15. PÉLDÁK FÉLCSOPORTOKRA ÉS CSOPORTOKRA

1. Az $\mathbb{R}^3$ tér vektorai a derékszögű koordinátarendszerben az $\mathbf{a} = (a_1, a_2, a_3)$ alakban adottak az $a_1, a_2, a_3 \in \mathbb{R}$ valós számokkal. A vektoriális szorzás kétváltozós művelete az $\mathbb{R}^3$ halmazon közismerten nem asszociatív: az $\mathbf{a} = (a_1, a_2, a_3)$ és $\mathbf{b} = (b_1, b_2, b_3)$ vektorokra

$$\mathbf{a} \times \mathbf{b} = (a_2b_3 - a_3b_2, a_3b_1 - a_1b_3, a_1b_2 - a_2b_1).$$

Az alábbiakban a skaláris szorzat felhasználásával megadjuk az $(\mathbf{a} \times \mathbf{b}) \times \mathbf{c}$ és $\mathbf{a} \times (\mathbf{b} \times \mathbf{c})$ szorzatokra vonatkozó ismert képleteket:

$$(\mathbf{a} \times \mathbf{b}) \times \mathbf{c} = (\mathbf{ac})\mathbf{b} - (\mathbf{bc})\mathbf{a}\ ,\ \mathbf{a} \times (\mathbf{b} \times \mathbf{c}) = (\mathbf{ac})\mathbf{b} - (\mathbf{ab})\mathbf{c}.$$

A fentiekből kitűnik, hogy az asszociatív azonosság csak kivételesen a $(\mathbf{bc})\mathbf{a} = (\mathbf{ab})\mathbf{c}$ esetben teljesül.

2. Tetszőleges A halmaz $a_1, a_2 \in A$ elemeivel képezhetjük az $x = (a_1, a_2)$ alakú rendezett párt, az ilyenek $A \times A$-val jelölt halmazán értelmezzük az $y = (b_1, b_2)$ elemet is használva az

$$x \circ y = (a_1, a_2) \circ (b_1, b_2) = (a_1, b_1)$$

kétváltozós műveletet. Az így kapott műveletre általában $(x \circ x) \circ y \neq x \circ (x \circ y)$, ami azt jelenti, hogy $\circ$ nem asszociatív, a következő azonosságok viszont könnyen ellenőrízhetőek: $x \circ y = (x \circ u) \circ y = x \circ (y \circ v)$.

3. Az $A \times A$ halmaz $x = (a_1, a_2)$ és $y = (b_1, b_2)$ elemeire legyen most:

$$x \circ y = (a_1, a_2) \circ (b_1, b_2) = (a_1, b_2).$$

Ez a kétváltozós művelet asszociatív, amelyre még az $xyz = xz$ és $x^2 = x$ azonosságok is teljesülnek. Az $(A \times A, \circ)$ félcsoportban: $xy = yx \Leftrightarrow x = y$, egység nem létezik (feltéve, hogy A-nak legalább két eleme van), balról (jobbról) egyszerűsíteni egyik elemmel sem lehet.

4. Bármely H halmazon az $x, y \in H$ elemekre $x \circ y = x$ egy kétváltozós asszociatív műveletet értelmez. Ebben az ún. **balzéró** $(H, \circ)$ félcsoportban: $xy = yx \Leftrightarrow x = y$, egység nem létezik (feltéve, hogy H-nak legalább két eleme van), egyetlen elemmel sem lehet balról egyszerűsíteni de minden elemmel lehet jobbról.

5. Az egész számokkal felírható $n \times n$-es mátrixok $M_n(\mathbb{Z})$ halmazán a mátrixok jól ismert szorzása asszociatív: az $A = [a_{ij}]$ és $B = [b_{ij}]$ mátrixokra $AB = [c_{ij}]$, ahol $c_{ij} = \sum_{r=1}^{n} a_{ir}b_{rj}$. A mátrixok szorzása nem kommutatív: $AB \neq BA$ az esetek többségében. Az egység közismert:

$$1_n = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Felcserélhető elemeket könnyen találunk: $AB = BA$ minden

$$B = \alpha_k A^k + \alpha_{k-1} A^{k-1} + ... + \alpha_1 A + \alpha_0 I$$

alakú mátrixra, ahol $\alpha_k, \alpha_{k-1}, ..., \alpha_1, \alpha_0 \in \mathbb{Z}$ és I az egységmátrix. A centrális elemek az $\alpha I, \alpha \in \mathbb{Z}$ alakú mátrixok. Balról is és jobbról is lehet egyszerűsíteni minden olyan A mátrixszal, amelyre $\det(A) \neq 0$. Ha $\det(A) = \pm 1$, akkor A-nak létezik (kétoldali) inverze.

6. Az egész A halmazon értelmezett és A-beli értékeket felvevő függvények $T(A)$ halmazán az $f, g \in T(A)$ kompozícióját az $(f \circ g)(x) = f(g(x))$ módon értelmezzük egy $x \in A$ elemre. Az így kapható $T(A)$ ún. **transzformáció félcsoportban** könnyen találunk felcserélhető elemeket, de általában $f \circ g \neq g \circ f$. Az identikus id_A leképezés lesz az egység. Balinverze az injektív, jobbinverze a szürjektív, (kétoldali) inverze a bijektív függvényeknek van.

7. Rögzítsük az $s \in H$ ún. szendvicselemet egy olyan H félcsoportban, amelyben a szorzást az elemek egymás után írásával jelöljük. Az $x, y \in H$ elemekre legyen $x \circ y = xsy$, amivel egy kétváltozós asszociatív műveletet értelmeztünk H-n:

$$(x \circ y) \circ z = (xsy)sz = xs(ysz) = x \circ (y \circ z).$$

Ugyanígy látható, hogy $x * y = ysx$ is asszociatív, speciálisan ha $x * y = yx$, akkor $(H, *)$-t az eredeti H **fordított félcsoportjának** nevezzük.

8. Legyen $\mathcal{F}(X)$ az olyan (n, f) párok halmaza, amelyekben $n \geq 1$ egész szám, $X \neq \emptyset$ egy tetszőleges halmaz és $f : \{1, 2, ..., n\} \to X$ egy függvény (sorozat). Az $(m, g) \in \mathcal{F}(X)$ elemet is használva értelmezzünk egy kétváltozós műveletet az alábbiak szerint:

$$(n, f) \circ (m, g) = (n + m, h),$$

ahol a $h : \{1, 2, ..., n + m\} \to X$ függvény az f és g sorozatok egymás után való írásával keletkezik, azaz

$$h(i) = \begin{cases} f(i) \text{ ha } 1 \leq i \leq n, \\ g(i - n) \text{ ha } n + 1 \leq i \leq n + m. \end{cases}$$

A $\circ$ asszociatív és $(\mathcal{F}(X), \circ)$-t az X által generált **szabad félcsoportnak** nevezzük, amelyben (n, f) egy n hosszúságú szó.

9. Kommutatív monoidokra példák az alábbiak.

(i) $(\mathbb{R}^+, +, 0)$ a nem negatív valós számok az összeadással.

(ii) $(\mathbb{C}[x], \cdot, 1)$ az x változó komplex együtthatós polinomjai a szorzással.

(iii) $(\mathbb{C}[x]\backslash\{0\}, \cdot, 1)$ az x változó komplex együtthatós nem zéró polinomjai a szorzással.

(iv) $(\mathcal{P}(A), \cup, \emptyset)$,$(\mathcal{P}(A), \cap, A)$ az A halmaz hatványhalmaza az unióval és a metszettel.

10. Példák kommutatív csoportokra.

(i) $(\mathbb{R}^+\backslash\{0\}, \cdot, 1)$ a pozitív valós számok a szorzással (ez részcsoportja az $(\mathbb{R}^* = \mathbb{R}\backslash\{0\}, \cdot, 1)$ csoportnak).

(ii) $(\mathbb{C}, +, 0)$ és $(\mathbb{C}^* = \mathbb{C}\backslash\{0\}, \cdot, 1)$ a komplex számok az összeadással és a nem zéró komplex számok a szorzással, $(\mathbb{C}[x], +, 0)$ az x változó komplex együtthatós polinomjai az összeadással.

(iii) $(M_{n\times m}(\mathbb{C}), +, 0)$ a komplex számokkal felírható $n \times m$-es mátrixok az összeadással.

(iv) $(\mathcal{P}(A), \triangle, \emptyset)$ az A halmaz hatványhalmaza a szimmetrikus differenciával (az $X, Y \subseteq A$ halmazokra $X \triangle Y = (X\backslash Y) \cup (Y\backslash X)$).

(v) $(\mathbb{Z}_n, +, 0)$ az egész számok maradékosztályai modulo n az összeadással, ez a $(\mathbb{Z}, +, 0)$ csoport faktorcsoportja az $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\} \lhd \mathbb{Z}$ normális részcsoport szerint.

(vi) $(U(\mathbb{Z}_n), \cdot, 1)$ az egész számok redukált maradékosztályai modulo n a szorzással: $U(\mathbb{Z}_n)$ elemei a $(\mathbb{Z}_n, \cdot, 1)$ monoid invertálható elemei által alkotott (rész)csoport.

11. Példák nem kommutatív csoportokra.

(i) $(\mathrm{Gl}_2(\mathbb{R}), \cdot, 1_2)$ a valós számokkal felírható 2×2-es invertálható mátrixok halmaza a mátrix szorzással és ennek a

$$\mathbb{K}^* = \left\{ \begin{bmatrix} u & v \\ -v & u \end{bmatrix} \mid u, v \in \mathbb{R} \text{ és } u^2 + v^2 \neq 0 \right\} \subseteq \mathrm{Gl}_2(\mathbb{R})$$

kommutatív részcsoportja (amely a $(\mathbb{C}^* = \mathbb{C}\backslash\{0\}, \cdot, 1)$ csoporttal izomorf).

(ii) $(\mathrm{Gl}_2(\mathbb{C}), \cdot, 1_2)$ a komplex számokkal felírható 2×2-es invertálható mátrixok halmaza a mátrix szorzással és ennek a

$$\mathbb{H}^* = \left\{ \begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \text{ és } a^2 + b^2 + c^2 + d^2 \neq 0 \right\} \subseteq \mathrm{Gl}_2(\mathbb{C})$$

részcsoportja valamint $(\mathbb{H}^*, \cdot, 1_2)$-nak az alábbi

$$\left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \pm \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \right\}$$

ún. **kvaternió részcsoportja**.

(iii) $(\mathrm{Gl}_n(\mathbb{C}), \cdot, 1_n)$ az **általános lineáris csoport**, a komplex számokkal felírható $n \times n$-es invertálható mátrixok halmaza a mátrix szorzással és ennek a

$$\mathrm{Scal}_n(\mathbb{C}) \subseteq \mathrm{Diag}_n(\mathbb{C}) \subseteq \mathrm{T}_n(\mathbb{C}) \subseteq \mathrm{Gl}_n(\mathbb{C})$$

részcsoportjai valamint az $\mathrm{UT}_n(\mathbb{C}) \subseteq \mathrm{T}_n(\mathbb{C})$ részcsoport, ahol

$\mathrm{T}_n(\mathbb{C}) = \left\{ [a_{ij}]_{n\times n} \mid [a_{ij}]_{n\times n} \in \mathrm{Gl}_n(\mathbb{C}), \text{ és } a_{ij} = 0 \text{ az } 1 \leq j < i \leq n \text{ egészekre} \right\}$ a
felső trianguláris mátrixok halmaza,

$\mathrm{UT}_n(\mathbb{C}) = \left\{ [a_{ij}]_{n\times n} \mid [a_{ij}]_{n\times n} \in \mathrm{T}_n(\mathbb{C}) \text{ és } a_{ii} = 1 \text{ az } 1 \leq i \leq n \text{ egészekre} \right\}$ a
felső unitrianguláris mátrixok halmaza,

$\mathrm{Diag}_n(\mathbb{C}) = \left\{ [a_{ij}]_{n\times n} \mid [a_{ij}]_{n\times n} \in \mathrm{Gl}_n(\mathbb{C}), \text{ és } a_{ij} = 0 \text{ az } i \neq j,\ 1 \leq i, j \leq n \text{ egészekre} \right\}$ a
diagonális mátrixok halmaza (ez kommutatív részcsoport),

$\mathrm{Scal}_n(\mathbb{C}) = \{u1_n \mid u \in \mathbb{C}\}$ a **skaláris mátrixok** halmaza.

(iv) $(\mathrm{Sym}(A), \circ, \mathrm{id}_A)$ a **szimmetrikus csoport**, az egész A halmazon értelmezett és A-beli értékeket felvevő bijektív (invertálható) függvények a szokásos kompozícióval.

(v) $(\mathcal{G}(K \subseteq L), \circ, \mathrm{id}_L)$ **Galois csoport**, a $K \subseteq L \subseteq \mathbb{C}$ testbővítés relatív automorfizmusai a szokásos kompozícióval.

12. Példák csoport homomorfizmusokra (kommutatív csoportok között).

(i) A $z \in \mathbb{C}\backslash\{0\}$ elemen az $\mathrm{abs}(z) = |z|$ módon értelmezett

$$\mathrm{abs} : \mathbb{C}\backslash\{0\} \longrightarrow \mathbb{R}^+\backslash\{0\}$$

leképezés a $(\mathbb{C}^* = \mathbb{C}\backslash\{0\}, \cdot, 1)$ csoportból az $(\mathbb{R}^+\backslash\{0\}, \cdot, 1)$ csoportba irányuló (szürjektív) homomorfizmus, amelynek a magja az egységkörív $\ker(\mathrm{abs}) = \{z \in \mathbb{C} \mid |z| = 1\}$.

(ii) Ha $w \in \mathbb{C}$, akkor az $f(x) \in \mathbb{C}[x]$ elemen az $\mathrm{ev}_w(f(x)) = f(w)$ módon értelmezett

$$\mathrm{ev}_w : \mathbb{C}[x] \longrightarrow \mathbb{C}$$

leképezés a $(\mathbb{C}[x], +, 0)$ csoportból a $(\mathbb{C}, +, 0)$ csoportba irányuló (szürjektív) homomorfizmus, amelynek a magja a w gyökkel rendelkező polinomokból áll.

(iii)

$$\mathrm{ev}_w : \mathbb{C}[x] \longrightarrow \mathbb{C} \text{ és } \deg : \mathbb{C}[x]\backslash\{0\} \longrightarrow \{0, 1, 2, ...\}$$

ún. monoid közötti homomorfizmusok, amelyek a $(\mathbb{C}[x], \cdot, 1)$ illetve a $(\mathbb{C}[x]\backslash\{0\}, \cdot, 1)$ monoidokból irányulnak a $(\mathbb{C}, \cdot, 1)$ illetve a $(\{0, 1, 2, ...\}, +, 0)$ monoidokba.

(iv) Ha $A \in M_{k\times n}(\mathbb{C})$ és $B \in M_{m\times l}(\mathbb{C})$, akkor az $X \in M_{n\times m}(\mathbb{C})$ elemen az

$\mathrm{m}_{(A,B)}(X) = AXB$ módon értelmezett

$$\mathrm{m}_{(A,B)} : M_{n\times m}(\mathbb{C}) \longrightarrow M_{k\times l}(\mathbb{C})$$

leképezés az $(M_{n\times m}(\mathbb{C}), +, 0)$ csoportból az $(M_{k\times l}(\mathbb{C}), +, 0)$ csoportba irányuló homomorfizmus.

(v) Ha $a \in A$, akkor az $X \in \mathcal{P}(A)$ elemen a $\chi_a(X) = \begin{cases} \overline{0} \text{ ha } a \notin X \\ \overline{1} \text{ ha } a \in X \end{cases}$ módon értelmezett

$$\chi_a : \mathcal{P}(A) \longrightarrow \mathbb{Z}_2$$

leképezés a $(\mathcal{P}(A), \triangle, \emptyset)$ csoportból a $(\mathbb{Z}_2, +, \overline{0})$ csoportba irányuló homomorfizmus, amelynek a magja az a elemet nem tartalmazó részhalmazokból áll.

(vi) Ha $k \in \mathbb{Z}$ és $(G, \circ, 1)$ kommutatív csoport, akkor a $g \in G$ elemen a $\mathrm{pow}_k(g) = g^k$ módon értelmezett

$$\mathrm{pow}_k : G \longrightarrow G$$

leképezés a $(G, \circ, 1)$ csoportból (önmagába azaz) $(G, \circ, 1)$-be irányuló homomorfizmus.

13. Példák csoport homomorfizmusokra.

(i) Bármely $(G, \circ, 1)$ csoport esetén a $g \in G$ elemen az $\mathrm{inv}(g) = g^{-1}$ módon értelmezett

$$\mathrm{inv} : G \longrightarrow G$$

leképezés a $(G, \circ, 1)$ csoportból a $(G, *, 1)$ ún. fordított csoportba irányuló izomorfizmus (az $x, y \in G$ elemekre $x * y = y \circ x$), amelynek az inverze saját maga: $(\mathrm{inv})^{-1} = \mathrm{inv}$, kommutatív csoport fordított csoportja önmaga.

(ii)

$$\det : \mathrm{Gl}_n(\mathbb{C}) \longrightarrow \mathbb{C}\backslash\{0\}$$

a $(\mathrm{Gl}_n(\mathbb{C}), \cdot, 1_n)$ csoportból a $(\mathbb{C}^* = \mathbb{C}\backslash\{0\}, \cdot, 1)$ csoportba irányuló (szürjektív) homomorfizmus.

(iii) Az $A \in \mathrm{Gl}_n(\mathbb{C})$ mátrixon az

$$A \longmapsto \begin{bmatrix} \boxed{A} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \begin{matrix} 0 & ... & 0 \end{matrix} & 1 \end{bmatrix}$$

módon értelmezett leképezés a $(\mathrm{Gl}_n(\mathbb{C}), \cdot, 1_n)$ csoportból a $(\mathrm{Gl}_{n+1}(\mathbb{C}), \cdot, 1_{n+1})$ csoportba irányuló injektív homomorfizmus.

(iv) Az

$$A = \begin{bmatrix} \boxed{\widetilde{A}} & \begin{matrix} u_1 \\ \vdots \\ u_{n-1} \end{matrix} \\ \begin{matrix} 0 & \ldots & 0 \end{matrix} & 1 \end{bmatrix}$$

alakban írható $A \in \mathrm{UT}_n(\mathbb{C})$ mátrixon az $A \longmapsto \widetilde{A}$ módon értelmezett leképezés az $(\mathrm{UT}_n(\mathbb{C}), \cdot, 1_n)$ csoportból az $(\mathrm{UT}_{n-1}(\mathbb{C}), \cdot, 1_{n-1})$ csoportba irányuló szürjektív homomorfizmus, amelynek a magja az alábbi

$$\left\{ \begin{bmatrix} \boxed{1_{n-1}} & \begin{matrix} u_1 \\ \vdots \\ u_{n-1} \end{matrix} \\ \begin{matrix} 0 & \ldots & 0 \end{matrix} & 1 \end{bmatrix} \mid u_1, u_2, ..., u_{n-1} \in \mathbb{C} \right\} \subseteq \mathrm{UT}_n(\mathbb{C})$$

kommutatív részcsoport.

(v) Az $A = [a_{ij}]_{n\times n} \in \mathrm{Gl}_n(\mathbb{C})$ mátrixon az

$$A \longmapsto A^{\mathtt{t}} = [a_{ji}]_{n\times n}$$

módon értelmezett transzponálás a $(\mathrm{Gl}_n(\mathbb{C}), \cdot, 1_n)$ csoportból annak a $(\mathrm{Gl}_n(\mathbb{C}), *, 1_n)$ fordított csoportjába irányuló izomorfizmus,

$$\mathrm{O}_n(\mathbb{R}) = \{A \in \mathrm{Gl}_n(\mathbb{R}) \mid AA^{\mathtt{t}} = 1_n\} \subseteq \mathrm{Gl}_n(\mathbb{R})$$

az ún. **ortogonális részcsoportja** a $(\mathrm{Gl}_n(\mathbb{R}), \cdot, 1_n)$ csoportnak.

(vi) A $\pi \in \mathrm{S}_n = \mathrm{Sym}(\{1, 2, ..., n\})$ permutáción a $P_\pi = \sum_{i=1}^{n} E_{\pi(i),i}$ módon értelmezett

$$P : \mathrm{S}_n \longrightarrow \mathrm{Gl}_n(\mathbb{C})$$

leképezés az $(\mathrm{S}_n, \circ, \mathrm{id}_n)$ szimmetrikus csoportból a $(\mathrm{Gl}_n(\mathbb{C}), \cdot, 1_n)$ csoportba irányuló injektív homomorfizmus; az $n \times n$-es P_π mátrixot nevezzük a π-hez tartozó **permutáció mátrixnak** (itt az $n \times n$-es $E_{\pi(i),i}$ ún. **standard mátrixegységben** a $\pi(i)$-edik sor és az i-edik oszlop kereszteződésében 1 áll, a többi helyen 0).

(vii) Ha $g_1, g_2, ..., g_n$ a $(G, \circ, 1)$ csoport elemeinek egy teljes és ismétlődés nélküli felsorolása (azaz $G = \{g_1, g_2, ..., g_n\}$ és $|G| = n$), akkor a $h \in G$ elemen a

$$\mathrm{C}_l(h) = \begin{pmatrix} g_1 & g_2 & . & . & . & g_n \\ hg_1 & hg_2 & . & . & . & hg_n \end{pmatrix} = \begin{pmatrix} g_1 & g_2 & . & . & . & g_n \\ g_{\pi(1)} & g_{\pi(2)} & . & . & . & g_{\pi(n)} \end{pmatrix}$$

módon értelmezett $\mathrm{C}_l : G \longrightarrow \mathrm{Sym}(\{g_1, g_2, ..., g_n\})$ leképezés a $(G, \circ, 1)$ csoportból a $(\mathrm{Sym}(\{g_1, g_2, ..., g_n\}), \circ, \mathrm{id})$ szimmetrikus csoportba irányuló injektív (ún. **Cayley**)

homomorfizmus.

(viii) Ha $K \subseteq L \subseteq \mathbb{C}$ véges testbővítés és a $K \subseteq T \subseteq L$ köztes számtest normális bővítése K-nak, akkor a $\Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmuson a $\mathrm{res}(\Phi) = \Phi \restriction T$ módon értelmezett

$$\mathrm{res} : \mathcal{G}(K \subseteq L) \longrightarrow \mathcal{G}(K \subseteq T)$$

leképezés a $(\mathcal{G}(K \subseteq L), \circ, \mathrm{id}_L)$ Galois csoportból a $(\mathcal{G}(K \subseteq T), \circ, \mathrm{id}_T)$ Galois csoportba irányuló homomorfizmus, amelynek a magja $\ker(\mathrm{res}) = \mathcal{G}(T \subseteq L)$.

(ix) Legyen $K \subseteq \mathbb{C}$ tetszőleges számtest és az $\alpha_1, \alpha_2 ..., \alpha_n \in \mathbb{C}$ számok egy $f(x) \in K[x]$ polinomnak az összes egymástól különböző gyökei, ekkor a

$$K \subseteq K(\alpha_1, \alpha_2 ..., \alpha_n) = K(f(x) = 0) = F$$

testbővítés az $f(x)$ polinom felbontási teste a K felett és a $\Phi \in \mathcal{G}(K \subseteq F)$ relatív automorfizmuson a

$$\overline{\Phi} = \begin{pmatrix} \alpha_1 & \alpha_2 & . & . & . & \alpha_n \\ \Phi(\alpha_1) & \Phi(\alpha_2) & . & . & . & \Phi(\alpha_n) \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & . & . & . & \alpha_n \\ \alpha_{\pi(1)} & \alpha_{\pi(2)} & . & . & . & \alpha_{\pi(n)} \end{pmatrix}$$

módon értelmezett $\Phi \longmapsto \overline{\Phi} = \pi$ leképezés a $(\mathcal{G}(K \subseteq F), \circ, \mathrm{id}_F)$ Galois csoportból a $(\mathrm{Sym}(\{\alpha_1, \alpha_2, ..., \alpha_n\}), \circ, \mathrm{id})$ szimmetrikus csoportba irányuló injektív homomorfizmus.

15.A.Definíció. A $\varnothing \neq C \subseteq \{1, 2, ..., n\}$ részhalmazt a $\pi \in \mathrm{Sym}(\{1, 2, ..., n\})$ **permutáció ciklusának** nevezzük, ha $\pi(C) = C$ és bármely $\varnothing \neq D \subset C$ valódi részhalmazra $\pi(D) \neq D$. Az

$$\mathrm{inv}(\pi) = \{(i, j) \mid 1 \leq i < j \leq n \text{ és } \pi(j) < \pi(i)\}$$

halmaz elemeit nevezzük a π **permutáció inverzióinak**. Ha $2 \leq m \leq n$ és $i_1, i_2, ..., i_m$ egymástól különböző elemei $\{1, 2, ..., n\}$-nek, akkor $(i_1, i_2, ..., i_m)$ jelölje azt a **ciklikusnak nevezett** $\mathrm{Sym}(\{1, 2, ..., n\})$-beli **permutációt**, amelyre $1 \leq k \leq m - 1$ és
$j \in \{1, 2, ..., n\} \setminus \{i_1, i_2, ..., i_m\}$ esetén

$$(i_1, i_2, ..., i_m)(i_k) = i_{k+1} \ , \ (i_1, i_2, ..., i_m)(i_m) = i_1 \text{ és } (i_1, i_2, ..., i_m)(j) = j.$$

Az $m = 2$ esetben az (i_1, i_2) alakú permutációt **transzpozíciónak** nevezzük.♡

15.1.Állítás. *Tetszőleges $1 \leq l \leq m$ egészre*

$$(i_l, i_{l+1}, ..., i_m, i_1, i_2, ..., i_{l-1}) = (i_1, i_2, ..., i_m),$$

továbbá

$$(i_1, i_2, ..., i_m) = (i_1, i_m) \circ (i_1, i_{m-1}) \circ ... \circ (i_1, i_2).$$

Az $\{i_1, i_2, ..., i_m\} \cap \{j_1, j_2, ..., j_r\} = \varnothing$ esetben

$$(i_1, i_2, ..., i_m) \circ (j_1, j_2, ..., j_r) = (j_1, j_2, ..., j_r) \circ (i_1, i_2, ..., i_m).$$

15.2.Állítás. *Ha $C, C', C'' \subseteq \{1, 2, ..., n\}$ ciklusai a $\pi \in \mathrm{Sym}(\{1, 2, ..., n\})$ permutációnak és $1 \leq i \leq n$, akkor $\{i, \pi(i), \pi^2(i), ..., \pi^k(i), ...\} \subseteq \{1, 2, ..., n\}$ ciklusa lesz π-nek, az $i \in C$ esetben*

$$C = \{i, \pi(i), \pi^2(i), ..., \pi^k(i), ...\} = \{i, \pi(i), \pi^2(i), ..., \pi^{m-1}(i)\}$$

és $\pi^m(i) = i$, ahol $m = |C|$. Alkalmazva a $\widehat{C} = (i, \pi(i), \pi^2(i), ..., \pi^{m-1}(i))$ jelölést, a $\widehat{C}$ ciklikus permutáció nem függ attól, hogy melyik $i \in C$ elemet választottuk:

$$\widehat{C} \restriction C = \pi \restriction C \text{ és } \widehat{C} \restriction \{1, 2, ..., n\} \setminus C = \mathrm{id}.$$

Ha $C' \neq C''$, akkor $C' \cap C'' = \varnothing$ és $\widehat{C'} \circ \widehat{C''} = \widehat{C''} \circ \widehat{C'}$. Az $\{1, 2, ..., n\}$ halmaz előáll a π permutáció összes különböző (és így páronként diszjunkt) $C_1, C_2, ..., C_t$ ciklusainak az egyesítéseként

$$\{1, 2, ..., n\} = C_1 \cup C_2 \cup ... \cup C_t,$$

továbbá

$$\pi = \widehat{C_1} \circ \widehat{C_2} \circ ... \circ \widehat{C_t}.$$

15.3.Következmény. *Az* $(\mathrm{S}_n, \circ, \mathrm{id})$ *szimmetrikus csoportban bármely* π *permutáció megkapható transzpozíciók szorzataként (kompozíciójaként).*

15.4.Állítás. *A* $\pi \in \mathrm{S}_n = \mathrm{Sym}(\{1, 2, ..., n\})$ *permutáción a*

$$\mathrm{sgn}(\pi) = (-1)^{|\mathrm{inv}(\pi)|}$$

módon értelmezett

$$\mathrm{sgn} : \mathrm{S}_n \longrightarrow \{-1, 1\}$$

leképezés az $(\mathrm{S}_n, \circ, \mathrm{id})$ *szimmetrikus csoportból a* $(\{-1, 1\}, \cdot, 1)$ *kételemű csoportba (ez utóbbi* $(\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}, \cdot, 1)$*-nak részcsoportja) irányuló szürjektív homomorfizmus, amelyre teljesül, hogy* $\mathrm{sgn}(\pi) = \det(P_\pi)$*, ahol* P_π *a* π*-hez tartozó* $n \times n$*-es permutáció mátrix.*

15.B.Definíció. Az $(\mathrm{S}_n, \circ, \mathrm{id})$ szimmetrikus csoport

$$\mathrm{A}_n = \ker(\mathrm{sgn}) = \{\pi \in \mathrm{S}_n \mid \mathrm{sgn}(\pi) = 1\} = \{\pi \in \mathrm{S}_n \mid |\mathrm{inv}(\pi)| \text{ páros szám}\} \lhd S_n$$

normális részcsoportját nevezzük (az n-ed fokú) **alternáló csoportnak**.♡

15.5.Tétel. *Ha* $n \geq 5$*, akkor az* $(\mathrm{A}_n, \circ, \mathrm{id})$ *alternáló csoport egyszerű, azaz* A_n*-nek csak triviális normális részcsoportjai vannak:* $N \lhd \mathrm{A}_n \iff N = \{\mathrm{id}\}$ *vagy* $N = \mathrm{A}_n$*.*

Bizonyítás. Legyen $N \lhd \mathrm{A}_n$ olyan normális részcsoport, amelyre $N \neq \{\mathrm{id}\}$ és tekintsünk egy tetszőleges $\mathrm{id} \neq \pi \in N$ permutációt, amelynek a páronként diszjunkt ciklusokra való felbontása

$$\pi = (i_1, i_2, ..., i_m) \circ (j_1, j_2, ..., j_r) \circ ...$$

alakú, ahol $(i_1, i_2, ..., i_m)$ a leghosszabb ciklusok egyike és $(j_1, j_2, ..., j_r)$ a további ciklusok (amennyiben vannak ilyenek) valamelyike. Tehát $m \geq r$ és az alábbi esetek lehetségesek.

1. $m \geq 4$, azaz $\pi = (i_1, i_2, i_3, i_4, ..., i_m)$ vagy $\pi = (i_1, i_2, i_3, i_4, ..., i_m) \circ (j_1, j_2, ..., j_r) \circ ....$
   Most $(i_1, i_2, i_3) \in \mathrm{A}_n$ és $\pi^{-1} \in N \lhd \mathrm{A}_n$ miatt
   $$(i_1, i_4, i_2) = \pi \circ (i_1, i_2, i_3) \circ \pi^{-1} \circ (i_1, i_2, i_3)^{-1} \in N,$$
   ami azt jelenti, hogy N tartalmaz három hosszúságú ciklust.

2. $m = 3$ és $2 \leq r \leq 3$, azaz $\pi = (i_1, i_2, i_3) \circ (j_1, j_2, j_3) \circ ...$ vagy $\pi = (i_1, i_2, i_3) \circ (j_1, j_2) \circ ....$
   Most $(i_1, i_2, j_1) \in \mathrm{A}_n$ és $\pi^{-1} \in N \lhd \mathrm{A}_n$ miatt
   $$(i_1, j_1, i_3, j_2, i_2) = \pi \circ (i_1, i_2, j_1) \circ \pi^{-1} \circ (i_1, i_2, j_1)^{-1} \in N,$$
   ami azt jelenti, hogy N tartalmaz öt hosszúságú ciklust. Ha ezt az öt hosszúságú ciklust választjuk az előbbi 1.részben π-nek, akkor megkapjuk, hogy N ebben az esetben is tartalmaz három hosszúságú ciklust.

3. $m = 3$ és (i_1, i_2, i_3) az egyetlen ciklusa π-nek, azaz $\pi = (i_1, i_2, i_3)$.
   Legyen $1 \leq j_1 \leq n$ az i_1, i_2, i_3 elemektől különböző, ekkor $(i_1, i_2, j_1) \in \mathrm{A}_n$ és $\pi^{-1} \in N \lhd \mathrm{A}_n$ miatt
   $$(i_1, i_2) \circ (i_3, j_1) = \pi \circ (i_1, i_2, j_1) \circ \pi^{-1} \circ (i_1, i_2, j_1)^{-1} \in N,$$
   ami azt jelenti, hogy N tartalmazza két diszjunkt transzpozíció szorzatát.

4. $m = 2$ (ilyenkor π-nek mindenképpen van még további ciklusa, hiszen $\pi = (i_1, i_2)$ nem A_n-beli) és $r = 2$, azaz $\pi = (i_1, i_2) \circ (j_1, j_2) \circ ....$

   Most $(i_1, i_2, j_1) \in \mathrm{A}_n$ és $\pi^{-1} \in N \lhd \mathrm{A}_n$ miatt

$$(i_1, j_1) \circ (i_2, j_2) = \pi \circ (i_1, i_2, j_1) \circ \pi^{-1} \circ (i_1, i_2, j_1)^{-1} \in N,$$

   ami azt jelenti, hogy N ebben az esetben is tartalmazza két diszjunkt transzpozíció szorzatát.

Az előbbi felsorolást áttekintve azt látjuk, hogy N mindenképpen tartalmazza két diszjunkt transzpozíció szorzatát, azaz léteznek olyan egymástól különböző $a, b, c, d \in \{1, 2, ..., n\}$ elemek, amelyekre $(a, b) \circ (c, d) \in N$. Ha $a', b', c', d' \in \{1, 2, ..., n\}$ egymástól különböző elemek, akkor az

$$\alpha = \begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \end{pmatrix} \text{ és } \beta = \begin{pmatrix} a & b & c & d \\ b' & a' & c' & d' \end{pmatrix}$$

permutációk (amelyek a nem jelölt helyeken identikusan hatnak) valamelyike páros, azaz $\alpha \in \mathrm{A}_n$ vagy $\beta \in \mathrm{A}_n$. Mivel

$$(a', b') \circ (c', d') = \alpha \circ (a, b) \circ (c, d) \circ \alpha^{-1} = \beta \circ (a, b) \circ (c, d) \circ \beta^{-1},$$

ezért $N \lhd \mathrm{A}_n$ miatt $(a', b') \circ (c', d') \in N$. Tehát N tartalmazza bármely két diszjunkt transzpozíció szorzatát. Ha $a, b, c \in \{1, 2, ..., n\}$ egymástól különböznek, akkor $n \geq 5$ miatt találunk olyan további $x, y \in \{1, 2, ..., n\}$ elemeket, hogy a, b, c, x, y mind különböző. Mivel

$$(a, b) \circ (a, c) = (a, b) \circ (x, y) \circ (x, y) \circ (a, c)$$

és az eddigiek szerint $(a, b) \circ (x, y) \in N$, $(x, y) \circ (a, c) \in N$, ezért $(a, b) \circ (a, c) \in N$. Tehát bármely két (nem feltétlenül diszjunkt) transzpozíció szorzatát tartalmazza N.
A 15.3.Következmény szerint tetszőleges $\sigma \in \mathrm{S}_n$ permutáció megkapható transzpozíciók szorzataként, ha $\sigma \in \mathrm{A}_n$, akkor egy ilyen szorzatban páros sok transzpozíció szerepelhet. Mivel balról jobbra kettesével szorozva a transzpozíciókat minden esetben N-beli permutációt kapunk és N-beli permutációk szorzata is N-beli, ezért $\sigma \in N$. Tehát $N = \mathrm{A}_n$.

□□□

15.6.Következmény. *Ha $n \geq 5$, akkor az $(\mathrm{A}_n, \circ, \mathrm{id})$ alternáló és az $(\mathrm{S}_n, \circ, \mathrm{id})$ szimmetrikus csoport nem feloldható.*

15.7.Tétel. *Ha $q \geq 2$ prímszám és az $(\mathrm{S}_q, \circ, \mathrm{id})$ szimmetrikus csoport $T \leq \mathrm{S}_q$ részcsoportja tartalmaz transzpozíciót (azaz $(i_1, i_2) \in T$ valamilyen $1 \leq i_1 < i_2 \leq q$ egészekre) és **tranzitív** (tetszőleges $i, j \in \{1, 2, ..., q\}$ elemekhez található olyan $\tau \in T$ permutáció, amelyre $\tau(i) = j$), akkor $T = \mathrm{S}_q$.*

Bizonyítás. Az $i, j \in \{1, 2, ..., q\}$ elemekre az $i \sim j$ reláció pontosan akkor teljesüljön, ha az (i, j) tranzpozícióra $(i, j) \in T$ és itt az egyébként érthető $(i, i) = \mathrm{id}$ megállapodást tesszük. Az így értelmezett $\sim$ reláció ekvivalencia, hiszen $(i, i) = \mathrm{id} \in T$ miatt $i \sim i$, az $(i, j) = (j, i)$ egyenlőség szerint az $i \sim j$ teljesülése a $j \sim i$ teljesülését eredményezi. Ha $i \sim j$ és $j \sim k$ egy további $k \in \{1, 2, ..., q\}$ elemmel, akkor elegendő azt az esetet tekinteni, amikor i, j, k különbözőek. Most

$$(i, k) = (j, k) \circ (i, j) \circ (j, k)$$

és az $(i,j),(j,k) \in T$ tartalmazások miatt $(i,k) \in T$. Tehát $\sim$ valóban reflexív, szimmetrikus és tranzitív. Legyen

$$\{1,2,...,q\} = E_1 \cup E_2 \cup ... \cup E_m$$

az $\{1,2,...,q\}$ halmaznak a $\sim$ ekvivalencia szerinti páronként diszjunkt E_r, $1 \leq r \leq m$ ekvivalencia osztályokra való felbontása. Ha az E_r és E_s ($1 \leq s \leq m$, $r \neq s$) különböző osztályokból kiválasztunk egy $a \in E_r$ és egy $b \in E_s$ elemet, akkor létezik olyan $\tau \in T$ permutáció, amelyre $\tau(a) = b$. Ha $k \in E_r$ egy további elem, akkor $a \sim k$ miatt $(a,k) \in T$ és

$$(b, \tau(k)) = (\tau(a), \tau(k)) = \tau \circ (a,k) \circ \tau^{-1} \in T$$

miatt $b \sim \tau(k)$. Tehát $\tau(k) \in E_s$, ami azt jelenti, hogy τ egy olyan $E_r \longrightarrow E_s$ függvény, amely injektív (τ permutáció volt). A véges E_r és E_s halmazok számosságára így azt kapjuk, hogy $|E_r| \leq |E_s|$, ami az r és s szerepének a felcserélésével a fordított $|E_s| \leq |E_r|$ egyenlőtlenséget, illetve az $e = |E_r| = |E_s|$ egyenlőséget eredményezi. Az eddigiek szerint az $\{1,2,...,q\}$ elemeinek a számára a $q = me$ egyenlőséget kapjuk, ami a q prím tulajdonsága miatt az $m = 1$ egyenlőséghez vezet, hiszen $e = 1$ az $1 \leq i_1 < i_2 \leq q$ elemekre teljesülő $(i_1, i_2) \in T$ tartalmazás, illetve $i_1 \sim i_2$ reláció miatt nem lehetséges. Mivel csak egyetlen ekvivalencia osztály van, ezért tetszőleges $i,j \in \{1,2,...,q\}$ elemekre $i \sim j$, azaz $(i,j) \in T$ teljesül. A 15.3.Következmény szerint bármely $\pi \in \mathrm{S}_q$ permutáció megkapható transzpozíciók szorzataként, továbbá T minden transzpozíciót és azoknak tetszőleges szorzatát is tartalmazza, ezért $\pi \in T$. Végeredményben a kívánt $T = \mathrm{S}_q$ egyenlőséget igazoltuk.

□□□