

1. (Az 1. feladatlap 7. feladata és a 2. feladatlap 5. feladata.)
Legyen K tetszőleges test. Igazoljuk, hogy K egyszerű (csak triviális kongruenciarelációi vannak).

Megoldás. Megtalálható az 1. és 2. feladatlapok megoldásvázlataiban.

2. (A 2. feladatlap 9. feladata.) Igazoljuk, hogy minden véges félcsoportban van idempotens elem.

Megoldás. Legyen $\mathcal{A} = \langle A, \cdot \rangle$ véges félcsoport, legyen $a \in A$ tetszőleges. Mivel A véges, ezért az

$$\{a^n : n \in \mathbb{N}\} \subseteq A$$

halmaz is véges. Van tehát $i < j \in \mathbb{N}$ úgy, hogy $a^i = a^j$. Emiatt $a^{i+1} = a^{j+1}$, $a^{i+2} = a^{j+2}$, illetve általában tetszőleges $c \in \mathbb{N}$ -re és $k \geq i$ -re $a^k = a^{k+c(j-i)}$. Legyen $k = i(j-i)$. Ekkor $k \geq i$, ezért $a^k \in \{a^i, \dots, a^{j-1}\}$ és emiatt

$$a^k a^k = a^{k+k} = a^{k+i(j-i)} = a^k.$$

3. Legyen $\mathcal{G}$ csoport, $H, K, L \subseteq G$ komplexusok, $a, b \in G$. Igazoljuk, hogy

- (a) ha $H \leq G$, akkor $b \in aH \iff aH = bH$;

Megoldás. $\Rightarrow$: Azt látjuk be, hogy $bH \subseteq aH$ és $aH \subseteq bH$.

$$b \in aH \rightsquigarrow bH \subseteq aHH \rightsquigarrow bH \subseteq aH.$$

Ebből két módon is befejezhetjük az érvelést:

- tudjuk, hogy aH és bH is ekvivalenciaosztálya ϱ -nak, ezért $aH = bH$. Vagy
- $b \in aH \rightsquigarrow a^{-1}b \in H \rightsquigarrow (a^{-1}b)^{-1} \in H^{-1} = H \rightsquigarrow b^{-1}a \in H \rightsquigarrow a \in bH$, innen, mint előbb $aH \subseteq bH$.

$\Leftarrow$: $bH = aH \rightsquigarrow b = be \in bH = aH$.

- (b) $a(H \cup K) = aH \cup aK$ sőt, $L(H \cup K) = LH \cup LK$ és $(H \cup K)L = HL \cup KL$;

Megoldás. $u \in a(H \cup K) \Leftrightarrow$ van $h \in (H \cup K) : u = ah \Leftrightarrow u = ah \in aH \cup aK$. A többi rész hasonlóan.

- (c) $H(K \cap L) \subseteq HK \cap HL$ és $(K \cap L)H \subseteq KH \cap LH$;

Megoldás. $u \in H(K \cap L) \Leftrightarrow$ van $h \in H, k \in K \cap L : u = hk \rightsquigarrow hk \in HK$ és $hk \in HL$. A tartalmazás nem fordítható meg, mert ha $u \in HK \cap HL$, akkor csak annyit tudunk, hogy van $h_1, h_2 \in H, k \in K$ és $l \in L$, hogy $u = h_1k$ és $u = h_2l$. A többi rész hasonlóan.

- (d) $(HK)^{-1} = K^{-1}H^{-1}$.

Megoldás. Csoportokban is: szorzatot úgy invertálunk, hogy a tényezők inverzeit fordított sorrendben szorozzuk össze: $(ab)^{-1} = b^{-1}a^{-1}$. Itt a jobboldal tényleg inverze ab -nek, mert $b^{-1}a^{-1}ab = b^{-1}b = e$. Ezért

$$u \in (HK)^{-1} \Leftrightarrow u^{-1} \in HK \Leftrightarrow \text{van } h \in H, k \in K : u^{-1} = hk \Leftrightarrow u = (hk)^{-1} = k^{-1}h^{-1} \Leftrightarrow u \in K^{-1}H^{-1}.$$

4. Legyen D_3 -ban t az AC oldal felezőmerőlegesére való tükrözés. Hány eleme van $\langle t \rangle$ -nek? Soroljuk fel H összes baloldali és összes jobboldali mellékosztályait. Igaz-e, hogy mindegyik baloldali mellékosztály jobboldali mellékosztály is?

Megoldás. Mivel a tükrözést 2-szer megismételve az identitást kapjuk, a $\langle t \rangle$ ciklikus csoportnak 2 eleme van $\rightsquigarrow$ Lagrange tétele szerint 3 darab baloldali és 3 darab jobboldali mellékosztálya van. Előadáson volt, hogy D_3 elemeit azonosíthatjuk a szabályos ABC háromszög csúcsainak permutációival. Tehát D_3 egy elemét $\begin{pmatrix} A & B & C \\ x & y & z \end{pmatrix}$ alakban adhatjuk meg, mely azt a permutációt jelöli, amely A -t, B -t és C -t rendre x -re y -ra, z -re képezi (itt tehát x, y és z is az ABC háromszög páronként különböző, de meg nem határozott csúcsait jelöli).

- $\langle t \rangle$ 3 darab (külön-külön 2-elemű) baloldali mellékosztálya (f jelöli a középpont körüli, 120° -os pozitív irányú forgatást):

$$\begin{aligned}
e\langle t \rangle: ee &= \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}, & et &= \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}; \\
f\langle t \rangle: fe &= \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}, & ft &= \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}; \\
f^2\langle t \rangle: f^2e &= \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}, & f^2t &= \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}.
\end{aligned}$$

• $\langle t \rangle$ 3 darab (külön-külön 2-elemű) jobboldali mellékosztálya:

$$\begin{aligned}
\langle t \rangle e: ee &= \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}, & te &= \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}; \\
\langle t \rangle f: ef &= \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}, & tf &= \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}; \\
\langle t \rangle f^2: ef^2 &= \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}, & tf^2 &= \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}.
\end{aligned}$$

Mivel az első lista második sora nem egyezik meg a második lista egyik sorával sem, ezért az $f\langle t \rangle$ baloldali mellékosztály nem jobboldali mellékosztály.

5. Van-e $Sym([10])$ -nek 2026 elemű részcsoportja?

Megoldás. Lagrange tétele szerint, ha lenne ilyen részcsoport, akkor 2026 osztója lenne $|Sym([10])| = 10!$ -nak, de $10!$ minden prímtényezője kisebb, mint 10. Ugyanakkor 2026-nak az 1013 egy 10-nél nagyobb prímosztója $\sim 2026 \nmid 10! \sim$ nincs ilyen csoport.

6. Legyen $\mathcal{G} = \langle G, \cdot, {}^{-1}, e \rangle$ véges csoport. Igazoljuk, hogy $\mathcal{G}$ generálható legfeljebb $1 + \log_2(|G|)$ darab (sőt legfeljebb $\log_2(|G|)$ darab) elemével (azaz van olyan $X \subseteq G$, melyre $|X| \leq \log_2(|G|)$ és $\langle X \rangle = \mathcal{G}$).

Megoldás. Amíg lehet, megadjuk G elemeinek egy $\langle x_0, x_1, x_2, \dots \rangle$ sorozatát úgy, hogy minden k -ra a $G_k = \langle \{x_0, \dots, x_k\} \rangle$ csoportra $|G_k| \geq 2^k$. Legyen $x_0 = e$. Ha $x_0, \dots, x_{k-1}$ adott már, és $G_{k-1} \neq G$, akkor legyen $x_k \in G - G_{k-1}$ tetszőleges. Mivel G_{k-1} valódi részcsoportja G_k -nak, és Lagrange tétele miatt $|G_{k-1}|$ osztója $|G_k|$ -nak, ezért $|G_k| \geq 2|G_{k-1}| \geq 2 \cdot 2^{k-1} = 2^k$. A konstrukció akkor akad meg, ha $G_{k-1} = G$. Ekkor egyrészt $|G| = |G_{k-1}| \geq 2^{k-1}$ azaz $\log_2(|G|) \geq k-1$, másrészt G_{k-1} -et generálja a k -elemű $\{x_0, \dots, x_{k-1}\}$ halmaz. A generáló elemek közül $x_0 = e$ el is hagyható, mert e -t úgyis begenerálja a többi elem.

7. Legyen $m \in \mathbb{N}$. Emlékeztető:

- $R \subseteq \mathbb{N}$ egy RMR (redukált maradérendszer $(\text{mod } m)$), ha $|R| = \varphi(m)$ és R elemei páronként inkongruensek $(\text{mod } m)$ (ezért $\mathbb{N}$ minden eleme kongruens R valamelyik elemével $(\text{mod } m)$).
- Euler-Fermat-tétel: Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 (\text{mod } m)$.

(a) Igazoljuk, hogy ha R egy RMR $(\text{mod } m)$, akkor $V = \{a/(\text{mod } m) : a \in R\}$ részcsoportja $\mathbb{Z}_m$ szorzásra vett reduktumának (itt $\mathbb{Z}_m$ a $(\text{mod } m)$ maradékosztályok szokásos gyűjteménye).

Megoldás. V zárt a szorzásra, mert m -hez relatív prímek szorzata is relatív prím marad m -hez. Továbbá V zárt az inverzképzésre is: legyen $a \in R$; mivel $(a, m) = 1$, ezért (pl. a Bev. Alg.-1 Jegyzőkönyv 3.27. tétele szerint) az $ax \equiv 1 (\text{mod } m)$ megoldható, a megoldás (maradékosztálya) lesz $a/(\text{mod } m)$ inverze. Ez az inverz benne lesz V -ben (szintén a Bev. Alg.-1 Jegyzőkönyv 3.27. miatt).

Más módon is beláthatjuk, hogy V zárt az inverzképzésre. Tanultuk, hogy ha R elemeit egy m -hez relatív prím a -val szorozzuk, akkor aR is RMR marad (ez volt a Bev. Alg.-1 Jegyzőkönyv 3.40. tétele). ezért, ha $a \in R$, akkor aR is RMR , tehát van $b \in aR$ úgy, hogy $b \equiv 1 (\text{mod } m)$. Mivel $b \in aR$, ezért van $c \in R$, hogy $b = ac$. Ezekből $ac \equiv b (\text{mod } m)$ azaz $ac \equiv 1 (\text{mod } m) \leadsto c$ inverze a -nak. Emiatt V invertálásra is zárt.

(b) A csoportelméleti Lagrange-tételt használva adjunk rövid bizonyítást az Euler-Fermat-tételre.

Megoldás. Tegyük fel, hogy $(a, m) = 1$. Legyen az $a/(\text{mod } m) \in V$ elem rendje V -ben k .

V egységelemét e^V -vel jelölve egyrészt $e^V = 1 \pmod{m}$, másrészt Lagrange tétele szerint ekkor k osztója $|V| = \varphi(m)$ -nek, mondjuk $\varphi(m) = kn$. Ekkor viszont

$$a^{\varphi(m)} = a^{kn} = (a^k)^n = e^V = 1 \pmod{m}.$$

8. Adjunk meg egy olyan végtelen G csoportot, melynek minden végesen generált részcsoportja véges (ilyenkor azt is mondjuk, hogy G lokálisan véges).

1. Megoldás. Az ötlet az, hogy megadunk egy végtelen $\mathcal{G}$ csoportot, mely előáll véges részcsoportjainak növe uniójaként: azaz

$$G = \bigcup_{n \in \mathbb{N}} G_n$$

teljesül a véges G_n részcsoportokra. Ha sikerül ilyen szituációt találni, akkor készen vagyunk, mert ekkor, minden véges $X \subseteq G$ -hez van $n \in \mathbb{N}$, hogy $X \subseteq G_n$. Viszont ekkor $\langle X \rangle \subseteq G_n$, ami G_n végsősége miatt véges marad. Legyen

$$G = \{z \in \mathbb{C} : (\exists n \in \mathbb{N}) z \text{ egy } 2^n\text{-edik egységgyök}\}.$$

Világos, hogy G zárt a komplex számok szokásos szorzására és a reciprokképzésre, ezért ezekkel a műveletekkel G csoportot alkot. Végül minden $n \in \mathbb{N}$ -re legyen

$$G_n = \{z \in \mathbb{C} : z \text{ egy } 2^n\text{-edik egységgyök}\}.$$

Világos, hogy mindegyik G_n véges, és hogy $G = \bigcup_{n \in \mathbb{N}} G_n$.

2. Megoldás. Legyenek a G_n csoportok azok, mint az előbb (vagy lehetnek akár bármilyen, kevésbé konkrét n -edrendű ciklikus csoportok is). Legyen

$$H = \{s \in \prod_{n \in \mathbb{N}} G_n : \text{majdnem minden } n\text{-re } s(n) = 1\}.$$

Könnyű meggondolni, hogy H részcsoportja a $\prod_{n \in \mathbb{N}} G_n$ direktszorzatnak, H végtelen (mert a G_n -ek egyre nagyobbak). De ha $X \subseteq H$, akkor van $N \in \mathbb{N}$ úgy, hogy minden $s \in X$ -re és $n > N$ -re $s(n) = 1$. Ezért $\langle X \rangle$ minden eleme is 1 marad N felett (azaz, ha $s \in \langle X \rangle$ és $n > N$, akkor $s(n) = 1$). De ilyen fajta elemből csak véges sok van, mert mindegyik G_n véges).

9. Igazoljuk, hogy ciklikus csoportok minden részcsoportja is ciklikus.

Megoldás. Tegyük fel, hogy a ciklikus $\mathcal{G}$ csoportot generálja az $a \in G$ elem, és legyen $H \leq G$. Azt kell belátni, hogy H ciklikus. Mivel $H \subseteq G = \langle a \rangle$, ezért $\{k \in \mathbb{N} : a^k \in H\} \neq \emptyset$. Legyen

$$n = \min\{k \in \mathbb{N} : a^k \in H\}.$$

Állítjuk, hogy $\langle a^n \rangle = H$. Ebből $\langle a^n \rangle \subseteq H$ világos (mert $a^n \in H$). A fordított irányú tartalmazáshoz legyen $b \in H$ tetszőleges. Mivel $H \leq G$, ezért van olyan $m \in \mathbb{N}$, hogy $b = a^m$. Osszuk maradékosan m -et n -el $\leadsto$ vannak $q, r \in \mathbb{N}$, hogy $0 \leq r < n$ és $m = qn + r$. Ekkor

$$a^r = a^{qn+r-qn} = a^{m-qn} = a^m a^{-qn}$$

és a jobboldal mindkét tényezője H -beli $\leadsto a^r \in H$, ami n és r választása miatt csak az $r = 0$ esetben lehet. Ezért $n|m$ így $b = a^m = a^{qn} = (a^n)^q \in \langle a^n \rangle$. Mivel $b \in H$ tetszőleges volt, ezért $H \subseteq \langle a^n \rangle$. Az eddigiekből: $H = \langle a^n \rangle$, vagyis H ciklikus, mert a^n (egyetlen elem) generálja.

A feladatlap letölthető innen:

<https://users.renyi.hu/~sagi/algebra1-2026osz-letoltesek.html>



Az érdekes kitekintésre nem írok megoldásokat.