Алгебра 1
– вежбе –

Славко Моцоња

Садржај

Полугрупе, моноиди, групе

1. Доказати да је алгебра $\mathbb{A}$ полугрупа. Испитати да ли се алгебра $\mathbb{A}$ може додефинисати до моноида и групе.

1. Нека је R скуп реалних бројева и $f : \mathrm{R} \longrightarrow \mathrm{R}$ произвољна бијекција. $\mathbb{A} = (\mathrm{R}, \star)$, где је $\star$ дефинисана са:
$$a \star b = f^{-1}(f(a) + f(b)).$$
2. Нека је $S \neq \emptyset$ произвољан скуп. $\mathbb{A} = (\mathcal{P}(S), \triangle)$.
3. Нека је $S \neq \emptyset$ произвољан скуп. $\mathbb{A} = (\mathcal{P}(S), \cap)$.
4. Нека је $M = \{A = (a_{ij}) \mid A \in \mathrm{M}_n(\mathbb{C}), \sum_{j=1}^{n} a_{ij} = 1, \text{ за све } 1 \leq i \leq n\}$. $\mathbb{A} = (M, \cdot)$. (M су све квадратне матрице реда n над комплексним бројевима код којих је збир елемената у свакој врсти једнак 1.)

Решење.

1. Јасно је да је $\star$ операција на R. Доказујемо асоцијативност.
$$\begin{aligned} a \star (b \star c) &= f^{-1}[f(a) + f(b \star c)] \\ &= f^{-1}[f(a) + f(f^{-1}(f(b) + f(c)))] \\ &= f^{-1}[f(a) + f(b) + f(c)] \\ &= f^{-1}[f(f^{-1}(f(a) + f(b))) + f(c)] \\ &= f^{-1}[f(a \star b) + f(c)] \\ &= (a \star b) \star c. \end{aligned}$$
Дакле, $\mathbb{A}$ јесте полугрупа.

Дефинишимо $e = f^{-1}(0)$. Тада је

$$\begin{aligned} a \star e &= f^{-1}[f(a) + f(e)] \\ &= f^{-1}[f(a) + f(f^{-1}(0))] \\ &= f^{-1}[f(a) + 0] \\ &= f^{-1}[f(a)] \\ &= a. \end{aligned}$$

Слично је $e \star a = e$, па је $(\mathrm{R}, \star, e)$ моноид.

Ако дефинишемо $a' = f^{-1}(-f(a))$, имамо:

$$\begin{aligned} a \star a' &= f^{-1}[f(a) + f(a')] \\ &= f^{-1}[f(a) + f(f^{-1}(-f(a)))] \\ &= f^{-1}[f(a) - f(a)] \\ &= f^{-1}[0] \\ &= e. \end{aligned}$$

Слично је $a' \star a = e$, па је $(\mathrm{R}, \star, ', e)$ група. Слично претходном рачуну, можемо доказати да је $\star$ комутативна операција, па је $(\mathrm{R}, \star, ', e)$ Абелова група.

Приметимо и следеће: f је изоморфизам $(\mathrm{R}, \star, ', e) \longrightarrow (R, +, -, 0)$. f је бијекција по услову задатка, па је довољно само доказати да је хомоморфизам. $f(e) = f(f^{-1}(0)) = 0$; $f(a') = f(f^{-1}(-f(a))) = -f(a)$; $f(a \star b) = f(f^{-1}(f(a) + f(b))) = f(a) + f(b)$. Дакле, f јесте хомоморфизам.

2. $\triangle$ је очигледно операција на скупу $\mathcal{P}(S)$, па треба проверити да је асоцијативна, тј. треба доказати скуповни идентитет $A \triangle (B \triangle C) = (A \triangle B) \triangle C$. Довољно је проверити да је $p \veebar (q \veebar r) \Leftrightarrow (p \veebar q) \veebar r$ таутологија, што радимо у следећој таблици:

p	q	r	p	$\veebar$	$(q$	$\veebar$	$r)$	$\Leftrightarrow$	$(p$	$\veebar$	$q)$	$\veebar$	r
0	0	0	0		0			1		0		0	
0	0	1	1		1			1		0		1	
0	1	0	1		1			1		1		1	
0	1	1	0		0			1		1		0	
1	0	0	1		0			1		1		1	
1	0	1	0		1			1		1		0	
1	1	0	0		1			1		0		0	
1	1	1	1		0			1		0		1	

Приметимо да је $A \triangle \emptyset = A = \emptyset \triangle A$, одакле је $(\mathcal{P}(S), \triangle, \emptyset)$ моноид. Такође, ако узмемо $A' = A$, имамо да је $A \triangle A' = A \triangle A = \emptyset = A' \triangle A$. Дакле, $(\mathcal{P}(S), \triangle, ', \emptyset)$ је Абелова група (комутативност је очигледна).

3. $(\mathcal{P}(S), \cap)$ јесте полугрупа, јер је јасно да је $\cap$ операција на $\mathcal{P}(S)$, која је асоцијативна. И више од тога, како је $A \cap S = A = S \cap A$, то је S неутрал за ову операцију, па је $(\mathcal{P}(S), \cap, S)$ моноид. Но, овај моноид се не може додефинисати до групе. Заиста, ако би A' био инверз од A, тада би имали $S = A \cap A' \subseteq A$, што је немогуће.

4. Познато је да је множење матрица асоцијативно, па ће $(M, \cdot)$ бити полугрупа ако је $\cdot$ операција на скупу M. Нека $A = (a_{ij}), B = (b_{ij}) \in M$, тј. $\sum_{j=1}^{n} a_{ij} = 1, \sum_{j=1}^{n} b_{ij} = 1$, за све $1 \leq i \leq n$. Нека је $C = AB$. Доказујемо да $C \in M$. Запишимо $C = (c_{ij})$, тада је

$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$. Треба да докажемо да је $\sum_{j=1}^{n} c_{ij} = 1$.

$$\begin{aligned}
\sum_{j=1}^{n} c_{ij} &= \sum_{j=1}^{n}\sum_{k=1}^{n} a_{ik}b_{kj} \\
&= a_{i1}b_{11} + a_{i2}b_{21} + \ldots + a_{in}b_{n1} \\
&+ a_{i1}b_{12} + a_{i2}b_{22} + \ldots + a_{in}b_{n2} \\
&+ \ldots \\
&+ a_{i1}b_{1n} + a_{i2}b_{2n} + \ldots + a_{in}b_{nn} \\
&= \sum_{k=1}^{n}\sum_{j=1}^{n} a_{ik}b_{kj} \\
&= \sum_{k=1}^{n} a_{ik} \sum_{j=1}^{n} b_{kj} \\
&= \sum_{k=1}^{n} a_{ik} \\
&= 1.
\end{aligned}$$

Дакле, $(M, \cdot)$ јесте полугрупа.

Приметите да јединична матрица E припада M. Одатле следи да $(M, \cdot, E)$ јесте моноид. Али такође матрица у којој се у првој колони налазе јединице, а на свим осталим местима нуле припада M. Та матрица очигледно нема инверз, па се $(M, \cdot, E)$ не може додефинисати до групе.

□

2. Доказати да се на скупу природних бројева N може дефинисати структура групе која је изоморфна са $(\mathrm{Q}, +, -, 0)$ (Q је скуп рационалних бројева).

Решење. Како је Q пребројив скуп, постоји бијекција $f : \mathrm{N} \longrightarrow \mathrm{Q}$. Дефинишимо операције $\oplus, \ominus$ и уочимо елемент e дефинисане са: $a \oplus b = f^{-1}(f(a) + f(b))$, $\ominus a = f^{-1}(-f(a))$, $e = f^{-1}(0)$. Сада можемо да докажемо, као у првом делу претходног задатка, да је $(\mathrm{N}, \oplus, \ominus, e)$ група изоморфна $(\mathrm{Q}, +, -, 0)$. □

3. Нека је $S \neq \emptyset$ произвољан скуп, $J(S) = \{f \mid f : S \xrightarrow{1\text{-}1} S\}$ и $N(S) = \{f \mid f : S \xrightarrow{\text{на}} S\}$. Алгебре $\mathbb{J}(S) = (J(S), \circ, \mathrm{id}_S)$ и $\mathbb{N}(S) = (N(S), \circ, \mathrm{id}_S)$ су очигледно моноиди. Доказати да у $\mathbb{J}(S)$ важи закон левог скраћивања, а у $\mathbb{N}(S)$ закон десног скраћивања.

Решење. Нека су $f, g, h \in J(S)$, такви да $f \circ g = f \circ h$. Треба да докажемо да је $g = h$. Узмимо произвољно $x \in S$. Тада је $f \circ g(x) = f \circ h(x)$, тј. $f(g(x)) = f(h(x))$. Како је f 1-1, тада је $g(x) = h(x)$. Како је x било произвољно, то је $g = h$.

Нека су сада $f, g, h \in N(S)$, такви да $f \circ h = g \circ h$. Треба да докажемо да је $f = g$. Узмимо произвољно $y \in S$. Како је h на, то постоји x тако да је $h(x) = y$. Имамо да је $f \circ h(x) = g \circ h(x)$, тј. $f(h(x)) = g(h(x))$. Одатле је $f(y) = g(y)$, па како је y било произвољно, то је $f = g$. □

4. Нека је $\mathbb{G} = (G, \star)$ комутативан групоид који задовољава закон $(x \star y) \star z = (z \star x) \star y$. Доказати да је $\mathbb{G}$ полугрупа.

Решење. Примењујући два пута дати закон и на крају комутативност имамо: $(x \star y) \star z = (z \star x) \star y = (y \star z) \star x = x \star (y \star z)$, што је и требало доказати. □

5. Нека је $(G, \cdot)$ коначна полугрупа.

1. Доказати да постоји елемент $b \in G$ такав да $b^2 = b$.

2. Доказати да за свако $k \geq 2$ постоји елемент $b \in G$ такав да $b^k = b$.

Решење. Нека је a произвољан елемент од G. Како је G коначан у низу елемената из G: $a, a^2, a^4, \cdot, a^{2^n}, \cdot$, постоје два a^{2^m} и a^{2^n}, таква да $m < n$ и $a^{2^m} = a^{2^n}$.

Тада за све $x \geq 1$ важи: $a^x a^{2^m} = a^x a^{2^n}$, тј. $a^{x+2^m} = a^{x+2^n}$. Како једначина $2(x + 2^m) = x + 2^n$ има целобројно решење, $x = 2^n - 2^{m+1}$, узимајући $b = a^{x+2^m}$, добијамо $b^2 = a^{2(x+2^m)} = a^{x+2^n} = a^{x+2^m} = b$.

Како је $b^2 = b$, тада је и $b^k = b$, што решава други део задатка. □

6. Нека је $(G, \star)$ полугрупа. Доказати да постоји скуп S и подскуп функција $F \subseteq S^S$ такав да је $(G, \star) \cong (F, \circ)$.

Решење. Нека је e неки елемент који не припада G. Узмимо $S = G \cup \{e\}$. Дефинишимо операцију $\sharp$ на S са:

$$a \sharp b = \begin{cases} a \star b & , a, b \in G \\ a & , b = e \\ b & , a = e \end{cases}$$

Скоро је очигледно да је $(S, \sharp)$ полугрупа у којој је e неутрални елемент. Означимо са $f_a : S \longrightarrow S$, $a \in S$, леву транслацију $f_a : x \mapsto a \sharp x$. Нека је $F = \{f_a \mid a \in G\}$ и $F' = F \cup \{f_e\}$. Приметимо да је $f_a \circ f_b(x) = f_a(f_b(x)) = f_a(b \sharp x) = a \sharp b \sharp x = f_{a \sharp b}(x)$, одакле је $f_a \circ f_b = f_{a \sharp b}$. Дакле, $(F', \circ)$ је групоид, заправо полугрупа, јер композиција функција јесте асоцијативна. Ако $a, b \in G$, тада $a \sharp b = a \star b \in G$, па је и $(F, \circ)$ полугрупа.

Доказујемо да је $\phi : G \longrightarrow F$, дато са $\phi(a) = f_a$ изоморфизам полугрупа $(G, \star)$ и $(F, \circ)$. Како се у f_a, за $a \in G$, слика a, то је ϕ на пресликавања. Ако је $f_a = f_b$, за $a, b \in G$, тада је $f_a(e) = f_b(e)$, тј. $a \sharp e = b \sharp e$, одакле $a = b$, што доказује да је ϕ 1-1.

Коначно, за $a, b \in G$, $\phi(a \star b) = f_{a \star b} = f_{a \sharp b} = f_a \circ f_b$ (сто смо већ доказали), па је ϕ и хомоморифзам. □

7. Нека је $(A, \mathcal{F}, \mathcal{C})$ алгебра, и нека је $\mathcal{L}$ непразан ланац подалгебри од A ($\mathcal{L}$ је скуп подалгебри од A, од којих су сваке две упоредиве у односу на инклузију). Доказати да је $B = \bigcup \mathcal{L}$ подалгебра од A. Такође, доказати да: ако неки закон важи у свим алгебрама из ланца $\mathcal{L}$, тада тај закон важи и у B.

Решење. Ако је $c \in \mathcal{C}$, тада је c константа садржана у свакој алгебри из $\mathcal{L}$, па је садржана и у њиховој унији B.

Ако је $f \in \mathcal{F}$ операција арности n. Доказујемо да је B затворена за f. Нека су $b_1, b_2, \ldots, b_n$ елементи из B. Како је B унија алгебри из $\mathcal{L}$, то $b_i \in H_i$, где све $H_i \in \mathcal{L}$. Како је $\mathcal{L}$ ланац, то међу $H_1, H_2, \ldots, H_n$ постоји највећи; означимо га са H. Тада $b_1, \ldots, b_n \in H$, па како је и H подалгебра од A, то $f(b_1, \ldots, b_n) \in H$. Како је H садржан у B, то $f(b_1, \ldots, b_n) \in B$.

Дакле, B јесте подалгебра од A.

Претпоставимо да закон $u(x_1, \ldots, x_n) = v(x_1, \ldots, x_n)$ (записан на одговарајућем језику) важи у свим алгебрама ланца $\mathcal{L}$. Треба да докажемо да за све $b_1, \ldots, b_n \in B$ важи $u(b_1, \ldots, b_n) = v(b_1, \ldots, b_n)$.

Када узмемо $b_1, \ldots, b_n \in B$, поново можемо да нађемо $H \in \mathcal{L}$ тако да $b_1, \ldots, b_n \in H$. Како закон важи у H, то је заиста $u(b_1, \ldots, b_n) = v(b_1, \ldots, b_n)$. □

8. Нека је $(G, \cdot)$ групоид који садржи неутрални елемент e.

1. Доказати да у G постоји максималан комутативан подгрупоид (максималан у односу на инклузију).

2. Доказати да у G постоји максималан подгрупоид који је група.

Решење. Посматрајмо фамилију $\mathcal{F} = \{H \mid H$ је подгрупоид који задовољава комутативност$\}$ и парцијално уређење $(\mathcal{F}, \subseteq)$. Максималан комутативан подгрупоид је управо максималан елемент уоченог парцијалног уређења. Приметимо да је $\mathcal{F}$ непразна фамилија, јер је $\{e\} \in \mathcal{F}$.

Ако је $\mathcal{L}$ непразан ланац, тада је (према претходном задатку) $\bigcup \mathcal{L}$ подгрупоид од G који задовољава комутативност. Дакле, $\bigcup \mathcal{L}$ је горње ограничење за ланац $\mathcal{L}$ у $\mathcal{F}$. Према Цорновој леми, $\mathcal{F}$ садржи максималан елемент у односу на инклузију.

У другом делу посматрајмо фамилију $\mathcal{F} = \{H \mid H$ је подгрупоид који је група са неутралом $e\}$. $\{e\} \in \mathcal{F}$, па је и овде $\mathcal{F}$ непразна.

Поново уочавајући непразан ланац $\mathcal{L}$, $\bigcup \mathcal{L}$ ће бити горње ограничење за $\mathcal{L}$ у $\mathcal{F}$. Према Цорновој леми налазимо максималан подгрупоид M од G који је група са неутралом e.

Докажимо и да је M максималан подгрупоид од G који је група. Ако је $M \subseteq N$ и N је подгрупоид који је група, тада, како $e \in N$ (јер $e \in M$) и како је e неутрал на G, закључујемо да је e неутрал и од N, па $N \in \mathcal{F}$, одакле $M = N$. □

9. Нека је $\mathbb{G} = (G, \cdot, ^{-1}, e)$ група. Доказати да важи:

1. закон левог и десног скраћивања;

2. неутрал e је јединствен;

3. инверз елемента x, x^{-1}, је јединствен.

Решење. Ако је $xy = xz$, после множења са x^{-1} са леве стране, добијамо $x^{-1}xy = x^{-1}xz$, одакле $ey = ez$, тј. $y = z$. Дакле, важи закон левог скраћивања.

Ако је $xz = yz$, после множења са z^{-1} са десне стране, добијамо $xzz^{-1} = yzz^{-1}$, одакле $xe = ye$, тј. $x = y$. Дакле, важи закон десног скраћивања.

Претпоставимо да је e' још један неутрал. Тада је $e = ee' = e'$. Прва једнакост важи зато што је e' неутралан, а друга зато што је e неутрал.

Претпоставимо да је x' још један инверз елемента x. $x' = x'e = x'xx^{-1} = ex^{-1} = x - 1$. Друга једнакост вази јер је x^{-1} инверз елемента x, а трећа једнакост зато што је x' инверз елемента x. □

10. Нека је $\mathbb{G} = (G, \star, ^{-1}, e)$ алгебра која задовољава законе асоцијативности, десног неутрала и десног инверза. Доказати да је $\mathbb{G}$ група.

Решење. Нека је $x \star e = x$ и $x \star x^{-1} = e$, за све x. Тада је $e = \underline{x^{-1}} \star (x^{-1})^{-1} = x^{-1} \star \underline{e} \star (x^{-1})^{-1} = x^{-1} \star x \star \underline{x^{-1} \star (x^{-1})^{-1}} = x^{-1} \star \underline{x \star e} = x^{-1} \star x$. Користећи ово сада имамо и $\underline{e} \star x = x \star \underline{x^{-1} \star x} = x \star e = x$. Дакле, важе и закон левог неутрала и левог инверза, па је $\mathbb{G}$ група. □

11. Нека је $(G, \cdot)$ полугрупа у којој за све $a, b \in G$ једначине $ax = b$ и $xa = b$ имају решење. Доказати да се $(G, \cdot)$ може додефинисати до групе.

Решење. Фиксирајмо елемент a. Према услову задатка једначина $x = a$ има решење; означимо га са e. Дакле, $ae = a$, тј. e је неутралан за множење a са десне стране.

Тврдимо да је e десни неутрал. Нека је t произвољан елемент; докажимо да је $te = t$. Према услову задатка једначина $xa = t$ има решење, означимо га са s; дакле $sa = t$. Тада је $te = s\underline{ae} = sa = t$, што је и требало да докажемо. Дакле, e јесте десни неутрал.

За произвољно t, једначина $tx = e$ има решење. Означимо неко решење те једначине са t^{-1}. Тада је t^{-1} десни инверз од t.

Како имамо дефинисан десни неутрал и десни инверз, на $(G, \cdot)$ се може проширити до групе. □

12. Нека је $(G, \cdot)$ коначна полугрупа у којој важе закони скраћивања. Доказати да се $(G, \cdot)$ може проширити до групе.

Решење. За свако a посматрајмо пресликавање $f_a : x \mapsto ax$. f_a је 1-1 пресликавање, јер из $f_a(x) = f_a(y)$, имамо $ax = ay$, тј. $x = y$, јер је дозвољено лево скраћивање.

Како је f_a 1-1, и како је G коначан скуп, то је f_a и на пресликавање, за све a.

Фиксирајмо сада неко a из G. Како је f_a на, то постоји неки елемент, означимо га са e, такав да је $f_a(e) = a$, тј. $ae = a$. Дакле, e је неутралан за множење са a са десне стране.

Докажимо да је e леви неутрал. Множећи $ae = a$ са десне стране произвољним елементом t, добијамо $aet = at$. Како је дозвољено лево скраћивање, добијамо $et = t$. Дакле, e је заиста леви неутрал у G. Када $et = t$ помножимо са t са леве стране, добијамо $tet = tt$, па како је дозвољено скраћивање и са десне стране, имамо $te = t$. Дакле, e је и десни неутрал.

Коначно, за произвољно t, како је f_t на пресликавање, постоји елемент, означимо га са t^{-1}, такав да је $f_t(t^{-1}) = e$, тј. $tt^{-1} = e$. t^{-1} је десни инверз за t.

Како се у G може дефинисати неутрал и десни инверз, то се $(G, \cdot)$ може проширити до групе. □

13. Нека је $(G, \cdot)$ коначна полугрупа у којој важи следећи закон: $ax = xb \implies a = b$. Доказати да се $(G, \cdot)$ може проширити до Абелове групе.

Решење. Уочимо да из асоцијативности имамо: $a(ba) = (ab)a$, па примењујући дати закон, закључујемо $ba = ab$, тј. закључујемо да важи комутативност.

Уочимо сада да из $ab = ac$, по комутативности следи $ab = ca$, па по уоченом закону је $b = c$. Дакле, важи закон левог скраћивања. Слично важи закон десног скраћивања, па како је G коначна полугрупа на њој се може додефинисати структура групе. □

14. Испитати да ли су следеће структуре $(G, \cdot)$ групе.

1. $G = \{a + bi \mid a, b \in \mathrm{R},\ a^2 + b^2 = 1\}$ и $\cdot$ је множење комплексних бројева.
2. $G = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathrm{Q},\ a^2 + b^2 + c^2 \neq 0\}$ и $\cdot$ је множење реалних бројева.
3. $G = \{(a, b) \mid a, b \in \mathrm{Q},\ a \neq 0\}$ и $(a, b) \cdot (c, d) = (ac, bc + c + d)$.
4. Нека је $n \geq 2$. $G = \{M_a \mid a \in \mathrm{Q},\ a \neq 0\}$, где је M_a матрица:
$$M_a = \begin{pmatrix} a & a & \cdots & a \\ a & a & \cdots & a \\ \vdots & \vdots & \ddots & \vdots \\ a & a & \cdots & a \end{pmatrix}_{n \times n}$$
и $\cdot$ је множење матрица.
5. $G = \left\{ x \mapsto \dfrac{ax + b}{cx + d} \middle| a, b, c, d \in \mathrm{Q},\ ad - bc = 1 \right\}$ и $\cdot$ је композиција функција.

Решење.

1. Нека $a+bi, c+di \in G$, тј. $a^2+b^2 = c^2+d^2 = 1$. Тада је $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$, а $(ac-bd)^2+(ad+bc)^2 = a^2c^2-2abcd+b^2d^2+a^2d^2+2abcd+b^2c^2 = a^2c^2+b^2d^2+a^2d^2+b^2c^2 = (a^2+b^2)(x^2+d^2) = 1\cdot 1 = 1$, одакле следи да $(a+bi)(c+di) \in G$. Дакле, G је затворен за $\cdot$.

   Асоцијативност множења комплексних бројева је позната. Приметимо да је $1 = 1+0i \in G$, па је 1 неутрал у G.

   Такође, приметимо за $a+bi \in G$, $(a+bi)(a-bi) = a^2+b^2 = 1$, одакле следи да је $a-bi \in G$ инверз елемнта $a+bi$. Дакле, G јесте група.

2. Докажимо да је $a+b\sqrt[3]{2}+c\sqrt[3]{4} = 0$ акко $a = b = c = 0$. Смер $\Rightarrow$ је очигледан. За смер $\Leftarrow$, претпоставимо да је $a+b\sqrt[3]{2}+c\sqrt[3]{4} = 0$ и претпоставимо за почетак да $a, b, c \in \mathrm{Z}$. Тада је $b\sqrt[3]{2}+c\sqrt[3]{4} = -a$. После дизања на трећи степен добијамо: $b^3 2 + 3b^2c\sqrt[3]{4}\sqrt[3]{4} + 3bc^2\sqrt[3]{2}\sqrt[3]{16} + c^3 4 = -a^3$, тј. $b^3 2 + 6b^2c\sqrt[3]{2} + 6bc^2\sqrt[3]{4} + c^3 4 = -a^3$, што можемо записати: $b^3 2 + 6bc(b\sqrt[3]{2}+c\sqrt[3]{4}) + c^3 4 = -a^3$. Ако се сетимо да је $b\sqrt[3]{2}+c\sqrt[3]{4} = -a^3$, добијамо $b^3 2 - 6abc + c^3 4 = -a^3$, или $a^3+2b^3+4c^3-6abc = 0$.

   Тврдимо да $2^n \mid a, b, c$, за све $n \geq 1$. Ово можемо доказати индукцијом по n. За $n = 1$, доказујемо да $2 \mid a, b, c$. Како видимо да су сви сабирци сем a^3 дељиви са 2, то мора и a^3 бити дељив са 2, тј. a мора бити дељив са 2, јер је 2 прост број. Запишимо $a = 2a'$ и заменом у једнакост добијамо: $8a'^3+2b^3+4c^3-12a'bc = 0$, која после дељења са 2 постаје: $4a'^3+b^3+2c^3-6a'bc = 0$. Сада видимо да $2 \mid b^3$, тј. $2 \mid b$. Ако запишемо $b = 2b'$, једнакост постаје: $4a'^3+8b'^3+2c^3-12a'b'c = 0$, тј. $2a'^3+4b'^3+c^3-6a'b'c = 0$. Коначно видимо да $2 \mid c^3$, тј. $2 \mid c$. Тиме је доказана база индукције.

   Претпоставимо да $2^n \mid a, b, c$ и докажимо $2^{n+1} \mid a, b, c$. Запишимо $a = 2^n a_0, b = a^n b_0, c = 2^n c_0$. Заменом у једнакост имамо: $2^{3n}a_0^3 + 2^{3n}2b_0^3 + 2^{3n}4c_0^3 - 2^{3n}6a_0b_0c_0 = 0$, одакле, после дељења са 2^{3n} добијамо: $a_0^3+2b_0^3+4c_0^3-6a_0b_0c_0 = 0$. Сада доказана база повлачи $2 \mid a_0, b_0, c_0$, па $2^{n+1} \mid a, b, c$.

   Доказано тврђење повлачи $a = b = c = 0$.

   Ако је сада $a, b, c \in \mathrm{Q}$, запишимо $a = a'/a'', b = b'/b'', c = c'/c''$, где $a'', b'', c'' \neq 0$. После множења $a+b\sqrt[3]{2}+c\sqrt[3]{4} = 0$ са $a''b''c''$ добијамо $a'b''c'' + a''b'c''\sqrt[3]{2} + a''b''c'\sqrt[3]{4} = 0$, где $a'b''c'', a''b'c'', a''b''c' \in \mathrm{Z}$. Према већ доказаном $a'b''c'' = a''b'c'' = a''b''c' = 0$, одакле следи $a' = b' = c' = 0$, па и $a = b = c = 0$.

   Дакле, за рационалне бројеве a, b, c, $a+b\sqrt[3]{2}+c\sqrt[3]{4} \in G$ акко $a^2+b^2+c^2 \neq 0$ акко a, b, c нису истовремено једнаки 0 акко $a+b\sqrt[3]{2}+c\sqrt[3]{4} \neq 0$.

   НАПОМЕНА. Приметите да одавде важи да је $a+b\sqrt[3]{2}+c\sqrt[3]{4} = a'+b'\sqrt[3]{2}+c'\sqrt[3]{4}$, за $a, b, c, a', b', c' \in \mathrm{Q}$, акко $(a-a')+(b-b')\sqrt[3]{2}+(c-c')\sqrt[3]{4} = 0$, тј. акко $a = a'$, $b = b'$ и $c = c'$. Дакле, Представљање елемента из G је јединствено у облику $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, за a, b, c. Можемо рећи да су $1, \sqrt[3]{2}, \sqrt[3]{4}$ линеарно независни над Q.

   Нека $a+b\sqrt[3]{2}+c\sqrt[3]{4}, a'+b'\sqrt[3]{2}+c'\sqrt[3]{4} \in G$. Тада је $(a+b\sqrt[3]{2}+c\sqrt[3]{4})(a'+b'\sqrt[3]{2}+c'\sqrt[3]{4}) = (aa'+2bc'+2cb')+(ab'+ba'+2cc')\sqrt[3]{2}+(ac'+bb'+ca')\sqrt[3]{4}$. Како је производ два ненула реална броја, ненула реалан број, то је G затворено за множење. Множење реалних бројева је свакако асоцијативно, и G садржи неутрал за множење, што је 1. Једино остаје питање да ли је затворено за инверз?

   Посматрајмо једначину по a', b', c', у којој су a, b, c параметри (такви да је бар један од њих различит од нуле), $(a+b\sqrt[3]{2}+c\sqrt[3]{4})(a'+b'\sqrt[3]{2}+c'\sqrt[3]{4}) = 1$, тј. $(aa'+2bc'+2cb')+(ab'+ba'+2cc')\sqrt[3]{2}+(ac'+bb'+ca')\sqrt[3]{4} = 1$. Према горњој напомени ова једначина има решења (и оно је јединствено) акко систем $aa'+2bc'+2cb' = 1, ab'+ba'+2cc' = 0, ac'+bb'+ca' = 0$ има решење. Детерминанта овог система је једнака $\begin{vmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{vmatrix} = a^3+2b^3+4c^3-6abc$, која је

различита од 0 како смо горе видели, јер нису сви a, b, c једнаки нула. Дакле, овај систем има решење (и то решење су очигледно рационални бројеви), па инверз од $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ припада G.

3. Докажимо затвореност дате структуре. Нека $(a, b), (c, d) \in G$, тада је $(a, b)(c, d) = (ac, bc + c + d)$, где су обе координате резултата рационалне и $ac \neq 0$, јер $a, c \neq 0$. Даље показујемо асоцијативност: $(a, b)[(c, d)(e, f)] = (a, b)(ce, de + e + f) = (ace, bce + ce + de + e + f) = (ac, bc + c + d)(e, f) = [(a, b)(c, d)](e, f)$.

   Неутрал треба за произвољан $(a, b) \in G$ да задовољава: $(a, b)(x, y) = (a, b)$, тј. $(ax, bx + x + y) = (a, b)$, одакле је $x = 1$ и $y = -1$. Како $(1, -1) \in G$, то је он неутрал у G.

   Инверз елемента $(a, b) \in G$, (x, y), треба да задовољава: $(a, b)(x, y) = (1, -1)$, тј. $(ax, bx + x + y) = (1, -1)$. Решавајући добијамо $x = 1/a$, $y = -(1 + a + b)/a$. Они су дефинисани, јер је $a \neq 0$, и одговарајући пар припада G, па закључујемо да је $(a, b)^{-1} = (1/a, -(1+a+b)/a)$.

4. Приметите да је $M_a = M_b$ акко $a = b$, и да је $M_a M_b = M_{nab}$.

   Ако $M_a, M_b \in G$, тј. $a, b \in \mathbb{Q}$ и $a, b \neq 0$, тада и $nab \in \mathbb{Q}$ и $nab \neq 0$, па $M_a M_b \in G$. Познато је да је множење матрица асоцијативно. Приметите и да је множење матрица у G чак и комутативно.

   Испитајмо да ли G има неутрал. Решавамо једначину $M_a M_x = M_a$, тј. $M_{nax} = M_a$, што је еквивалентно са $x = 1/n$. Како $M_{1/n} \in G$, то је неутрал у G.

   Коначно, испитајмо да ли M_a има инверз у G. Решавамо једначину $M_a M_x = M_{1/n}$, одакле је $M_{nax} = M_{1/n}$, па добијамо $x = 1/n^2 a$. Дакле, $M_a^{-1} = M_{1/n^2 a}$.

5. Нека $f, g \in G$, где $f : x \mapsto \frac{ax+b}{cx+d}$ и $g : x \mapsto \frac{a'x+b'}{c'x+d'}$ и $ad - bc = a'd' - b'c' = 1$. Тада $g \circ f : x \mapsto \dfrac{a'\frac{ax+b}{cx+d} + b'}{c'\frac{ax+b}{cx+d} + d'} = \dfrac{\frac{(aa'+cb')x+(ba'+db')}{cx+d}}{\frac{(ac'+cd')x+(bc'+dd')}{cx+d}} = \dfrac{(aa'+cb')x + (ba'+db')}{(ac'+cd')x + (bc'+dd')}$ и $(aa' + cb')(bc' + dd') - (ba' + db')(ac' + cd') = aba'c' + ada'd' + bcb'c' + cdb'd' - aba'c' - bca'd' - adb'c' - cdb'd' = ada'd' + bcb'c' - bca'd' - adb'c' = (ad - bc)(a'd' - b'c') = 1 \cdot 1 = 1$, одакле $g \circ f \in G$. Познато је да је композиција функција асоцијативна.

   Приметите да је $\mathrm{id} : x \mapsto \frac{1x+0}{0x+1}$, па $\mathrm{id} \in G$, и очигледно је id неутрал у G.

   Израчунали смо да за $f, g \in G$, где $f : x \mapsto \frac{ax+b}{cx+d}$ и $g : x \mapsto \frac{a'x+b'}{c'x+d'}$ важи $g \circ f : x \mapsto \dfrac{(aa'+cb')x + (ba'+db')}{(ac'+cd')x + (bc'+dd')}$. Тражећи инверз од f (који је фиксиран) решавамо једначину $g \circ f = \mathrm{id}$. Добијамо два система једначина. Први по непознатима a', b': $aa' + cb' = 1, ba' + db' = 0$, и други по непознатима c', d': $ac' + cd' = 0, bc' + dd' = 1$. Лако се види да су решења овог система: $a' = d, b' = -b, c' = -c, d' = a$, и није тешко проверити да је $x \mapsto \frac{dx-b}{-cx+a}$ инверз од f, који, приметимо, припада G.

   Дакле, G јесте група.

□

Диедарска група

Нека је $\Pi_n = A_1 A_2 \ldots A_n$ правилан n-тоугао у равни ω. Са D_n означавамо скуп свих изометрија f равни ω које пресликавају Π_n на себе. Очигледно је $\mathbb{D}_n = (\mathsf{D}_n, \circ, ^{-1}, \varepsilon)$ група, где је f^{-1} инверзно пресликавање од f, а ε је коинциденција (идентичко пресликавање) равни ω.

Неке познате особине изометрија су: темена од Π_n се сликају на темена од Π_n; ако се теме A_i слика у A_j, тада се теме A_{i+1} слика или у A_{j-1} или у A_{j+1}, и страница $A_i A_{i+1}$ се слика на $A_j A_{j-1}$ или на $A_j A_{j+1}$.

15. Доказати да D_n има $2n$ елемената и одредити све елементе од D_n.

Решење. Нека је $A_1A_2\dots A_n$ правилан n-тоугао и нека је f изометрија равни која га слика на себе. Тада је $f(A_1)$ неко од темена $A_1, A_2, \dots, A_n$, тј. A_1 се може сликати на n начина. Када пресликамо A_1, A_2 се мора пресликати тако да буде суседно са сликом од A_1, дакле када пресликамо A_1, A_2 можемо пресликати на 2 начина. Коначно приметимо да када пресликамо A_1 и A_2, слике свих осталих темена су тиме одређене. Дакле, имамо $2n$ начина за пресликавање правилног n-тоугла на себе, тј. D_n има $2n$ елемената.

Одредимо те елементе. (Означимо са $A_0 = A_n$ и $A_{n+1} = A_1$.) Претпоставимо да се A_1 слика у A_i, где $1 \leq i \leq n$. Тада се A_2 слика или у A_{i-1} или у A_{i+1}.

(Ако нацртате слику, следеће објашњење ће бити јасније.)

Ако се A_2 слика у A_{i+1}, приметимо да је тада дата трансформација ротација $\mathcal{R}_{O,2(i-1)\pi/n}$, где је O центар датог n-тоугла. Специјално, ако је $i = 1$ у питању је коинциденција ε. Све ове трансформације су директне (чувају оријентацију равни).

Ако се A_2 слика у A_{i-1}, приметимо да је у питању осна рефлексија $\mathcal{S}_p$, где је p симетрала дужи A_1A_i, ако је $i \neq 1$, или је p симетрала дужи A_2A_n, ако је $i = 1$. Лако се види да су дате праве заиста осе симетрије целог n-тоугла. Све ове трансформације су индиректне (мењају оријентацију равни).

Дакле, D_n чине n ротација и n осних рефлексија □

16. Одредити D_3 и написати "таблицу множења" у $\mathbb{D}_3$.

Решење. Нека је ABC правилан троугао и O његов центар. Лако је видети да су једине изометрије равни које пресликавају ABC на себе: ε, $\mathcal{R}_{O,2\pi/3}$, $\mathcal{R}_{O,4\pi/3}$, $\mathcal{S}_{AO}$, $\mathcal{S}_{BO}$ и $\mathcal{S}_{CO}$.

Запишимо како ова пресликавања сликају темена ABC:

$$\varepsilon : \begin{pmatrix} A\,B\,C \\ A\,B\,C \end{pmatrix}, \qquad \mathcal{R}_{O,2\pi/3} : \begin{pmatrix} A\,B\,C \\ B\,C\,A \end{pmatrix}, \qquad \mathcal{R}_{O,4\pi/3} : \begin{pmatrix} A\,B\,C \\ C\,A\,B \end{pmatrix},$$

$$\mathcal{S}_{OA} : \begin{pmatrix} A\,B\,C \\ A\,C\,B \end{pmatrix}, \qquad \mathcal{S}_{OB} : \begin{pmatrix} A\,B\,C \\ C\,B\,A \end{pmatrix}, \qquad \mathcal{S}_{OC} : \begin{pmatrix} A\,B\,C \\ B\,A\,C \end{pmatrix}.$$

Сада можемо да запишемо таблицу множења у $\mathbb{D}_n$:

$\circ$	ε	$\mathcal{R}_{O,2\pi/3}$	$\mathcal{R}_{O,4\pi/3}$	$\mathcal{S}_{OA}$	$\mathcal{S}_{OB}$	$\mathcal{S}_{OC}$
ε	ε	$\mathcal{R}_{O,2\pi/3}$	$\mathcal{R}_{O,4\pi/3}$	$\mathcal{S}_{OA}$	$\mathcal{S}_{OB}$	$\mathcal{S}_{OC}$
$\mathcal{R}_{O,2\pi/3}$	$\mathcal{R}_{O,2\pi/3}$	$\mathcal{R}_{O,4\pi/3}$	ε	$\mathcal{S}_{OB}$	$\mathcal{S}_{OC}$	$\mathcal{S}_{OA}$
$\mathcal{R}_{O,4\pi/3}$	$\mathcal{R}_{O,4\pi/3}$	ε	$\mathcal{R}_{O,2\pi/3}$	$\mathcal{S}_{OC}$	$\mathcal{S}_{OA}$	$\mathcal{S}_{OB}$
$\mathcal{S}_{OA}$	$\mathcal{S}_{OA}$	$\mathcal{S}_{OC}$	$\mathcal{S}_{OB}$	ε	$\mathcal{R}_{O,4\pi/3}$	$\mathcal{R}_{O,2\pi/3}$
$\mathcal{S}_{OB}$	$\mathcal{S}_{OB}$	$\mathcal{S}_{OA}$	$\mathcal{S}_{OC}$	$\mathcal{R}_{O,2\pi/3}$	ε	$\mathcal{R}_{O,4\pi/3}$
$\mathcal{S}_{OC}$	$\mathcal{S}_{OC}$	$\mathcal{S}_{OB}$	$\mathcal{S}_{OA}$	$\mathcal{R}_{O,4\pi/3}$	$\mathcal{R}_{O,2\pi/3}$	ε

□

17. Ако са ρ означимо ротацију $\mathcal{R}_{O,2\pi/3}$, а са σ било коју од рефлексија $\mathcal{S}_{OA}$, $\mathcal{S}_{OB}$, $\mathcal{S}_{OC}$ из претходног задатка, тада је: $\mathsf{D}_3 = \{\varepsilon, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\}$, $\sigma^2 = \rho^3 = \varepsilon$, $\sigma\rho = \rho^2\sigma$ и $\rho\sigma = \sigma\rho^2$.

Решење. Очигледно је $\{\varepsilon, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\} \subseteq \mathsf{D}_3$. Довољно је доказати да су сви елементи из скупа $\{\varepsilon, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\}$ различити да бисмо доказали једнакост. $\varepsilon, \rho, \rho^2$ су очигледно различите директне изометрије. Како су $\sigma, \sigma\rho, \sigma\rho^2$ индиректне изометрије, то су оне различите од $\varepsilon, \rho, \rho^2$. Остаје да докажемо да су $\sigma, \sigma\rho, \sigma\rho^2$ међусобно различити. Међутим то следи директно према законима скраћивања и чињеници да су $\varepsilon, \rho, \rho^2$ различити.

$\sigma^2 = \rho^3 = \varepsilon$ је очигледно.

Приметимо $(\sigma\rho)^2 = \varepsilon$, јер је $\sigma\rho$ рефлексија. Тада је $\sigma\rho\sigma\rho = \varepsilon$. Ако помножимо ову једнакост са десна са $\rho^2\sigma$, добијамо $\sigma\rho\sigma\rho\rho^2\sigma = \rho^2\sigma$, одакле је $\sigma\rho\sigma\sigma = \rho^2\sigma$, тј. $\sigma\rho = \rho^2\sigma$.

Коначно имамо $\rho\sigma = \rho^3\rho\sigma = \rho^2\rho^2\sigma = \rho^2\sigma\rho = \sigma\rho\rho = \sigma\rho^2$. □

18. Одредити D_4 и написати таблицу множења у $\mathbb{D}_4$.

Решење. Одредићемо само D_4, остављамо писање таблице за самосталан рад. Ако је $ABCD$ квадрат чији је центар O, а p и q редом заједничке нормале страница AB и CD, односно AD и BC, тада је лако видети да су елементи од D_4: $\varepsilon, \mathcal{R}_{O,\pi/2}, \mathcal{R}_{O,\pi}, \mathcal{R}_{O,3\pi/2}, \mathcal{S}_{AC}, \mathcal{S}_{BD}, \mathcal{S}_p, \mathcal{S}_q$. □

19. Ако са ρ означимо ротацију $\mathcal{R}_{O,\pi/2}$, а са σ било коју од рефлексија $\mathcal{S}_{AC}$, $\mathcal{S}_{BD}$, $\mathcal{S}_p$, $\mathcal{S}_q$ из претходног задатка, тада је: $\mathsf{D}_4 = \{\varepsilon, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$, $\sigma^2 = \rho^4 = \varepsilon$, $\sigma\rho = \rho^3\sigma$ и $\rho\sigma = \sigma\rho^3$.

Решење. Очигледно је $\{\varepsilon, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\} \subseteq \mathsf{D}_3$. Довољно је доказати да су сви елементи из скупа $\{\varepsilon, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$ различити да бисмо доказали једнакост. $\varepsilon, \rho, \rho^2, \rho^3$ су очигледно различите директне изометрије. Како су $\sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3$ индиректне изометрије, то су оне различите од $\varepsilon, \rho, \rho^2, \rho^3$. Остаје да докажемо да су $\sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3$ међусобно различити. Међутим то следи директно према законима скраћивања и чињеници да су $\varepsilon, \rho, \rho^2, \rho^3$ различити.

$\sigma^2 = \rho^4 = \varepsilon$ је очигледно.

Приметимо $(\sigma\rho)^2 = \varepsilon$, јер је $\sigma\rho$ рефлексија. Тада је $\sigma\rho\sigma\rho = \varepsilon$. Ако помножимо ову једнакост са десна са $\rho^3\sigma$, добијамо $\sigma\rho\sigma\rho\rho^3\sigma = \rho^3\sigma$, одакле је $\sigma\rho\sigma\sigma = \rho^3\sigma$, тј. $\sigma\rho = \rho^3\sigma$.

Коначно имамо $\rho\sigma = \rho^4\rho\sigma = \rho^2\rho^3\sigma = \rho^2\sigma\rho = \rho^4\rho^2\sigma\rho = \rho^3\rho^3\sigma\rho = \rho^3\sigma\rho\rho = \sigma\rho\rho\rho = \sigma\rho^3$. □

20. Ако са ρ означимо ротацију $\mathcal{R}_{O,2\pi/n}$, а са σ било коју од рефлексија правилног n-тоугла, тада је: $\mathsf{D}_n = \{\varepsilon, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}\}$, $\sigma^2 = \rho^n = \varepsilon$, $\sigma\rho = \rho^{n-1}\sigma$ и $\rho\sigma = \sigma\rho^{n-1}$.

Решење. Очигледно је $\{\varepsilon, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}\} \subseteq \mathsf{D}_n$. Довољно је доказати да су сви елементи из скупа $\{\varepsilon, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}\}$ различити да бисмо доказали једнакост. $\varepsilon, \rho, \rho^2, \ldots, \rho^{n-1}$ су очигледно различите директне изометрије. Како су $\sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}$ индиректне изометрије, то су оне различите од $\varepsilon, \rho, \rho^2, \ldots, \rho^{n-1}$. Остаје да докажемо да су $\sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}$ међусобно различити. Међутим то следи директно према законима скраћивања и чињеници да су $\varepsilon, \rho, \rho^2, \ldots, \rho^{n-1}$ различити.

$\sigma^2 = \rho^n = \varepsilon$ је очигледно.

Приметимо $(\sigma\rho)^2 = \varepsilon$, јер је $\sigma\rho$ рефлексија. Тада је $\sigma\rho\sigma\rho = \varepsilon$. Ако помножимо ову једнакост са десна са $\rho^{n-1}\sigma$, добијамо $\sigma\rho\sigma\rho\rho^{n-1}\sigma = \rho^{n-1}\sigma$, одакле је $\sigma\rho\sigma\sigma = \rho^{n-1}\sigma$, тј. $\sigma\rho = \rho^{n-1}\sigma$.

Слично је $(\rho\sigma)^2 = \varepsilon$, јер је и $\rho\sigma$ рефлексија. Тада је $\rho\sigma\rho\sigma = \varepsilon$. Ако помножимо ову једнакост са лева са $\sigma\rho^{n-1}$, добијамо $\sigma\rho^{n-1}\rho\sigma\rho\sigma = \sigma\rho^{n-1}$, одакле је $\sigma\sigma\rho\sigma = \sigma\rho^{n-1}$, тј. $\rho\sigma = \sigma\rho^{n-1}$. □

Подгрупе

Подскуп H групе G је подгрупа групе G, $H \leq G$, ако важи:

1) ако $x, y \in H$, тада $xy \in H$;

2) ако $x \in H$, тада $x^{-1} \in H$;

3) $e \in H$.

21. Подскуп H групе G је подгрупа групе G акко је непразан и важи: ако $x, y \in H$, тада $xy^{-1} \in H$.

Решење. Докажимо прво смер $\Rightarrow$). Ако $H \leq G$, тада је H непразан, јер $e \in H$ (према 3) из дефиниције). Такође, ако $x, y \in H$, тада $x, y^{-1} \in H$ (према 2) из дефиниције), а одатле $xy^{-1} \in H$ (према 1) из дефиниције).

Сада доказујемо $\Leftarrow$). Како је H непразан, изаберимо $t \in H$. Према услову тада $tt^{-1} \in H$, тј. $e \in H$, што доказује 3) из дефиниције. Претпоставимо да $x \in H$, тада из $e, x \in H$, према услову, следи $ex^{-1} \in H$, тј. $x^{-1} \in H$, што доказује 2) из дефиниције. Коначно ако $x, y \in H$, тада према управо доказаном $x, y^{-1} \in H$, па према услову $x(y^{-1})^{-1} \in H$, тј. $xy \in H$, што доказује 1) из дефиниције. □

Ако су $H, K \subseteq G$, $a, b \in G$, тада дефинишемо следеће скупове (подскупове од G): $HK = \{xy \mid x \in H, y \in K\}$, $H^{-1} = \{x^{-1} \mid x \in H\}$, $aH = \{ax \mid x \in H\}$, $Hb = \{xb \mid x \in H\}$, $aHb = \{axb \mid x \in H\}$. Скуп aH зовемо леви транслат од H, Hb је десни транслат од H, aHb је двострани транслат од H. Специјално двострани транслат aHa^{-1} зовемо коњугат од H.

Приметите да је подскуп H од G подгрупа од G акко: $HH \subseteq H$, $H^{-1} \subseteq H$ и $e \in H$. Такође, непразана подскуп H од G је подгрупа од G акко $HH^{-1} \subseteq H$.

22. Пресликавање $f : H \longrightarrow aH$, дефинисано на очигледан начин $f : x \mapsto ax$, је бијекција. Слично $x \mapsto xb$ је бијекција $H \longrightarrow Hb$, и $x \mapsto axb$ је бијекција $H \longrightarrow aHb$.

Решење. f је очигледно добро дефинисано на пресликавање. Ако је $f(x) = f(y)$, тј. ако је $ax = ay$, тада је због скраћивања и $x = y$, што доказује да је f 1-1. □

23. Наћи пример групе G и подскупа $H \subseteq G$ таквих да: $e \in H$, $HH \subseteq H$, али да H није подгрупа.

Решење. Уочимо групу $\mathbb{Q}$ рационалних бројева у односу на сабирање. Уочимо њен подскуп $H = \{q \in \mathbb{Q} \mid q \geq 0\}$. Јасно је да $0 \in H$, да је $H + H = H$, али H није подгрупа – наиме фале инверзи. □

24. Ако је H коначан непразан подскуп од G такав да је $HH \subseteq H$, тада је H подгрупа од G.

Решење. Како је H непразан, он садржи неки елемент a. Како је $HH \subseteq H$, то је за $x \in H$, $ax \in H$, па је $f : x \mapsto ax$ пресликавање $f : H \longrightarrow H$, које је како смо већ доказали 1-1. Како је H коначан, то је f на. Према томе постоји елемент $b \in H$ такаб да је $f(b) = a$, тј. $ab = a$. После скраћивања са a закључујемо $b = e$. Дакле, $e \in H$.

Поново користећи чињеницу да је за било који $a \in H$, $f : x \mapsto ax$ бијекција $H \longrightarrow H$, закључујемо да постоји елемент $b \in H$ тако да $f(b) = e$, тј. $ab = e = aa^{-1}$. После скраћивања са добијамо, $b = a^{-1}$, тј. H је затворен за инверзе.

Како је већ према услову задатка H био затворен за операцију, то је H подгрупа од G. □

25. Нека је $\mathcal{F}$ непразна фамилија подгрупа групе G. Доказати да је $\bigcap \mathcal{F}$ подгрупа групе G.

Решење. Приметимо да e припада сваком члану фамилије $\mathcal{F}$, па припада и $\bigcap \mathcal{F}$. Такође, ако $x \in \bigcap \mathcal{F}$, тада x припада сваком члану фамилије $\mathcal{F}$, па и x^{-1} припада сваком члану фамилије $\mathcal{F}$, па $x^{-1} \in \bigcap \mathcal{F}$. Коначно, ако $x, y \in \bigcap \mathcal{F}$, тада x, y припадају сваком члану фамилије $\mathcal{F}$, па и xy припада сваком члану фамилије $\mathcal{F}$, па $xy \in \bigcap \mathcal{F}$. □

Последица Нека је $S \subseteq G$ непразан подскуп од G, и нека је $\mathcal{F}_S = \{H \leq G \mid S \subseteq G\}$. Према претходном задатку је $\bigcap \mathcal{F}_S$ подгрупа од G, која очигледно садржи S. Она је и најмања подгрупа од G која садржи S (јер је пресек свих таквих), и њу зовемо *подгрупа генерисана са* S и означавамо $\langle S \rangle = \bigcap \mathcal{F}_S$. Приметите да директно према дефиницији важи: ако је $H \leq G$ и $S \subseteq H$, тада $\langle S \rangle \leq H$.

26. Нека су $H, K \leq G$. Доказати да је $H \cup K \leq G$ акко $H \subseteq K$ или $K \subseteq H$.

Решење. Ако је $H \subseteq K$ или $K \subseteq H$, тада је $H \cup K = K$ или $H \cup K = H$, па је свакако $H \cup K \leq G$.

Са друге стране, ако $H \not\subseteq K$ и $K \not\subseteq H$, изаберимо $a \in H \setminus K$ и $b \in K \setminus H$, тада $ab \notin H$ (јер би у супротном $b = a^{-1}(ab)$ припадало H) и $ab \notin K$ (јер би у супротном $a = (ab)b^{-1}$ припадало K). Дакле, $a, b \in H \cup K$, али $ab \notin H \cup K$, одакле следи $H \cup K \not\leq G$. □

27. Одредити све подгрупе од D_3.

Решење. Сетимо се да је $\mathsf{D}_3 = \{\varepsilon, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\}$, где је ρ ротација за $2\pi/3$, а σ произвољна симетрија. Одавде следи да, ако подгрупа H садржи ρ и произвољну симетрију, H мора да буде једнака D_3. У случају D_3 приметимо и да ако H садржи ρ^2, тада H садржи и $(\rho^2)^2 = \rho^4 = \rho$. Дакле, ако H садржи једну ротацију, садржи их обе, и такође ако садржи произвољу ротацију и произвољну симетрију мора да буде једнака D_3.

Одредимо сада све подгрупе од D_3.

Претпоставимо да подгрупа H садржи бар две симетрије. Тада H садржи и њихов производ, који није ε јер су различите, а јесте директна трансформација, према томе њихов производ је нека ротација. Дакле, H садржи симетрију и ротацију, па је једнака D_3.

Претпоставимо да подгрупа H садржи тачно једну симетрију. Ако H садржи ротацију, онда је једнака D_3, па садржи све симетрије, што је у супротности са претпоставком. Дакле, H поред дате симетрије и коинциденције не садржи ниста више. Према томе H је једнака $\{\varepsilon, \sigma\}$, $\{\varepsilon, \sigma\rho\}$ или $\{\varepsilon, \sigma\rho^2\}$. Лако се види да ово јесу подгрупе од D_3.

Коначно, претпоставимо да подгрупа H не садржи симетрије. Ако H не садржи ни ротацију, у питању је тривијална подгрупа $\{\varepsilon\}$. Ако H садржи ротацију, како смо видели, садржи обе, па је $H = \{\varepsilon, \rho, \rho^2\}$, и лако се види да она јесте подгрупа.

Дакле, све подгрупе од D_3 су: $\{\varepsilon\}$, $\{\varepsilon, \sigma\}$, $\{\varepsilon, \sigma\rho\}$, $\{\varepsilon, \sigma\rho^2\}$, $\{\varepsilon, \rho, \rho^2\}$ и D_3. □

28. Одредити све подгрупе од D_4.

Решење. Сетимо се да је $\mathsf{D}_4 = \{\varepsilon, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$, где је ρ ротација за $2\pi/4$, а σ је произвољна симетрија. ОДавде следи да ако подгрупа H садржи ρ и произвољну симетрију, она је једнака D_4. Такође приметимо да ако H садржи ρ^3, тада H садржи и $(\rho^3)^3 = \rho^9 = \rho$, одакле следи: ако H садржи ρ или ρ^3, тада H садржи све ротације и такође ако H садзрхи ρ или ρ^3 и произвољну симетрију, тада је H једнака D_4.

Најпре ћемо доказати да ако H садржи неки од следећих скупова: $\{\sigma, \sigma\rho\}$, $\{\sigma, \sigma\rho^3\}$, $\{\sigma\rho, \sigma\rho^2\}$, $\{\sigma\rho^2, \sigma\rho^3\}$, тада је $H = \mathsf{D}_4$. Заиста, ако H садржи неке од наведених парова симетрија, тада H садржи и њихов производ, који су редом једнаки: $\sigma\sigma\rho = \rho$, $\sigma\sigma\rho^3 = \rho^3$, $\sigma\rho\sigma\rho^2 = \sigma\sigma\rho^3\rho^2 = \rho$ и $\sigma\rho^2\sigma\rho^3 = \sigma\sigma\rho^2\rho^3 = \rho$. Дакле, H садржи неку од ротација ρ или ρ^3 и неку симетрију, па је $H = \mathsf{D}_4$.

Ако H садржи бар три симетрије, тада H мора да садржи неки од паровба симетрија из претходнох пасуса, па је $H = \mathsf{D}_4$.

Претпоставимо да H садржи тачно две симетрије. Према претходном H садржи или $\{\sigma, \sigma\rho^2\}$ или $\{\sigma\rho, \sigma\rho^3\}$. Са једне стране, како су то једине две симетрије које садржи H, H не сме да садржи ротације ρ и ρ^3. Са друге стране, мора да садржи производ те две симетрије,

који су редом једнаки: $\sigma\sigma\rho^2 = \rho^2$ и $\sigma\rho\sigma\rho^3 = \sigma\sigma\rho^3\rho^3 = \rho^2$. Дакле, $H = \{\varepsilon, \sigma, \sigma\rho^2, \rho^2\}$ или $H = \{\varepsilon, \sigma\rho, \sigma\rho^3, \rho^2\}$. Лако се види да ово јесу подгрупе од H. Приметите да су оне и Абелове.

Претпоставимо да H садржи тачно једну симетрију σ'. Тада H не садржи преостале три симетрије, а такође не сме да садржи ниједну ротацију ρ^i, јер би у супротном садржала $\sigma'\rho^i$, што би била друга симетрија у њој. Дакле, $H = \{\varepsilon, \sigma\}$, $H = \{\varepsilon, \sigma\rho\}$, $H = \{\varepsilon, \sigma\rho^2\}$ или $H = \{\varepsilon, \sigma\rho^3\}$. Лако се види да ово јесу подгрупе од D_4.

Коначно, претпоставимо да H не садржи ниједну симетрију. Ако H не садржи ниједну ротацију, H је тривијална подгрупа $\{\varepsilon\}$. Ако H садржи ротацију ρ или ρ^3, како смо видели тада је $H = \{\varepsilon, \rho, \rho^2, \rho^3\}$, и лако се види да ово јесте подгрупа од D_4. Ако H садржи ротацију, а не садржи ни ρ ни ρ^3, тада је $H = \{\varepsilon, \rho^2\}$, и такође се лако види да ово јесте подгрупа.

Дакле, све подгрупе од D_4 су: $\{\varepsilon\}$, $\{\varepsilon, \sigma\}$, $\{\varepsilon, \sigma\rho\}$, $\{\varepsilon, \sigma\rho^2\}$, $\{\varepsilon, \sigma\rho^3\}$, $\{\varepsilon, \rho^2\}$, $\{\varepsilon, \sigma, \sigma\rho^2, \rho^2\}$, $\{\varepsilon, \sigma\rho, \sigma\rho^3, \rho^2\}$, $\{\varepsilon, \rho, \rho^2, \rho^3\}$ и D_4. □

29. Одредити све подгрупе од $(\mathsf{Z}, +, -, 0)$.

Решење. Приметимо да за $n \geq 0$, $n\mathsf{Z} = \{nx \mid x \in \mathsf{Z}\}$ (скуп целих бројева дељивих са n) јесте подгрупа од Z. (За $n = 0$, то је тривијална подгрупа $\{0\}$, за $n = 1$ то је цела група Z.) Доказаћемо да не постоји ниједна више подгрупа.

Нека је $H \leq \mathsf{Z}$. Приметимо да $H \cap \mathsf{Z}^+ \neq \emptyset$, па изаберимо најмањи позитиван природан број n такав да $n \in H$. Тврдимо $H = n\mathsf{Z}$. Како $n \in H$, јасно је да $n\mathsf{Z} \subseteq H$. Са друге стране, ако $x \in H$, запишимо $x = nq + r$, где $0 \leq r < n$. Тада је $r = x - nq \in H$, јер $x \in H$ и $nq \in H$. Међутим како је n био најм,ањи позитиван природан број који припада H, како $r \in H$ и како $0 \leq r < n$, закључујемо да је $r = 0$. Дакле, $x = nq \in n\mathsf{Z}$. □

30. Доказати да је $\mathsf{D}_m \leq \mathsf{D}_n$ акко $m \mid n$.

Решење. Претпоставимо да $m \mid n$, и нека је $n = km$. Нека је $A_1A_2 \ldots A_n$ правилан n-тоугао, чији је центар O. Приметимо да је тада $A_1A_{k+1}A_{2k+1} \ldots A_{(m-1)k+1}$ правилан m-тоугао. Означимо са ρ ротацију око O за $2\pi/n$, а са σ симетрију у односу на A_1O. Тада је ρ^k ротација за $2\pi/m$, а σ је и симетрија уоченог m-тоугла, па је $\mathsf{D}_m = \{\varepsilon, \rho^k, \rho^{2k}, \ldots, \rho^{(m-1)k}, \sigma, \sigma\rho^k, \sigma\rho^{2k}, \ldots, \sigma\rho^{(m-1)k}, \} \leq \{\varepsilon, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}\} = \mathsf{D}_n$.

Ако је $\mathsf{D}_m \leq \mathsf{D}_n$, тада D_m садржи ротацију за $2\pi/m$, тј. елемент R такав да $R^m = \varepsilon$, и m је најмањи позитиван природан број такав да $R^m = \varepsilon$. Како је $m > 2$ и $R \in \mathsf{D}_n$, тада R не може бити симетрија у D_n јер би тада имали $R^2 = \varepsilon$, па према томе је R ротација и у D_n. Ротације у D_n су ρ^k, $1 \leq k < n$, и све оне задовољавају $(\rho^k)^n = \varepsilon$. Запишимо $n = qm + r$, $0 \leq r < m$. Како је $R = \rho^k$, за неко k, тада је $\varepsilon = (\rho^k)^n = R^n = R^{qm+r} = (R^m)^q R^r = \varepsilon^q R^r = R^r$, па како је m био најмањи позитиван природан број такав да $R^m = \varepsilon$, закључујемо да $r = 0$, тј. $n = qm$ и $m \mid n$.[1] □

Цикличне групе

Циклична група Кажемо да је група G циклична, ако постоји елемент $a \in G$ такав да је $G = \langle a \rangle$.

31. Нека је $G = \langle a \rangle$. Доказати да је $G = \{a^m \mid m \in \mathsf{Z}\}$. (По дефиницији: $a^0 = e$, $a^n = a^{n-1}a$, $a^{-n} = (a^n)^{-1}$, за $n \geq 1$.) Специјално, циклична група је највише пребројива.

[1] Ако знамо Лагранжову теорему, тада $\mathsf{D}_m \leq \mathsf{D}_n$ повлачи $|\mathsf{D}_m| \mid |\mathsf{D}_n|$, тј. $2m \mid 2n$, односно $m \mid n$.

Решење. Означимо са $H = \{a^m \mid m \in \mathsf{Z}\}$. Како $a \in G$, то очигледно $H \subseteq G$.

Докажимо да је $H \leq G$. $e = a^0 \in H$. За $a^m, a^n \in H$ имамо $a^m a^n = a^{m+n} \in H$. И за $a^m \in H$, $(a^m)^{-1} = a^{-m} \in H$. Дакле $H \leq G$. Како $a \in H$, то $\langle a \rangle \leq H$, па имамо $G = \langle a \rangle \leq H \leq G$, што доказује $G = \{a^m \mid m \in \mathsf{Z}\}$. □

32. Нека је G коначна група реда n.

1) Ако $a \in G$, доказати да за неко $k \leq n$ важи $a^k = e$.

2) Ако је k позитиван природан број такав да $a^k = e$, тада је $\langle a \rangle = \{e, a, a^2, \ldots, a^{k-1}\}$.

3) Ако је $G = \langle a \rangle$, тада је n најмањи позитиван природни број такав да $a^n = e$.

4) Ако је $G = \langle a \rangle$, тада је $G = \{e, a, a^2, \ldots, a^{n-1}\}$.

Решење.

1) Нека $a \in G$. Тада је $a, a^2, a^3, \ldots, a^{n+1}$ неких $n+1$ елемената из G. Како G има n елемената, то закључујемо да они нису сви различити, па постоје $1 \leq i < j \leq n+1$ такви да је $a^i = a^j$. После скраћивања са a^i, добијамо $a^{j-i} = e$. Приметите само да је $1 \leq j - i \leq n$, одакле тврђење следи ако узмемо $k = j - i$.

2) Видели смо да је $\langle a \rangle = \{a^m \mid m \in \mathsf{Z}\}$, па је $\{e, a, a^2, \ldots, a^{k-1}\} \subseteq \langle a \rangle$.

   Докажимо и обратно. Нека је $x \in \langle a \rangle$, тада је $x = a^m$, за неко $m \in \mathsf{Z}$. Запишимо $m = kq + r$, где $0 \leq r < k$. Тада је $x = a^m = a^{kq+r} = (a^k)^q a^r = e^q a^r = ea^r = a^r \in \{e, a, a^2, \ldots, a^{k-1}\}$.

3) Нека је k најмањи позитиван природан број такав да $a^k = e$. Према првом делу задатка $k \leq n$. Докажимо да је $k = n$.

   Према другом делу задатка имамо $G = \langle a \rangle = \{e, a, a^2, \ldots, a^{k-1}\}$, па како G има n елемената, а скуп на десној страни k елемената, и како је $k \leq n$, то закључујемо да је $k = n$ (и специјално да су сви елементи у скупу на десној страни једнакости различити).

4) Ово је последица другог и трећег дела.

□

33. Циклична група је Абелова.

Решење. Нека је $G = \langle a \rangle$. И нека $x, y \in G$. Тада је $x = a^m$, $y = a^n$, за неке $m, n \in \mathsf{Z}$, па је $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$. □

34. Доказати да је подгрупа цикличне групе, циклична.

Решење. Нека је $H \leq G = \langle a \rangle$ и $H \neq \langle e \rangle$ (тривијална подгрупа је очигледно циклична). Тада је $H \cap \{a^n \mid n \geq 1\} \neq \emptyset$, па изаберимо најмањи позитиван природан број k такав да $a^k \in H$. Тврдимо да је $H = \langle a^k \rangle$.

Како $a^k \in H$, то $\langle a^k \rangle \leq H$. Обратно, ако $x \in H$, тада је $x = a^m$, за неко $m \in \mathsf{Z}$. Запишимо $m = kq + r$, где $0 \leq r < k$. Тада је $a^m = a^{kq+r} = (a^k)^q a^r$, одакле је $a^r = (a^k)^{-q} a^m$, што припада H, јер и $(a^k)^{-q}$ и a^m припадају H. Како је k најмањи позитиван природан број такав да $a^k \in H$, и како је $r < k$, то закључујемо да је $r = 0$, па је $m = kq$, одакле, $x = a^m = (a^k)^q \in \langle a^k \rangle$. □

35. 1) Доказати да је свака коначно генерисана група подгрупа од $(\mathsf{Q}, +, -, 0)$ циклична.
2) Доказати да Q није циклична.

Решење. 1) Нека је $S = \{a_1/b_1, a_2/b_2, \ldots, a_n/b_n\}$, где $a_i \in \mathsf{Z}$, а $b_i \in \mathsf{N}^+$. Докажимо да је $\langle S\rangle$ циклична. Уочимо $b = b_1 b_2 \ldots b_n \in \mathsf{N}^+$. Приметимо да за свако i, $a_i/b_i = a_i(b/b_i)/b$ и да је $a_i(b/b_i) \in \mathsf{Z}$, па одатле закључујемо да $a_i/b_i \in \langle 1/b\rangle$. Дакле, $S \subseteq \langle 1/b\rangle$, одакле и $\langle S\rangle \leq \langle 1/b\rangle$. Према томе $\langle S\rangle$ је подгрупа цикличне, па је и сама циклична.

2) Претпоставимо супротно да је $\mathsf{Q} = \langle a/b\rangle$, где $a \in \mathsf{Z}$, $b \in N^+$. Приметимо да тада $a/b \in \langle 1/b\rangle$, одакле је $\mathsf{Q} = \langle a/b\rangle \leq \langle 1/b\rangle \leq \mathsf{Q}$, одакле је $\mathsf{Q} = \langle 1/b\rangle$. Како је $\langle 1/b\rangle = \{m/b \mid m \in \mathsf{Z}\}$, то је контрадикција, јер $1/2b \in \mathsf{Q}$, али $1/2b \notin \langle 1/b\rangle$, јер $1/2 \notin \mathsf{Z}$. □

Коментар Приметимо да је $(\mathsf{Z}, +, -, 0) = \langle 1\rangle$, тј. Z је пример бесконачне цикличне групе. Такође, $(\mathsf{Z}_n, +_n, -_n, 0) = \langle 1\rangle$, где је $n \geq 1$, је пример цикличне групе са n елемената. У следећем задатку ћемо доказати да су до на изоморфизам оне и једине цикличне групе.

36. Нека је $G = \langle a\rangle$.

1) Ако је G бесконачна, тада $G \cong \mathsf{Z}$.

2) Ако је $|G| = n$ (где $n \geq 1$), тада $G \cong \mathsf{Z}_n$.

Решење. 1) Сетимо се да је $G = \{a^m \mid m \in \mathsf{Z}\}$. Уочимо пресликавање $f : \mathsf{Z} \longrightarrow G$ дато са $f(m) = a^m$. f је очигледно добро дефинисано на пресликавње. Докажимо да је 1-1. Ако пртпоставимо супротно, да за неке $m < n$ важи $a^m = a^n$, тада је $a^{n-m} = e$, па је према неком од претходних задатака $G = \langle a\rangle = \{e, a, a^2, \ldots, a^{n-m-1}\}$, што је у контрадикцији са чињеницом да је G бесконачна.

Коначно, како је $f(m+n) = a^{m+n} = a^m a^n = f(m)f(n)$, то је f и хомоморфизам, па је f жељени изоморфизам између G и Z.

2) Сетимо се да је $G = \{e, a, a^2, \ldots, a^{n-1}\}$. Уочимо пресликавање $f : \mathsf{Z}_n \longrightarrow G$ дато са $f(k) = a^k$. f је очигледно добро дефинисано на пресликавње. Како је на, и како домен и кодомен пресликавања имају по n елемената, то је f и 1-1. Коначно, докажимо да је f хоморфизам. Треба да проверимо да је $f(k +_n l) = f(k)f(l)$, тј. $a^{k+_n l} = a^k a^l = a^{k+l}$. Сетимо се да је $k +_n l = \mathrm{rest}(k+l, n) = r$, где је $k + l = qn + r$ и $0 \leq r < n$. Тада је $a^{k+l} = a^{qn+r} = (a^n)^q a^r = a^r$, што је и требало доказати. □

37. Нека је $G = \langle a\rangle$ циклична група са n елемената.

1) $a^m = e$ ако и само ако $n \mid m$;

2) ако је $H \leq G$ и $|H| = m$, тада $m \mid n$;

3) ако је $m \mid n$, тада постоји јединствена подгрупа $H \leq G$ таква да $|H| = m$.

Решење. 1) Ако $n \mid m$, тада је $m = nk$, па је $a^m = (a^n)^k = e^k = e$, што доказује смер $\Leftarrow$). За доказ $\Rightarrow$), запишимо $m = qn + r$, где $0 \leq r < n$. Тада је $e = a^m = (a^n)^q a^r = a^r$, а како је n најмањи позитиван природан број такав да $a^n = e$, то је $r = 0$, па је $m = qn$, тј. $n \mid m$.

2) Можемо претпоставити да је H нетривијална подгрупа. Како је $G = \{e, a, a^2, \ldots, a^{n-1}\}$, изаберимо најмањи позитиван природан број $k < n$ такав да $a^k \in H$. Тврдимо $H = \langle a^k\rangle$. Инклузија $\supseteq$) је очигледна. За $\subseteq$) уочимо $x = a^l \in H$, и запишимо $l = kq + r$, $0 \leq r < k$. Тада је $x = a^l = (a^k)^q a^r$, па како $x, a^k \in H$, одатле и $a^r \in H$, одакле је $r = 0$, по избору броја k. Према томе $l = kq$, одакле $x = a^l = (a^k)^q \in \langle a^k\rangle$.

Дакле, $H = \langle a^k\rangle$ и $|H| = m$, па према првом делу задатка (примењеном на цикличну групу H) $(a^k)^s = e$ ако и само ако $m \mid s$. Приметимо да је $(a^k)^n = (a^n)^k = e^k = e$, одакле $m \mid n$.

3) Претпоставимо $m \mid n$ и $n = mk$. Најпре ћемо доказати егзистенцију подгрупе са m елемената. Нека је $H = \langle a^k\rangle$. Тврдимо $|H| = m$. Најпре уочимо да су $e, a^k, a^{2k}, \ldots, a^{m-1}k$ различити елементи подгрупе H и приметимо да их има m. Ако је $x \in H$, тада је $x = (a^k)^l$, па ако запишемо $l = mq + r$, $0 \leq r < m$, добијамо $x = (a^k)^l = (a^k)^{mq+r} = (a^{km})^q (a^k)^r = (a^n)^q (a^k)^r =$

$(a^k)^r \in \{e, a^k, a^{2k}, \ldots, a^{(m-1)k}\}$, одакле закључујемо да је $H = \{e, a^k, a^{2k}, \ldots, a^{(m-1)k}\}$, тј. H заиста јесте подгрупа са m елемената.

Коначно доказујемо јединственост. Претпоставимо да је K подгрупа са m елемената. Како је K циклична (као подгрупа цикличне), то је $K = \langle a^l \rangle$, за неко l. Запишимо $l = qk + r$, $0 \leq r < k$. Тада је $ml = qkm + rm = qn + rm$ и $0 \leq rm < km = n$. Сада имамо $a^{ml} = e$, јер је K реда m, а са друге стране $a^{ml} = (a^n)^q a^{rm} = a^{rm}$. Одавде је $a^{rm} = e$, па како је $rm < n$, то је $rm = 0$, одакле је $r = 0$. Дакле, $l = qk$, па је $a^l = (a^k)^q \in \langle a^k \rangle = H$. Одавде, $K = \langle a^l \rangle \leq H$, па како K и H имају по m елмената, закључујемо да је $K = H$. □

Коментар Нека је $n \geq 1$. Дефинишемо функцију $\tau : \mathsf{N}^+ \longrightarrow \mathsf{N}^+$ са $\tau(n) = \sum_{d|n} 1$, тј. $\tau(n)$ је број делилаца броја n. Према претходном задатку циклична група са n елемената има $\tau(n)$ подгрупа.

38. Нека је $G = \langle a \rangle$ циклична група са n елемената.

1) Ако $(n, k) = 1$, тада је $G = \langle a^k \rangle$.

2) Ако је $G = \langle a^k \rangle$, тада је $(n, k) = 1$.

Решење. Сетимо се да је $(n, k) = 1$ ако и само ако постоје $p, q \in \mathsf{Z}$ такви да $pn + qk = 1$.

1) Претпоставимо да $(n, k) = 1$ и нека су $p, q \in \mathsf{Z}$ такви да $pn + qk = 1$. Тада је $a = a^1 = a^{pn+qk} = (a^n)^p (a^k)^q = (a^k)^q \in \langle a^k \rangle$. Одавде је $G = \langle a \rangle \leq \langle a^k \rangle \leq G$, па је $G = \langle a^k \rangle$.

2) Ако је $G = \langle a^k \rangle$, тада је $a = (a^k)^q$, одакле је $a^{kq-1} = e$. Одавде $n \mid kq - 1$, па постоји $p \in \mathsf{Z}$ такав да $np = kq - 1$, тј. $-pn + qk = 1$, одакле је $(k, n) = 1$. □

Коментар Нека је $n \geq 1$. Дефинишемо Ојлеров скуп $\Phi_n = \{k \mid 1 \leq k \leq n, (k, n) = 1\}$. Ојлерова функција је функција $\varphi : \mathsf{N}^+ \longleftarrow \mathsf{N}^+$ дефинисана са $\varphi(n) = |\Phi_n|$. Према претходном задатку циклична група са n елемената има $\varphi(n)$ генератора.

39. Ако је $|G| = p$, где је p прост број, тада је G циклична.

Решење. Нека је $a \in G$, $a \neq e$. Према Лагранжовој теореми $|\langle a \rangle| \mid |G| = p$. Како је p прост и како $|\langle a \rangle| > 1$, закључујемо да $|\langle a \rangle| = p$, па како $\langle a \rangle \leq G$ и како и $\langle a \rangle$ и G имају p елемената, то $G = \langle a \rangle$ □

Ред елемента

Ред елемента $a \in G$ је $r(a) = |\langle a \rangle|$. Већ смо видели да је $\langle a \rangle = \{a^m \mid m \in \mathsf{Z}\}$ највише пребројив скуп. Према томе $r(a) \in \mathsf{N}^+$ или $r(a) = \aleph_0$. Такође смо видели, ако је $r(a) \in \mathsf{N}^+$, тада је $r(a)$ најмањи позитиван природан број такав да је $a^{r(a)} = e$.

40. $a^m = e$ акко $r(a) \mid m$.

Решење. $\Rightarrow$) Претпоставимо да $a^m = e$. Запишимо $m = r(a)q + r$, $0 \leq r < r(a)$. Тада је $e = a^m = (a^{r(a)})^q a^r = a^r$, па како је $r < r(a)$ и како је $r(a)$ најмањи позитиван природан број такав да $a^{r(a)} = e$, закључујемо да је $r = 0$, тј. $m = r(a)q$ и $r(a) \mid m$.

$\Leftarrow$) Ако $r(a) \mid m$, тада је $m = r(a)q$, па је $a^m = (a^{r(a)})^q = e^q = e$. □

41. Нека је $|G| = n$. Тада за све $a \in G$ важи $r(a) \mid n$. Специјално за све $a \in G$ важи $a^n = e$.

Решење. Приметимо да по Лагранжовој теореми имамо $r(a) = |\langle a \rangle| \mid |\langle G \rangle| = n$. □

42. Нека $a, b, g \in G$.

1) $r(a^{-1}) = r(a)$;

2) $r(g^{-1}ag) = r(a)$;

3) $r(ab) = r(ba)$;

4) ако је $f : G \longrightarrow H$ хомоморфизам, тада $r(f(a)) \mid r(a)$;

5) ако је $f : G \longrightarrow H$ изоморфизам, тада $r(f(a)) = r(a)$.

Решење. 1) Претпоставимо да је $r(a) \in \mathsf{N}^+$. Тада је $(a^{-1})^{r(a)} = \underbrace{a^{-1}a^{-1}\dots a^{-1}}_{r(a)} = (\underbrace{aa\dots a}_{r(a)})^{-1} = e^{-1} = e$. Дакле, $r(a^{-1}) \mid r(a)$. Према томе и $r(a) = r((a^{-1})^{-1}) \mid r(a^{-1})$; дакле, $r(a) = r(a^{-1})$.

Ако је $r(a) = \aleph_0$, тада је и $r(a^{-1}) = \aleph_0$, јер би у супротном, према претходно доказаном, било $r(a) = r((a^{-1})^{-1}) = r(a^{-1}) \in \mathsf{N}^+$.

2) Претпоставимо да је $r(a) \in \mathsf{N}^+$. Тада је $(g^{-1}ag)^{r(a)} = \underbrace{g^{-1}agg^{-1}ag\dots g^{-1}ag}_{r(a)} = g^{-1}\underbrace{aa\dots a}_{r(a)}g = g^{-1}eg = e$. Дакле, $r(g^{-1}ag) \mid r(a)$. Према томе и $r(a) = r(gg^{-1}agg^{-1}) \mid r(g^{-1}ag)$; дакле, $r(a) = r(g^{-1}ag)$.

Ако је $r(a) = \aleph_0$, тада је и $r(g^{-1}ag) = \aleph_0$, јер би у супротном, према претходно доказаном, било $r(a) = r(gg^{-1}agg^{-1}) = r(g^{-1}ag) \in \mathsf{N}^+$.

3) Приметимо да је $ab = b^{-1}(ba)b$, па је $r(ab) = r(ba)$ према делу 2).

4) Овде претпостављамо да је $r(a) \in \mathsf{N}^+$. Тада је $f(a)^{r(a)} = \underbrace{f(a)f(a)\dots f(a)}_{r(a)} = f(\underbrace{aa\dots a}_{r(a)}) = f(e) = e$, одакле $r(f(a)) \mid r(a)$.

5) Ако је $f : G \longrightarrow H$ изоморфизам, знамо да је тада и $f^{-1} : H \longrightarrow G$ изоморфизам.

Претпоставимо да је $r(a) \in \mathsf{N}^+$. Према 4) имамо да $r(f(a)) \mid r(a)$. Према 4), примењено на хомоморфизам f^{-1} и елемент $f(a) \in H$, имамо $r(a) = r(f^{-1}(f(a))) \mid r(f(a))$. Дакле, $r(f(a)) = r(a)$.

Ако је $r(a) = \aleph_0$, тада је и $r(f(a)) = \aleph_0$, јер би у супротном, према претходно доказаном, било $r(a) = r(f^{-1}(f(a))) = r(f(a)) \in \mathsf{N}^+$. □

43. Претпоставимо да је G Абелова група и $a, b \in G$ елементи коначних редова.

1) $r(ab) \mid [r(a), r(b)]$;

2) ако је $\langle a\rangle \cap \langle b\rangle = \langle e\rangle$, тада је $r(ab) = [r(a), r(b)]$;

3) ако је $(r(a), r(b)) = 1$, тада је $r(ab) = r(a)r(b)$.

Решење. 1) Приметимо да је $(ab)^{[r(a),r(b)]} = a^{[r(a),r(b)]}b^{[r(a),r(b)]} = ee = e$, где прва једнакост важи због комутативности, а друга јер $r(a) \mid [r(a), r(b)]$ и $r(b) \mid [r(a), r(b)]$. Дакле, $r(ab) \mid [r(a), r(b)]$.

2) Претпоставимо да је $\langle a\rangle\langle\lfloor\rangle = \langle\lceil\rangle$. Према претходном делу $r(ab) \mid [r(a), r(b)]$. Са друге стране $e = (ab)^{r(ab)} = a^{r(ab)}b^{r(ab)}$, због комутативности. Одавде је $a^{r(ab)} = b^{-r(ab)}$. Како лева страна ове једнакости припада $\langle a\rangle$, а десна $\langle b\rangle$, то уочени елемент $a^{r(ab)} = b^{-r(ab)}$ припада $\langle a\rangle \cap \langle b\rangle = \langle e\rangle$, одакле је $a^{r(ab)} = b^{-r(ab)} = e$. Зато $r(a) \mid r(ab)$ и $r(b) \mid r(ab)$, па и $[r(a), r(b)] \mid r(ab)$.

3) Нека је $(r(a), r(b)) = 1$. Према Лагранжовој теореми $|\langle a\rangle \cap \langle b\rangle| \mid |\langle a\rangle|, |\langle b\rangle|$, тј. $|\langle a\rangle \cap \langle b\rangle| \mid r(a), r(b)$. Према томе $|\langle a\rangle \cap \langle b\rangle| \mid (r(a), r(b)) = 1$, па је $|\langle a\rangle \cap \langle b\rangle| = 1$, одакле је $\langle a\rangle \cap \langle b\rangle = \langle e\rangle$. Према претхосном делу је $r(ab) = [r(a), r(b)] = r(a)r(b)$, јер $(r(a), r(b)) = 1$. □

44. У групи $\mathrm{GL}_2(\mathsf{Q})$ уочимо $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ и $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Израчунати $r(a)$, $r(b)$ и $r(ab)$.

Решење. Приметимо да је $a^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, одакле је $a^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Дакле, $a, a^2 \neq E$ и $r(a) \mid 4$, па закључујемо $r(a) = 4$.

Даље је $b^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ и $b^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, одакле је $r(b) = 3$.

$ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Индукцијом доказујемо да је $(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, за $n \geq 1$. За $n = 1$, тврђење очигледно важи. Претпоставимо да је $(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, тада је $(ab)^{n+1} = (ab)^n(ab) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$. Дакле, $(ab)^n \neq E$, за $n \geq 1$, па је $r(ab) = \aleph_0$. □

45.

1) Сви елементи, сем 0, у Z су бесконачног реда.

2) Доказати да $(\mathsf{Q}_0, \cdot, ^{-1}, 1)$ није циклична, где је $\mathsf{Q}_0 = \mathsf{Q} \setminus \{0\}$.

Решење. 1) Нека је $m \in \mathsf{Z}$, $m \neq 0$. Како не постоји позитиван природан број n такав да је $nm = 0$, то је $r(m) = \aleph_0$.

2) Приметите да је $r(-1) = 2$. Ако би Q_0 била циклична, како је бесконачна, морала би бити изоморфна Z. Како изоморфизми чувају редове, то би значило да у Z постоји елемент реда 2, што није тачно према 1). □

Симетрична група

Нека је X непразан скуп и нека је $\mathsf{S}_X = \left\{ f \mid X \xrightarrow[\text{на}]{\text{1-1}} X \right\}$. Тада је $\mathbb{S}_X = (\mathsf{S}_X, \circ, ^{-1}, \mathrm{id}_X)$ група коју зовемо *симетрична група скупа* X или *група пермутација скупа* X. Група S_X је још означава и са $\mathrm{Sym}(X)$.

46. Ако је $|X| = |Y|$, тада је $\mathsf{S}_X \cong \mathsf{S}_Y$.

Решење. Како је $|X| = |Y|$, то постоји бијекција $\phi : X \longrightarrow Y$. Дефинишимо пресликавање $\phi_* : \mathsf{S}_X \longrightarrow \mathsf{S}_Y$ са: за $f \in \mathsf{S}_X$, $\phi_*(f) = \phi f \phi^{-1}$. Јасно је да $\phi_*(f) \in \mathsf{S}_Y$. Тврдимо да је ϕ_* изоморфизам група.

Ако је $\phi_*(f) = \phi_*(g)$, тј. $\phi f \phi^{-1} = \phi g \phi^{-1}$, тада је $f = g$, јер су све функције бијекције, па је дозвољено њиово скраћивање и са леве и са десне стране. Дакле, ϕ_* је 1-1.

Ако је $h \in \mathsf{S}_Y$, тада је $\phi^{-1} h \phi \in \mathsf{S}_X$ и $\phi_*(\phi^{-1} h \phi) = \phi\phi^{-1} h \phi\phi^{-1} = h$, па је ϕ_* на.

Коначно, $\phi_*(fg) = \phi f g \phi^{-1} = \phi f \phi^{-1} \phi g \phi^{-1} = \phi_*(f)\phi_*(g)$, одакле је ϕ_* хомоморфизам. □

Коментар Ако је $|X| = n$, тада је према претходном задатку $\mathsf{S}_X \cong \mathsf{S}_{\{1,2,\ldots,n\}}$, па је довољно све радити у $\mathsf{S}_{\{1,2,\ldots,n\}}$, а њу краће означавамо са S_n.

47. $|\mathsf{S}_n| = n!$. Специјално, за све $f \in \mathsf{S}_n$ важи $f^{n!} = \mathrm{id}$.

Решење. Одредити $|\mathsf{S}_n|$ је заправо питање колико има пермутација скупа $\{1, 2, \ldots, n\}$. 1 можемо пресликати у неки од n елемената, па онда 2 можемо пресликати у неки од преосталих $n-1$, 3 у неки од преосталих $n-2$, итд. Дакле, закључујемо да имамо $n!$ пермутација уоченог скупа. □

48. Ако $m \leq n$, тада се S_m на природан начин утапа у S_n. Дакле, можемо сматрати $\mathsf{S}_m \leq \mathsf{S}_n$.

Решење. Нека је $m \leq n$. Дефинишимо пресликавања $i : \mathsf{S}_m \longrightarrow \mathsf{S}_n$, са: за $f \in \mathsf{S}_m$ и $x \in \{1, 2, \ldots, n\}$

$$i(f)(x) = \begin{cases} f(x) & 1 \leq x \leq m \\ x & m < x \leq n \end{cases}.$$

Лако се види да $i(f) \in \mathsf{S}_n$, и доказујемо да је i мономорфизам.

Ако је $i(f) = i(g)$. Тада је за $1 \leq x \leq m$: $f(x) = i(f)(x) = i(g)(x) = g(x)$, одакле следи $f = g$, па је i 1-1.

Доказујемо да је $i(fg) = i(f)i(g)$. За $m < x \leq n$ је $i(fg)(x) = x = i(f)(x) = i(f)(i(g)(x)) = (i(f)i(g))(x)$. За $1 \leq x \leq m$ најпре приметимо да је $1 \leq g(x) \leq m$, одакле је $i(fg)(x) = (fg)(x) = f(g(x)) = i(f)(g(x)) = i(f)(i(g)(x)) = (i(f)i(g))(x)$. Дакле, $i(fg) = i(f)i(g)$. □

49. У S_5 су дате пермутације $f : \begin{pmatrix} 1&2&3&4&5 \\ 3&1&2&5&4 \end{pmatrix}$ и $g : \begin{pmatrix} 1&2&3&4&5 \\ 2&3&5&1&4 \end{pmatrix}$. Израчунати fg, gf, f^{-1} и $(fg)^{-1}$.

Решење. Видимо:

$$\begin{array}{lllll} 1 \overset{g}{\mapsto} 2 \overset{f}{\mapsto} 1 \\ 2 \overset{g}{\mapsto} 3 \overset{f}{\mapsto} 2 \\ 3 \overset{g}{\mapsto} 5 \overset{f}{\mapsto} 4 \\ 4 \overset{g}{\mapsto} 1 \overset{f}{\mapsto} 3 \\ 5 \overset{g}{\mapsto} 4 \overset{f}{\mapsto} 5 \end{array} \quad \text{и} \quad \begin{array}{lllll} 1 \overset{f}{\mapsto} 3 \overset{g}{\mapsto} 5 \\ 2 \overset{f}{\mapsto} 1 \overset{g}{\mapsto} 2 \\ 3 \overset{f}{\mapsto} 2 \overset{g}{\mapsto} 3 \\ 4 \overset{f}{\mapsto} 5 \overset{g}{\mapsto} 4 \\ 5 \overset{f}{\mapsto} 4 \overset{g}{\mapsto} 1 \end{array}$$

одакле је $fg : \begin{pmatrix} 1&2&3&4&5 \\ 1&2&4&3&5 \end{pmatrix}$ и $gf : \begin{pmatrix} 1&2&3&4&5 \\ 5&2&3&4&1 \end{pmatrix}$. Такође, јасно је да $f^{-1} : \begin{pmatrix} 1&2&3&4&5 \\ 2&3&1&5&4 \end{pmatrix}$ и $(fg)^{-1} : \begin{pmatrix} 1&2&3&4&5 \\ 1&2&4&3&5 \end{pmatrix}$. □

Дисјунктне пермутације Кажемо да су пермутације $f, g \in \mathsf{S}_X$ дисјунктне ако за свако $x \in X$ важи: $f(x) = x$ или $g(x) = x$.

50. Ако су $f, g \in \mathsf{S}_X$ дисјунктне пермутације, доказати $fg = gf$.

Решење. Нека је $x \in X$ произвољно. Доказаћемо да је $fg(x) = gf(x)$. Како су f, g дисјунктне, важи један од три случаја:

1° $f(x) = x$ и $g(x) = x$. Тада је $fg(x) = f(g(x)) = f(x) = x = g(x) = g(f(x)) = gf(x)$.

2° $f(x) = x$ и $g(x) \neq x$. Како је g 1-1 и како је $g(x) \neq x$, то је $g(g(x)) \neq g(x)$, па због претпоставке дисјунктности мора бити $f(g(x)) = g(x)$. тада је $fg(x) = f(g(x)) = g(x) = g(f(x)) = gf(x)$.

3° $f(x) \neq x$ и $g(x) = x$. Како је f 1-1 и како је $f(x) \neq x$, то је $f(f(x)) \neq f(x)$, па због претпоставке дисјунктности мора бити $g(f(x)) = f(x)$. тада је $fg(x) = f(g(x)) = f(x) = g(f(x)) = gf(x)$.

□

Нека је $f \in \mathsf{S}_n$ фиксирана пермутација. На скупу $[n] = \{1, 2, \ldots, n\}$ дефинишемо релацију $\sim_f$ са: $a \sim_f b$ акко $(\exists k \geq 1)\ f^k(a) = b$.

51. $\sim_f$ је релација еквиваленције на $[n]$.

Решење. Сетимо се да је $f^{n!} = \mathrm{id}$, па је $f^{n!}(a) = \mathrm{id}(a) = a$, одакле је $a \sim_f a$, што доказује рефлексивност. Претпоставимо да је $a \sim_f b$. Претпостављајући да $a \neq b$ можемо закључити да постоји $k < n!$ такав да $f^k(a) = b$. Међутим тада је $f^{n!-k}(b) = a$, па је $b \sim_f a$, што доказује симетричност. Коначно, ако је $a \sim_f b$ и $b \sim_f c$, тада је $f^k(a) = b$ и $f^l(b) = c$, па је $f^{k+l}(a) = c$, одакле је $a \sim_f c$, тј. важи транзитивност. □

Циклична пермутација или циклус $f \in \mathsf{S}_n$ је циклична пермутација или циклус ако највише једна $\sim_f$-класа еквиваленција има више од једног елемента.

52. Ако су све $\sim_f$ класе једночлане, тада је $f = \mathrm{id}$. За id кажемо да је празан циклус и означавамо га $\lfloor\rfloor$.

Решење. Нека је $a \in [n]$ произвољан елемент. Приметимо да је $a/\sim_f = \{f^k(a) \mid k \leq 1\}$, док је са друге стране, према претпоставци, $a/\sim_f = \{a\}$. Специјално то значи да је $f(a) = a$, па како је a било произвољно, закључујемо да је $f = \mathrm{id}$. □

53. Нека су $f \in \mathsf{S}_n$ и $a \in [n]$ произвољни. Дефинишемо f_a са:

$$f_a(x) = \begin{cases} f(x) & x \in a/\sim_f \\ x & \text{иначе} \end{cases}.$$

Тада је f_a циклична пермутација.

Решење. Приметимо најпре да $f_a \in \mathsf{S}_n$. Заиста, како је класа $a/\sim_f$ затворена за пермутовање са f, то је f_a пермутација која $a/\sim_f$ пермутује као и f, док фиксира све остале елементе.

Доказујемо да је f_a циклична пермутација, тј. да релација $\sim_{f_a}$ има највише једну вишечлану класу. По дефиницији f_a, за све $x \notin a/\sim_f$ важи да је $x/\sim_{f_a} = \{x\}$ једночлана класа. Тврдимо: ако $x \in a/\sim_f$, тада је $x/\sim_{f_a} = a/\sim_{f_a}$, одакле следи да је $a/\sim_{f_a}$ једина (можда) вишечлана класа. Довољно је да докажемо $a \sim_{f_a} x$. Како је $a \sim_f x$, то постоји $k \geq 1$ такав да $f^k(a) = x$. Индукцијом по i доказујемо да $f^i(a) = f_a^i(a)$. Заиста, за $i = 1$, $f(a) = f_a(a)$, јер $a \in a/\sim_f$. Ако претпоставимо да $f^i(a) = f_a^i(a)$, тада закључујемо да $f_a^i(a) \in a/\sim_f$, па је $f^{i+1}(a) = f(f^i(a)) = f(f_a^i(a)) = f_a(f_a^i(a)) = f_a^{i+1}(a)$, што смо и желели да докажемо.

Дакле, $f_a^k(a) = f^k(a) = x$, па заиста важи $a \sim_{f_a} x$. □

54. Нека су $f \in \mathsf{S}_n$ и $a, b \in [n]$ произвољни. Тада су цикличне пермутације f_a и f_b или једнаке (ако $a \sim_f b$) или дисјунктне (ако $a \not\sim_f b$).

Решење. Ако $a \sim_f b$, тада је $a/\sim_f = b/\sim_f$, одакле је јасно да $f_a = f_b$.

Ако $a \not\sim_f b$, тада $a/\sim_f \cap b/\sim_f = \emptyset$. Тада за све $x \in [n]$ важи: $x \notin a/\sim_f$ или $x \notin b/\sim_f$, одакле следи $f_a(x) = x$ или $f_b(x) = x$. Према томе, f_a и f_b су дисјунктне. □

55. Нека је $f = \begin{pmatrix} 1&2&3&4&5&6&7&8&9 \\ 4&5&8&7&9&2&1&3&6 \end{pmatrix} \in \mathsf{S}_9$. Колико класа има $\sim_f$, и за сваку класу записати одговарајућу цикличну пермутацију.

Решење. Како $1 \overset{f}{\mapsto} 4 \overset{f}{\mapsto} 7 \overset{f}{\mapsto} 1$, $2 \overset{f}{\mapsto} 5 \overset{f}{\mapsto} 9 \overset{f}{\mapsto} 6 \overset{f}{\mapsto} 2$ и $3 \overset{f}{\mapsto} 8 \overset{f}{\mapsto} 3$, то имамо три $\sim_f$ класе: $1/\sim_f = \{1,4,7\}$, $2/\sim_f = \{2,5,9,6\}$ и $3/\sim_f = \{3,8\}$. Одговарајуће цикличне пермутације су:

$$f_1 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 4\,2\,3\,7\,5\,6\,1\,8\,9 \end{pmatrix}, \qquad f_2 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 1\,5\,3\,4\,9\,2\,7\,8\,6 \end{pmatrix}, \qquad f_3 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 1\,2\,8\,4\,5\,6\,7\,3\,9 \end{pmatrix}.$$

□

Коментар Ако је $f \neq \lfloor\rceil$ циклична пермутација, ако је $a/\sim_f$ одговарајућа једина вишечлана класа, и ако је k најмањи позитиван природан број такав да $f^k(a) = a$, онда се циклус f записује са: $\lfloor a, f(a), f^2(a), \ldots, f^{k-1}(a)\rceil$. У претходном задатку $f_1 = \lfloor 1,4,7\rceil$, $f_2 = \lfloor 2,5,9,6\rceil$, $f_3 = \lfloor 3,8\rceil$. Приметите ако је $a \sim_f b$ и $f^i(a) = b$, тада је k и најмањи позитиван природан број такав да је $f^k(b) = b$ (Проверити!) и $\lfloor a, f(a), f^2(a), \ldots, f^{k-1}(a)\rceil = \lfloor b, f(b), f^2(b), \ldots, f^{k-1}(b)\rceil = \lfloor f^i(a), f^{i+1}(a), f^{i+2}(a), \ldots, f^{i+k-1}(a)\rceil$. У претходном задатку $f_1 = \lfloor 1,4,7\rceil = \lfloor 4,7,1\rceil = \lfloor 7,1,4\rceil$, $f_2 = \lfloor 2,5,9,6\rceil = \lfloor 5,9,6,2\rceil = \lfloor 9,6,2,5\rceil = \lfloor 6,2,5,9\rceil$, $f_3 = \lfloor 3,8\rceil = \lfloor 8,3\rceil$.

56. Нека је $f \in \mathsf{S}_n$ произвољна пермутација, и нека су $a_1, a_2, \ldots, a_k \in [n]$ представници свих $\sim_f$-класа еквиваленције. Тада је $f = f_{a_1} f_{a_2} \ldots f_{a_k}$.

Решење. Доказаћемо да је за све $x \in [n]$: $f(x) = f_{a_1} f_{a_2} \ldots f_{a_k}(x)$. Нека је $x \in [n]$ произвољно и узмимо $x \in a_i/\sim_f$ (приметите да свако $x \in [n]$ припада тачно једној $\sim_f$-класи). Тада је $f(x) = f_{a_i}(x)$, $f_{a_j}(x) = x$ за $j \neq i$, и како f_{a_i} комутира са свим f_{a_j} за $j \neq i$, јер су дисјунктне, имамо: $f_{a_1} f_{a_2} \ldots f_{a_k}(x) = f_{a_i} f_{a_1} \ldots f_{a_{i-1}} f_{a_{i+1}} \ldots f_{a_k}(x) = f_{a_i} f_{a_1} \ldots f_{a_{i-1}} f_{a_{i+1}} \ldots f_{a_{k-1}}(x) = f_{a_i} f_{a_1} \ldots f_{a_{i-1}} f_{a_{i+1}} \ldots f_{a_{k-2}}(x) = \ldots = f_{a_i}(x)$, што смо желели да докажемо. □

Циклусна декомпозиција Декомпозиција пермутације f у производ дисјунктних циклуса из претходног задатка се зове циклусна декомпозиција.

57.

1) Доказати да је $\lfloor a_1, a_2, \ldots, a_{k-1}, a_k\rceil^{-1} = \lfloor a_k, a_{k-1}, \ldots, a_2, a_1\rceil$.

2) Доказати да је $f\lfloor a_1, a_2, \ldots, a_{k-1}, a_k\rceil f^{-1} = \lfloor f(a_1), f(a_2), \ldots, f(a_{k-1}), f(a_k)\rceil$.

Решење. 1) Означимо $f = \lfloor a_1, a_2, \ldots, a_{k-1}, a_k\rceil$ и $g = \lfloor a_k, a_{k-1}, \ldots, a_2, a_1\rceil$. Нека је $x \in [n]$. Ако $x \notin \{a_1, a_2, \ldots a_k\}$, тада је $f(x) = x$, па и $f^{-1}(x) = x$, и $g(x) = x$. Ако је $x = a_i$, за $1 < i \leq k$, тада је $f(a_{i-1}) = a_i$, па је $f^{-1}(a_i) = a_{i-1}$, и $g(a_i) = a_{i-1}$. Коначно ако је $x = a_1$, тада је $f(a_k) = a_1$, па је $f^{-1}(a_1) = a_k$, и $g(a_1) = a_k$.

2) Означимо $g = \lfloor a_1, a_2, \ldots, a_{k-1}, a_k\rceil$ и $h = \lfloor f(a_1), f(a_2), \ldots, f(a_{k-1}), f(a_k)\rceil$. Нека $x \in [n]$. Ако $x \notin \{f(a_1), \ldots, f(a_k)\}$, тада $f^{-1}(x) \notin \{a_1, \ldots, a_k\}$, па је $fgf^{-1}(x) = f(g(f^{-1}(x))) = f(f^{-1}(x)) = x$, и $h(x) = x$. Ако је $x = f(a_i)$, $1 \leq i < k$, тада је $fgf^{-1}(x) = fgf^{-1}(f(a_i)) = fg(a_i) = f(a_{i+1})$, и $h(x) = h(f(a_i)) = f(a_{i+1})$. Коначно ако је $x = f(a_k)$, тада је $fgf^{-1}(x) = fgf^{-1}(f(a_k)) = fg(a_k) = f(a_1)$, и $h(x) = h(f(a_k)) = f(a_1)$. □

58.

1) Ред цикличне пермутације је једнак њеној дужини: $r(\lfloor a_0, a_1, \ldots, a_{k-1}\rceil) = k$.

2) Ако су пермутације f и g дисјунктне, тада је $r(fg) = \text{НЗС}(r(f), r(g))$.

3) Ако је $f = f_1 f_2 \ldots f_k$ циклична декомпозиција пермутације f, тада је $r(f) = \text{НЗС}(r(f_1), r(f_2), \ldots, r(f_k))$.

Решење. 1) Означимо са $f = \lfloor a_0, a_1, \ldots, a_{k-1} \rceil$. Индукцијом по $i \geq 1$ лако се може доказати да је $f^i(a_j) = a_{i+j \mod k}$. Одавде закључујемо да је k најмањи позитиван природан број такав да $f^k = \lfloor \rceil$, одакле је $r(f) = k$.

2) Означимо $r(f) = k$, $r(g) = l$. Због дисјунктности је $(fg)^{[k,l]} = f^{[k,l]} g^{[k,l]} = \lfloor \rceil \lfloor \rceil = \lfloor \rceil$, јер $k, l \mid [k,l]$. Дакле, $r(fg) \mid [k,l]$. Са друге стране $\lfloor \rceil = (fg)^{r(fg)} = f^{r(fg)} g^{r(fg)}$, одакле је $f^{r(fg)} = g^{-r(fg)}$. Тврдимо да је $f^{r(fg)} = \lfloor \rceil$. Нека $x \in [n]$. Ако $f(x) = x$, тада је и $f^{r(fg)}(x) = x$. Ако је $f(x) \neq x$, тада је $g(x) = x$ (због дисјунктности), па је $g^{-r(fg)}(x) = x$, и како је $f^{r(fg)} = g^{-r(fg)}$, то је $f^{r(fg)}(x) = x$. Дакле, $\lfloor \rceil = f^{r(fg)} = g^{-r(fg)}$, одакле $k, l \mid r(fg)$, па и $[k,l] \mid r(fg)$.

3) Следи из 1) и 2). □

59. Који се природни бројеви јављају као редови елемената у групи S_8? Дати пример елемента максималног реда.

Решење. Свака $f \in \mathsf{S}_8$ има циклусну декомпозицију. Према претходном задатку ред зависи само од дужина циклуса у циклусној декомпозицији, па је довољно описати које су могуће дужине циклуса у циклусној декомпозицији.

Сваки елемент из [8] није фиксиран са највише једним циклусом из циклусне декомпозиције, одакле закључујемо да је збир дужина циклуса у циклусној декомпозицији највише 8 (ако посматрамо и циклусе дужине 1, можемо да претпоставимо у збиру дужине циклуса дају тачно 8). Сви начини да 8 запишемо као збир позитивних природних бројева су: $8 = 7+1 = 6+2 = 6+1+1 = 5+3 = 5+2+1 = 5+1+1+1 = 4+4 = 4+3+1 = 4+2+2 = 4+2+1+1 = 3+3+2 = 3+3+1+1 = 3+2+2+1 = 3+2+1+1+1 = 3+1+1+1+1+1 = 2+2+2+2 = 2+2+2+1+1 = 2+2+1+1+1+1 = 2+1+1+1+1+1+1 = 1+1+1+1+1+1+1+1$. НЗСови сабирака из претходних збирова су редом: $8, 7, 6, 6, 15, 10, 5, 4, 12, 4, 4, 6, 3, 6, 6, 3, 2, 2, 2, 2, 1$, што су уједно и све могућности за ред неког елемента у S_8. Највећи могући ред је 15, који добијамо ако је f у циклусној декомпозицији производ једног 5-цкла и једног 3-цикла, нпр. ако је $f = \lfloor 1,2,3,4,5 \rceil \lfloor 6,7,8 \rceil$. □

60. Израчунати редове елемената ... у групи ...

Решење. □

61.

1) Доказати да је $\lfloor a_1, a_2, \ldots, a_k \rceil = \lfloor a_1, a_2, \ldots, a_i \rceil \lfloor a_i, a_{i+1}, \ldots, a_k \rceil$.

2) Доказати да је $\lfloor a_1 a_2, \ldots, a_k \rceil = \lfloor a_1, a_2 \rceil \lfloor a_2, a_3 \rceil \lfloor a_3, a_4 \rceil \ldots \lfloor a_{k-1}, a_k \rceil$.

3) Ако је $T_0 = \{\lfloor a, b \rceil \mid a, b \in [n],\ a < b\}$, доказати да је $\mathsf{S}_n = \langle T_0 \rangle$.

Решење. 1) Нека $x \in [n]$. Ако $x \notin \{a_1, \ldots, a_k\}$, тада очигледно обе стране једнакости фиксирају x. Ако $x = a_j$, $1 \leq j < i$, тада лева страна једнакости слика x у a_{j+1}, а такође $\lfloor a_1, a_2, \ldots, a_i \rceil \lfloor a_i, a_{i+1}, \ldots, a_k \rceil (a_j) = \lfloor a_1, a_2, \ldots, a_i \rceil (a_j) = a_{j+1}$. Ако $x = a_j$, $i \leq j < k$, тада лева страна једнакости слика x у a_{j+1}, а такође $\lfloor a_1, a_2, \ldots, a_i \rceil \lfloor a_i, a_{i+1}, \ldots, a_k \rceil (a_j) = \lfloor a_1, a_2, \ldots, a_i \rceil (a_{j+1}) = a_{j+1}$, јер $j+1 > i$. Коначно, ако $x = a_k$, тада лева страна једнакости слика x у a_1, а такође $\lfloor a_1, a_2, \ldots, a_i \rceil \lfloor a_i, a_{i+1}, \ldots, a_k \rceil (a_k) = \lfloor a_1, a_2, \ldots, a_i \rceil (a_i) = a_1$.

2) следи вишеструком применом 1).

3) Приметимо да је $\lfloor a, b \rceil = \lfloor b, a \rceil$. Како се свака пермутација може записати као производ дисјунктних циклуса, како се према 2) сваки циклус може записати као производ транспозиција, то се и свака пермутација може записати као производ транспозиција. Када приметимо и да је $\lfloor a, b \rceil = \lfloor b, a \rceil$, то добијамо $\langle T_0 \rangle = \mathsf{S}_n$. □

62.

1) Нека је $f = ts$ производ две транспозиције и $s(a) \neq a$. Тада је или $f = \lfloor\rceil$ или је $f = t's'$ производ две транспозиције такве да $t'(a) \neq a$ и $s(a) = a$.

2) Нека је $\lfloor\rceil = t_1t_2, \dots t_k$ производ транспозиција. Тада се $\lfloor\rceil$ може записати и као производ $k-2$ транспозиције.

3) Нека је $\lfloor\rceil = t_1t_2, \dots t_k$ производ транспозиција. Тада је k паран број.

4) Нека је $f = t_1t_2 \dots t_k = s_1s_2 \dots s_l$ записана као два производа транспозиција. Тада је $k = l \mod 2$.

Решење. 1) Нека је $s = \lfloor a, b\rceil$ и нека је $t = \lfloor c, d\rceil$. Имамо четири случаја:

1° $\{a, b\} = \{c, d\}$. Тада је $f = ts = \lfloor a, b\rceil\lfloor a, b\rceil = \lfloor\rceil$.

2° $\{a, b\} \cap \{c, d\} = \{a\}$, нпр. $c = a$. Тада је $f = ts = \lfloor a, d\rceil\lfloor a, b\rceil = \lfloor d, a\rceil\lfloor a, b\rceil = \lfloor d, a, b\rceil = \lfloor a, b, d\rceil = \lfloor a, b\rceil\lfloor b, d\rceil$; узмимо $t' = \lfloor a, b\rceil$ и $s' = \lfloor b, d\rceil$.

3° $\{a, b\} \cap \{c, d\} = \{b\}$, нпр. $c = b$. Тада је $f = ts = \lfloor b, d\rceil\lfloor a, b\rceil = \lfloor d, b\rceil\lfloor b, a\rceil = \lfloor d, b, a\rceil = \lfloor a, d, b\rceil = \lfloor a, d\rceil\lfloor d, b\rceil$; узмимо $t' = \lfloor a, d\rceil$ и $s' = \lfloor d, b\rceil$.

4° $\{a, b\} \cap \{c, d\} = \emptyset$. Тада је, због дисјунктности, $f = ts = \lfloor c, d\rceil\lfloor a, b\rceil = \lfloor a, b\rceil\lfloor c, d\rceil$; узмимо $t' = \lfloor a, b\rceil$ и $s' = \lfloor c, d\rceil$.

2) Претпоставимо да је $\lfloor\rceil = t_1t_2 \dots t_k$ производ транспозиција и да је $t_k = \lfloor a, b\rceil$, тј. $t_k(a) \neq a$. Јасно је да је $k > 1$, јер $\lfloor\rceil$ није једнака транспозицији. Претпоставимо супротно да се $\lfloor\rceil$ не може записати као производ $k-2$ транспозиције.

Тврђење. За све i, $0 \leq i \leq k-1$, $\lfloor\rceil$ се може записати као производ k транспозиција $s_1s_2 \dots s_k$ таквих да $s_{k-i}(a) \neq a$ и $s_j(a) = a$, за $j > k - i$.

Доказ. Доказ изводимо индукцијом по i. За $i = 0$ тврђење следи према полазној претпоставци. Претпоставимо да је $\lfloor\rceil = s_1s_2 \dots s_k$, тако да $s_{k-i}(a) \neq a$ и $s_j(a) = a$, за $j > k - i$. Докажимо да тврђење важи за $i + 1$. Уочимо $s_{k-i-1}s_{k-i}$. $s_{k-i-1}s_{k-i} \neq \lfloor\rceil$, јер би у супротном $\lfloor\rceil = s_1 \dots s_{k-i-2}s_{k-i+1} \dots s_k$ била записана као производ $k-2$ транспозиције. Према делу 1), можемо изабрати s'_{k-i-1} и s'_{k-i} такве да $s'_{k-i-1}s'_{k-i} = s_{k-i-1}s_{k-i}$, $s'_{k-i-1}(a) \neq a$ и $s_{k-i}(a) = a$. Сада је $\lfloor\rceil = s_1 \dots s_{k-i-1}s_{k-i} \dots s_k = s_1 \dots s'_{k-i-1}s'_{k-i} \dots s_k$, одакле следи доказ индукцијског корака. ■

Према тврђењу, за $i = k - 1$, имамо да је $\lfloor\rceil = s_1s_2 \dots s_k$, где $s_1(a) \neq a$ и $s_j(a) = a$, за $j > 1$. Тада пермутација на левој страни фиксира a, а пермутација на десној не фиксира, што је контрадикција.

3) Претпоставимо да можемо записати $\lfloor\rceil$ као производ k транспозиција. Тада пре 2) је можемо записати и као производ $k-2$ транспозиције, па поново према 2) и као производ $k-4$ транспозиције, итд. Ако је k непаран, добијамо да је $\lfloor\rceil$ једнак транспозицији, што није могуће. Према томе k је парно.

4) Нека је $f = t_1t_2 \dots t_k = s_1s_2 \dots s_l$ записан на два начина као производ транспозиција. Тада је $\lfloor\rceil = ff^{-1} = t_1t_2 \dots t_k(s_1s_2 \dots s_l)^{-1} = t_1t_2 \dots t_ks_l^{-1} \dots s_2^{-1}s_1^{-1} = t_1t_2 \dots t_ks_l \dots s_2s_1$ записана као производ $k + l$ транспозиција, па је према 3) $k + l$ парно, одакле је $k = l \mod 2$. □

Парност пермутације Ако је произвољна пермутација $f = t_1t_2 \dots t_k$ записана као производ транспозиција, тада дефинишемо њену *парност* да буде број $p(f) = (-1)^k$. Према претходном задатку, парност је добро дефинисано пресликавање $p : \mathsf{S}_n \longrightarrow \{-1, 1\}$. За пермутације парности 1 кажемо да су *парне*, а за пермутације парности -1 кажемо да су *непарне*.

63. Доказати:

1) $p(fg) = p(f)p(g)$.

2) $p(f^{-1}) = p(f)$.

3) $p(gfg^{-1}) = p(f)$.

4) $p(\lfloor a_1, a_2, \ldots, a_k \rceil) = (-1)^{k-1}$.

5) Ако је $f = f_1 f_2 \ldots f_k$ циклусна декомпозиција, тада је $p(f) = (-1)^{r(f_1)+r(f_2)+\ldots+r(f_k)-k}$.

Решење. Нека су $f = t_1 t_2 \ldots t_k$ и $g = s_1 s_2 \ldots s_l$ записи пермутација f и g као производи транспозиција. Тада је $p(f) = (-1)^k$ и $p(g) = (-1)^l$. Како је $fg = t_1 t_2 \ldots t_k s_1 s_2 \ldots s_l$ и $f^{-1} = (t_1 t_2 \ldots t_k)^{-1} = t_k^{-1} \ldots t_2^{-1} t_1^{-1} = t_k \ldots t_2 t_1$, то је $p(fg) = (-1)^{k+l} = (-1)^k (-1)^l = p(f)p(g)$ и $p(f^{-1}) = (-1)^k = p(f)$.

Даље је $p(gfg^{-1}) = p(g)p(f)p(g^{-1}) = p(g)p(f)p(g) = p(f)(p(g))^2 = p(f)$, јер је $(p(g))^2 = 1$.

$p(\lfloor a_1, a_2, \ldots, a_k \rceil) = (-1)^{k-1}$ следи из $\lfloor a_1, a_2, \ldots, a_k \rceil = \lfloor a_1, a_2 \rceil \lfloor a_2, a_3 \rceil \ldots \lfloor a_{k-1}, a_k \rceil$.

Коначно, 5) следи из 1) и 4). □

64. Израчунати парности пермутација ... у групи ...

Решење. □

Алтернирајућа група Нека је $\mathsf{A}_n = \{f \in \mathsf{S}_n \mid p(f) = 1\}$ скуп свих парних пермутација. Доказаћемо да је A_n подгрупа од S_n, коју зовемо *алтернирајућа група*.

65.

1) $\mathsf{A}_n \leq \mathsf{S}_n$.

2) $|\mathsf{S}_n : \mathsf{A}_n| = 2$.

3) $|\mathsf{A}_n| = n!/2$.

4) $\mathsf{A}_n \lhd \mathsf{S}_n$.

Решење. Према претходном задатку, ако $f, g \in \mathsf{A}_n$, тј. ако $p(f) = p(g) = 1$, тада је $p(fg^{-1}) = p(f)p(g^{-1}) = p(f)p(g) = 1$, одакле $fg^{-1} \in \mathsf{A}_n$, што доказује да је $\mathsf{A}_n \leq \mathsf{S}_n$. За $f \in \mathsf{A}_n$ и $g \in \mathsf{S}_n$ имамо да $p(gfg^{-1}) = p(f) = 1$, такође према претходном задатку, па $gfg^{-1} \in \mathsf{A}_n$, што доказује да је $\mathsf{A}_n \lhd \mathsf{S}_n$.

Изаберимо $f \notin \mathsf{A}_n$ (такво f постоји – нпр. било која транспозиција). Тада је $p(f) = -1$. Доказаћемо да је $\mathsf{S}_n = \mathsf{A}_n \sqcup f\mathsf{A}_n$, одакле следи да A_n има два косета, тј. $|\mathsf{S}_n : \mathsf{A}_n| = 2$. Како су све пермутације из A_n парне, и како је f непарна, то следи да су све пермутације из скупа $f\mathsf{A}_n$ непарне. Према томе $\mathsf{A}_n \cap f\mathsf{A}_n = \emptyset$, па остаје да докажемо да је $\mathsf{S}_n = \mathsf{A}_n \cup f\mathsf{A}_n$. Нека је $g \in \mathsf{S}_n$ произвољно. Ако је g парна, тада $g \in \mathsf{A}_n$. Ако је g непарна, како је $g = ff^{-1}g$, и како $p(f^{-1}g) = p(f^{-1})p(g) = p(f)p(g) = (-1) \cdot (-1) = 1$, то $f^{-1}g \in \mathsf{A}_n$, па $g \in f\mathsf{A}_n$.

Како је $2 = |\mathsf{S}_n : \mathsf{A}_n| = |\mathsf{S}_n|/|\mathsf{A}_n| = n!/|\mathsf{A}_n|$, одакле је $|\mathsf{A}_n| = n!/2$. □

66. Нека је пермутација $f \in \mathsf{A}_n$ таква да је $r(f) = 2$. Доказати да постоји пермутација $g \in \mathsf{S}_n$ таква да $g^2 = f$.

Решење. Уочимо најпре следеће: $\lfloor a,b,c,d\rceil^2 = \lfloor a,b,c,d\rceil\lfloor a,b,c,d\rceil = \lfloor a,c\rceil\lfloor b,d\rceil$.

Претпоставимо да је $f \in \mathsf{A}_n$ и запишимо циклусну декомпозицију $f = f_1 f_2 \dots f_k$. Како је $2 = r(f) = \text{НЗС}(r(f_1), r(f_2), \dots, r(f_k))$, одакле закључујемо да за све i важи $r(f_i) = 2$, тј. f_i су транспозиције. Како је f парна, то је k парно. Дакле, $f = \lfloor a_1,b_1\rceil\lfloor c_1,d_1\rceil\lfloor a_2,b_2\rceil\lfloor c_2,d_2\rceil\dots\lfloor a_l,b_l\rceil\lfloor c_l,d_l\rceil = \lfloor a_1,c_1,b_1,d_1\rceil^2\lfloor a_2,c_2,b_2,d_2\rceil^2\dots\lfloor a_l,c_l,b_l,d_l\rceil^2 = (\lfloor a_1,c_1,b_1,d_1\rceil\lfloor a_2,c_2,b_2,d_2\rceil\dots\lfloor a_l,c_l,b_l,d_l\rceil)^2$, због дисјунктоности. Сада узмимо $g = \lfloor a_1,c_1,b_1,d_1\rceil\lfloor a_2,c_2,b_2,d_2\rceil\dots\lfloor a_l,c_l,b_l,d_l\rceil$. □

67. Означимо са $T_0 = \{\lfloor a,b\rceil \mid a,b \in [n],\ a<b\}$; знамо $\mathsf{S}_n = \langle T_0\rangle$.

1) Доказати да $\mathsf{S}_n = \langle T_1\rangle$, где је $T_1 = \{\lfloor i,i+1\rceil \mid 1 \le i < n\}$.

2) Доказати да $\mathsf{S}_n = \langle T_2\rangle$, где је $T_2 = \{\lfloor 1,i\rceil \mid 1 < i \le n\}$.

3) Доказати да $\mathsf{S}_n = \langle T_3\rangle$, где се $T_3 = \{\lfloor 1,2\rceil, \lfloor 1,2,3,\dots,n\rceil\}$.

4) Доказати да $\mathsf{S}_n = \langle T_4\rangle$, где се $T_4 = \{\lfloor 1,2\rceil, \lfloor 2,3,4,\dots,n\rceil\}$.

Решење. 1) Нека је $\lfloor a,b\rceil \in T_0$ и $a<b$; нека је $b = a+k$. Ако је $k=1$, тада је $\lfloor a,b\rceil = \lfloor a,a+1\rceil \in T_1$. Ако је $k>1$ тада имамо:

$$\begin{aligned}
\lfloor a,b\rceil &= \lfloor a,a+k\rceil \\
&= \lfloor a,a+k\rceil\lfloor a,a+1,a+2,\dots,a+k\rceil\lfloor a,a+1,a+2,\dots,a+k\rceil^{-1} \\
&= \lfloor a,a+k\rceil\lfloor a+k,a,a+1,a+2,\dots,a+k-1\rceil\lfloor a+k,a+k-1,a+k-2,\dots,a\rceil \\
&= \lfloor a,a+k\rceil\lfloor a+k,a\rceil\lfloor a,a+1\rceil\lfloor a+1,a+2\rceil\dots\lfloor a+k-2,a+k-1\rceil \\
&\quad \lfloor a+k,a+k-1\rceil\lfloor a+k-1,a+k-2\rceil\dots\lfloor a+1,a\rceil \\
&= \lfloor a,a+1\rceil\lfloor a+1,a+2\rceil\dots\lfloor a+k-2,a+k-1\rceil \\
&\quad \lfloor a+k-1,a+k\rceil\lfloor a+k-2,a+k-1\rceil\dots\lfloor a,a+1\rceil \in \langle T_1\rangle
\end{aligned}$$

Доказали смо да $T_0 \subseteq \langle T_1\rangle$, одакле $\mathsf{S}_n = \langle T_0\rangle \le \langle T_1\rangle$, па је $\mathsf{S}_n = \langle T_1\rangle$.

2) Нека је $\lfloor i,i+1\rceil \in T_1$, $1 \le i < n$. Ако је $i=1$, тада је $\lfloor i,i+1\rceil = \lfloor 1,2\rceil \in T_2$. Ако је $i>1$ тада имамо: $\lfloor i,i+1\rceil = \lfloor 1,i\rceil\lfloor 1,i+1\rceil\lfloor 1,i\rceil \in \langle T_2\rangle$. Доказали смо да $T_1 \subseteq \langle T_2\rangle$, одакле $\mathsf{S}_n = \langle T_1\rangle \le \langle T_2\rangle$, па је $\mathsf{S}_n = \langle T_2\rangle$.

3) Нека је $\lfloor i,i+1\rceil \in T_1$, $1 \le i < n$. Ако је $i=1$, тада је $\lfloor i,i+1\rceil = \lfloor 1,2\rceil \in T_3$. Ако је $i>1$ тада имамо: $\lfloor i,i+1\rceil = \lfloor 1,2,3,\dots,n\rceil^{i-1}\lfloor 1,2\rceil\lfloor 1,2,3,\dots,n\rceil^{-(i-1)} \in \langle T_3\rangle$. Доказали смо да $T_1 \subseteq \langle T_3\rangle$, одакле $\mathsf{S}_n = \langle T_1\rangle \le \langle T_3\rangle$, па је $\mathsf{S}_n = \langle T_3\rangle$.

4) Приметимо само да је $\lfloor 1,2,3,\dots,n\rceil = \lfloor 1,2\rceil\lfloor 2,3,\dots,n\rceil \in \langle T_4\rangle$. Дакле, $T_3 \subseteq \langle T_4\rangle$, одакле $\mathsf{S}_n = \langle T_3\rangle \le \langle T_4\rangle$, па је $\mathsf{S}_n = \langle T_4\rangle$. □

68. За $n \ge 3$ доказати:

1) $A_n = \langle S_0\rangle$, где је $S_0 = \{\lfloor a,b,c\rceil \mid a,b,c \in [n],\ a<b<c\}$;

2) $A_n = \langle S_1\rangle$, где је $S_1 = \{\lfloor 1,2,i\rceil \mid 2 < i \le n\}$.

Решење. 1) Најпре ћемо доказати да се свака пермутација $f \in \mathsf{A}_n$ може записати као производ 3-циклова. Нека је $f = t_1 s_1 t_2 s_2 \dots t_k s_k$ производ транспозиција (парно много њих, јер $f \in \mathsf{A}_n$). Посматрајмо парове $t_i s_i$, за произвољно i. Нека је $t_i = \lfloor a,b\rceil$ и $s_i = \lfloor c,d\rceil$. Ако је $\{a,b\} = \{c,d\}$, тада $t_i s_i = \lfloor\rceil$ је празан циклус. Ако је $|\{a,b\} \cap \{c,d\}| = 1$, нпр. $a=c$, тада $t_i s_i = \lfloor a,b\rceil\lfloor a,d\rceil = \lfloor b,a\rceil\lfloor a,d\rceil = \lfloor b,a,d\rceil$ је 3-цикл. Коначно ако је $\{a,b\} \cap \{c,d\} = \emptyset$, тада $t_i s_i = \lfloor a,b\rceil\lfloor c,d\rceil = \lfloor a,b\rceil\lfloor b,c\rceil\lfloor b,c\rceil\lfloor c,d\rceil = \lfloor a,b,c\rceil\lfloor b,c,d\rceil$ производ два 3-цикла. Када у запису f као производ транспозиција одговарајуће парове транспозиција заменимо 3-цикловима добијамо да је f производ 3-циклова.

Нека су a,b,c различити елементи. Цикличним померањем циклуса $\lfloor a,b,c\rceil$ можемо претпоставити да је a најмањи међу њима. Ако је $b<c$, тада је $\lfloor a,b,c\rceil \in S_0$. Ако је $b>c$, тада

је $\lfloor a,b,c\rceil^{-1} = \lfloor c,b,a\rceil = \lfloor a,c,b\rceil \in S_0$. Дакле сваки 3-цикл или припада S_0 или његов инверз припада S_0, што завршава доказ тврђења.

2) Доказали смо да се свака пермутација може представити као производ транспозиција облика $\lfloor 1,i\rceil$, за $2 < i \leq n$. Ако $f \in \mathsf{A}_n$, тада у таквом представљању f има парно много транспозиција, тј. $f = \lfloor 1,a_1\rceil\lfloor 1,b_1\rceil\lfloor 1,a_2\rceil\lfloor 1,b_2\rceil \ldots \lfloor 1,a_k\rceil\lfloor 1,b_k\rceil$. Посматрајмо $\lfloor 1,a_i\rceil\lfloor 1,b_i\rceil$. Ако је $a_i = b_i$, тада је $\lfloor 1,a_i\rceil\lfloor 1,b_i\rceil = \lfloor\rceil$. Ако је $a_i \neq b_i = 2$, тада је $\lfloor 1,a_i\rceil\lfloor 1,b_i\rceil = \lfloor 1,a_i\rceil\lfloor 1,2\rceil = \lfloor a_i,1\rceil\lfloor 1,2\rceil = \lfloor a_i,1,2\rceil = \lfloor 1,2,a_i\rceil$. Ако је $b_i \neq a_i = 2$, тада је $\lfloor 1,a_i\rceil\lfloor 1,b_i\rceil = \lfloor 1,2\rceil\lfloor 1,b_i\rceil = \lfloor 2,1\rceil\lfloor 1,b_i\rceil = \lfloor 2,1,b_i\rceil = \lfloor 1,b_i,2\rceil = \lfloor 1,2,b_i\rceil^{-1}$. Ако је $a_i \neq b_i$, $a_i,b_i > 2$, тада је $\lfloor 1,a_i\rceil\lfloor 1,b_i\rceil = \lfloor 1,a_i\rceil\lfloor 1,2\rceil\lfloor 1,2\rceil\lfloor 1,b_i\rceil = \lfloor 1,2,a_i\rceil\lfloor 1,b_i,2 = \lfloor 1,2,a_i\rceil\lfloor 1,2,b_i\rceil^{-1}$. После замене узастопних парова, добијамо доказ тврђења. □

69. За $n \geq 5$ доказати да је $A_n = \langle S_2\rangle$, где је $S_2 = \{\lfloor a,b\rceil\lfloor c,d\rceil \mid a,b,c \in [n],\ \{a,b\} \cap \{c,d\} = \emptyset,\ a < b,\ c < d\}$. (Елементе скупа S_2 зовемо дупле транспозиције.)

Решење. Нека је $\lfloor a,b,c\rceil$ произвољан 3-цикл. Како је $n \geq 5$, можемо изабрати $d,e \notin \{a,b,c\}$. Тада је $\lfloor a,b,c\rceil = \lfloor a,b\rceil\lfloor b,c\rceil = \lfloor a,b\rceil\lfloor d,e\rceil\lfloor d,e\rceil\lfloor b,c\rceil$. Приметимо да $\lfloor a,b\rceil\lfloor d,e\rceil, \lfloor d,e\rceil\lfloor b,c\rceil \in S_2$, па $\lfloor a,b,c\rceil \in \langle S_2\rangle$. Дакле, $S_0 \in \langle S_2\rangle$, па $\mathsf{A}_n = \langle S_0\rangle \leq \langle S_2\rangle$, одакле $\mathsf{A}_n = \langle S_2\rangle$. □

Нормалне подгрупе и количничке групе

Унутрашњи аутоморфизам За $a \in G$, дефинишемо пресликавање $\sigma_a : G \longrightarrow G$ са $\sigma_a(x) = a^{-1}xa$. σ_a је аутоморфизам групе G, који зовемо унутрашњи аутоморфизам групе G. Скуп свих унутрашњих аутоморфизама означавамо са $\mathrm{Inn}(G) = \{\sigma_a \mid a \in G\}$.

Нормална подгрупа Подгрупа $H \leq G$ је нормална, у ознаци $H \triangleleft G$, ако је инваријантна у односу на све унутрашње аутоморфизме, тј. за све $a \in G$ важи $\sigma_a(H) = H$, или $aHa^{-1} = H$.

70. Нека је $H \leq G$. Следећи искази су еквивалентни:

1) $H \triangleleft G$;

2) за све $a \in G$ важи $aHa^{-1} \subseteq H$;

3) за све $a \in G$ и све $h \in H$ важи $aha^{-1} \in H$.

Решење. 1) $\Rightarrow$ 2) и 2) $\Rightarrow$ 3) је тривијално. Докажимо 3) $\Rightarrow$ 1). Претпоставимо да важи 3) и докажимо да за све $a \in G$ важи $aHa^{-1} = H$. Нека је $x \in aHa^{-1}$, тј. $x = aha^{-1}$, за неко $h \in H$. Тада је $x \in H$ према 3), што доказује $aHa^{-1} \subseteq H$. Нека сада $x \in H$. Тада, према 3), $a^{-1}xa = a^{-1}x(a^{-1}))^{-1} \in H$, тј. $a)^{-1}xa = h$, за неко $h \in H$. Даље је $x = aha^{-1} \in aHa^{-1}$, што доказује $H \subseteq aHa^{-1}$. □

71. Нека је $H \leq G$ индекса 2. Доказати да је $H \triangleleft G$.

Решење. Према Лагранжовој теореми H има само два лева косета: H и aH, за било које $a \notin H$, као и само два десна косета: H и Ha, за било које $a \notin H$. Када год $a \notin H$, имамо да је $G = H \sqcup aH = H \sqcup Ha$.

Нека је $a \in G$ произвољно. Ако $a \in H$, тада је $a^{-1}Ha \subseteq H$, јер је H подгрупа. Ако $a \notin H$, тада је $G = H \sqcup aH = H \sqcup Ha$, па је $H \setminus H = aH = Ha$, одакле је $a^{-1}Ha = H$, што завршава доказ да је H нормална. □

72.

1) Нека је $K \leq H \leq G$. Ако је $K \lhd G$, тада је $K \lhd H$.

2) Дати пример групе G и подгрупа H и K таквих да $K \lhd H \lhd G$, али $K \not\lhd G$.

Решење. 1) Нека су $h \in H$, $k \in K$ произвољни. Довољно је доказати да $hkh^{-1} \in K$. Међутим, како $h \in G$ и како $K \lhd G$, то тривијално важи.

2) Нека је $G = \mathsf{D}_4$. Уочимо $K = \{\varepsilon, \sigma\}$ и $H = \{\varepsilon, \sigma, \rho^2, \sigma\rho^2\}$. Тада је $K \leq H \leq G$ и више: K је индекса два у H и H је индекса два у G, па је $K \lhd H \lhd G$. Како је $\rho^{-1}\sigma\rho = \rho^{-1}\rho^3\sigma = \rho^2\sigma \notin K$, то $K \not\lhd G$. □

73. Нека су $H, K \leq G$.

1) Ако је $H \lhd G$ или $K \lhd G$, тада је $HK \leq G$.

2) Ако су $H, K \lhd G$, тада је $HK \lhd G$.

Решење. Претпоставимо нпр. да је $H \lhd G$. Тада је $HK = \bigcup_{k\in K} Hk = \bigcup_{k\in K} kH = KH$, где средња једнакост следи због нормалности H. Сада имамо $HKHK = HHKK = HK$ и $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$, одакле следи $HK \leq G$.

Ако $H, K \lhd G$, тада за све $g \in G$ имамо $gHK = HgK = HKg$, одакле прва једнакост важи због нормалности H, а друга због нормалности K, па је $HK \lhd G$. □

74. Нека је $H \lhd G$. Доказати да је $aH\,bH = abH$ и $(aH)^{-1} = a^{-1}H$. Ако је $aH = cH$ и $bH = dH$, тада је $abH = cdH$ и $a^{-1}H = c^{-1}H$.

Решење. Како је $b^{-1}Hb = H$, то је $bH = Hb$, па имамо $aH\,bH = aH\,Hb$. Како је $H\,H = H$, јер је H подгрупа, то је $aH\,bH = aHb$, па када поново приметимо $Hb = bH$, добијамо $aH\,bH = abH$. Слично, $(aH)^{-1} = H^{-1}a^{-1} = Ha^{-1}$, јер је H подгрупа, а онда је даље $(aH)^{-1} = a^{-1}H$, због нормалности.

Ако је $aH = cH$ и $bH = dH$, тада је $abH = aH\,bH = cH\,dH = cdH$, и $a^{-1}H = (aH)^{-1} = (cH)^{-1} = c^{-1}H$. □

Количничка група Ако је $H \lhd G$, тада је $(G/H, \cdot, ^{-1}, H)$ група, где је $G/H = \{aH \mid a \in G\}$, а $\cdot$ је дефинисано са: $aH \cdot bH = abH$, и $^{-1}$ је дефинисано са: $(aH)^{-1} = a^{-1}H$. Ред количничке групе G/H је једнак индексу $|G : H|$.

75.

1) Ако је G Абелова група, онда су све подгрупе од G нормалне.

2) Дати пример не-Абелове групе код које су све подгрупе нормалне.

Решење. Ако је G Абелова, $H \leq G$ и $a \in G$, тада је $aH = \{ah \mid h \in H\} = \{ha \mid h \in H\} = Ha$, одакле следи $H \lhd G$.

Уочимо скуп $\mathsf{K}_8 = \{1, -1, i, -i, j, -j, k, -k\}$ и операцију $\cdot$ на K_8 дефинисану таблицом:

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Дата операција је асоцијативна, а из таблице се лако види да је 1 неутрал за $\cdot$, и да сваки елемент има инверз. Групу K_8 зовемо *група кватерниона*. Лако можемо израчунати да је $r(-1) = 2$ и $r(i) = r(-i) = r(j) = r(-j) = r(k) = r(-k) = 4$.

Подгрупе групе кватерниона су: $\langle 1\rangle$, $\langle -1\rangle$, $\langle i\rangle$, $\langle j\rangle$, $\langle k\rangle$ и K_8, ово се лако да проверити, и лако се да проверити да су све оне нормалне. □

76. Доказати да је $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$.

Решење. Најпре докажимо да је $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$. Приметимо да је $\mathrm{id}_G = \sigma_e$, одакле $\mathrm{id}_G \in \mathrm{Inn}(G)$. Такође, $\sigma_a\sigma_b(x) = \sigma_a(bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \sigma_{ab}(x)$, одакле је $\sigma_a\sigma_b = \sigma_{ab} \in \mathrm{Inn}(G)$. Сада имамо и $\mathrm{id}_G = \sigma_e = \sigma_{aa^{-1}} = \sigma_a\sigma_{a^{-1}}$, одакле $\sigma_a^{-1} = \sigma_{a^{-1}} \in \mathrm{Inn}(G)$. Дакле, $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

За $f \in \mathrm{Aut}(G)$ имамо $f\sigma_a f^{-1}(x) = f(af^{-1}(x)a^{-1}) = f(a)f(f^{-1}(x))f(a)^{-1} = f(a)xf(a)^{-1} = \sigma_{f(a)}(x)$, одакле је $f\sigma_a f^{-1} = \sigma_{f(a)} \in \mathrm{Inn}(G)$. Дакле, $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$. □

Центар групе Центар групе G је $\mathrm{Z}(G) = \{a \in G \mid (\forall x \in G)\, ax = xa\}$, тј. скуп свих елемената који комутирају са свим елементима групе G. Приметите да је G Абелова акко је $\mathrm{Z}(G) = G$.

77.

1) $\mathrm{Z}(G) \leq G$.

2) $H \leq \mathrm{Z}(G)$ повлачи $H \triangleleft G$. Специјално, $\mathrm{Z}(G) \triangleleft G$.

Решење. Очигледно $e \in \mathrm{Z}(G)$. Ако $a \in \mathrm{Z}(G)$, тада за све $x \in G$ имамо $ax = xa$. Множећи ову једнакост са a^{-1} и са леве и са десне стране добијамо: $xa^{-1} = a^{-1}x$, за све $x \in G$, одакле $a^{-1} \in \mathrm{Z}(G)$. Коначно, ако $a, b \in \mathrm{Z}(G)$, за све $x \in G$, имамо $abx = axb = xab$, где прва једнакост важи из $b \in \mathrm{Z}(G)$, а друга из $a \in \mathrm{Z}(G)$. Дакле, $ab \in \mathrm{Z}(G)$, одакле коначно $\mathrm{Z}(G) \leq G$.

Претпоставимо да $H \leq \mathrm{Z}(G)$. За $h \in H$ и $g \in G$ имамо $ghg^{-1} = hgg^{-1} = h \in H$, где прва једнакост важи јер $h \in H \subseteq \mathrm{Z}(G)$. Дакле, $H \triangleleft G$. □

78. Одредити $\mathrm{Z}(G)$ где је:

1) $G = \mathsf{K}_8$;

2) $G = \mathsf{D}_n$, $n \geq 3$;

3) $G = \mathsf{S}_n$, $n \geq 3$;

4) $G = \mathsf{A}_n$, $n \geq 3$.

Решење. 1) $\mathrm{Z}(\mathsf{K}_8) = \{1, -1\} = \langle -1 \rangle$, што се лако види из Кејлијеве таблице за K_8.

2) Нека је $\sigma\rho^i$, $0 \leq i < n$, произвољна симетрија. Приметимо да је $\rho \cdot \sigma\rho^i = \sigma\rho^{-1}\rho^i = \sigma\rho^i \cdot \rho^{-1} \neq \sigma\rho^i \cdot \rho$, одакле следи да $\sigma\rho^i \notin \mathrm{Z}(\mathsf{D}_n)$. Дакле, $\mathrm{Z}(\mathsf{D}_n) \leq \langle \rho \rangle$.

$\varepsilon \in \mathrm{Z}(\mathsf{D}_n)$. Приметимо да $\rho^i \in \mathrm{Z}_{\mathsf{D}_n}$, $1 \leq i < n$, акко за све симетрије $\sigma\rho^j$ важи $\rho^i\sigma\rho^j = \sigma\rho^j\rho^i$, акко $\sigma\rho^{-i}\rho^j = \sigma\rho^j\rho^i$, акко $\rho^{-i} = \rho^i$, акко $\rho^{2i} = \varepsilon$, акко $r(\rho) = n \mid 2i$. Како је $2 \leq 2i < 2n$, то је $n \mid 2i$ еквивалентно са $n = 2i$. Дакле, ако је n непарно, тада је $\mathrm{Z}(\mathsf{D}_n) = \langle \varepsilon \rangle$, а ако је n парно, тада је $\mathrm{Z}(\mathsf{D}_n) = \{\varepsilon, \rho^{n/2}\}$.

3) Доказаћемо да је $\mathrm{Z}(\mathsf{S}_n) = \langle \lfloor\rceil \rangle$, за $n \geq 3$. Нека је $f \in \mathsf{S}_n$, $f \neq \lfloor\rceil$, и нека је $f = f_1 f_2 \dots f_k$ њена циклусна декомпозиција. Можемо да претпоставимо да је $r(f_1) \geq r(f_2) \geq \dots \geq r(f_k) \geq 2$, јер дисјунктни циклуси комутирају. Имамо неколико случајева.

1° $\underline{r(f_1) \geq 3}$. Запишимо $f_1 = \lfloor a, b, c, \dots\rceil$. Уочимо $\lfloor a, b\rceil \in \mathsf{S}_n$. Тада је:

$$\begin{aligned}
\lfloor a,b\rceil f \lfloor a,b\rceil &= \lfloor a,b\rceil f_1 f_2 \dots f_k \lfloor a,b\rceil \\
&= \lfloor a,b\rceil f_1 \lfloor a,b\rceil f_2 \dots f_k \\
&= \lfloor a,b\rceil \lfloor a,b,c,\dots\rceil \lfloor a,b\rceil f_2 \dots f_k \\
&= \lfloor b,a,c,\dots\rceil f_2 \dots f_k \\
&\neq f_1 f_2 \dots f_k \\
&= f.
\end{aligned}$$

Дакле, $\lfloor a, b\rceil f \lfloor a, b\rceil \neq f$, одакле $\lfloor a, b\rceil f \neq f \lfloor a, b\rceil$, па $f \notin \mathrm{Z}(\mathsf{S}_n)$.

Надаље можемо да претпоставимо да је $r(f_1) = r(f_2) = \dots = r(f_k) = 2$.

2° $\underline{k \geq 2}$. Запишимо $f_1 = \lfloor a, b\rceil$, $f_2 = \lfloor c, d\rceil$. Уочимо $\lfloor a, b, c\rceil \in \mathsf{S}_n$. Тада је:

$$\begin{aligned}
\lfloor a,b,c\rceil f \lfloor a,b,c\rceil^{-1} &= \lfloor a,b,c\rceil f_1 f_2 f_3 \dots f_k \lfloor a,b,c\rceil^{-1} \\
&= \lfloor a,b,c\rceil f_1 f_2 \lfloor a,b,c\rceil^{-1} f_3 \dots f_k \\
&= \lfloor a,b,c\rceil \lfloor a,b\rceil \lfloor c,d\rceil \lfloor a,b,c\rceil^{-1} f_3 \dots f_k \\
&= \lfloor b,c\rceil \lfloor a,d\rceil f_3 \dots f_k \\
&\neq f_1 f_2 f_3 \dots f_k \\
&= f.
\end{aligned}$$

Дакле, $\lfloor a, b, c\rceil f \lfloor a, b, c\rceil^{-1} \neq f$, одакле $\lfloor a, b, c\rceil f \neq f \lfloor a, b, c\rceil$, па $f \notin \mathrm{Z}(\mathsf{S}_n)$.

3° $\underline{f = f_1 = \lfloor a, b\rceil}$. Како је $n \geq 3$, уочимо $\lfloor a, b, c\rceil \in \mathsf{S}_n$. Тада је:

$\lfloor a, b, c\rceil f \lfloor a, b, c\rceil^{-1} = \lfloor a, b, c\rceil \lfloor a, b\rceil \lfloor a, b, c\rceil^{-1} = \lfloor b, c\rceil \neq \lfloor a, b\rceil = f$. Дакле, $\lfloor a, b, c\rceil f \lfloor a, b, c\rceil^{-1} \neq f$, одакле $\lfloor a, b, c\rceil f \neq f \lfloor a, b, c\rceil$, па $f \notin \mathrm{Z}(\mathsf{S}_n)$.

Доказали смо: ако $f \neq \lfloor\rceil$, тада $f \notin \mathrm{Z}(\mathsf{S}_n)$, одакле следи $\mathrm{Z}(\mathsf{S}_n) = \langle \lfloor\rceil \rangle$.

4) Како $|\mathsf{A}_3| = 3$, то је A_3 циклична група реда 3, па је Абелова и $\mathrm{Z}(\mathsf{A}_3) = \mathsf{A}_3$. Претпоставимо да је $n \geq 4$; доказаћемо да је $\mathrm{Z}(\mathsf{A}_n) = \langle \lfloor\rceil \rangle$. Нека је $f \in \mathsf{A}_n$, $f \neq \lfloor\rceil$, и нека је $f = f_1 f_2 \dots f_k$ њена циклусна декомпозиција (у S_n). Поново претпоставимо да је $r(f_1) \geq r(f_2) \geq \dots \geq r(f_k) \geq 2$. Имамо неколико случајева.

1° $\underline{r(f_1) = 2}$. Како је f парна пермутација, то закључујемо да је k парно, специјално да је $k \geq 2$. Сада мжемо искористити рачун из случаја 2° из 3) да закључимо да неки 3-цикл (који је наравно из A_n) не комутира са f, па $f \notin \mathrm{Z}(\mathsf{A}_n)$.

2° $\underline{r(f_1) = 3,\ k = 1}$. Запишимо $f = f_1 = \lfloor a, b, c\rceil$. Како је $n \geq 4$, уочимо дуплу транспозицију $\underline{\lfloor a, b\rceil\lfloor c, d\rceil \in \mathsf{A}_n}$. Тада је:

$$\begin{aligned}\lfloor a,b\rceil\lfloor c,d\rceil f\lfloor a,b\rceil\lfloor c,d\rceil &= \lfloor a,b\rceil\lfloor c,d\rceil\lfloor a,b,c\rceil\lfloor a,b\rceil\lfloor c,d\rceil\\ &= \lfloor b,a,d\rceil\\ &\neq \lfloor a,b,c\rceil\\ &= f.\end{aligned}$$

Дакле, $\lfloor a, b\rceil\lfloor c, d\rceil f\lfloor a, b\rceil\lfloor c, d\rceil \neq f$, одакле $\lfloor a, b\rceil\lfloor c, d\rceil f \neq f\lfloor a, b\rceil\lfloor c, d\rceil$, па $f \notin \mathrm{Z}(\mathsf{A}_n)$.

3° $\underline{r(f_1) = 3,\ k \geq 2}$. Запишимо $f_1 = \lfloor a, b, c\rceil$, $f_2 = \lfloor d, \ldots\rceil$. Уочимо дуплу транспозицију $\lfloor a, b\rceil\lfloor c, d\rceil \in \mathsf{A}_n$. Тада је:

$$\begin{aligned}\lfloor a,b\rceil\lfloor c,d\rceil f\lfloor a,b\rceil\lfloor c,d\rceil &= \lfloor a,b\rceil\lfloor c,d\rceil f_1f_2f_3\ldots f_k\lfloor a,b\rceil\lfloor c,d\rceil\\ &= \lfloor a,b\rceil\lfloor c,d\rceil f_1f_2\lfloor a,b\rceil\lfloor c,d\rceil f_3\ldots f_k\\ &= \lfloor a,b\rceil\lfloor c,d\rceil\lfloor a,b,c\rceil\lfloor d,\ldots\rceil\lfloor a,b\rceil\lfloor c,d\rceil f_3\ldots f_k\\ &= \lfloor b,a,d\rceil\lfloor c,\ldots\rceil f_3\ldots f_k\\ &\neq f_1f_2f_3\ldots f_k\\ &= f.\end{aligned}$$

Дакле, $\lfloor a, b\rceil\lfloor c, d\rceil f\lfloor a, b\rceil\lfloor c, d\rceil \neq f$, одакле $\lfloor a, b\rceil\lfloor c, d\rceil f \neq f\lfloor a, b\rceil\lfloor c, d\rceil$, па $f \notin \mathrm{Z}(\mathsf{A}_n)$.

4° $\underline{r(f_1) \geq 4}$. Запишимо $f_1 = \lfloor a, b, c, d, \ldots\rceil$. Уочимо $\lfloor a, b, c\rceil \in \mathsf{A}_n$. Тада је:

$$\begin{aligned}\lfloor a,b,c\rceil f\lfloor a,b,c\rceil^{-1} &= \lfloor a,b,c\rceil f_1f_2\ldots f_k\lfloor a,b,c\rceil^{-1}\\ &= \lfloor a,b,c\rceil f_1\lfloor a,b,c\rceil^{-1}f_2\ldots f_k\\ &= \lfloor a,b,c\rceil\lfloor a,b,c,d,\ldots\rceil\lfloor a,b,c\rceil^{-1}f_2\ldots f_k\\ &= \lfloor b,c,a,d,\ldots\rceil f_2\ldots f_k\\ &\neq f_1f_2\ldots f_k\\ &= f.\end{aligned}$$

Дакле, $\lfloor a, b, c\rceil f\lfloor a, b, c\rceil^{-1} \neq f$, одакле $\lfloor a, b, c\rceil f \neq f\lfloor a, b, c\rceil$, па $f \notin \mathrm{Z}(\mathsf{A}_n)$.

Доказали смо: ако $f \neq \lfloor\,\rceil$, тада $f \notin \mathrm{Z}(\mathsf{A}_n)$, одакле следи $\mathrm{Z}(\mathsf{A}_n) = \langle\lfloor\,\rceil\rangle$. □

Централизатор Централизатор подскупа $S \subseteq G$ у групи G је $\mathrm{C}_G(S) = \{b \in G \mid (\forall x \in S)\, bx = xb\}$. Када је $S = \{a\}$, тада је $\mathrm{C}_G(a) = \mathrm{C}_G(\{a\}) = \{b \in G \mid ab = ba\}$. Очигледно важе следеће ствари: $\mathrm{Z}(G) \subseteq \mathrm{C}_G(S)$, $\mathrm{C}_G(G) = \mathrm{Z}(G)$, $\mathrm{C}_G(S) = \bigcap_{a\in S} \mathrm{C}_G(a)$. Ако знамо о којој групи је реч, уместо C_G пишемо само C.

79. Доказати:

1) $\mathrm{C}_G(S) \leq G$;

2) не мора бити $S \subseteq \mathrm{C}_G(S)$, али важи $S \subseteq \mathrm{C}_G(\mathrm{C}_G(S))$;

3) $S \subseteq T$ повлачи $\mathrm{C}_G(T) \subseteq \mathrm{C}_G(S)$ и $S \subseteq \mathrm{C}_G(T)$ акко $T \subseteq \mathrm{C}_G(S)$;

4) $\langle a\rangle \triangleleft \mathrm{C}_G(a)$.

Решење. 1) Очигледно $e \in \mathrm{C}_G(S)$. Ако $a \in \mathrm{C}_G(S)$, тада за произвољно $s \in S$ важи $as = sa$. Множећи ову једнакост са a^{-1} и са леве и са десне стране добијамо $sa^{-1} = a^{-1}s$, па како је $s \in S$ било произвољно, закључујемо да $a^{-1} \in \mathrm{C}_G(S)$. Коначно, ако $a, b \in \mathrm{C}_G(S)$, тада за произвољно $s \in S$ важи $as = sa$ и $bs = sb$. Одавде је $abs = asb = sab$, па како је $s \in S$ било произвољно, закључујемо $ab \in \mathrm{C}_G(S)$. Дакле, $\mathrm{C}_G(S) \leq G$.

2) Да не мора бити $S \subseteq \mathrm{C}_G(S)$ видећемо у следећем задатку под 3). Претпоставимо да је $s \in S$. Тада за све $a \in \mathrm{C}_G(S)$ важи $as = sa$, што значи да $s \in \mathrm{C}_G(\mathrm{C}_G(S))$. Дакле, $S \subseteq \mathrm{C}_G(\mathrm{C}_G(S))$.

3) $S \subseteq T$ повлачи $\mathrm{C}_G(T) \subseteq \mathrm{C}_G(S)$ је очигледно: ако x комутира са елеменатима скупа T, тада он комутира и са елементима његовог подскупа S. Ако је $S \subseteq \mathrm{C}_G(T)$, тада је $T \subseteq \mathrm{C}_G(\mathrm{C}_G(T)) \subseteq \mathrm{C}_G(S)$, и слично се доказује обратна импликација.

4) Очигледно $a \in \mathrm{C}_G(a)$, па како је $\mathrm{C}_G(a) \leq G$, то $\langle a \rangle \leq \mathrm{C}_G(a)$. Нека $x \in \langle a \rangle$ и $y \in \mathrm{C}_G(a)$; доказујемо $yxy^{-1} \in \langle a \rangle$. Знамо да је $x = a^m$, за неко $m \in \mathsf{Z}$. Ако је $m = 0$, тада је $x = e$, па $yxy^{-1} = e \in \langle a \rangle$. Ако је $m \geq 1$, тада је $yxy^{-1} = y\underbrace{aa, \ldots a}_{m}y^{-1} = ay\underbrace{a, \ldots a}_{m-1}y^{-1} = aay\underbrace{a, \ldots a}_{m-2}y^{-1} = \ldots = a^m yy^{-1} = a^m \in \langle a \rangle$. Ако је $m \leq -1$, тада је $yxy^{-1} = ya^m y^{-1} = (ya^{-m}y^{-1})^{-1} = (a^{-m})^{-1} = a^m \in \langle a \rangle$, где смо користили $-m \geq 1$ и претходно доказано. Дакле, $\langle a \rangle \triangleleft \mathrm{C}_G(a)$. □

80. Израчунати $\mathrm{C}_G(S)$, где је:

1) $G = \mathsf{D}_n$, $S = \{\rho\}$;

2) $G = \mathsf{D}_n$, $S = \{\sigma\}$;

3) $G = \mathsf{D}_n$, $S = \{\rho, \sigma\}$;

4) $G = \mathsf{S}_{10}$, $S = \{\lfloor 1, 2 \rceil \lfloor 3, 4, 5, 6, 7 \rceil\}$;

Решење. 1) Знамо да $\langle \rho \rangle \subseteq \mathrm{C}_{\mathsf{D}_n}(\rho)$, па остаје да испитамо да ли нека симетрија комутира са ρ. Имамо: $\rho \cdot \sigma\rho^k = \sigma\rho^k \cdot \rho$ акко $\sigma\rho^{-1}\rho^k = \sigma\rho^k\rho$ акко $\rho^{k-1} = \rho^{k+1}$ акко $k - 1 = k + 1 \mod n$, што је немогуће за $n \geq 3$. Дакле, $\mathrm{C}_{\mathsf{D}_n}(\rho) = \langle \rho \rangle$.

2) Знамо да $\langle \sigma \rangle \subseteq \mathrm{C}_{\mathsf{D}_n}(\sigma)$, па остаје да испитамо да ли ротације ρ^k, $1 \leq k < n$, и симетрије $\sigma\rho^k$, $1 \leq k < n$, комутирају са σ. Имамо: $\sigma\rho^k = \rho^k\sigma$ акко $\sigma\rho^k = \sigma\rho^{-k}$ акко $\rho^k = \rho^{-k}$ акко $k = -k \mod n$ акко $n = 2k$ (последње акко важи јер $1 \leq k < n$). Такође имамо: $\sigma\sigma\rho^k = \sigma\rho^k\sigma$ акко $\sigma\sigma\rho^k = \sigma\sigma\rho^{-k}$ акко $\rho^k = \rho^{-k}$ акко $k = -k \mod n$ акко $n = 2k$. Дакле, ако је n парно, тада је $\mathrm{C}_{\mathsf{D}_n}(\sigma) = \{\varepsilon, \sigma, \rho^{n/2}, \sigma\rho^{n/2}\} = \langle \sigma, \rho^{n/2} \rangle$, а ако је n непарно, тада је $\mathrm{C}_{\mathsf{D}_n}(\sigma) = \langle \sigma \rangle$.

3) Знамо $\mathrm{C}_{\mathsf{D}_n}(\sigma, \rho) = \mathrm{C}_{\mathsf{D}_n}(\sigma) \cap \mathrm{C}_{\mathsf{D}_n}(\rho)$. Према претходна два дела имамо: ако је n парно, тада је $\mathrm{C}_{\mathsf{D}_n}(\sigma, \rho) = \{\varepsilon, \rho^{n/2}\}$, а ако је n непарно, тада је $\mathrm{C}_{\mathsf{D}_n}(\sigma, \rho) = \langle \varepsilon \rangle$.

4) Рачунамо пермутације које комутирају са $\lfloor 1, 2 \rceil \lfloor 3, 4, 5, 6, 7 \rceil$. Нека је $f \in \mathsf{S}_{10}$ таква да $f\lfloor 1, 2 \rceil \lfloor 3, 4, 5, 6, 7 \rceil = \lfloor 1, 2 \rceil \lfloor 3, 4, 5, 6, 7 \rceil f$, тј. $f\lfloor 1, 2 \rceil \lfloor 3, 4, 5, 6, 7 \rceil f^{-1} = \lfloor 1, 2 \rceil \lfloor 3, 4, 5, 6, 7 \rceil$. Пермутација на левој страни је једнака $\lfloor f(1), f(2) \rceil \lfloor f(3), f(4), f(5), f(6), f(7) \rceil$, одакле закључујемо да f комутира са $\lfloor 1, 2 \rceil \lfloor 3, 4, 5, 6, 7 \rceil$ акко $\lfloor f(1), f(2) \rceil \lfloor f(3), f(4), f(5), f(6), f(7) \rceil = \lfloor 1, 2 \rceil \lfloor 3, 4, 5, 6, 7 \rceil$. Из јединствености циклусне декомпозиције следи да је $\lfloor f(1), f(2) \rceil = \lfloor 1, 2 \rceil$ и $\lfloor f(3), f(4), f(5), f(6), f(7) \rceil = \lfloor 3, 4, 5, 6, 7 \rceil$. Одавде приметимо да $f(1) \in \{1, 2\}$, док је $f(2)$ форсирана избором $f(1)$. Слично, $f(3) \in \{3, 4, 5, 6, 7\}$, а $f(4), f(5), f(6), f(7)$ су форсирани избором $f(3)$. Избори $f(8), f(9), f(10) \in \{8, 9, 10\}$ су произвољни (форсирани су једино чињеницом да је f пермутација). Према томе имамо $2 \cdot 5 \cdot 6 = 60$ могућности за пермутацију f. Дакле, $|\mathrm{C}_{\mathsf{S}_{10}}(\lfloor 1, 2 \rceil \lfloor 3, 4, 5, 6, 7 \rceil)| = 60$ и сви елементи датог централизатора су горе описани. □

Нормализатор скупа $S \subseteq G$ у групи G је $\mathrm{N}_G(S) = \{g \in G \mid gS = Sg\}$, дакле скуп свих елемената који комутирају са скупом S. Очигледно је нормализатор једночланог скупа једнак његовом централизатору, и очигледно је да увек важи $\mathrm{C}_G(S) \subseteq \mathrm{N}_G(S)$.

81. Доказати да је $\mathrm{N}_G(S) \leq G$.

Решење. Очигледно $e \in \mathrm{N}_G(S)$. Ако $a \in \mathrm{N}_G(S)$, тада $aS = Sa$, па множењем ове једнакости са a^{-1} са леве и са десне стране добијамо $Sa^{-1} = a^{-1}S$, одакле $a \in \mathrm{N}_G(S)$. Такође, ако $a, b \in \mathrm{N}_G(S)$, тада $abS = aSb = Sab$, где прва једнакост важи јер $b \in \mathrm{N}_G(S)$, а друга јер $a \in \mathrm{N}_G(S)$. Дакле, $ab \in \mathrm{N}_G(S)$. □

82. Доказати $H \lhd \mathrm{N}_G(H)$. Ако $H, K \leq G$, доказати $H \lhd K$ акко $K \leq \mathrm{N}_G(H)$.

Специјално, $\mathrm{N}_G(H)$ је највећа подгрупа од G у којој је H нормална. Дакле, $H \lhd G$ акко $\mathrm{N}_G(H) = G$.

Решење. $H \lhd \mathrm{N}_G(H)$ јер по дефиницији за све $g \in \mathrm{N}_G(H)$ важи $gH = Hg$.

$H \lhd K$ акко за све $k \in K$ важи $kH = Hk$ акко по дефиницији $K \leq \mathrm{N}_G(H)$. □

83. $\mathrm{C}_G(S) \lhd \mathrm{N}_G(S)$.

Решење. Ако $n \in \mathrm{N}_G(S)$ и $c \in \mathrm{C}_G(S)$, доказујемо да $ncn^{-1} \in \mathrm{C}_G(S)$. Узмимо произвољно $s \in S$ и посматрајмо $ncn^{-1}s(ncn^{-1})^{-1} = ncn^{-1}snc^{-1}n^{-1}$. Како је n из нормализатора, то је $n^{-1}sn = s' \in S$; одавде је $ns'n^{-1} = s$. Сада је $ncn^{-1}snc^{-1}n^{-1} = ncs'c^{-1}n^{-1} = ns'n^{-1} = s$, где смо изкористили да је c у централизатору од S, па је $cs'c^{-1} = s'$. Дакле, ncn^{-1} комутира са произвољним $s \in S$, па $ncn^{-1} \in \mathrm{C}_G(S)$, што смо и желели. □

Језгро подгрупе Нека је $H \leq G$. Језгро подгрупе H је $\mathrm{Core}(H) = \bigcap_{g \in G} gHg^{-1}$. Како знамо да су gHg^{-1} подгрупе од G, то је $\mathrm{Core}(H)$ подгрупа од G као пресек подгрупа од G. Такође, јасно је да је $\mathrm{Core}(H) \leq H$, јер је H једна од чланова пресека у $\mathrm{Core}(H)$.

84.

1. $\mathrm{Core}(H) \lhd G$.
2. Нека је $K \leq H$. Доказати: ако је $K \lhd G$, тада је $K \leq \mathrm{Core}(H)$.

Дакле, $\mathrm{Core}(H)$ је највећа подгрупа од H нормална у G. Такође, $H \lhd G$ акко $H = \mathrm{Core}(H)$.

Решење. 1) За све $a \in G$ имамо $a\mathrm{Core}(H)a^{-1} = a\bigcap_{g \in G} gHg^{-1}a^{-1} = \bigcap_{g \in G} agH(ag)^{-1} = \mathrm{Core}(H)$, где последња једнакост важи јер је $g \mapsto ag$ бијекција на G, па када g прође G, тада и ag прође G – пресеци су исти.

2) Ако $K \lhd G$, тада за све $g \in G$ имамо $gKg^{-1} = K$, а такође $gKg^{-1} \leq gHg^{-1}$ (јер $K \leq H$). Дакле, за све $g \in G$ имамо $K \leq gHg^{-1}$, па $K \leq \bigcap_{g \in G} gHg^{-1} = \mathrm{Core}(H)$. □

Комутатор елемената a и b у групи G је елемент $[a, b] = aba^{-1}b^{-1}$. Приметите да a и b комутирају акко им је комутатор $[a, b] = e$.

85. Доказати: $[a, b]^{-1} = [b, a]$; $g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$; $f([a, b]) = [f(a), f(b)]$, где је $f : G \longrightarrow H$ било који хомоморфизам група.

Решење. $[a,b]^{-1} = (aba^{-1}b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1}b^{-1}a^{-1} = bab^{-1}a^{-1} = [b,a]$.

$g[a,b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} = [gag^{-1}, gbg^{-1}]$.

$f([a,b])\ f(aba^{-1}b^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1} = [f(a), f(b)]$. □

Извод групе G је подгрупа $D(G) = \langle [a,b] : a,b \in G \rangle$. Како је инверз комутатора комутатор, приметите да су елементи подгрупе $D(G)$ коначни производи комутатора: $D(G) = \{[a_1,b_1][a_2,b_2]\dots[a_k,b_k] \mid k \geq 1, a_i, b_i \in G\}$.

86. Доказати: $D(G) \triangleleft G$. Доказати да је $G/D(G)$ Абелова.

Група $G/D(G)$ се зове абелизација групе G и означава се са G^{ab}.

Решење. Нека $x \in D(G)$ и $g \in G$. Тада је $x = [a_1,b_1][a_2,b_2]\dots[a_k,b_k]$, па је $gxg^{-1} = g[a_1,b_1][a_2,b_2]\dots[a_k,b_k]g^{-1} = g[a_1,b_1]g^{-1}g[a_2,b_2]g^{-1}\dots g[a_k,b_k]g^{-1} =$
$[ga_1g^{-1}, gb_1g^{-1}][ga_2g^{-1}, gb_2g^{-1}]\dots[ga_kg^{-1}, gb_kg^{-1}] \in D(G)$, одакле следи да је $D(G) \triangleleft G$.

Приметимо да је у $G/D(G)$: $[aD(G), bD(G)] = aD(G)\,bD(G)\,(aD(G))^{-1}(bD(G))^{-1} = aD(G)\,bD(G)\,a^{-1}D(G)\,b^{-1}D(G) = (aba^{-1}b^{-1})D(G) = [a,b]D(G) = D(G)$, где последња једнакост важи јер $[a,b] \in D(G)$. Према томе комутатор произвољна два косета у $G/D(G)$ је тривијалан, одакле следи да та два косета комутирају, па је $G/D(G)$ Абелова група. □

87. Доказати: G је Абелова акко $D(G) = \langle e \rangle$ акко $G^{ab} = G$.

Доказати: ако је $H \triangleleft G$ и G/H Абелова, тада је $D(G) \leq H$. Дакле, $D(G)$ је најмања нормална подгрупа од G чији је количник Абелов.

Решење. Први део је очигледан.

Приметимо у G/H: $H = [aH, bH] = [a,b]H$, где прва једнакост важи због абеловости, а друга се изводи слично као у решењу претходног задатка. Одавде закључујемо да $[a,b] \in H$, тј. H садржи све комутаторе, па према томе садржи и подгрупу коју они генеришу, а то је $D(G)$. □

88. Израчунати изводе следећих група: D_n, S_n, A_n, где $n \geq 3$.

Решење. Питање рачуна извода групе је питање рачуна свих комутатора. Зато ћемо израчунати шта све може бити комутатор.

У случају групе D_n имамо три случаја. Комутатор две ротације је тривијалан јер ротације међусобно комутирају. Рачунамо комутатор ротације и симетрије: $[\rho^k, \sigma\rho^l] = \rho^k\sigma\rho^l\rho^{-k}\sigma\rho^l = \rho^k\rho^{-l}\sigma\sigma\rho^k\rho^l = \rho^{2k} \in \langle\rho^2\rangle$. Рачунамо комутатор две симетрије: $[\sigma\rho^k, \sigma\rho^l] = \sigma\rho^k\sigma\rho^l\sigma\rho^k\sigma\rho^l = \rho^{-k}\sigma\sigma\rho^l\rho^{-k}\sigma\sigma\rho^l = \rho^{2(l-k)} \in \langle\rho^2\rangle$. Према томе сви комутатори припадају $\langle\rho^2\rangle$, одакле и $D(\mathsf{D}_n) \leq \langle\rho^2\rangle$. Приметимо још и да је $[\rho,\sigma] = \rho\sigma\rho^{-1}\sigma = \rho\sigma\sigma\rho = \rho^2$, одакле закључујемо да $\rho^2 \in D(\mathsf{D}_n)$, па и $\langle\rho^2\rangle \leq D(\mathsf{D}_n)$. Дакле, $D(\mathsf{D}_n) = \langle\rho^2\rangle$.

У случају када је n непарно, како је $(2,n) = 1$, то је $\langle\rho^2\rangle = \langle\rho\rangle$, и у том случају извод чине све ротације. У случају када је n парно, тада извод чине све ротације генерисане са ρ^2.

Пре него што почнемо да рачунамо комутаторе пермутација приметимо да, ако $f, g \in \mathsf{S}_n$, тада је $[f,g] = fgf^{-1}g^{-1}$ парна пермутација (Размислите!). Према томе $D(\mathsf{S}_n) \leq \mathsf{A}_n$. Ако је $\lfloor a,b,c \rceil$ произвољан 3-цикл, тада имамо $\lfloor a,b,c \rceil = \lfloor a,b \rceil \lfloor b,c \rceil = \lfloor a,b \rceil \lfloor a,c \rceil \lfloor a,b \rceil \lfloor a,c \rceil = [\lfloor a,b \rceil, \lfloor a,c \rceil]$, одакле закључујемо да $\lfloor a,b,c \rceil \in D(\mathsf{S}_n)$, па како 3-циклови генеришу A_n, то закључујемо $\mathsf{A}_n \leq D(\mathsf{S}_n)$. Дакле, $D(\mathsf{S}_n) = \mathsf{A}_n$.

Остаје да израчунамо $D(\mathsf{A}_n)$. За $n = 3$, A_3 има 3 елемента, те је она циклична, специјално и Абелова, па је $D(\mathsf{A}_3)$ тривијална група.

За $n \geq 5$ ћемо доказати да је $D(\mathsf{A}_n) = \mathsf{A}_n$. Уочимо прозивољан 3-цикл $\lfloor a,b,c \rceil$ и како је $n \geq 5$ изаберимо $d, e \notin \{a,b,c\}$. Посматрајмо $f = \lfloor a,b \rceil \lfloor d,e \rceil$ и $g = \lfloor a,c \rceil \lfloor d,e \rceil$ из A_n. Тада

је $[f,g] = \lfloor a,b\rceil\lfloor d,e\rceil\lfloor a,c\rceil\lfloor d,e\rceil\lfloor a,b\rceil\lfloor d,e\rceil\lfloor a,c\rceil\lfloor d,e\rceil = \lfloor a,b,c\rceil$. Према томе 3-цикли припадају $D(\mathsf{A}_n)$, па како они генеришу A_n имамо $\mathsf{A}_n \leq D(\mathsf{A}_n) \leq \mathsf{A}_n$, тј. $D(\mathsf{A}_n) = \mathsf{A}_n$.

Остаје да одредимо $D(\mathsf{A}_4)$. Лако се види да су елементи A_4 у циклусној декомпозицији или 3-цикл или дупла транспозиција. Они су: $\lfloor\rceil$, $\lfloor 1,2,3\rceil$, $\lfloor 1,3,2\rceil$, $\lfloor 1,2,4\rceil$, $\lfloor 1,4,2\rceil$, $\lfloor 1,3,4\rceil$, $\lfloor 1,4,3\rceil$, $\lfloor 2,3,4\rceil$, $\lfloor 2,4,3\rceil$, $\lfloor 1,2\rceil\lfloor 3,4\rceil$, $\lfloor 1,3\rceil\lfloor 2,4\rceil$ и $\lfloor 1,4\rceil\lfloor 2,3\rceil$. Такође се лако види да је $V = \{\lfloor\rceil, \lfloor 1,2\rceil\lfloor 3,4\rceil, \lfloor 1,3\rceil\lfloor 2,4\rceil, \lfloor 1,4\rceil\lfloor 2,3\rceil\}$ једна (Абелова) подгрупа од A_4 (изоморфна са $\mathsf{Z}_2 \times \mathsf{Z}_2$ – проверите!). Приметите да V садржи све дупле транспозиције. Доказаћемо да је $D(\mathsf{A}_4) = V$. Комутатор две дупле транспозиције је тривијалан (приметили смо горе да је V Абелова). Одредимо комутатор 3– цикла и дупле транспозиције: нека је f 3-цикл, а g дупла транспозиција; тада је $[f,g] = fgf^{-1}g^{-1}$ и fgf^{-1} је дупла транспозиција (као коњугат дупле транспозиције) и g^{-1} је дупла транспозиција, па $[f,g] \in V$. Коначно, одредимо комутатор два 3-цикла: ако су f,g 3-цикли, тада имамо две могућности: или f,g фиксирају исти елемент или f,g не фиксирају исти елемент. Ако f,g фиксирају исти елемент, тада $\langle f\rangle = \langle g\rangle$, па је $[f,g] = \lfloor\rceil$. Ако не фиксирају исти елемент, тада f можемо да запишемо као $f = \lfloor a,b,x\rceil$, а g као $g = \lfloor a,b,y\rceil$ или $g = \lfloor b,a,y\rceil$. У првом случају $[f,g] = \lfloor a,b,x\rceil\lfloor a,b,y\rceil\lfloor a,x,b\rceil\lfloor a,y,b\rceil = \lfloor a,b\rceil\lfloor x,y\rceil \in V$, а у другом $[f,g] = \lfloor a,b,x\rceil\lfloor b,a,y\rceil\lfloor a,x,b\rceil\lfloor b,y,a\rceil = \lfloor a,y\rceil\lfloor b,x\rceil \in V$. Коначно закључујемо $D(\mathsf{A}_n) \leq V$. Из последњег рачуна је јасно да можемо сваку дуплу транспозицију да напишемо као комутатор два 3-цикла, па је заправо $D(\mathsf{A}_n) = V$. □

Елементарна теорија бројева

Аритметичка функцијан (АФ) За функцију $f : \mathsf{N}^+ \longrightarrow \mathsf{C}$ кажемо да је аритметичка ако задовољава $f(1) = 1$.

Мултипликативна аритметичка функција (МАФ) За аритметичку функцију f кажемо да је мултипликативна ако задовољава $f(mn) = f(m)f(n)$, кад год $(m,n) = 1$.

89. МАФ f је одређена својим вредностима на степенима простих бројева. Доказати.

Решење. Претпоставимо да је $n \in \mathsf{N}^+$, $n \neq 1$. Тада према Основној теореми аритметике, n можемо написати као $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$, где су p_i прости, а α_i позитивни природни бројеви. Приметимо да мултипликативност функције f повлачи:

$$\begin{aligned} f(n) &= f(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}) \\ &= f(p_1^{\alpha_1})f(p_2^{\alpha_2}\dots p_k^{\alpha_k}) && \text{јер } (p_1^{\alpha_1}, p_2^{\alpha_2}\dots p_k^{\alpha_k}) = 1 \\ &= f(p_1^{\alpha_1})f(p_2^{\alpha_2})f(p_3^{\alpha_3}\dots p_k^{\alpha_k}) && \text{јер } (p_2^{\alpha_2}, p_3^{\alpha_3}\dots p_k^{\alpha_k}) = 1 \\ &= \dots \\ &= f(p_1^{\alpha_1})f(p_2^{\alpha_2})\dots f(p_k^{\alpha_k}), \end{aligned}$$

одакле следи тврђење задатка. □

90. Доказати да су следеће функције МАФ:

1) $\varepsilon(n) = \begin{cases} 1, & n = 1 \\ 0, & n \neq 1 \end{cases}$; 2) $\mathbb{1}(n) = 1$; 3) $\mathrm{I}(n) = n$;

4) за $k \geq 0$, $\mathrm{I}_k(n) = n^k$, (приметимо $\mathrm{I}_0 = \mathbb{1}$, $\mathrm{I}_1 = \mathrm{I}$); 5) $\mu(n) = \begin{cases} 1, & n = 1 \\ (-1)^k, & n = p_1p_2\dots p_k \\ 0, & \text{иначе} \end{cases}$.

(Када напишемо $n = p_1p_2\dots p_k$ подразумевамо да је n производ k међусобно **различитих** простих бројева. Ако је смисао другачији, биће посебно наглашено. Функцију μ зовемо Мебиусова функција.)

Решење. Све наведене функције су очигледно аритметичке. Такође, очигледно је да функције 1) – 4) задовољавају $f(mn) = f(m)f(n)$, за произвољне m, n, па специјално јесу мултипликативне. Докажимо да је μ мултипликативна. Претпоставимо да $(m, n) = 1$ и претпоставимо да $m, n > 1$ (ако је m или n једнако 1, тврђење је тривијално). Доказаћемо да је $\mu(mn) = \mu(m)\mu(n)$. Запишимо $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ и $n = q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}$. $(m, n) = 1$ значи да је $\{p_1, p_2, \dots, p_k\} \cap \{q_1, q_2, \dots, q_l\} = \emptyset$. Тада је $mn = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}$ запис mn према Основној теореми аритметике. По дефиницији $\mu(mn) = (-1)^{k+l}$ акко $\alpha_i = \beta_j = 1$, за све $1 \le i \le k, 1 \le j \le l$, иначе је $\mu(mn) = 0$. Ако је $\alpha_i = \beta_j = 1$, за све $1 \le i \le k, 1 \le j \le l$, тада је $\mu(m) = (-1)^k$, $\mu(n) = (-1)^l$, па је $\mu(m)\mu(n) = (-1)^{k+l}$. Ако је бар неки од α_i или β_j већи од 1, тада је бар један од $\mu(m), \mu(n)$ једнак 0, па је свакако $\mu(m)\mu(n) = 0$. Дакле, $\mu(mn) = \mu(m)\mu(n)$. □

Дирихлеова конволуција Ако су f и g две АФ, дефинишемо функцију (која је такође АФ) $f * g$ са: $f * g(n) = \sum_{d|n} f(d)g(n/d)$. Операцију $*$ на АФ зовемо Дирихлеова конволуција.

91. Доказати:

1) $*$ је комутативна операција;

2) $*$ је асоцијативна операција;

3) ако су f, g МАФ, тада је и $f * g$ МАФ;

4) $\varepsilon * f = f * \varepsilon = f$;

5) $\mu * \mathbb{1} = \mathbb{1} * \mu = \varepsilon$;

6) (Мебиусова теорема инверзије) $F = \mathbb{1} * f$ акко $f = \mu * F$.

Решење. Приметимо најпре да је $f * g(n) = \sum_{d|n} f(d)g(n/d) = \sum_{\substack{(d_1,d_2)\\ d_1 d_2 = n}} f(d_1)g(d_2)$, одакле је јасно да је $*$ комутативна операција. Такође, $f * (g * h)(n) = \sum_{\substack{(d_1,d_1')\\ d_1 d_1' = n}} f(d_1) g * h(d_1') =$

$$= \sum_{\substack{(d_1,d_1')\\ d_1 d_1' = n}} f(d_1) \sum_{\substack{(d_2,d_3)\\ d_2 d_3 = d_1'}} g(d_2)h(d_3) = \sum_{\substack{(d_1,d_1')\\ d_1 d_1' = n}} \sum_{\substack{(d_2,d_3)\\ d_2 d_3 = d_1'}} f(d_1)g(d_2)h(d_3) =$$

$$= \sum_{\substack{(d_1,d_2,d_3)\\ d_1 d_2 d_3 = n}} f(d_1)g(d_2)h(d_3),$$

и сличан рачун показује да је

$$(f * g) * h(n) = \sum_{\substack{(d_1,d_2,d_3)\\ d_1 d_2 d_3 = n}} f(d_1)g(d_2)h(d_3),$$

одакле следи да је $*$ асоцијативна операција.

Докажимо сада 3). Претпоставимо да је $(m, n) = 1$. Приметимо да постоји природна бијекција између скупова $\{(d_1, d_2) : d_1 \mid m, d_2 \mid n\}$ и $\{d : d \mid mn\}$, дата са $(d_1, d_2) \mapsto d_1 d_2$. Заиста, ако је $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $n = q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}$, из $(m, n) = 1$ следи $p_i \ne q_j$, и ако $d \mid mn$, тада је $d = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k} q_1^{\delta_1} q_2^{\delta_2} \dots q_l^{\delta_l}$, $0 \le \gamma_i \le \alpha_i$, $0 \le \delta_j \le \beta_j$, одакле је јасно да је d јединствено одређен

својим "p-делом", који дели m, и својим "q-делом" који дели n. Такође, приметимо ако $d_1 \mid m$, $d_2 \mid n$, и $(m,n)=1$, тада $(d_1,d_2)=1$ и $(m/d_1, n/d_2)=1$. Одавде имамо следећи рачун:

$$\begin{aligned} f*g(mn) &= \sum_{d\mid mn} f(d)g(mn/d) \\ &= \sum_{d_1\mid m, d_2\mid n} f(d_1d_2)g(mn/d_1d_2) \\ &= \sum_{d_1\mid m, d_2\mid n} f(d_1)f(d_2)g(m/d_1)g(n/d_2) \\ &= \sum_{d_1\mid m}\sum_{d_2\mid n} f(d_1)g(m/d_1)f(d_2)g(n/d_2) \\ &= \sum_{d_1\mid m} f(d_1)g(m/d_1)\sum_{d_2\mid n} f(d_2)g(n/d_2) \\ &= f*g(m)f*g(n), \end{aligned}$$

одакле следи да је $f*g$ мултипликативна.

4) $f*\varepsilon(1)=1=f(1)$, а за $n>1$ је $f*\varepsilon(n)=\sum_{d\mid n} f(d)\varepsilon(n/d) = f(n)\varepsilon(1)+\sum_{\substack{d\mid n\\ d<n}} f(d)\varepsilon(n/d) =$ $f(n)+\sum_{\substack{d\mid n\\ d<n}} f(d)\cdot 0 = f(n)$.

5) Како су μ и $\mathbb{1}$ МАФ, то је и $\mu*\mathbb{1}$ МАФ, па је довољно одредити њене вредности на степенима простих бројева. За $\alpha>0$ имамо: $\mu*\mathbb{1}(p^\alpha)=\sum_{d\mid p^\alpha}\mu(d)\mathbb{1}(p^\alpha/d)=\sum_{i=0}^{\alpha}\mu(p^i)\mathbb{1}(p^{\alpha-i}) =$ $\mu(1)+\mu(p)+\mu(p^2)+\ldots+\mu(p^\alpha)=1+(-1)+0+\ldots 0=0$. Одавде закључујемо да је $\mu*\mathbb{1}=\varepsilon$.

6) Ако је $F=\mathbb{1}*f$, тада је $\mu*F=\mu*\mathbb{1}*f=\varepsilon*f=f$, а ако је $f=\mu*F$, тада је $\mathbb{1}*f=\mathbb{1}*\mu*F=\varepsilon*F=F$. □

92. Нека је $\tau(n)=\sum_{d\mid n} 1$ број делилаца броја n.

1) Доказати да је τ МАФ.

2) Израчунати $\tau(n)$.

3) Доказати да је $\tau(n)$ непаран број ако и само ако је n квадрат.

Решење. Приметимо: $\tau(n)=\sum_{d\mid n}1=\sum_{d\mid n}1\cdot 1=\sum_{d\mid n}\mathbb{1}(d)\mathbb{1}(n/d)=\mathbb{1}*\mathbb{1}(n)$. Дакле, $\tau=\mathbb{1}*\mathbb{1}$, па је τ МАФ као конволуција две МАФ. Према томе да бисмо израчунали τ, довољно је израчунати је на степенима простих бројева. Очигледно $\tau(p^\alpha)=\alpha+1$ (делиоци p^α су облика p^i, где $0\le i\le\alpha$).

Нека је $n>1$ и $n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$. $\tau(n)$ је непаран број акко $\tau(p_1^{\alpha_1})\tau(p_2^{\alpha_2})\ldots\tau(p_k^{\alpha_k})$ је непаран акко $\tau(p_i^{\alpha_i})$ је непаран за све $1\le i\le k$ акко α_i+1 је непаран за све $1\le i\le k$ акко α_i је паран за све $1\le i\le k$ акко $\alpha_i=2\beta_i$ за све $1\le i\le k$ акко $n=(p_1^{\beta_1}p_2^{\beta_2}\ldots p_k^{\beta_k})^2$. □

93. Нека је $\sigma(n)=\sum_{d\mid n} d$ збир делилаца броја n.

1) Доказати да је σ МАФ.

2) Израчунати $\sigma(n)$.

3) Доказати да је $\sigma(n)$ непаран број ако и само ако је n квадрат или је n два пута квадрат.

Решење. Приметимо: $\sigma(n) = \sum_{d|n} d = \sum_{d|n} d \cdot 1 = \sum_{d|n} \mathrm{I}(d)\mathbb{1}(n/d) = \mathrm{I} * \mathbb{1}(n)$. Дакле, $\sigma = \mathrm{I} * \mathbb{1}$, па је σ МАФ као конволуција две МАФ. Према томе да бисмо израчунали σ, довољно је израчунати је на степенима простих бројева. $\sigma(p^\alpha) = \sum_{i=0}^{\alpha} p^i = \frac{p^{\alpha+1}-1}{p-1}$.

Нека је $n > 1$ и $n = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, где $\alpha \geq 0$, а p_i су непарни прости. $\sigma(n)$ је непаран број акко $\sigma(2^\alpha)\sigma(p_1^{\alpha_1}) \dots \sigma(p_k^{\alpha_k})$ је непаран број акко $\sigma(2^\alpha)$ је непаран број и $\sigma(p_1^{\alpha_1})$ је непаран број за све $1 \leq i \leq k$ акко $2^{\alpha+1} - 1$ је непаран број и $1 + p_i + p_i^2 + \dots + p_i^{\alpha_i}$ је непаран број за све $1 \leq i \leq k$ акко $1 + p_i + p_i^2 + \dots + p_i^{\alpha_i}$ је непаран број за све $1 \leq i \leq k$ акко $\alpha_i + 1$је непаран број за све $1 \leq i \leq k$ акко α_i је паран број за све $1 \leq i \leq k$ акко $\alpha_i = 2\beta_i$ за све $1 \leq i \leq k$ акко $n = 2^\alpha (p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k})^2 = \begin{cases} (2^{\alpha/2} p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k})^2 & \alpha \text{ паран} \\ 2(2^{(\alpha-1)/2} p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k})^2 & \alpha \text{ непаран} \end{cases}$. □

Производ АФ Ако су f, g АФ, можемо дефинисати њихов производ fg са $fg(n) = f(n)g(n)$. fg је очигледно АФ, и ако су f, g МАФ, тада је и fg МАФ, јер за $(m, n) = 1$ имамо $fg(mn) = f(mn)g(mn) = f(m)f(n)g(m)g(n) = f(m)g(m)f(n)g(n) = fg(m)fg(n)$. Такође, ако је f АФ, са $|f|$ означимо њену апсолутну вредност дефинисану са $|f|(n) = |f(n)|$. И $|f|$ је очигледно АФ, а ако је f МАФ, тада је и $|f|$ МАФ јер за $(m, n) = 1$ имамо $|f|(mn) = |f(mn)| = |f(m)f(n)| = |f(m)||f(n)| = |f|(m)|f|(n)$.

94. Нека је $\lambda(n) = \begin{cases} 1, & n = 1 \\ (-1)^{\alpha_1+\alpha_2+\dots+\alpha_n}, & n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \end{cases}$. λ зовемо Лиувилова функција.

1) Доказати да је λ МАФ.

2) Израчунати $\sum_{d|n} \lambda(d)$ и $\sum_{d|n} \lambda(d)|\mu(n/d)|$.

Решење. Лако се види да је λ МАФ.

Приметимо да је $\sum_{d|n} \lambda(d) = \sum_{d|n} \lambda(d) \cdot 1 = \sum_{d|n} \lambda(d)\mathbb{1}(n/d) = \lambda * \mathbb{1}(n)$, одакле видимо да је тражена сума МАФ као конволуција две МАФ, па је довољно израчунати је на степенима простих бројева. $\sum_{d|p^\alpha} \lambda(d) = \sum_{i=0}^{\alpha} \lambda(p^i) = 1 + \lambda(p) + \lambda(p^2) + \lambda(p^3) + \dots + \lambda(p^\alpha) = 1 + (-1) + 1 + (-1) + \dots + (-1)^\alpha = \begin{cases} 0 & \alpha \text{ непарно} \\ 1 & \alpha \text{ парно} \end{cases}$. Према томе, ако је $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $\sum_{d|n} \lambda(d) = 1$ акко су сви α_i парни, иначе је 0. Дакле, $\sum_{d|n} \lambda(d) = 1$ акко је n квадрат, иначе је 0.

Приметимо $\sum_{d|n} \lambda(d)|\mu(n/d)| = \sum_{d|n} \lambda(d)|\mu|(n/d) = \lambda * |\mu|(n)$, одакле закључујемо да је тражена сума МАФ као конволуција две МАФ, па је довољно израчунати је на степенима простих бројева. $\sum_{d|p^\alpha} \lambda(d)|\mu(n/d)| = \sum_{i=0}^{\alpha} \lambda(p^i)|\mu(p^{\alpha-i})| = \lambda(p^\alpha)|\mu(1)| + \lambda(p^{\alpha-1})|\mu(p)| + 0 = (-1)^\alpha + (-a)^{\alpha-1} = 0$.
Према томе тражена сума је једнака ε, тј. $\lambda * |\mu| = \varepsilon$. □

Ојлерова функција Нека је за $n \geq 1$, $\Phi_n = \{k \mid 1 \leq k \leq n, (k, n) = 1\}$. Скуп Φ_n зовемо Ојлеров скуп. Дефинишемо (очигледно АФ) $\varphi : \mathsf{N}^+ \longrightarrow \mathsf{N}$ са $\varphi(n) = |\Phi_n|$. Дакле, $\varphi(n)$ је број узајамно простих бројева са n, мањих од n. Функцију φ зовемо Ојлерова функција.

95.

1) $\sum_{d|n} \varphi(d) = n$, тј. $\varphi * \mathbb{1} = \mathrm{I}$.

2) $\varphi = \mathrm{I} * \mu$, тј. $\varphi(n) = \sum_{d|n} d\mu(n/d) = \sum_{d|n} n/d\mu(d) = n \sum_{d|n} \mu(d)/d$.

3) φ је МАФ.

Решење. Главни проблем је доказати 1). 2) следи из 1) по Мебиусовој теореми инверзије, а 3) следи из 2) јер је конволуција две МАФ поново МАФ.

1) Нека је G циклична група реда n. Посматрајмо подскупове ог G: $G_d = \{g \in G \mid r(g) = d\}$. Дакле, G_d чине сви елементи групе G реда d. Како нам Лагранжова теорема каже да ред елемента дели ред групе, то закључујемо да је $G = \bigsqcup_{d|n} G_d$, одакле је $n = \sum_{d|n} |G_d|$. Одавде је довољно још доказати да је $|G_d| = \varphi(d)$.

Ако су $a, b \in G_d$, тада и a и b генеришу цикличне подгрупе од G са d елемената. Међутим како је код цикличних група таква подгрупа јединствена, то закључујемо да је $\langle a \rangle = \langle b \rangle$. Према томе број елемената у G_d је једнак броју генератора подгрупе $\langle a \rangle$. Међутим, знамо да је a^k генератор од $\langle a \rangle$ акко $(k, r(a)) = 1$, тј. $(k, d) = 1$. Према томе $\langle a \rangle$ има $\varphi(d)$ генератора, тј. $|G_d| = \varphi(d)$. □

96. Израчунати $\varphi(n)$.

Решење. Како је φ МАФ, довољно је израчунати њене вредности на степенима простих бројева.

$\varphi(p^\alpha)$ је број природних бројева мањих од p^α узајамно простих са p^α. Број k, $1 \le k \le p^\alpha$, није узајамно прост са p^α акко је дељив са p. Бројеви дељиви са p су: $p, 2p, 3p, \ldots, p \cdot p, (p+1)p, \ldots, p^{\alpha-1}p = p^\alpha$, или сваки p-ти број је дељив са p. Према томе постоји $p^{\alpha-1}$ бројева који нису узајамно прости са p^α, па је $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - 1/p)$.

Дакле, ако је $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, тада је $\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \ldots \varphi(p_k^{\alpha_k}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \ldots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) = p_1^{\alpha_1}(1 - 1/p_1)p_2^{\alpha_2}(1 - 1/p_2) \ldots p_k^{\alpha_k}(1 - 1/p_k) = n(1 - 1/p_1)(1 - 1/p_k) \ldots (1 - 1/p_k) = n \prod_{\substack{p|n \\ p \text{ прост}}} (1 - 1/p)$. □

97. Израчунати следеће суме:

1) $\sum_{d|n} \mu(n/d)\tau(d)$; 2) $\sum_{d|n} \mu(n/d)\sigma(d)$; 3) $\sum_{d|n} \mu(d)\varphi(d)$;

4) $\sum_{d|n} \mu(d)^2\varphi(d)^2$; 5) $\sum_{d|n} \mu(d)/\varphi(d)$.

Решење. 1) Сетимо се да је $\tau = \mathbb{1} * \mathbb{1}$. Зато је $\sum_{d|n} \mu(n/d)\tau(d) = \mu * \tau(n) = \mu * \mathbb{1} * \mathbb{1}(n) = \varepsilon * \mathbb{1}(n) = \mathbb{1}(n) = 1$.

2) Сетимо се да је $\sigma = \mathbb{1} * \mathrm{I}$. Зато је $\sum_{d|n} \mu(n/d)\sigma(d) = \mu * \sigma(n) = \mu * \mathbb{1} * \mathrm{I}(n) = \varepsilon * \mathrm{I}(n) = \mathrm{I}(n) = n$.

3) $\mu\varphi$ је МАФ као производ МАФ. Израчунајмо најпре $\mu\varphi(n)$; довољно је израчунати на степенима простих бројева. $\mu\varphi(p^\beta) = \mu(p^\beta)\varphi(p^\beta) = \begin{cases} 0 & \beta \ge 2 \\ 1 - p & \beta = 1 \end{cases}$

Сада је $\sum_{d|n}\mu(d)\varphi(d) = \sum_{d|n}\mu\varphi(d) = \mathbb{1}*\mu\varphi(n)$, $\mathbb{1}*\mu\phi$ је МАФ, па је довољно израчунати тражену суму на степенима простих бројева. $\sum_{d|p^\alpha}\mu\varphi(d) = \sum_{i=0}^{\alpha}\mu\varphi(p^i) = \mu\varphi(1)+\mu\varphi(p)+\mu\varphi(p^2)+\ldots+\mu\varphi(p^\alpha) = 1+1-p+0+\ldots+0 = 2-p$.

Дакле, за $n = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, $\sum_{d|n}\mu(d)\varphi(d) = (2-p_1)(2-p_2)\ldots(2-p_k)$.

4) $\mu^2\varphi^2$ је МАФ као производ МАФ. Израчунајмо најпре $\mu^2\varphi^2(n)$; довољно је израчунати на степенима простих бројева. $\mu^2\varphi^2(p^\beta) = \mu(p^\beta)^2\varphi(p^\beta)^2 = \begin{cases} 0 & \beta \geq 2 \\ (p-1)^2 & \beta = 1 \end{cases}$

Сада је $\sum_{d|n}\mu(d)^2\varphi(d)^2 = \sum_{d|n}\mu^2\varphi^2(d) = \mathbb{1}*\mu^2\varphi^2(n)$, $\mathbb{1}*\mu^2\phi^2$ је МАФ, па је довољно израчунати тражену суму на степенима простих бројева. $\sum_{d|p^\alpha}\mu^2\varphi^2(d) = \sum_{i=0}^{\alpha}\mu^2\varphi^2(p^i) = \mu^2\varphi^2(1)+\mu^2\varphi^2(p)+\mu^2\varphi^2(p^2)+\ldots+\mu^2\varphi^2(p^\alpha) = 1+(p-1)^2+0+\ldots+0 = p^2-2p+2$.

Дакле, за $n = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, $\sum_{d|n}\mu(d)\varphi(d) = (p_1^2-2p_1+2)(p_2^2-2p_2+2)\ldots(p_k^2-2p_k+2)$.

5) μ/φ је МАФ као количник МАФ (приметите да је количник дефинисан, јер $\varphi(n)\neq 0$, за све $n \geq 0$). Израчунајмо најпре $\mu/\varphi(n)$; довољно је израчунати на степенима простих бројева. $\mu/\varphi(p^\beta) = \mu(p^\beta)/\varphi(p^\beta) = \begin{cases} 0 & \beta \geq 2 \\ 1/(1-p) & \beta = 1 \end{cases}$

Сада је $\sum_{d|n}\mu(d)/\varphi(d) = \sum_{d|n}\mu/\varphi(d) = \mathbb{1}*\mu/\varphi(n)$, $\mathbb{1}*\mu/\phi$ је МАФ, па је довољно израчунати тражену суму на степенима простих бројева. $\sum_{d|p^\alpha}\mu/\varphi(d) = \sum_{i=0}^{\alpha}\mu/\varphi(p^i) = \mu/\varphi(1)+\mu/\varphi(p)+\mu/\varphi(p^2)+\ldots+\mu/\varphi(p^\alpha) = 1+1/(1-p)+0+\ldots+0 = (p-2)/(p-1)$.

Дакле, за $n = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, $\sum_{d|n}\mu(d)\varphi(d) = (p_1-2)(p_2-2)\ldots(p_k-2)/(p_1-1)(p_2-1)\ldots(p_k-1)$.

□

98. Израчунати $\sum_{\substack{1\leq k\leq n\\(k,n)=1}} k$.

Решење. За $n = 1, 2$ је лако израчунати дату суму. Нека је $n \geq 3$. Приметимо да је $(k,n) = 1$ акко $(n-k,n) = 1$. Такође приметимо да за $(k,n) = 1$ важи $k \neq n-k$. Према томе елементи узајамно прости са n се јављају у паровима: $(k, n-k)$. Сума сваког пара је n, а парова очигледно има $\phi(n)/2$. Према томе, дата сума је једнака $n\phi(n)/2$. □

Дирихлеов инверз АФ f је функција g (која се испостави да је АФ) таква да је $f*g = \varepsilon$ (дакле, инвезна функција у односу на операцију конволуције). Примера ради, видели смо да су $\mathbb{1}$ и μ међусобно једна другој Дирихлеов инверз, такође, λ и $|\mu|$ су једна другој Дирихлеов инверз.

Ако је f АФ, она има Дирихлеов инверз: посматрајмо једнакост $f*g = \varepsilon$. $f*g(1) = \varepsilon(1) = 1$ значи $f(1)g(1) = 1$, па како је $f(1) = 1$, мора бити и $g(1) = 1$. За $n > 1$ имамо $f*g(n) = \varepsilon(n) = 0$, тј. $0 = \sum_{d|n}f(d)g(n/d) = f(1)g(n)+\sum_{\substack{d|n\\d>1}}f(d)g(n/d) = g(n)+\sum_{\substack{d|n\\d>1}}f(d)g(n/d)$, одакле је

$g(n) = -\sum_{\substack{d|n \\ d>1}} f(d)g(n/d)$, па видимо да се вредност од g може израчунати из вредности f и раније израчунатих вредности од g. Према томе, Дирихлеов инверз од f постоји и јесте АФ.

Ако је f МАФ, испоставља се да јој је Дирихлеов инверз g МАФ, па је довољно спровести претходни рачун на степенима простих бројева, тј.

$$g(p^\alpha) = -\sum_{\substack{d|p^\alpha \\ d>1}} f(d)g(n/d) = -\sum_{i=1}^{\alpha} f(p^i)g(p^{\alpha-i}).$$

99. Израчунати Дирихлеове инверзе фукнција:
1) τ; 2) σ; 3) φ.

Решење. 1) Означимо са g Дирихлеов инверз од τ. $g(1) = 1$. Према датој формули рачунамо $g(p^\alpha)$.

$g(p) = -\tau(p)g(1) = -2$;
$g(p^2) = -\tau(p)g(p) - \tau(p^2)g(1) = -2 \cdot (-2) - 3 = 1$;
$g(p^3) = -\tau(p)g(p^2) - \tau(p^2)g(p) - \tau(p^3)g(1) = -2 \cdot 1 - 3 \cdot (-2) - 4 = 0$;
$g(p^4) = -\tau(p)g(p^3) - \tau(p^2)g(p^2) - \tau(p^3)g(p) - \tau(p^4)g(1) = -2 \cdot 0 - 3 \cdot 1 - 4 \cdot (-2) - 5 = 0$.

Сада већ наслућујемо шта ће бити инверз од τ. Посматрајмо МАФ g дату са $g(1) = 1$ и $g(p^\alpha) = \begin{cases} -2 & \alpha = 1 \\ 1 & \alpha = 2 \\ 0 & \alpha \geq 3 \end{cases}$ Докажимо да је $\tau * g = \varepsilon$. Јасно је $\tau * g(1) = \varepsilon(1)$. Како су и τ и уочена g МАФ, то је и $\tau * g$ МАФ, па је довољно проверити да је $\tau * g = \varepsilon$ на степенима простих бројева.

$\tau * g(p^\alpha) = 0$, за $\alpha = 1, 2, 3, 4$, што се види из рачуна горе (тако смо дефинисали g). Ако је $\alpha \geq 5$ имамо: $\tau * g(p^\alpha) = \tau(p^\alpha)g(1) + \tau(p^{\alpha-1})g(p) + \tau(p^{\alpha-2})g(p^2) + \tau(p^{\alpha-3})g(p^3) + \ldots \tau(1)g(p^\alpha) = (\alpha+1) \cdot 1 + \alpha \cdot (-2) + (\alpha-1) \cdot 1 + (\alpha-2) \cdot 0 + \ldots + 1 \cdot 0 = 0 = \varepsilon(p^\alpha)$, што смо и желели да докажемо.

2) Означимо са g Дирихлеов инверз од σ. $g(1) = 1$. Према датој формули рачунамо $g(p^\alpha)$.

$g(p) = -\sigma(p)g(1) = -(p+1)$;
$g(p^2) = -\sigma(p)g(p) - \sigma(p^2)g(1) = -(p+1) \cdot (-(p+1)) - (p^2+2+1) = p$;
$g(p^3) = -\sigma(p)g(p^2) - \sigma(p^2)g(p) - \sigma(p^3)g(1) = -(p+1) \cdot p - (p^2+p+1) \cdot (-(p+1)) - (p^3+p^2+p+1) = 0$;
$g(p^4) = -\sigma(p)g(p^3) - \sigma(p^2)g(p^2) - \sigma(p^3)g(p) - \sigma(p^4)g(1) = -(p+1) \cdot 0 - (p^2+p+1) \cdot p - (p^3 + p^2 + p + 1) \cdot (-(p+1)) - (p^4 + p^3 + p^2 + p + 1) = 0$.

Сада већ наслућујемо шта ће бити инверз од σ. Посматрајмо МАФ g дату са $g(1) = 1$ и $g(p^\alpha) = \begin{cases} -(p+1) & \alpha = 1 \\ p & \alpha = 2 \\ 0 & \alpha \geq 3 \end{cases}$ Докажимо да је $\sigma * g = \varepsilon$. Јасно је $\sigma * g(1) = \varepsilon(1)$. Како су и σ и уочена g МАФ, то је и $\sigma * g$ МАФ, па је довољно проверити да је $\sigma * g = \varepsilon$ на степенима простих бројева.

$\sigma * g(p^\alpha) = 0$, за $\alpha = 1, 2, 3, 4$, што се види из рачуна горе (тако смо дефинисали g). Ако је $\alpha \geq 5$ имамо: $\sigma * g(p^\alpha) = \sigma(p^\alpha)g(1) + \sigma(p^{\alpha-1})g(p) + \sigma(p^{\alpha-2})g(p^2) + \sigma(p^{\alpha-3})g(p^3) + \ldots \sigma(1)g(p^\alpha) = \sum_{i=0}^{\alpha} p^i - (p+1)\sum_{i=0}^{\alpha-1} p^i + p\sum_{i=0}^{\alpha-2} p^i + 0 \ldots + 0 = \sum_{i=0}^{\alpha} p^i - \sum_{i=0}^{\alpha-1} p^{i+1} - \sum_{i=0}^{\alpha-1} p^i + \sum_{i=0}^{\alpha-2} p^{i+1} = (\sum_{i=0}^{\alpha} p^i - \sum_{i=1}^{\alpha} p^i) + \big(-\sum_{i=0}^{\alpha-1} p^i + \sum_{i=1}^{\alpha-1} p^i\big) = 1 - 1 = 0 = \varepsilon(p^\alpha)$, што смо и желели да докажемо.

3) Означимо са g Дирихлеов инверз од φ. $g(1) = 1$. Према датој формули рачунамо $g(p^\alpha)$.

$g(p) = -\varphi(p)g(1) = 1 - p$;
$g(p^2) = -\varphi(p)g(p) - \varphi(p^2)g(1) = -(p-1) \cdot (1-p) - (p^2-p) = 1-p$;
$g(p^3) = -\varphi(p)g(p^2) - \varphi(p^2)g(p) - \varphi(p^3)g(1) = -(p-1) \cdot (1-p) - (p^2-p) \cdot (1-p) - (p^3-p^2) = 1-p$.

Сада већ наслућујемо шта ће бити инверз од φ. Посматрајмо МАФ g дату са $g(1) = 1$ и $g(p^\alpha) = 1 - p$ Докажимо да је $\varphi * g = \varepsilon$. Јасно је $\varphi * g(1) = \varepsilon(1)$. Како су и φ и уочена g МАФ, то је и $\varphi * g$ МАФ, па је довољно проверити да је $\varphi * g = \varepsilon$ на степенима простих бројева.

$\varphi * g(p^\alpha) = 0$, за $\alpha = 1, 2, 3$, што се види из рачуна горе (тако смо дефинисали g). Ако је $\alpha \geq 4$ имамо: $\varphi * g(p^\alpha) = \varphi(p^\alpha)g(1) + \varphi(p^{\alpha-1})g(p) + \ldots + \varphi(1)g(p^\alpha) = (p^\alpha - p^{\alpha-1}) + (1-p)(p^{\alpha-1} - p^{\alpha-2} + p^{\alpha-2} - p^{\alpha-3} + \ldots + p - 1 + 1) = p^\alpha - p^{\alpha-1} + (1-p)p^{\alpha-1} = 0 = \varepsilon(p^\alpha)$, што смо и желели да докажемо. □

Ојлерова теорема $(\Phi_n, \cdot_n)$ је група (зовемо је Ојлерова група) и њен ред је $\varphi(n)$. Према Лагранжовој теореми за $k \in \Phi_n$ имамо $k^{\varphi(n)} = 1$ у Φ_n, тј. $k^{\varphi(n)} = 1 \mod n$. Дакле, ако $1 \leq k \leq n$ и $(k, n) = 1$, тада је $k^{\varphi(n)} = 1 \mod n$. Ако је $(a, n) = 1$, тада је $a = qn + k$, где $1 \leq k < n$ и важи $(k, n) = 1$, па је $a^{\varphi(n)} = k^{\varphi(n)} \mod n = 1 \mod n$. Према томе Ојлерова теорема каже: ако $(a, n) = 1$, тада је $a^{\varphi(n)} = 1 \mod n$. Специјално, ако узмемо за $n = p$ прост број добијамо Малу Фермаову теорему: ако $p \nmid a$, тада је $a^{p-1} = 1 \mod p$.

100. Израчунати остатак при дељену $x = 3333^{3333^{3333}}$ са 25.

Решење. Најпре приметимо да је $x = 3333^{3333^{3333}} = 8^{3333^{3333}} \mod 25$, јер је $3333 = 8 \mod 25$. Користимо Ојлерову теорему: $(8, 25) = 1$, па је $8^{\varphi(25)} = 1 \mod 25$. Знамо да је $\varphi(25) = 25 - 5 = 20$, па је $8^{20} = 1 \mod 25$, те ако запишемо $3333^{3333} = 20q + r$, тада је $x = 8^{20q+r} \mod 25 = (8^2 0)^q 8^r \mod 25 = 8^r \mod 25$. Израчунајмо зато r.

r је остатак при дељењу $y = 3333^{3333}$ са 20. Како је $3333 = 13 \mod 20$, то је $y = 3333^{3333} = 13^{3333} \mod 20$. КОристимо поново Ојлерову теорему: $(13, 20) = 1$ и $\varphi(20) = \varphi(4)\varphi(5) = 8$, па је $13^8 = 1 \mod 20$. Ако запишемо $3333 = 8q' + r'$, тада је $y = 13^{8q'+r'} \mod 20 = (13^8)^{q'} 13^{r'} \mod 20 = 13^{r'} \mod 20$. Израчунајмо зато r'.

r' је остатак при дељењу 3333 са 8, па се лако види да је $r' = 5$. Сада се враћамо назад. $y = 13^{r'} \mod 20 = 13^5 \mod 20 = 169 \cdot 169 \cdot 13 \mod 20 = 9 \cdot 9 \cdot 13 \mod 20 = 81 \cdot 13 \mod 20 = 1 \cdot 13 \mod 20 = 13 \mod 20$. Дакле, $r = 13$. Поново се враћамо назад. $x = 8^r \mod 25 = 8^{13} \mod 25 = 8 \cdot (8^3)^4 \mod 25 = 8 \cdot 512^4 \mod 25 = 8 \cdot 12^4 \mod 25 = 8 \cdot 144 \cdot 144 \mod 25 = 8 \cdot (-6) \cdot (-6) \mod 25 = 8 \cdot 36 \mod 25 = 8 \cdot 11 \mod 25 = 88 \mod 25 = 13$. Дакле, тражени остатак је 13. □

101. Ако су p и q различити непарни прости бројеви такви да $p - 1 \mid q - 1$, и ако је n такав да $(n, pq) = 1$, доказати да је $n^{q-1} = 1 \mod pq$.

Решење. Како је $(n, pq) = 1$, то је и $(n, p) = 1$ и $(n, q) = 1$. По Ојеровој теореми (или Малој Фермаовој теореми) је $n^{p-1} = 1 \mod p$ и $n^{q-1} = 1 \mod q$. Како $p - 1 \mid q - 1$, то $q - 1 = (p - 1)k$, па је $n^{q-1} = n^{(p-1)k} = (n^{p-1})^k = 1^k \mod p = 1 \mod p$. Према томе: $n^{q-1} = 1 \mod p$ и $n^{q-1} = 1 \mod q$, тј. $p, q \mid n^{q-1} - 1$, па како је $(p, q) = 1$, то и $pq \mid n^{q-1} - 1$, тј. $n^{q-1} = 1 \mod pq$. □

Кинеска теорема о остацима Нека су $m_1, m_2, \ldots, m_k$ по паровима узајамно прости бројеви и $a_1, a_2, \ldots, a_k$ произвољни цели бројеви. Тада систем конгруенција

$$x = a_i \mod m_i,\ 1 \leq i \leq k$$

има решење, и постоји јединствено решење x_0 које задовољава $0 \leq x_0 < M = m_1 m_2 \ldots m_k$, а сва остала су дата формулом $x = x_0 + tM$, где $t \in \mathsf{Z}$.

Конструктивни доказ (који користимо у задацима) изгледа овако. Означимо са $M_i = m/m_i$, $1 \leq i \leq k$. Према услову за бројеве $m_1, m_2, \ldots, m_k$ имамо да је $(m_i, M_i) = 1$, $1 \leq\leq k$. Према томе постоје цели бројеви α_i, β_i такви да $\alpha_i m_i + \beta_i M_i = 1$. Приметимо да је $\beta_i M_i = 1 \mod m_i$ (што следи из дате једнакости по модулу m_i) и очигледно $\beta_i M_i = 0 \mod m_j$, када $j \neq i$.

Посматрајмо $x' = \beta_1 M_1 a_1 + \beta_2 M_2 a_2 + \ldots + \beta_k M_k a_k$. $x' = \beta_i M_i a_i \mod m_i$, јер сви остали сабирци нестану по модулу m_i, а одавде је $x' = \beta_i M_i a_i \mod m_i = 1 \cdot a_i \mod m_i = a_i \mod m_i$, и ово важи за све $1 \leq i \leq k$. Дакле, x' је једно решење датог система. Ако узмемо x_0 да је остатак при дељењу x' са M, тада је $x_0 = x' \mod M$, па је $x_0 = x' \mod m_i = a_i \mod m_i$, за све $1 \leq i \leq k$, тј. и x_0 је једно решење датог система које задовољава и $0 \leq x_0 < M$.

Дато решење је јединствено, јер ако је x_1 још једно решење система такво да $0 \leq x_1 < M$, тада је $-M < x_0 - x_1 < M$, и $x_0 - x_1 = 0 \mod m_i$, за све $1 \leq i \leq k$, па је $x_0 - x_1 = 0 \mod M$, а једини елемент већи од $-M$ и мањи од M дељив са M је 0, па је $x_0 - x_1 = 0$, тј. $x_0 = x_1$.

Према томе, ако је x произвољно решење, тада је $x = x_0 \mod M$, па је $x = x_0 + tM$, за неко цело t. А такође $x_0 + tM$ очигледно јесу решења датог система, јер x_0 јесте решење.

Алгоритам за налажење решења једначине $ax + by = 1$ Ако $(a, b) = 1$, тада $ax + by = 1$ има целобројно решење. Дајемо један алгоритам за његово налажење. Уожимо матрицу $A_0 = \begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$. Градимо низ матрица $(A_i)_{i\geq 0}$ на следећи начин: матрицу A_{i+1} добијамо тако што помножимо неку врсту (свеједно коју) матрице A_i ненула целим број λ и додамо је другој врсти, док она сама остаје непромењена. Изграђене матрице имају занимљиву особину: ако означимо са a_i^{jk} елемент на месту (j, k) у матрици A_i, тада је $a_i^{11} = a_i^{12}a + a_i^{13}b$ и $a_i^{21} = a_i^{22}a + a_i^{23}b$. Докажимо ово индукцијом по i. За $i = 0$ је лако јер: $a_0^{11} = a$ и $a_0^{12}a + a_0^{13}b = 1 \cdot a + 0 \cdot b = a$, и слично $a_0^{21} = b$ и $a_0^{22}a + a_0^{23}b = 0 \cdot a + 1 \cdot b = b$.

Претпоставимо да је $a_i^{11} = a_i^{12}a + a_i^{13}b$ и $a_i^{21} = a_i^{22}a + a_i^{23}b$. Без умањења општости претпоставимо да смо A_{i+1} добили тако што смо ПРВУ врсту матрице A_i помножили са λ и додали је ДРУГОЈ врсти. Тада је $a_{i+1}^{11} = a_i^{11}$, $a_{i+1}^{12} = a_i^{12}$ и $a_{i+1}^{13} = a_i^{13}$, па је $a_{i+1}^{11} = a_{i+1}^{12}a + a_{i+1}^{13}b$, јер је то важило по индукцијској хипотези и у матрици A_i. Што се тиче друге врсте, њени елементи су: $a_{i+1}^{21} = a_i^{21} + \lambda a_i^{11}$, $a_{i+1}^{22} = a_i^{22} + \lambda a_i^{12}$ и $a_{i+1}^{23} = a_i^{23} + \lambda a_i^{13}$. Тада је $a_{i+1}^{22}a + a_{i+1}^{23}b = (a_i^{22} + \lambda a_i^{12})a + (a_i^{23} + \lambda a_i^{13})b = (a_i^{22}a + a_i^{23}b) + \lambda(a_i^{12}a + a_i^{13}b) = a_i^{21} + \lambda a_i^{11} = a_{i+1}^{21}$. Тиме је доказ завршен.

Дакле, ако полазећи од матрице A_0, користећи дату трансформацију, смањујемо апсолутну вредност елемената у првој колони, како $(a, b) = 1$, у једном тренутку ћемо завршити са 1 негде у првој колони, тада према претходно доказаном ће нам решење бити записано у врсти која садржи ту 1.

Примера ради, $(110, 273) = 1$, нађимо x, y тако да $110x + 273y = 1$. Урадимо алгоритам:

$$\begin{pmatrix} 110 & 1 & 0 \\ 273 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 110 & 1 & 0 \\ 53 & -2 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 4 & 5 & -2 \\ 53 & -2 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 4 & 5 & -2 \\ 1 & -67 & 27 \end{pmatrix}.$$

Решење је: $1 = -67 \cdot 110 + 27 \cdot 273$, а трансформисали смо овако: 1) прву врсту помножену са -2 смо додали другој; 2) другу врсту помножену са -2 смо додали првој; 3) прву врсту помножену са -13 смо додали другој.

102. Решити систем конгруенција: $x = 2 \mod 7$, $x = 1 \mod 11$, $x = 9 \mod 13$.

Решење. Пратимо алгоритам дат у доказу Кинеске теореме о остацима. $(7, 11 \cdot 13) = 1$ па запишимо $\alpha_1 \cdot 7 + \beta_1 \cdot 11 \cdot 13 = 1$. Занима нас неко решење ове једнакости.

$$\begin{pmatrix} 7 & 1 & 0 \\ 143 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 7 & 1 & 0 \\ 3 & -20 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 41 & -2 \\ 3 & -20 & 1 \end{pmatrix}$$

Дакле, узмимо $\beta_1 = -2$. $(11, 7 \cdot 13) = 1$ па запишимо $\alpha_2 \cdot 11 + \beta_2 \cdot 7 \cdot 13 = 1$. Занима нас неко решење ове једнакости.

$$\begin{pmatrix} 11 & 1 & 0 \\ 91 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 11 & 1 & 0 \\ 3 & -8 & 1 \end{pmatrix} \mapsto \begin{pmatrix} -1 & 33 & -4 \\ 3 & -8 & 1 \end{pmatrix}$$

Дакле, узмимо $\beta_2 = 4$. $(13, 7 \cdot 11) = 1$ па запишимо $\alpha_3 \cdot 13 + \beta_3 \cdot 7 \cdot 11 = 1$. Занима нас неко решење ове једнакости.

$$\begin{pmatrix} 13 & 1 & 0 \\ 77 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 13 & 1 & 0 \\ -1 & -6 & 1 \end{pmatrix}$$

Дакле, узмимо $\beta_3 = -1$.

Једно решење датог система је: $x' = \beta_1 \cdot 11 \cdot 13 \cdot 2 + \beta_2 \cdot 7 \cdot 13 \cdot 1 + \beta_3 \cdot 7 \cdot 11 \cdot 9 = -2 \cdot 11 \cdot 13 \cdot 2 + 4 \cdot 7 \cdot 13 \cdot 1 + (-1) \cdot 7 \cdot 11 \cdot 9 = \ldots = -901$. Канонско решење по модулу $7 \cdot 11 \cdot 13 = 1001$ је $x_0 = 100$. □

103. Решити систем конгруенција: $x = 2 \mod 4$, $2x = 1 \mod 5$, $3x = 1 \mod 7$.

Решење. Приметимо да је $2 \cdot 3 = 1 \mod 5$, па је $2x = 1 \mod 5$ акко $x = 3 \mod 5$ (када прву једнакост помножимо са 3 добијемо другу, а када другу помножимо са 2 добијемо прву). Такође, $3 \cdot 5 = 1 \mod 7$, па је $3x = 1 \mod 7$ акко $x = 5 \mod 7$. Тиме смо свели проблем на решавање система: $x = 2 \mod 4$, $x = 3 \mod 5$, $x = 5 \mod 7$. Користимо алгоритам дат у доказу Кинеске теореме о остацима.

$(4, 5 \cdot 7) = 1$ и очигледно је $9 \cdot 4 - 1 \cdot 5 \cdot 7 = 1$. $(5, 4 \cdot 7) = 1$ и очигледно је $-11 \cdot 5 + 2 \cdot 4 \cdot 7 = 1$. $(7, 4 \cdot 5) = 1$ и очигледно је $-17 \cdot 7 + 6 \cdot 4 \cdot 5 = 1$. Према томе једно решење је $x' = -1 \cdot 5 \cdot 7 \cdot 2 + 2 \cdot 4 \cdot 7 \cdot 3 + 6 \cdot 4 \cdot 5 \cdot 5 = -70 + 168 + 600 = 698$. Канонско решење по модулу $4 \cdot 5 \cdot 7 = 140$ је $x_0 = 138$. □

104. Одредити последње две цифре броја $n = 402^{303^{204}}$.

Решење. Задатак је заправо наћи остатак при дељењу $402^{303^{204}}$ са 100. $100 = 4 \cdot 25$ и $(4, 25) = 1$, па ћемо наћи остатак при дељењу n са 4 и n са 25, па ћемо на то применити Кинеску теорему о остацима.

Очигледно је $n = 0 \mod 4$. $n = 402^{303^{204}} = 2^{303^{204}} \mod 25$. Како је $(2, 25) = 1$ можемо применити Ојлерову теорему.

Дакле, тражимо $303^{204} \mod \varphi(25)$, тј. $303^{204} \mod 20$. $303^{204} = 3^{204} \mod 20$. Како је $(3, 20) = 1$ можемо и овде применити Ојлерову теорему.

Дакле, тражимо $204 \mod \varphi(20)$, тј. $204 \mod 8$. Очигледно је $204 = 4 \mod 8$. Сада се враћамо у назад.

$204 = 8q + 4$, па је $303^{204} = 3^{204} \mod 20 = (3^8)^q 3^4 \mod 20 = 3^4 \mod 20 = 81 \mod 20 = 1 \mod 20$, јер је према Ојлеровој теореми $3^8 = 1 \mod 20$. Поново идемо корак у назад.

$303^{204} = 20q' + 1$, па је $n = 2^{303^{204}} \mod 25 = (2^{20})^{q'} 2^1 \mod 25 = 2 \mod 25$, јер је према Ојлеровој теореми $2^{20} = 1 \mod 20$. Према томе $n = 2 \mod 25$.

Сада решавамо систем: $x = 0 \mod 4$, $x = 2 \mod 25$. Решење је јасно и без примене Кинеске теореме о остацима: $x_0 = 52$, тј. $n = 52 \mod 100$. Према томе последње две цифре броја n су 52. □

105. Наћи остатак при дељењу $n = 1406^{2010}$ са $1105 = 5 \cdot 13 \cdot 17$.

Решење. Наћи ћемо остатке при дељењу n са 5, 13 и 17, па ћемо применити Кинеску теорему о остацима.

$n = 1406^{2010} = 1^{2010} \mod 5 = 1 \mod 5$.

$n = 1406^{2010} = 2^{2010} \mod 13$. Како је $\varphi(13) = 12$, како је $(2, 13) = 1$ и како је $2010 = 6 \mod 12$, то је према Ојлеровој теореми $n = 2^{2010} \mod 13 = 2^6 \mod 13 = 64 \mod 13 = -1 \mod 13$.

$n = 1406^{2010} = 12^{2010} \mod 17$. Како је $\varphi(17) = 16$, како је $(12, 17) = 1$ и како је $2010 = 10 \mod 16$, то је према Ојлеровој теореми $n = 12^{2010} \mod 17 = 12^{10} \mod 17 = (-5)^{10} \mod 17 = 5^{10} \mod 17 = 25^5 \mod 17 = 8^5 \mod 17 = 8 \cdot 64 \cdot 64 \mod 17 = 8 \cdot 13 \cdot 13 \mod 17 = 8 \cdot (-4) \cdot (-4) \mod 17 = 8 \cdot 16 \mod 17 = 8 \cdot (-1) \mod 17 = -8 \mod 17 = 9 \mod 17$.

Сада посматрамо систем: $x = 1 \mod 5$, $x = -1 \mod 13$, $x = 9 \mod 17$. Његово канонско решење је решење задатка. Примењујемо Кинеску теорему о остацима.

$13 \cdot 17 = 221$ и:

$$\begin{pmatrix} 5 & 1 & 0 \\ 221 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 5 & 1 & 0 \\ 1 & -44 & 1 \end{pmatrix}$$

$5 \cdot 17 = 85$ и:

$$\begin{pmatrix} 13 & 1 & 0 \\ 85 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 13 & 1 & 0 \\ 7 & -6 & 1 \end{pmatrix} \mapsto \begin{pmatrix} -1 & 13 & -2 \\ 7 & -6 & 1 \end{pmatrix}$$

$5 \cdot 13 = 65$ и:

$$\begin{pmatrix} 17 & 1 & 0 \\ 65 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 17 & 1 & 0 \\ -3 & -4 & 1 \end{pmatrix} \mapsto \begin{pmatrix} -1 & -23 & 6 \\ -3 & -4 & 1 \end{pmatrix}$$

Пратећи алгоритам, једно решење је $x' = 1 \cdot 221 \cdot 1 + 2 \cdot 85 \cdot (-1) + (-6) \cdot 65 \cdot 9 = 221 - 170 - 3510 = -3459$. Канонско решење по модулу 1105 је $x_0 = 961$. □

Риманова зета функција

Прва теорема о изоморфизму

Језгро хомоморфизам Нека је $f : G \longrightarrow H$ хомоморфизам група. Језгро хомоморфизма f је $\mathrm{Ker}(f) = \{g \in G \mid f(g) = e_H\} \subseteq G$, дакле скуп свих елемената из G који се сликају у неутрал у H.

106. Доказати да је $\mathrm{Ker}(f) \triangleleft G$.

Решење. Најпре докажимо да је $\mathrm{Ker}(f) \leq G$. Како је $f(e_G) = e_H$, то $e_G \in \mathrm{Ker}(f)$. Ако $x \in \mathrm{Ker}(f)$, тј. ако $f(x) = e_H$, тада $f(x^{-1}) = f(x)^{-1} = e_H^{-1} = e_H$, па и $x^{-1} \in \mathrm{Ker}(f)$. Коначно, ако $x, y \in \mathrm{Ker}(f)$, тј. ако $f(x) = f(y) = e_H$, тада $f(xy) = f(x)f(y) = e_H e_H = e_H$, па и $xy \in \mathrm{Ker}(f)$. Дакле, $\mathrm{Ker}(f) \leq G$.

Ако $x \in \mathrm{Ker}(f)$, тј. ако $f(x) = e_H$, и ако је $g \in G$ произвољан елемент, тада је $f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)e_H f(g)^{-1} = f(g)f(g)^{-1} = e_H$, па $gxg^{-1} \in \mathrm{Ker}(f)$, што доказује да $\mathrm{Ker}(f) \triangleleft G$. □

107. Доказати да је f 1-1 акко $\mathrm{Ker}(f) = \langle e_G \rangle$.

Решење. $\Rightarrow$) Нека је f 1-1. Нека је $x \in \mathrm{Ker}(f)$. Тада је $f(x) = e_H = f(e_G)$, па како је f 1-1, то је $x = e_G$. Дакле, $\mathrm{Ker}(f) = \langle e_G \rangle$.

$\Leftarrow$) Нека је $\mathrm{Ker}(f) = \langle e_G \rangle$. Нека је $f(x) = f(y)$. Тада је $e_H = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$, тј. $xy^{-1} \in \mathrm{Ker}(f)$, па како је $\mathrm{Ker}(f) = \langle e_G \rangle$, то је $xy^{-1} = e_G$, одакле следи $x = y$. Дакле, f је 1-1. □

Слика хомоморфизма Нека је $f : G \longrightarrow H$ хомоморфизам група. Слика хомоморфизма f је $\mathrm{Im}(f) = \{f(g) \mid g \in G\} \subseteq H$, дакле скуп свих слика елемената из G. Приметимо да је f на акко $\mathrm{Im}(f) = H$.

108. Доказати да је $\mathrm{Im}(f) \leq H$.

Решење. Како је $e_H = f(e_G)$, то $e_H \in \mathrm{Im}(f)$. Нека $x \in \mathrm{Im}(f)$, тј. нека је $x = f(a)$, за неко $a \in G$. Тада је $x^{-1} = f(a)^{-1} = f(a^{-1})$, па и $x^{-1} \in \mathrm{Im}(f)$. Коначно, нека $x, y \in \mathrm{Im}(f)$, тј. $x = f(a)$, $y = f(b)$, за неке $a, b \in G$. Тада $xy = f(a)f(b) = f(ab)$, па и $xy \in \mathrm{Im}(f)$. Дакле, $\mathrm{Im}(f) \leq H$. □

109. Одредити језгро следећих хомоморфизама.

1) $f : \mathsf{Z} \longrightarrow \mathsf{Z}_n$, $f(a) = a \mod n$.

2) $f : (G, \cdot) \longrightarrow (\mathsf{R}_0, \cdot)$, $G = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a, b \in \mathsf{R},\ b \neq 0 \right\}$, $\mathsf{R}_0 = \mathsf{R} \setminus \{0\}$, $f : \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mapsto b$.

3) $f : G_1 \times G_2 \longrightarrow G_1$, $f(a, b) = a$.

4) Нека је $H \triangleleft G$. $\pi : G \longrightarrow G/H$, $\pi(a) = aH$.

Решење. 1) $a \in \mathrm{Ker}(f)$ акко $f(a) = 0$, тј. акко $a \mod n = 0$ акко $n \mid a$. Дакле, $\mathrm{Ker}(f) = n\mathsf{Z} = \{nx \mid x \in \mathsf{Z}\}$.

2) $\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \in \mathrm{Ker}(f)$ акко $f\left(\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}\right) = 1$ акко $b = 1$. Дакле, $\mathrm{Ker}(f) = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathsf{R} \right\}$.

3) $(a, b) \in \mathrm{Ker}(f)$ акко $f(a, b) = e_{G_1}$ акко $a = e_{G_1}$. Дакле, $\mathrm{Ker}(f) = \{(e_{G_1}, b) \mid b \in G_2\} = \langle e_{G_1} \rangle \times G_2$.

4) $a \in \mathrm{Ker}(\pi)$ акко $\pi(a) = H$ акко $aH = H$ акко $a \in H$. Дакле, $\mathrm{Ker}(f) = H$.

Видели смо да је $\mathrm{Ker}(f)$ нормална подгрупа од G. Део 4) каже и да је свака нормална подгрупа језгро неког хомоморфизма. □

Прва теорема о изоморфизму Нека је $f : G \longrightarrow H$ хомоморфизам група. Видели смо да је $\mathrm{Ker}(f) \triangleleft G$, па има смисла говорити о групи $G/\mathrm{Ker}(f)$. Теорема тврди: $G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$.

110. Доказати: $G/\mathrm{Z}(G) \cong \mathrm{Inn}(G)$.

Решење. Посматрајмо пресликавање $f : G \longrightarrow \mathrm{Inn}(G)$ дато са $f(a) = \sigma_a$. Приметимо да је $f(ab) = \sigma_{ab} = \sigma_a\sigma_b = f(a)f(b)$ (другу једнакост смо раније доказали), одакле следи да је f хомоморфизам група. f је очигледно на, па је $\mathrm{Im}(f) = \mathrm{Inn}(G)$.

Одредимо језгро: $a \in \mathrm{Ker}(f)$ акко $f(a) = \mathrm{id}_G$ акко $\sigma_a = \mathrm{id}_G$ акко $(\forall x \in G)\, \sigma_a(x) = x$ акко $(\forall x \in G)\, axa^{-1} = x$ акко $(\forall x \in G)\, ax = xa$ акко $a \in \mathrm{Z}(G)$. Дакле, $\mathrm{Ker}(f) = \mathrm{Z}(G)$.

Према првој теореми о изоморфизму имамо: $G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$, тј. $G/\mathrm{Z}(G) = \mathrm{Inn}(G)$. □

111. Нека је $U = \{z \in \mathsf{C} \mid |z| = 1\}$. U је група у односу на множење комплексних бројева. Доказати:

1) $(\mathsf{C}_0, \cdot)/U \cong (\mathsf{R}^+, \cdot)$, где $\mathsf{C}_0 = \mathsf{C} \setminus \{0\}$, $\mathsf{R}^+ = \{x \in \mathsf{R} \mid x > 0\}$;

2) $(\mathsf{R}, +)/(\mathsf{Z}, +) \cong U$.

Решење. 1) Посматрајмо пресликавање $f : \mathsf{C}_0 \longrightarrow \mathsf{R}^+$ дато са $f(z) = |z|$. f је добро дефинисано пресликавање и важи $f(zw) = |zw| = |z||w| = f(z)f(w)$, тј. f је хомоморфизам група.

f је очигледно на, јер за свако $a \in \mathsf{R}^+$ имамо $f(a) = |a| = a$. Зато је $\mathrm{Im}(f) = \mathsf{R}^+$. Одредимо језгро: $z \in \mathrm{Ker}(f)$ акко $f(z) = 1$ акко $|z| = 1$ акко $z \in U$. Дакле, $\mathrm{Ker}(f) = U$.

Прва теорема о изморфизму сада каже: $\mathsf{C}_0/U \cong \mathsf{R}^+$.

2) Посматрајмо пресликавање $f : \mathsf{R} \longrightarrow \mathsf{C}_0$ дато са $f(a) = \cos a + i \sin a$. f је добро дефинисано пресликавање, јер за свако $a \in \mathsf{R}$ важи $\cos a + i \sin a \neq 0$. Такође $f(a+b) = \cos(a+b) + i \sin(a+b) = \cos a \cos b - \sin a \sin b + i \sin a \cos b + i \cos a \sin b = (\cos a + i \sin a)(\cos b + i \sin b) = f(a)f(b)$, тј. f је хомоморфизам група.

Докажимо да је $\mathrm{Im}(f) = U$. Ако је $z \in \mathrm{Im}(f)$, тада је $z = \cos a + i \sin a$ за неко $a \in \mathsf{R}$. Тада је $|z| = \sqrt{\cos^2 a + \sin^2 a} = 1$, па $z \in U$. Такође, ако $z \in U$, тј. ако $|z| = 1$, и ако запишемо $z = \alpha + i\beta$, тада је $\alpha^2 + \beta^2 = 1$, па постоји $a \in \mathsf{R}$ такав да $\cos a = \alpha$ и $\sin a = \beta$, па је $f(a) = z$, тј. $z \in \mathrm{Im}(f)$.

Израчунајмо језгро датог хомоморфизма. $a \in \mathrm{Ker}(f)$ акко $f(a) = 1$ акко $\cos a + i \sin a = 1$ акко $\cos(a) = 1$ и $\sin(a) = 0$ акко $a = 2k\pi$ за неко $k \in \mathsf{Z}$. Дакле, $\mathrm{Ker}(f) = \{2k\pi \mid k \in \mathsf{Z}\}$. Приметимо да је $k \mapsto 2k\pi$ очигледно изоморфизам између Z и $\mathrm{Ker}(f)$. Дакле, $\mathrm{Ker}(f) \cong \mathsf{Z}$.

Прва теорем о изоморфизму каже: $\mathsf{R}/\mathsf{Z} \cong U$. □

Абелове групе

О цикличним групама Група G је циклична акко постоји елемент $a \in G$ тако да је $G = \langle a \rangle$. Прва последица дефиниције је да је циклична група Абелова. Из Лагранжове теореме следи да група простог реда мора бити циклична.

Бесконачна циклична група је изоморфна групи $\mathsf{Z} = (\mathsf{Z}, +, 0)$; коначна циклична група реда n је изоморфна групи $\mathsf{Z}_n = (\mathsf{Z}_n, +_n, 0)$ ($\mathsf{Z}_n = \{0, 1, 2, \ldots n-1\}$, а $a +_n b = a + b \pmod n$). Приметите да је $\mathsf{Z} = \langle 1 \rangle$ и $\mathsf{Z}_n = \langle 1 \rangle$. Дакле, до на изоморфизам постоје једна бесконачна циклична група и по једна циклична група реда n, за свако $n \geq 1$.

Z има само два генератора: 1 и -1. Z_n има $\varphi(n)$ генератора: $\mathsf{Z}_n = \langle k \rangle$ акко $(k, n) = 1$. Или, ако је $G = \langle a \rangle$ циклична група реда n (чији је генератор a), тада је a^k генератор групе G акко $(k, n) = 1$.

Подгрупа цикличне групе је такође циклична. Нетривијалне подгрупе групе Z су само $n\mathsf{Z}$, $n \geq 1$, које су све бесконачне (дакле изоморфне самој групи чије су подгрупе). Нека је H подгрупа реда m групе Z_n. По Лагранжовој теореми ред групе m дели n, и како је она циклична, то је H изоморфна Z_m. Дакле, једини кандидати за подгрупу групе Z_n су групе изоморфне Z_m, за $m \mid n$. Важи и обрат. Ако $m \mid n$ тада Z_n садржи јединствену (!) подгрупу изоморфну Z_m. Ова чињеница нам омогућава да лако избројимо број елемената неког фиксираног реда у цикличној групи.

Означимо са $B(r, G)$ број елемената реда r у групи G. Тада, према претходној причи о генераторима, важи $B(n, \mathsf{Z}_n) = \varphi(n)$. Ако $m \nmid n$, према Лагранжовој теореми следи да је $B(m, \mathsf{Z}_n) = 0$. Нека $m \mid n$. Уочимо јединствену подгрупу $H \cong \mathsf{Z}_m$ групе Z_n. Сваки елемент реда m мора да генерише баш H (због јединствености подгрупе H), па припада H. Дакле $B(m, \mathsf{Z}_n) = B(m, H) = B(m, \mathsf{Z}_m) = \varphi(m)$.

Абелове групе

112. Доказати да је група $G = (G, \cdot, e)$ Абелова акко је $x \mapsto x^{-1}$ аутоморфизам групе G. □

113. Подсетимо се ($r(a)$ је ред елемента a):

1. $r(a^k) = \dfrac{r(a)}{(r(a), k)}$;
2. ако је G Абелова група, $r(ab) \mid [r(a), r(b)]$;
3. у групи $G_1 \times G_2$ важи $r(a, b) = [r(a), r(b)]$.

□

114. Нека је G Абелова група, а m и n узајамно прости природни бројеви. Нека је E_k скуп елемената реда k у G. Нека је $f : E_m \times E_n \longrightarrow E_{mn}$ пресликавање дато са $f(a, b) = ab$. Доказати да је f бијекција. Последица: ако су m и n узајамно прости, тада је $B(mn, G) = B(m, G)B(n, G)$.

Решење. Најпре докажимо да је f добро дефинисано, тј. да $ab \in E_{mn}$, ако $a \in E_m$ и $b \in E_n$. Очигледно је $(ab)^{mn} = e$. Ако је r ред елемента ab, то значи да $r \mid mn$. Са друге стране $e = (ab)^r = a^r b^r$, одакле је $a^r = b^{-r}$. $r(a^r)$ дели m, а $r(b^{-r})$ дели n, одакле следи да овај број дели и $(m,n) = 1$, тј. $a^r = b^{-r} = e$, одакле $m \mid r$ и $n \mid r$, па и $[m,n] = mn \mid r$. Дакле, $r = mn$ или $ab \in E_{mn}$.

Докажимо сада да је f 1-1. Претпоставимо да је $a_1 b_1 = a_2 b_2$, тј. $a_2^{-1} a_1 = b_2 b_1^{-1}$. Према претходном задатку ред овог елемента дели m (због његовог представљања на левој страни једнакости) и такође дели n (због представљања на десној страни). Према томе ред овог елемента дели и $(m,n) = 1$, одакле је $a_2^{-1} a_1 = b_2 b_1^{-1} = e$, тј. $a_1 = a_2$ и $b_1 = b_2$.

Коначно докажимо да је f на. Нека $c \in E_{mn}$. Како је $(m,n) = 1$ имамо $pm + qn = 1$, одакле је и $(p,n) = (q,m) = 1$. Према формули из претходног задатка је $r(c^m) = n$ и $r(c^n) = m$, па применом исте формуле на елементе c^m и c^n добијамо $r(c^{mp}) = n$ и $r(c^{nq}) = m$, тј. $c^{nq} \in E_m$ и $c^{mp} \in E_n$ и тада је $f(c^{nq}, c^{mp}) = c^{nq+mp} = c$. □

115. Доказати да је $\mathsf{Z}_{mn} \cong \mathsf{Z}_m \times \mathsf{Z}_n$ акко $(m,n) = 1$.

Решење. ($\Rightarrow$) Нека је $\mathsf{Z}_{mn} \cong \mathsf{Z}_m \times \mathsf{Z}_n$. Како у Z_{mn} постоји елемент реда mn, то и у $\mathsf{Z}_m \times \mathsf{Z}_n$ постоји елемент (a,b) реда mn. Тада је $mn = r(a,b) = [r(a), r(b)]$. Такође, како $r(a) \mid m$ и $r(b) \mid n$, тада $[r(a), r(b)] \mid [m,n] = mn/(m,n)$, одакле следи да је $(m,n) = 1$.

($\Leftarrow$) Нека је $(m,n) = 1$. Уочимо пресликавање $f : \mathsf{Z}_{mn} \longrightarrow \mathsf{Z}_m \times \mathsf{Z}_n$ дато са

$$f(a) = (a \pmod m, a \pmod n).$$

f је изоморфизам група. (Проверите!) □

Тероема о коначно генерисаним Абеловим групама Свака коначно генереисана Абелова група је изоморфна (коначном) производу цикличних група. Специјално, коначна Абелова група је изоморфна производу коначних цикличних група.

Нормална форма коначне Абелове групе Ако је G коначна Абелова група, тада постоје бројеви $m_1, m_2, \ldots, m_k$ који задовољавају $m_1 \mid m_2 \mid m_3 \mid \ldots \mid m_k$, тако да $G \cong \mathsf{Z}_{m_1} \times \mathsf{Z}_{m_2} \times \ldots \times \mathsf{Z}_{m_k}$. Бројеви m_i се називају инваријантни фактори групе G. Приметите да ред сваког елемента у G дели m_k, као и да постоје елементи реда m_k, тј. m_k је максимални ред елемента у G.

Експонент групе G је најмањи природан број n, ако постоји, такав да за свако $a \in G$ важи $a^n = e$. Према претходној причи, експонент Абелове групе G је m_k, где је m_k највећи инваријантни фактор.

116. Нека је F поље и нека је $G \leq F^\star$ коначна подгрупа. Доказати да је G циклична.

Решење. G је коначна Абелова група, па нека је m_k њен експонент, тј. њен највећи инваријантан фактор. Приметите да је $|G| \geq m_k$. Тада за све $a \in G$ важи $a^{m_k} = 1$ ($1 \in F$ је неутрал групе G). Према томе полином $x^{m_k} - 1$ има бар $|G|$ нула у F. Али како полином степена m_k не може имати више од m_k нула у пољу, то је једино могуће када је $|G| = m_k$, тј. када у нормалног форми групе G важи $k = 1$ и $G \cong \mathsf{Z}_{p_1}$. □

Елементарна форма коначне Абелове групе Ако је G коначна Абелова група, тада постоје прости бројеви $p_1, p_2, \ldots, p_k$ и природни бројеви $m_1, m_2, \ldots, m_k$, тако да $G \cong \mathsf{Z}_{p_1^{m_1}} \times \mathsf{Z}_{p_2^{m_2}} \times \ldots \times \mathsf{Z}_{p_k^{m_k}}$. Бројеви $p_i^{m_i}$ се називају елементарни делитељи групе G.

117. Нека је $G = \mathsf{Z}_{100} \times \mathsf{Z}_{200} \times \mathsf{Z}_{300} \times \mathsf{Z}_{400}$. Одредити елементарну и нормалну форму групе G.

Решење. У решењу користимо еквиваленцију: $\mathsf{Z}_{mn} \cong \mathsf{Z}_m \times \mathsf{Z}_n$ акко $(m,n)=1$. $\mathsf{Z}_{100} = \mathsf{Z}_{2^2\cdot 5^2} \cong \mathsf{Z}_{2^2} \times \mathsf{Z}_{5^2}$, $\mathsf{Z}_{200} = \mathsf{Z}_{2^3\cdot 5^2} \cong \mathsf{Z}_{2^3} \times \mathsf{Z}_{5^2}$, $\mathsf{Z}_{300} = \mathsf{Z}_{2^2\cdot 3\cdot 5^2} \cong \mathsf{Z}_{2^3} \times \mathsf{Z}_3 \times \mathsf{Z}_{5^2}$, $\mathsf{Z}_{400} = \mathsf{Z}_{2^4\cdot 5^2} \cong \mathsf{Z}_{2^4} \times \mathsf{Z}_{5^2}$. Тада је, после прераспоређивања чланова директног производа (што је изоморфизам!), $G \cong \mathsf{Z}_{2^2} \times \mathsf{Z}_{2^2} \times \mathsf{Z}_{2^3} \times \mathsf{Z}_{2^4} \times \mathsf{Z}_3 \times \mathsf{Z}_{5^2} \times \mathsf{Z}_{5^2} \times \mathsf{Z}_{5^2} \times \mathsf{Z}_{5^2} \times$, што је елементарна форма групе G.

Како је $\mathsf{Z}_{2^4} \times \mathsf{Z}_3 \times \mathsf{Z}_{5^2} \cong \mathsf{Z}_{2^4\cdot 3\cdot 5^2} = \mathsf{Z}_{1200}$, $\mathsf{Z}_{2^3} \times \mathsf{Z}_{5^2} \cong \mathsf{Z}_{2^3\cdot 5^2} = \mathsf{Z}_{200}$ и $\mathsf{Z}_{2^2} \times \mathsf{Z}_{5^2} \cong \mathsf{Z}_{2^2\cdot 5^2} = \mathsf{Z}_{100}$, добијамо да је $G \cong \mathsf{Z}_{100} \times \mathsf{Z}_{100} \times \mathsf{Z}_{200} \times \mathsf{Z}_{1200}$, где $100 \mid 100 \mid 200 \mid 1200$, што је нормална форма групе G. □

118. Да ли је за неко n $\mathsf{Z}_{20} \times \mathsf{Z}_{30}$ изоморфно са:

1. $\mathsf{Z}_{60} \times \mathsf{Z}_n$?
2. $\mathsf{Z}_{50} \times \mathsf{Z}_n$?

Решење. Приметимо да $\mathsf{Z}_{20} \times \mathsf{Z}_{30}$ има 600 елемената и да јој је елементарна форма једнака $\mathsf{Z}_2 \times \mathsf{Z}_{2^2} \times \mathsf{Z}_3 \times \mathsf{Z}_5 \times \mathsf{Z}_5$. Такође приметимо да ова група нема елемент реда 25.

1. Ако изоморфизам постоји, то мора $60 \cdot n = 600$, тј. $n = 10$. Елементарна форма групе $\mathsf{Z}_{60} \times \mathsf{Z}_{10}$ је $\mathsf{Z}_2 \times \mathsf{Z}_{2^2} \times \mathsf{Z}_3 \times \mathsf{Z}_5 \times \mathsf{Z}_5$, па је одговор да дата група јесте изоморфна са $\mathsf{Z}_{60} \times \mathsf{Z}_{10}$.
2. Слично као малопре, ако изоморфизам постоји, то n мора бити једнако 12. Елементарна форма групе $\mathsf{Z}_{50} \times \mathsf{Z}_{12}$ је $\mathsf{Z}_2 \times \mathsf{Z}_{2^2} \times \mathsf{Z}_3 \times \mathsf{Z}_{5^2}$. Ова група има елемент реда 25, док горња група $\mathsf{Z}_{20} \times \mathsf{Z}_{30}$ нема, па је одговор да тражено n не постоји.

□

119. Одредити до на изоморфизам све Абелове групе реда 1800.

Решење. Довољно је да одредимо све могуће елементарне форме Абелове групе реда 1800. Одредићемо одмах и њихове нормалне форме. Како је $1800 = 2^3 3^2 5^2$, имамо следеће могућности:

1. $G_1 = \mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_3 \times \mathsf{Z}_3 \times \mathsf{Z}_5 \times \mathsf{Z}_5 \cong \mathsf{Z}_2 \times \mathsf{Z}_{30} \times \mathsf{Z}_{30}$;
2. $G_2 = \mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_3 \times \mathsf{Z}_3 \times \mathsf{Z}_{5^2} \cong \mathsf{Z}_2 \times \mathsf{Z}_6 \times \mathsf{Z}_{150}$;
3. $G_3 = \mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_{3^2} \times \mathsf{Z}_5 \times \mathsf{Z}_5 \cong \mathsf{Z}_2 \times \mathsf{Z}_{10} \times_{90}$;
4. $G_4 = \mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_{3^2} \times \mathsf{Z}_{5^2} \cong \mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_{450}$;
5. $G_5 = \mathsf{Z}_2 \times \mathsf{Z}_{2^2} \times \mathsf{Z}_3 \times \mathsf{Z}_3 \times \mathsf{Z}_5 \times \mathsf{Z}_5 \cong \mathsf{Z}_{30} \times \mathsf{Z}_{60}$;
6. $G_6 = \mathsf{Z}_2 \times \mathsf{Z}_{2^2} \times \mathsf{Z}_3 \times \mathsf{Z}_3 \times \mathsf{Z}_{5^2} \cong \mathsf{Z}_6 \times \mathsf{Z}_{300}$;
7. $G_7 = \mathsf{Z}_2 \times \mathsf{Z}_{2^2} \times \mathsf{Z}_{3^2} \times \mathsf{Z}_5 \times \mathsf{Z}_5 \cong \mathsf{Z}_{10} \times \mathsf{Z}_{180}$;
8. $G_8 = \mathsf{Z}_2 \times \mathsf{Z}_{2^2} \times \mathsf{Z}_{3^2} \times \mathsf{Z}_{5^2} \cong \mathsf{Z}_2 \times \mathsf{Z}_{900}$;
9. $G_9 = \mathsf{Z}_{2^3} \times \mathsf{Z}_3 \times \mathsf{Z}_3 \times \mathsf{Z}_5 \times \mathsf{Z}_5 \cong \mathsf{Z}_{15} \times \mathsf{Z}_{120}$;
10. $G_{10} = \mathsf{Z}_{2^3} \times \mathsf{Z}_3 \times \mathsf{Z}_3 \times \mathsf{Z}_{5^2} \cong \mathsf{Z}_3 \times \mathsf{Z}_{600}$;
11. $G_{11} = \mathsf{Z}_{2^3} \times \mathsf{Z}_{3^2} \times \mathsf{Z}_5 \times \mathsf{Z}_5 \cong \mathsf{Z}_5 \times \mathsf{Z}_{360}$;
12. $G_{12} = \mathsf{Z}_{2^3} \times \mathsf{Z}_{3^2} \times \mathsf{Z}_{5^2} \cong \mathsf{Z}_{1800}$.

Из нормалних форми се види да су наведене групе међусобно неизоморфне – максималан ред елемента је у свакој различит. □

120. Ако је $(m, |G_2|) = 1$, доказати да је $B(m, G_1 \times G_2) = B(m, G_1)$.

Решење. Довољно је доказати да су једини елементи реда m у $G_1 \times G_2$ облика (a, e), где је $a \in G_1$ елемент реда m, а e неутрал групе G_2. (Приметите да је елемент облика (a, e) истог реда као и a.)

Претпоставимо да је (a, b) елемент реда m, тада је $[r(a), r(b)] = m$. То значи да $r(b) \mid m$, а такође из Лагранжове теореме следи да $r(b) \mid |G_2|$. Према претпоставци задатка закључујемо да $r(b) = 1$, тј. $b = e$. Како је сада $m = [r(a), 1]$, то $r(a) = m$. □

121. Одредити број елемената максималног реда у свакој Абеловој групи реда 1800.

Решење. Оваквих група, као што смо видели, има 12 неизоморфних. Кренимо редом:

1. У $G_1 = \mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_3 \times \mathsf{Z}_3 \times \mathsf{Z}_5 \times \mathsf{Z}_5 \cong \mathsf{Z}_2 \times \mathsf{Z}_{30} \times \mathsf{Z}_{30}$ максималан ред елемента је 30, дакле рачунамо $B(30, G_1)$. Гледајмо у елементарну форму. Према неком од претходних задатака важи $B(30, G_1) = B(2, G_1)B(3, G_1)B(5, G_1)$, а према претходном задатку $B(2, G_1) = B(2, \mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_2)$, $B(3, G_1) = B(3, \mathsf{Z}_3 \times \mathsf{Z}_3)$ и $B(5, G_1) = B(5, \mathsf{Z}_5 \times \mathsf{Z}_5)$. У групи $\mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_2$ сви елементи сем неутрала су реда 2, па је $B(2, G_1) = 7$; у групи $\mathsf{Z}_2 \times \mathsf{Z}_3$ сви елементи сем неутрала су реда 3, па је $B(3, G_1) = 8$; у групи $\mathsf{Z}_5 \times \mathsf{Z}_5$ сви елементи сем неутрала су реда 5, па је $B(5, G_1) = 24$. Дакле, $B(30, G_1) = 7 \cdot 8 \cdot 24$.

2. У $G_2 = \mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_3 \times \mathsf{Z}_3 \times \mathsf{Z}_{5^2} \cong \mathsf{Z}_2 \times \mathsf{Z}_6 \times \mathsf{Z}_{150}$ максималан ред елемента је $150 = 2 \cdot 3 \cdot 5^2$. Као малопре $B(150, G_1) = B(2, G_1)B(3, G_1)B(5^2, G_1)$ и као малопре $B(2, G_1) = 7$ и $B(3, G_1) = 8$. $B(5^2, G_1) = B(5^2, \mathsf{Z}_{5^2}) = \varphi(5^2) = 20$. Дакле, $B(150, G_1) = 7 \cdot 8 \cdot 20$.

5. У $G_5 = \mathsf{Z}_2 \times \mathsf{Z}_{2^2} \times \mathsf{Z}_3 \times \mathsf{Z}_3 \times \mathsf{Z}_5 \times \mathsf{Z}_5 \cong \mathsf{Z}_{30} \times \mathsf{Z}_{60}$ максималан ред елемента је $60 = 2^2 \cdot 3 \cdot 5$ и $B(60, G_5) = B(2^2, G_5)B(3, G_5)B(5, G_5)$, при чему је $B(3, G_5) = 8$, $B(5, G_5) = 24$. Израчунајмо и $B(2^2, G_5)$. $B(2^2, G_5) = B(2^2, \mathsf{Z}_2 \times \mathsf{Z}_{2^2})$. Ако $(a, b) \in \mathsf{Z}_2 \times \mathsf{Z}_{2^2}$, како $r(a, b) = [r(a), r(b)]$ и $r(a) \in \{1, 2\}$, а $r(b) \in \{1, 2, 4\}$, $r(a, b) = 4$ акко $r(b) = 4$. Дакле, $B(4, \mathsf{Z}_2 \times \mathsf{Z}_{2^2}) = |\mathsf{Z}_2| \cdot B(4, \mathsf{Z}_{2^2}) = 2 \cdot \varphi(2^2) = 4$. Дакле, $B(60, G_5) = 4 \cdot 8 \cdot 24$.

12. У $G_{12} = \mathsf{Z}_{2^3} \times \mathsf{Z}_{3^2} \times \mathsf{Z}_{5^2} \cong \mathsf{Z}_{1800}$ максималан ред елмента је 1800, и $B(1800, G_{12}) = B(1800, \mathsf{Z}_{1800}) = \varphi(1800) = \varphi(2^3)\varphi(3^2)\varphi(5^2) = 4 \cdot 6 \cdot 20$.

□

122. Одредити број елемената реда $36 = 2^2 3^2$ у групи $G = \mathsf{Z}_2 \times \mathsf{Z}_{2^2} \times \mathsf{Z}_{2^4} \times \mathsf{Z}_{3^3} \times \mathsf{Z}_{3^3}$.

Решење. $B(36, G) = B(4, G)B(9, G)$, и $B(4, G) = B(4, \mathsf{Z}_2 \times \mathsf{Z}_{2^2} \times \mathsf{Z}_{2^4})$ и $B(9, G) = B(9, \mathsf{Z}_{3^3} \times \mathsf{Z}_{3^3})$.

У $\mathsf{Z}_2 \times \mathsf{Z}_{2^2} \times \mathsf{Z}_{2^4}$ елементи имају редове 1, 2, 4, 8 и 16. Елементи чији ред дели 4 се налазе у подгрупи изоморфној са $\mathsf{Z}_2 \times \mathsf{Z}_{2^2} \times \mathsf{Z}_{2^2}$, а елементи чији ред дели 2 се налазе у подгрупи изоморфној $\mathsf{Z}_2 \times \mathsf{Z}_2 \times \mathsf{Z}_2$. То значи да су елементи реда 4 они који јесу у подгрупи изоморфној са $\mathsf{Z}_2 \times \mathsf{Z}_{2^2} \times \mathsf{Z}_{2^2}$, а нису у подгрупи изоморфној са $\mathsf{Z}_2 \times \mathsf{Z}_{2^2} \times \mathsf{Z}_{2^2}$. Према томе, $B(4, \mathsf{Z}_2 \times \mathsf{Z}_4 \times \mathsf{Z}_{16}) = 2 \cdot 4 \cdot 4 - 2 \cdot 2 \cdot 2 = 32 - 8 = 24$.

У $\mathsf{Z}_{27} \times \mathsf{Z}_{27}$ елементи имају редове 1, 3, 9 и 27. Елементи чији ред дели 9 се налазе у подгрупи изоморфној са $\mathsf{Z}_{3^2} \times \mathsf{Z}_{3^2}$, дакле има их 81. Елементи чији ред дели 3 се налазе у подгрупи изоморфној са $\mathsf{Z}_3 \times \mathsf{Z}_3$, дакле има их 9. Према томе, елементи реда 9 су тачно они који се налазе у подгрупи изоморфној са $\mathsf{Z}_{3^2} \times \mathsf{Z}_{3^2}$, а не назале се у подгрупи изоморфној са $\mathsf{Z}_3 \times \mathsf{Z}_3$, па је $B(9, \mathsf{Z}_{27} \times \mathsf{Z}_{27}) = 81 - 9 = 72$. □