).

$\bar{f}$ csoportmorfizmus, mert $\forall x \text{Ker } f, y \text{Ker } f \in G/\text{Ker } f \Rightarrow \bar{f}((x \text{Ker } f)(y \text{Ker } f)) = \bar{f}((xy) \text{Ker } f) = f(xy) = f(x)f(y) = \bar{f}(x \text{Ker } f)\bar{f}(y \text{Ker } f)$.

$\bar{f}$ szürjektív, mert $\forall z \in \text{Im } f \Rightarrow \exists x \in G : z = f(x)$ és így $\bar{f}(x \text{Ker } f) = f(x) = z$. Továbbá $\bar{f}$ injektív, mert $\bar{f}(x \text{Ker } f) = \bar{f}(y \text{Ker } f) \Rightarrow f(x) = f(y) \Rightarrow f(xy^{-1}) = e' \Rightarrow xy^{-1} \in \text{Ker } f \Rightarrow x \text{Ker } f = y \text{Ker } f$. $\square$

Ha $f : G \rightarrow G'$ egy csoportmorfizmus legyen $i : \text{Im } f \rightarrow G'$, $i(y) = y$ az ún. **kanonikus injekció** és $p = p_{\text{Ker } f} : G \rightarrow G/\text{Ker } f$, $p(x) = x \text{Ker } f$ a $\text{Ker } f$ szerinti kanonikus projekció. Akkor az homomorfizmus-tétel szerint $i \circ \bar{f} \circ p = f$, azaz a 4. ábrán lévő diagram kommutatív.

7.C. Feladatok

▼ 1. Legyenek $a, b \in \mathbb{R}$, $a \neq 0$ és $f_{a,b} : \mathbb{R} \rightarrow \mathbb{R}$, $f_{a,b}(x) = ax + b$.

i) Igazoljuk, hogy $G = \{f_{a,b} : a \in \mathbb{R}^*, b \in \mathbb{R}\}$ csoport a függvénykompozícióra nézve és $H = \{f_{a,0} : a \in \mathbb{R}^*\}$, valamint $N = \{f_{1,b} : b \in \mathbb{R}\}$ ennek részcsoportjai.

ii) Igazoljuk, hogy H részcsoportja G -nek, N normálrészcsoportja G -nek és $(G/N, \circ) \simeq (\mathbb{R}^*, \cdot)$.

iii) H normálrészcsoportja-e G -nek?

Megoldás. i)-ii) Használjuk a részcsoportok jellemzési tételét. G csoport, mert részcsoportja az összes $f : \mathbb{R} \rightarrow \mathbb{R}$ bijektív függvény csoportjának. Valóban, $\forall f_{a,b}, f_{c,d} \in G$: $f_{a,b} \circ f_{c,d} = f_{ac,ad+b} \in G$, $f_{a,b}$ inverze $f_{1/a, -b/a} \in G$. Ugyanígy $H, N \leq G$ és $H \trianglelefteq G$, mert $\forall f_{a,b} \in G, f_{1,d} \in N$: $f_{a,b} \circ f_{1,d} \circ f_{1/a, -b/a} = f_{a,ad+b} \circ f_{1/a, -b/a} = f_{1,1+ad} \in N$.

iii) H nem normálosztó.

▼ 2. Legyen $(G, \cdot)$ egy csoport és $\Delta(G) = \{(g, g) : g \in G\}$. Igazoljuk, hogy

i) $\Delta(G) \leq G \times G$, $\Delta(G) \simeq G$,

ii) $\Delta(G)$ akkor és csak akkor normálrészcsoport, ha G kommutatív,

iii) Ha G kommutatív, akkor $(G \times G)/\Delta(G) \simeq G$.

Megoldás. i) $f : \Delta(G) \rightarrow G$, $f((g, g)) = g$ izomorfizmus.

ii) $\Delta(G)$ normális $G \times G$ -ben $\Leftrightarrow (x, y)(g, g)(x, y)^{-1} = (xgx^{-1}, ygy^{-1}) \in \Delta(G)$, $\forall (x, y) \in G \times G, \forall (g, g) \in \Delta(G)$ $\Leftrightarrow (*) xgx^{-1} = ygy^{-1}$, $\forall (x, y) \in G \times G, \forall (g, g) \in \Delta(G)$. Ez ekvivalens azzal, hogy G kommutatív. Valóban, ha G kommutatív, akkor a fenti (*) egyenlőség: $g = g$ igaz, ha pedig (*) igaz, akkor legyen ebben $g = y$ és kapjuk, hogy $xy = yx$.

iii) Ha G kommutatív, legyen $F : G \times G \rightarrow G$, $F((g, h)) = gh^{-1}$. Ez izomorfizmus, $\text{Ker } F = \Delta(G)$ és alkalmazzuk a homomorfizmustételt.

★ ▼ 3. Legyen $H = \{z \in \mathbb{C} : |z| = 1\}$ és $U = \{z \in \mathbb{C} \mid \exists n \in \mathbb{N}^* : z^n = 1\}$, ahol $(H, \cdot)$ és $(U, \cdot)$ csoportok, U az egységgyökök csoportja. Igazoljuk, hogy

a) $(\mathbb{C}/\mathbb{R}, +) \simeq (\mathbb{R}, +)$,

b) $(\mathbb{C}^*/H, +) \simeq (\mathbb{R}_+^*, \cdot)$,

c) $(\mathbb{C}^*/\mathbb{R}_+^*, \cdot) \simeq (H, \cdot)$,

d) $(\mathbb{R}/\mathbb{Z}, +) \simeq (H, \cdot)$,

e) $(\mathbb{Q}/\mathbb{Z}, +) \simeq (U, \cdot)$.

Megoldás. Alkalmazzuk a homomorfizmus-tételt a következő homomorfizmusokra:

a) $f : \mathbb{C} \rightarrow \mathbb{R}$, $f(z) = \text{Im } z$, b) $f : \mathbb{C}^* \rightarrow \mathbb{R}^*$, $f(z) = |z|$, c) $f : \mathbb{C}^* \rightarrow \mathbb{C}^*$, $f(z) = \frac{z}{|z|}$, d) $f : \mathbb{R} \rightarrow \mathbb{C}^*$, $f(x) = \cos(2\pi x) + i \sin(2\pi x)$, e) $f : \mathbb{Q} \rightarrow \mathbb{C}^*$, $f(m/n) = \cos(2\pi m/n) + i \sin(2\pi m/n)$. ★

8. Permutációcsoportok

8.A. Inverzió, előjel, alternáló csoport

Az n -edfokú szimmetrikus csoportot vagy teljes permutációcsoportot, jelölése S_n , 3.B.5-ben definiáltuk.. Itt $|S_n| = n!$. Ha $\sigma \in S_n$, akkor az (i, j) elempár **inverziója** σ -nak, ha $i < j$ és $\sigma(i) > \sigma(j)$. A σ permutáció inverzióinak számát $\text{Inv}(\sigma)$ jelöli.

$\text{sgn}(\sigma) = (-1)^{\text{Inv}(\sigma)}$ a σ permutáció **előjele**, σ **páros permutáció**, ha $\text{sgn}(\sigma) = +1$ és σ **páratlan permutáció**, ha $\text{sgn}(\sigma) = -1$.

Az (i, j) , $i < j$ párok száma $\binom{n}{2}$, ezért $0 \leq \text{Inv}(\sigma) \leq \binom{n}{2}$. Itt $\text{Inv}(\sigma) = 0 \Leftrightarrow \sigma = e$ az identikus permutáció. Továbbá $\text{Inv}(\sigma) = \binom{n}{2} \Leftrightarrow \sigma(i) = n - i + 1, \forall 1 \leq i \leq n$, azaz

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ n & n-1 & \dots & 1 \end{pmatrix}$$

Ha $n \geq 2$ és $j < k$, akkor a $\tau_{jk} \in S_n$,

$$\tau_{jk}(i) = \begin{cases} k, & i = j, \\ j, & i = k, \\ i, & i \neq j, k \end{cases}$$

permutációt **transzpozíciónak** nevezzük, itt

$$\tau_{jk} = \begin{pmatrix} 1 & \dots & j-1 & j & j+1 & \dots & k-1 & k & k+1 & \dots & n \\ 1 & \dots & j-1 & k & j+1 & \dots & k-1 & j & k+1 & \dots & n \end{pmatrix}$$

Itt $j(k-j)$ inverziót alkot, $j+1, j+2, \dots, k-1$ mindegyike 1 inverziót alkot és más inverzió nincs, tehát $\text{Inv}(\tau_{jk}) = (k-j) + (k-j-1) = 2(k-j) - 1$, ezért τ_{jk} páratlan permutáció.

8.A.1. Tétel. a) Minden $\sigma \in S_n$ esetén

$$\text{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

b) $\text{sgn} : S_n \rightarrow \{-1, +1\}$, $\text{sgn}(\sigma) = (-1)^{\text{Inv}(\sigma)}$ szürjektív csoportmorfizmus,

c) A_n részcsoportja S_n -nek, mi több: $A_n = \text{Ker } \text{sgn} \trianglelefteq S_n$, A_n neve n -edfokú **alternáló csoport** és $|A_n| = n!/2$.

Bizonyítás. a) σ bijektív, ezért $\forall i, j \in \{1, 2, \dots, n\}, i < j \Rightarrow \exists k, \ell \in \{1, 2, \dots, n\} : \sigma(k) = i, \sigma(\ell) = j$ és $k > \ell \Leftrightarrow (i, j)$ inverziója σ -nak. Következik, hogy a

$$\prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

szorzat egyszerűsíthető és a -1 tényezők száma éppen az inverziók száma.

b) ha $\sigma, \tau \in S_n$, akkor

$$\begin{aligned} \text{sgn}(\sigma \circ \tau) &= \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} = \\ &= \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \prod_{1 \leq i < j \leq n} \frac{\tau(j) - \tau(i)}{j - i} = \text{sgn}(\sigma) \text{sgn}(\tau), \end{aligned}$$

itt a $\tau(1), \tau(2), \dots, \tau(n)$ számok megadják az $1, 2, \dots, n$ számokat τ bijektivitása miatt.

sgn szürjektív, mert $\text{sgn}(e) = 1$ és $\text{sgn}(\tau_{jk}) = -1$, ahol τ_{jk} egy transzpozíció.

c) $e \in A_n$, továbbá, ha $\sigma, \tau \in A_n$, akkor mivel sgn morfizmus: $\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau) = 1 \cdot 1 = 1$, tehát $\sigma\tau \in A_n$; ha $\sigma \in A_n$, akkor $\text{sgn}(\sigma^{-1}) = (\text{sgn}(\sigma))^{-1} = 1^{-1} = 1$, ahonnan $\sigma^{-1} \in A_n$. Következik, hogy $A_n \leq S_n$.

Legyen $\tau \in S_n$ egy rögzített transzpozíció. Mivel sgn morfizmus, következik, hogy $\phi : A_n \rightarrow S_n \setminus A_n$, $\phi(\sigma) = \sigma\tau$ egy jól értelmezett bijektív függvény. Innen kapjuk, hogy $|A_n| = |S_n \setminus A_n| = \frac{n!}{2}$. Ugyanakkor $A_n \trianglelefteq S_n$, mert az előzőek szerint $[S_n : A_n] = 2$.

Másképp: A homomorfizmus-tételből $S_n/A_n \simeq U_2 = \{-1, +1\}$, innen $|S_n/A_n| = [S_n : A_n] = 2$ és $|S_n| = [S_n : A_n]|A_n|$, ahonnan $n! = 2|A_n|$ és $|A_n| = n!/2$. $\square$

8.A.2. Feladat. $\blacktriangledown$ Határozzuk meg az S_n -beli transzpozíciók számát.

Válasz. $\binom{n}{2}$.

8.B. Diszjunkt permutációk, orbitok, ciklus

A σ és τ permutációkat **diszjunkt permutációknak** nevezzük, ha minden $i \in \{1, 2, \dots, n\}$ esetén a $\sigma(i) = i$ vagy a $\tau(i) = i$ egyenlőségek közül legalább az egyik fennáll.

8.B.1. Példa. $\bullet$ A

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 4 & 1 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 2 & 5 & 6 \end{pmatrix} \in S_6$$

permutációk diszjunktak.

8.B.2. Tétel. Ha σ és τ diszjunkt permutációk, akkor $\sigma\tau = \tau\sigma$.

Bizonyítás. Legyen $\forall i \in \{1, 2, \dots, n\}$. Ha $\sigma(i) = \tau(i) = i$, akkor $\sigma(\tau(i)) = \sigma(i) = i = \tau(\sigma(i))$.

Ha $\sigma(i) = j \neq i$, akkor $\sigma(j) \neq j$ és $\tau(i) = i, \tau(j) = j$. Következik, hogy $\sigma(\tau(i)) = \sigma(i) = j$ és $\tau(\sigma(i)) = \tau(j) = j$. Hasonlóan, ha $\tau(i) \neq i$. $\square$

Legyen $\sigma \in S_n$ rögzített és tekintsük a következő relációt: $i \sim^\sigma j \Leftrightarrow \exists p \in \mathbb{Z} : \sigma^p(i) = j$.

8.B.3. Példa. $\bullet$ A

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix} \in S_6$$

permutációra pl. $1 \sim^\sigma 3$ és $4 \sim^\sigma 6$, mert $\sigma(1) = 3, \sigma^2(4) = 6$, de $1 \not\sim^\sigma 4$.

8.B.4. Tétel. Minden $\sigma \in S_n$ esetén $\sim^\sigma$ egy ekvivalenciareláció.

Bizonyítás. $i \sim^\sigma i$, mert $\sigma^0(i) = e(i) = i$. Ha $i \sim^\sigma j$, akkor $\exists p \in \mathbb{Z} : \sigma^p(i) = j \Rightarrow \sigma^{-p}(j) = i \Rightarrow j \sim^\sigma i$. Ha $i \sim^\sigma j, j \sim^\sigma k$, akkor $\exists p \in \mathbb{Z} : \sigma^p(i) = j, \exists q \in \mathbb{Z} : \sigma^q(j) = k \Rightarrow \sigma^{p+q}(i) = k \Rightarrow i \sim^\sigma k$. $\square$

Tekintsük a $\sim^\sigma$ reláció szerinti $\{1, 2, \dots, n\} / \sim^\sigma = \{O_1, O_2, \dots, O_r\}$ faktorhalmazt, ennek véges sok eleme van, hiszen S_n is véges. Itt $O_1, O_2, \dots, O_r$ -et a σ **permutáció pályáinak** vagy **orbitjainak** nevezzük.

8.B.5. Példa. $\bullet$ Az előbbi példában $O_1 = \{1, 3\}, O_2 = \{2\}, O_3 = \{4, 5, 6\}$ (ugyanahhoz az orbitához tartoznak, azaz relációban vannak azok a számok, amelyek között „kapcsolat”, „átjárás” van alkalmazva a σ -t).

Ha $i \in \{1, 2, \dots, n\}$ tetszőleges, akkor az i -t tartalmazó orbit, jelölés O_{j_i} , megadható így: $O_{j_i} = \{\sigma^p(i) : p \in \mathbb{Z}\} = \{\dots, \sigma^{-1}(i), i, \sigma(i), \sigma^2(i), \dots\}$, de ez véges sok elemből áll, hiszen részhalmaza az $\{1, 2, \dots, n\}$ halmaznak, ezért a $\sigma^p(i)$ elemek nem lehetnek mind különbözőek. Létezik olyan $k, \ell, k > \ell$, amelyekre $\sigma^k(i) = \sigma^\ell(i)$, innen $\sigma^{k-\ell}(i) = \sigma^0(i) = i$, tehát van olyan pozitív p kitevő, amelyre $\sigma^p(i) = i$ (Másképp: az S_n csoportban $\sigma^{n!} = e$ (lásd 5.D.2), innen $\sigma^{n!}(i) = e(i) = i$ és következik, hogy van olyan pozitív p kitevő, amelyre $\sigma^p(i) = i$). Legyen ℓ_i a legkisebb ilyen pozitív kitevő: $\ell_i = \min\{k \in \mathbb{N}^* : \sigma^k(i) = i\}$. Így $O_{j_i} = \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{\ell_i-1}(i)\}$ és az O_{j_i} elemeinek száma $|O_{j_i}| = \ell_i$, ezt az **orbit hosszának** nevezzük.

A σ permutációt **ciklusnak** nevezzük, ha legfeljebb egy olyan orbitja van, amely 1-nél hosszabb. Ez azt jelenti, hogy $\sigma \in S_n$ egy ciklus, ha léteznek olyan $i_1, i_2, \dots, i_\ell \in \{1, 2, \dots, n\}$ különböző számok, ahol $1 \leq \ell \leq n$, hogy $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{\ell-1}) = i_\ell, \sigma(i_\ell) = i_1$ és $\sigma(i) = i$, ha $i \notin \{i_1, i_2, \dots, i_\ell\}$. Azt mondjuk, hogy ekkor σ egy ℓ -hosszúságú ciklus, jelölés $\sigma = (i_1 i_2 \dots i_\ell)$ és az $O_\sigma = \{i_1, i_2, \dots, i_\ell\}$ halmazt a σ **pályájának** vagy **orbitjának** nevezzük.

8.B.6. Példák. $\bullet$ A

$$\gamma = (1536) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 6 & 4 & 3 & 1 & 7 & 8 \end{pmatrix} \in S_8$$

permutáció egy 4 hosszúságú ciklus.

$\bullet$ A

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix} \in S_6$$

permutáció, lásd 8.B.3., nem ciklus, de felbontható ciklusok szorzatára: $\sigma = (13)(2)(456)$.

$\bullet$ Minden transzpozíció egy 2 hosszúságú ciklus: $\tau_{ij} = (ij)$.

A γ ciklus hossza akkor és csak akkor 1, ha $\gamma = e$ az identikus permutáció. Ha γ egy ciklus, akkor minden $i \in O_\gamma$ esetén $\gamma = (i \gamma(i) \gamma^2(i) \dots \gamma^{\ell-1}(i))$ és $\gamma^\ell(i) = i$.

8.B.7. Tétel. Egy ℓ hosszúságú ciklus felbontható $\ell - 1$ transzpozíció szorzatára, így előjele $(-1)^{\ell-1}$.

Bizonyítás. Azonnali, hogy $\sigma = (i_1 i_2 \dots i_\ell) = (i_1 i_\ell)(i_1 i_{\ell-1}) \dots (i_1 i_2)$. Mivel $\text{sgn}(\tau_{ij}) = \text{sgn}(i j) = -1$, következik, hogy $\text{sgn}(\sigma) = (-1)^{\ell-1}$. $\square$

A $\gamma = (i_1 i_2 \dots i_\ell)$ és $\delta = (j_1 j_2 \dots j_m)$ ciklusok akkor és csak akkor diszjunktak, ha orbitjaik diszjunktak, azaz ha $\{i_1, i_2, \dots, i_\ell\} \cap \{j_1, j_2, \dots, j_m\} = \emptyset$.

8.B.8. Feladat. $\blacktriangledown$ Határozzuk meg az S_n -beli ℓ hosszúságú ciklusok számát.

Válasz. $(\ell - 1)! \binom{n}{\ell}$.

8.C. Felbontási tétel

8.C.1. Tétel. Minden n -edfokú permutáció felírható diszjunkt ciklusok szorzataként és ez a felírás egyértelmű, eltekintve a ciklusok sorrendjétől.

8.C.2. Példa. $\bullet$ A

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 6 & 5 & 9 & 1 & 8 & 7 & 4 \end{pmatrix} \in S_9$$

permutáció orbitjai $O_1 = \{1, 3, 6\}$, $O_2 = \{2\}$, $O_3 = \{4, 5, 9\}$, $O_4 = \{7, 8\}$ és $\sigma = (136)(2)(459)(78) = (78)(136)(459)$, ahol az 1 hosszúságú ciklus elhagyható.

Ennek a permutációnak a típusa $(1, 1, 2, 0, 0, 0, 0, 0, 0)$.

Általában, azt mondjuk, hogy a $\sigma \in S_n$ **permutáció típusa** $(k_1, k_2, \dots, k_n)$, ha σ felbontható k_1 számú 1 hosszúságú, k_2 számú 2 hosszúságú, ..., k_n számú n hosszúságú diszjunkt ciklus szorzatára, ahol $k_1 + 2k_2 + \dots + nk_n = n$.

8.C.3. Következmény. A transzpozíciók halmaza generálja S_n -et, azaz minden n -edfokú permutáció felírható transzpozíciók szorzataként, de ez a felbontás nem egyértelmű.

Bizonyítás. Az előző Tétel alapján elegendő belátni, hogy minden nemtriviális (nem 1 hosszúságú) ciklus előállítható transzpozíciók szorzataként, de ez következik a 8.B.7-ből. Ez a felbontás nem egyértelmű, mert például $(123) = (13)(12) = (12)(13)(23)(12)$. $\square$

Ha egy σ permutáció páros (páratlan), akkor σ -nak bármely transzpozíciók szorzataként való felírásában a tényezők száma páros (páratlan).

8.D. Feladatok

$\blacktriangledown$ 1. Ha $n \geq 3$, akkor S_n nem kommutatív csoport, mi több, S_n centruma $Z(S_n) = \{e\}$. Ha $n \geq 4$, akkor $Z(A_n) = \{e\}$.

Megoldás. Tegyük fel, hogy $\exists \sigma \in Z(S_n) : \sigma \neq e \Rightarrow \exists i : j = \sigma(i) \neq i$. Mivel $n \geq 3$, következik, hogy $\exists k \neq i, k \neq j$, és tekintsük a $\tau = (jk)$ transzpozíciót. Akkor $(\sigma\tau)(i) = \sigma(\tau(i)) = \sigma(i) = j$ és $(\tau\sigma)(i) = \tau(\sigma(i)) = \tau(j) = k$, ellentmondás.

$\star$ Ha $\exists \sigma \in Z(A_n) : \sigma \neq e \Rightarrow \exists i : j = \sigma(i) \neq i$. Mivel $n \geq 4$, következik, hogy $\exists k, \ell$ úgy, hogy i, j, k, ℓ páronként különbözők, s legyen $\tau = (jk\ell) \in A_n$. Akkor $(\sigma\tau)(i) = \sigma(\tau(i)) = \sigma(i) = j$ és $(\tau\sigma)(i) = \tau(\sigma(i)) = \tau(j) = k$, ellentmondás. $\star$

$\blacktriangledown$ 2. Mutassuk meg, hogy a következő halmazok generálják A_n -et:

a) a 3 hosszúságú ciklusok,

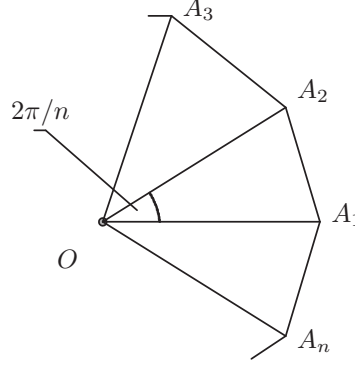
$\star$ b) $\{(123), (124), \dots, (12n)\}$. $\star$

Megoldás. a) Ha a, b, c különbözőek, akkor $(ab)(b,c) = (abc)$, $(a,b)(c,d) = (cad)(abc)$, ezért bármely 2 transzpozíció szorzata felírható 3-ciklusok szorzataként, és használjuk, hogy minden páros permutáció páros számú transzpozíció szorzata.

9. Struktúratételek

9.A. A diédercsoport

Legyen $n \in \mathbb{N}, n \geq 3$ és legyen P_n egy szabályos n -szög az $\mathcal{S}$ síkban. Tekintsük a P_n egybevágósági transzformációit, vagyis az olyan távolságtartó $f : \mathcal{S} \rightarrow \mathcal{S}$ függvényeket, amelyek a P_n sokszöget önmagába viszik át.



5. ábra

A P_n egybevágósági transzformációi a kompozíció művelettel egy $2n$ -edrendű nemkommutatív csoportot alkotnak, amelyet n -edfokú **diédercsoport**nak nevezünk. Jelölés: $(D_n, \circ)$ vagy $(D_n, \cdot)$.

Valóban, legyen O a P_n középpontja és legyenek $A_1, A_2, \dots, A_n$ a csúcsai, lásd 5. ábra. Minden ilyen f transzformációt meghatározza az, hogy hova kerül két csúcs, pl. A_1 és A_2 , tehát f -et meghatározza $f(A_1)$ és $f(A_2)$.

Jelölje $\rho = \rho_{2\pi/n}$ a O körüli $2\pi/n$ szöggel való rotációt (tehát $\rho(A_1) = A_2, \rho(A_2) = A_3$) és jelölje σ az OA_1 egyenesre való tükrözést ($\sigma(A_1) = A_1, \sigma(A_2) = A_n$).

Akkor $\rho^k = \rho_{2k\pi/n}$ a $2k\pi/n$ szöggel való rotáció, ahol $1 \leq k \leq n-1$ (itt $\rho^k(A_1) = A_{k+1}, \rho^k(A_2) = A_{k+2}$, ahol konvenció: $A_{n+1} = A_1$) és $\rho^n = \rho_0 = e$ az identikus transzformáció. Továbbá $\sigma^2 = e$ és $e, \rho, \dots, \rho^{n-1}, \sigma, \rho\sigma, \dots, \rho^{n-1}\sigma$ különböző transzformációk. Valóban, ha $0 \leq k \leq n-1$, akkor $(\rho^k\sigma)(A_1) = \rho^k(\sigma(A_1)) = \rho^k(A_1) = A_{k+1}$ és $(\rho^k\sigma)(A_2) = \rho^k(\sigma(A_2)) = \rho^k(A_n) = A_k$.

Ha most f egy tetszőleges egybevágósági transzformáció és $f(A_1) = A_{j+1}$, ahol $0 \leq j \leq n-1$, akkor $f(A_2)$ -re két lehetőség van: $f(A_2) = A_j$ vagy $f(A_2) = A_{j+2}$, ahol konvenció: $A_0 = A_n, A_{n+1} = A_1$. Tehát f vagy a ρ^j rotáció vagy a $\rho^j\sigma$ transzformáció. Tehát $f = \rho^j$ vagy $f = \rho^j\sigma$.

Ezzel igazoltuk, hogy az n -edfokú D_n diédercsoportra $|D_n| = 2n$ és

$$D_n = \{e, \rho, \rho^2, \dots, \rho^{n-1}, \sigma, \rho\sigma, \rho^2\sigma, \dots, \rho^{n-1}\sigma\},$$

ahol ρ és σ az előbbieken definiált transzformációk.

Megjegyzések: 1. Itt $\rho^k\sigma$ egy t szimmetriatengelyre való tükrözés. Ha $k = 2m-1$ páratlan, akkor t az $A_m A_{m+1}$ szakasz felezőmerőlegese, ha pedig $k = 2m$ páros, akkor t az OA_{m+1} egyenes.

2. Igazoljuk, hogy $\sigma\rho = \rho^{n-1}\sigma = \rho^{-1}\sigma$. Valóban, $(\sigma\rho)(A_1) = \sigma(\rho(A_1)) = \sigma(A_2) = A_n$, $(\rho^{n-1}\sigma)(A_1) = \rho^{n-1}(\sigma(A_1)) = \rho^{n-1}(A_1) = A_n$ és $(\sigma\rho)(A_2) = \sigma(\rho(A_2)) = \sigma(A_3) = A_{n-1}$, $(\rho^{n-1}\sigma)(A_2) = \rho^{n-1}(\sigma(A_2)) = \rho^{n-1}(A_n) = A_{n-1}$. A második egyenlőség pedig $\rho^n = e$ miatt igaz.

3. A $\rho^n = e, \sigma^2 = e$ és $\sigma\rho = \rho^{n-1}\sigma$ összefüggések meghatározzák D_n műveletábráját.

4. Ugyanakkor $\rho^k\sigma$ inverze önmaga: $(\rho^k\sigma)^{-1} = \rho^k\sigma$, azaz $(\rho^k\sigma)^2 = e$, $0 \leq k < n$. Ez következik abból, hogy $\rho^k\sigma$ egy szimmetriatengelyre való tükrözés, lásd fennebb, és számolással is igazolható: $(\rho^k\sigma)^2 = \rho^k\sigma\rho^k\sigma = \rho^k(\sigma\rho)\rho^{k-1}\sigma = \rho^k(\rho^{-1}\sigma)\rho^{k-1}\sigma = \rho^{k-1}\sigma\rho^{k-1}\sigma = \dots = \rho\sigma\rho\sigma = \rho(\sigma\rho)\sigma = \rho(\rho^{-1}\sigma)\sigma = \sigma^2 = e$.

5. A D_n diédercsoport absztrakt definíciója a következő :

$$D_n = \{e, x, x^2, \dots, x^{n-1}, y, xy, x^2y, \dots, x^{n-1}y\},$$

ahol $x^n = y^2 = e, xy = x^{n-1}y$. Másképp:

$$D_n = \langle x, y | x^n = y^2 = e, xy = x^{n-1}y \rangle.$$

Itt x és y a generálóelemek és rájuk a fenti definiáló relációk vonatkoznak.

6. Ha a P_n sokszög csúcsait $1, 2, \dots, n$ -nel jelöljük, akkor minden f transzformáció egy S_n -beli permutáció. Így D_n azonosítható S_n egy részcsoporthal (izomorf vele).

7. Ha $n = 3$, akkor mivel $D_3 \leq S_3$ és $|D_3| = 6$, következik, hogy $D_3 = S_3$, pontosabban $D_3 \simeq S_3$.

Definiálhatjuk a D_2 és D_1 csoportokat is. D_2 az olyan téglalap transzformációcsoportja, amely nem négyzet, ez éppen a Klein-csoport: $D_2 = \langle x, y | x^2 = y^2 = e, yx = xy \rangle$, $|D_2| = 4$.

Továbbá D_1 az egyenlőszárú (nem szabályos) háromszög transzformációcsoportja. Ez két transzformációból áll: az e identikus (0° -kal való rotáció) és az alap felezőmerőlegesére vett s szimmetria, ahol $s^2 = e$. Itt $D_1 = \{e, s\}$, $|D_1| = 2$.

9.A.2. Feladat. ▼ a) Készítsük el D_4 műveletábráját.

★ b) Határozzuk meg D_4 részcsoporthait és normálosztóit.

Megoldás. a)

$$D_4 = \{e, \rho, \rho^2, \rho^3, \sigma, \rho\sigma, \rho^2\sigma, \rho^3\sigma\},$$

ahol $\rho^4 = e, \sigma^2 = e, \sigma\rho = \rho^3\sigma$.

★ b) D_4 részcsoporthainak rendje 1, 2, 4, 8 lehet. Ezek $H_1 = \{e\}$, a másodrendű részcsoporthok $H = \{e, x\}$ alakúak, ahol $x^2 = e$. Öt ilyen találunk: $H_2 = \{e, \sigma\}$, $H_3 = \{e, \rho\sigma\}$, $H_4 = \{e, \rho^2\sigma\}$, $H_5 = \{e, \rho^3\sigma\}$, $H_6 = \{e, \rho^2\}$.

A negyedrendű részcsoporthok $H = \{e, x, x^2, x^3\}$, $x^4 = e$ alakú ciklikusak vagy Klein-félék: $H = \{1, x, y, xy\}$, ahol $x^2 = y^2 = e, xy = yx$. Egy ciklikus részcsoporth van: $H_7 = \{e, \rho, \rho^2, \rho^3\}$ és 2 Klein-féle: $H_8 = \{e, \rho^2, \sigma, \rho^2\sigma\}$ és $H_9 = \{e, \rho^2, \rho\sigma, \rho^3\sigma\}$.

Van még a $H_{10} = D_4$ részcsoporth.

A fenti 10 részcsoporthból 6 normálrészcsoporth: H_1, H_{10} a triviálisak, H_7, H_8, H_9 indexe 2, H_6 pedig két normálrészcsoporth metszete: $H_6 = H_7 \cap H_8$. A többi 4, tehát H_2, H_3, H_4, H_5 nem normálrészcsoporth, mert pl. $\rho\sigma\rho^{-1} = \rho\sigma\rho^3 = \rho(\sigma\rho)\rho^2 = \rho(\rho^3\sigma)\rho^2 = \rho^4\sigma\rho^2 = \sigma\rho^2 = \rho^3\sigma\rho = \rho^2\sigma \notin H_2$.

Megjegyzés: $\{e, \sigma\} \trianglelefteq \{e, \rho^2, \sigma, \rho^2\sigma\} \trianglelefteq D_4$ (rendre 2 indexűek), de $\{e, \sigma\} \not\trianglelefteq D_4$. ★

9.B. A $2p$ rendű csoportok

A csoportelmélet egyik fontos feladata az összes létező csoporttípus leírása. Láttuk már, hogy csak egyfajta prímszámrendű csoport létezik. Tehát egy-egy olyan csoport van, amelynek rendje $2, 3, 5, 7, 11, 13, 17, 19, \dots$, ezek ciklikusak (és kommutatívak).

Nézzük most a $2p$ rendű csoportokat, ahol p prímszám. Szükségünk van a következő eredményre:

9.B.1. Tétel. Legyen $(G, \cdot)$ egy véges csoport úgy, hogy $\forall x \in G : x^2 = e$. Akkor G kommutatív és létezik $k \in \mathbb{N}$ úgy, hogy $|G| = 2^k$.

Bizonyítás. $\forall x, y \in G : e = (xy)^2 = xyxy, e = ee = x^2y^2 = xxyy \Rightarrow xy = yx$.

A második állítást $|G| = n$ -szerinti indukcióval bizonyítjuk. Ha $|G| = 1$ vagy $|G| = 2$, akkor az állítás igaz. Tegyük fel, hogy az állítás igaz minden n -nél kisebbrendű csoportra és legyen $|G| = n$. Legyen $x \in G, x \neq e$ és $N = \langle x \rangle$ az x által generált részcsoporth, $N = \{e, x\}$, hiszen $x^2 = e$. Továbbá G kommutatív, ezért $N \trianglelefteq G$ és $G/N = |G|/2 = n/2 < n$ és $\forall yN \in G/N : (yN)^2 = y^2N = eN = N$, ami a G/N faktorcsoporth egységeleme.

Így G/N -re alkalmazva az indukciós feltételt: $|G| = 2^k$, ahonnan $|G| = |G/N||N| = 2^{k+1}$. □

A következő tétel a a diédercsoport fontosságára is rávilágít.

9.B.2. Tétel. Ha a G csoport rendje $|G| = 2p$, ahol $p \geq 2$ prímszám, akkor $G \simeq (\mathbb{Z}_{2p}, +)$ vagy $G \simeq (D_p, \circ)$.

★ **Bizonyítás.** Minden $x \in G$ elem rendje osztója a csoport rendjének (Tétel), azaz $\forall x \in G : o(x) = 1, 2, p$ vagy $2p$. Ha $\exists x \in G : o(x) = 2p$, akkor G ciklikus: $G = \langle x \rangle \simeq (\mathbb{Z}_{2p}, +)$.

Ellenkező esetben $\forall x \in G, x \neq e : o(x) = 2$ vagy $o(x) = p$. Ha $p = 2$, akkor $\forall x \in G, x \neq e : o(x) = 2$ és a műveletábra elemzésével a $D_2 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ Klein-féle csoportot kapjuk.

Ha $p \geq 3$, akkor $|G| \neq 2^k$ és az előző Tétel alapján következik, hogy létezik $x \in G : o(x) = p$ és legyen $N = \langle x \rangle = \{e, x, x^2, \dots, x^{p-1}\}$. Mivel $|N| = p$, ezért $|G/N| = 2$, azaz N egy 2 indexű részcsoporth, ezért $N \trianglelefteq G$, lásd 6. szakasz, és $\forall y \in G \setminus N : G/N = \{N, yN\}$, $yN = Ny$, $(yN)^2 = N$ (mert $(yN)^2 = yN \Rightarrow yN = N$, nem lehet) és $(yN)^p = yN$ (p páratlan). Ugyanakkor $yx \in yN \Rightarrow yN = (yx)N$. Tehát $y^p \neq e$, $(yx)^p \neq p$, s mivel minden elem rendje 2 vagy p , következik, hogy $o(y) = o(yx) = 2$.

Továbbá, $yx \in yN = Ny \Rightarrow \exists k \in \{1, 2, \dots, p-1\} : yx = x^k y$, itt $k \neq 0$, mert $k = 0$ -ra $yx = y \Rightarrow x = e$, ellentmondás. Itt $e = (yx)^2 = yxyx = x^k y^2 x = x^{k+1}$, tehát $o(x) = p = k + 1 \Rightarrow k = p - 1$, $yx = x^{p-1} y$.

Így $G = N \cup Ny = \{e, x, x^2, \dots, x^{p-1}, y, xy, \dots, x^{p-1}y\}$, ahol $o(x) = p$, $o(y) = 2$ és $yx = x^{p-1}y$, tehát $G \simeq D_p$, a diédercsoport. □★

Tehát két-két olyan csoport van, amelynek rendje 4, 6, 10, 14, 22, ..., ezek egyike ciklikus, a másik a diédercsoport.

9.C. A p^2 rendű csoportok

Igazolható továbbá:

9.C.1. Tétel. Ha a G csoport rendje $|G| = p^2$, ahol $p \geq 2$ prímszám, akkor G kommutatív és $G \simeq (\mathbb{Z}_{p^2}, +)$ vagy $G \simeq (\mathbb{Z}_p \times \mathbb{Z}_p, +)$. $\square$

Tehát két-két olyan csoport van, amelynek rendje 4, 9, 25, ..., ezek kommutatívak, az egyik ciklikus, a másik két ciklikus csoport direkt szorzata.

A legkisebb rendű csoport, amely nem szerepel a fentiekben, a 8-adrendű. Igazolható, hogy a G kommutatív esetben 3 lehetőség van: $G \simeq (\mathbb{Z}_8, +)$ ciklikus, vagy $G \simeq (\mathbb{Z}_2 \times \mathbb{Z}_4, +)$ vagy $G \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, +)$. Ha G nem kommutatív, akkor 2 eset van: $G \simeq D_4$ a diédercsoport vagy $G \simeq Q$ a kvaterniócsoport.

Továbbá a 12 elemű csoportok száma 5, 15 elemű csoport egyféle van, a ciklikus csoport, a 16 elemű csoportok száma pedig 14. Ezek meghatározása több előismeretet és több számolást igényel.