Задаци из Алгебре

1. Испитати који од следећих скупова чине групу у односу на операцију множења по модулу 14:

   а) $G_1 = \{1, 3, 5\}$, б) $G_2 = \{1, 3, 5, 7\}$, в) $G_3 = \{1, 7, 13\}$, г) $G_4 = \{1, 9, 11, 13\}$, д) $G_5 = \{1, 3, 5, 9, 11, 13\}$.

   Решење: Овај задатак решавамо посматрањем Кејлијеве таблице операције $\cdot_{14}$ на датим скуповима.

   а) Кејлијева таблица има следећи облик

$\cdot_{14}$	1	3	5
1	1	3	5
3	3	9	1
5	5	1	11

   .

   Како се број 9 не налази у скупу G_1, закључујемо да $\cdot_{14}$ није операција на G_1, а самим тим $(G_1, \cdot_{14})$ није група.

   б) По делу под а) закључујемо да се у Кејлијевој таблици налази број 9, па $\cdot_{14}$ није операција у односу на скуп G_2. Дакле, $(G_2, \cdot_{14})$ није група.

   в) Кејлијева таблица има следећи облик

$\cdot_{14}$	1	7	13
1	1	7	13
7	7	7	7
13	13	7	1

   .

   Видимо да 7 нема инверз у G_3, те закључујемо да $(G_3, \cdot_{14})$ није група.

   г) Кренимо да попуњавамо Кејлијеву таблицу

$\cdot_{14}$	1	9	11	13
1	1	9	11	13
9	9	11	1	5
11	11			
13	13			

   .

   Како се у таблици налази број 5, који није у скупу G, то $\cdot_{14}$ није операција на скупу G (и није потребно да наставимо са попуњавањем таблице). Закључујемо да $(G_4, \cdot_{14})$ није група.

   д) Кејлијева таблица има следећи облик

$\cdot_{14}$	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

   .

   На основу ове таблице закључујемо да је $\cdot_{14}$ операција на скупу G. Како је $\cdot_n$ асоцијативна операција за сваки природан број n, то је и $\cdot_{14}$ асоцијативна операција (на скупу G). Неутрал операције $\cdot_{14}$ је $1 \in G$.

   Из Кејлијеве таблице није тешко „прочитати" инверзе елемената: инверз елемента у i-тој врсти је елемент из j-те колоне ако и само ако се у пресеку i-те врсте и j-те колоне налази 1 (овде користимо и чињеницу да је $\cdot_{14}$ комутативна операција). Дакле, инверз од 1 је 1, од 3 је 5, од 5 је 3, од 9 је 11, од 11 је 9, а инверз од 13 је 13. Дакле, $(G_5, \cdot_{14})$ јесте група.

2. Доказати да подскуп од $\{1, 2, \ldots, 21\}$, који садржи неки паран број и број 11 не може чинити групу у односу на операцију множења бројева по модулу 22.

Решење: Нека је $G \subseteq \{1, 2, \ldots, 21\}$ такав да је $(G, \cdot_{22})$ група и G садржи неки паран број $2k$ (где је $k \in \mathbb{N}$), као и број 11. Како је $2k \in G$ и $11 \in G$, то је због затворености операције $\cdot_{22}$ и $2k \cdot_{22} 11 \in G$. Међутим, $2k \cdot 11 = 22k$, па је $2k \cdot_{22} 11 = 0$, чиме је добијена контрадикција (јер $0 \notin G$).

3. Одредити ред сваког елемента из $\mathbb{Z}_5$, $\mathbb{Z}_9$ и $\mathbb{Z}_{14}$.

Решење:

а) Нека је $k \in \{1, 2, 3, 4\}$ реда r. То значи да је у групи $\mathbb{Z}_5$ испуњено $rk = 0$, а то заправо значи да у $\mathbb{Z}$ важи: $5 \mid rk$. С обзиром да је 5 прост број, добијамо да $5 \mid r$ или $5 \mid k$. Јасно је да друга релација не може бити испуњена, па закључујемо да $5 \mid r$, те је $r \geqslant 5$. Но, јасно је да је $5k = 0$ у $\mathbb{Z}_5$ за све k, па закључујемо да је сваки елемент из $\mathbb{Z}_5 \setminus \{0\}$ реда 5.

б) Нека је $k \in Z_9 \setminus \{0\}$ реда r. То значи да је $rk = 0$ у $\mathbb{Z}_9$, односно да $9 \mid rk$ у $\mathbb{Z}$. Како 9 није прост број, добро је размотрити два случаја.

$3 \nmid k$. То значи да су 9 и k узајамно прости и из чињенице да $9 \mid rk$ следи да $9 \mid r$. У овом случају је дакле $r \geqslant 9$, а како је сигурно $9k = 0$, добијамо да је $r = 9$.

$3 \mid k$. Дакле, $k \in \{3, 6\}$, тј. $k = 3l$, где $l \in \{1, 2\}$. Из $9 \mid rk$, добијамо да $9 \mid 3rl$, те $3 \mid rl$. Како је 3 прост број, добијамо да $3 \mid r$, или $3 \mid l$. Како је јасно да $3 \nmid l$, добијамо да $3 \mid r$, те је $r \geqslant 3$. Но, $3k = 0$ у $\mathbb{Z}_9$ за $k \in \{3, 6\}$, па је за те елементе ред једнак 3.

в) Нека је $k \in Z_{15} \setminus \{0\}$ реда r. То значи да је $rk = 0$ у $\mathbb{Z}_{15}$, односно да $15 \mid rk$ у $\mathbb{Z}$. Како 15 није прост број, то и овде имамо два случаја.

$3 \mid k$. Дакле, $k \in \{3, 6, 9, 12\}$ те је $k = 3l$, где $l \in \{1, 2, 3, 4\}$. Из $15 \mid rk$ добијамо да $15 \mid 3rl$, те $5 \mid rl$. Како је 5 прост број и $5 \nmid l$, добијамо да $5 \mid r$. Као и у претходним случајевима, можемо да закључимо да је у овом случају ред елемента k једнак баш 5.

$5 \mid k$. У овом случају $k \in \{5, 10\}$, те је $k = 5l$, где $l \in \{1, 2\}$. Из $15 \mid rk$ добијамо да $15 \mid 5rl$, те $3 \mid rl$. Следи да $3 \mid r$ и да је ред елемента k у овом случају једнак баш 3.

Приметимо да су ови случајеви раздвојени јер не постоји $k \in Z_{15} \setminus \{0\}$ које је дељиво и за 3 и са 5. Такође, резултат смо могли добити и коришћењем формуле за ред елемента уз чињеницу да је 1 генератор у овим групама и да је $k = k1$, али смо желели да ипак то прикажемо директно за ове примере.

4. Нека је g елемент групе G. Доказати да је $G = \{gx : x \in G\}$, при чему је $gx \neq gy$ за $x \neq y$.

Решење: Докажимо прво да је скуп $H = \{gx : x \in G\}$ једнак G.

Доказ за $H \subseteq G$. Нека је $h \in H$. Тада је $h = gx$ за неко $x \in G$. Како је $g, x \in G$, то због затворености операције на скупу G важи и $gx \in G$, тј. $h \in G$.

Доказ за $G \subseteq H$. Нека је $h \in G$. Како је $g^{-1} \in G$, то због затворености операције на G важи и $g^{-1}h \in G$. По дефиницији скупа H је $g(g^{-1}h) = h \in H$, чиме је доказ једнакости $G = H$ завршен.

Да бисмо доказали други део тврђења, претпоставимо да је $gx = gy$, за неке $x, y \in G$. Множењем ове једнакости слева са g^{-1} добијамо $x = y$, што је и требало доказати.

5. Нека елементи x, y и xy неке групе G имају ред 2. Доказати да је $xy = yx$.

Решење: Дакле, на основу услова задатка имамо да је

$$x^2 = y^2 = (xy)^2 = e.$$

Тада имамо и следеће:

$$(xy)(xy) = (xy)^2 = e = ee = x^2y^2 = (xx)(yy),$$

односно,

$$xyxy = xxyy.$$

Ако ову једнакост слева помножимо са x^{-1}, а здесна са y^{-1} добијамо

$$yx = xy,$$

што се и тражило.

6. Нека је $G = \mathbb{Q} \cap [0,1)$. На скупу G задата је операција $\oplus$ са:

$$x \oplus y = \begin{cases} x+y, & 0 \leqslant x+y < 1 \\ x+y-1, & x+y \geqslant 1. \end{cases}$$

Показати да је G бесконачна Абелова група чији су сви елементи коначног реда.

Решење: Нека је $x, y \in G$. Јасно је да је тада $x \oplus y \in \mathbb{Q}$. Проверимо да је и $x \oplus y \in [0,1)$. Ако је $0 \leqslant x+y < 1$, тада је $x \oplus y = x+y \in [0,1)$; ако је $x+y \geqslant 1$, тада је $x \oplus y = x+y-1$, па како је $x+y < 2$ (јер је $x, y < 1$), то је и у овом случају $x \oplus y \in [0,1)$. Дакле, $\oplus$ је операција на G.

Докажимо да је $\oplus$ асоцијативна операција. Нека је $x, y, z \in G$. Приметимо да у дефиницији операције $\oplus$ имамо „два случаја". То нам сугерише да ћемо и приликом доказивања асоцијативности имати неколико случајева, које разликујемо како бисмо могли да израчунамо $(x \oplus y) \oplus z$ и $x \oplus (y \oplus z)$.

Случај 1. $0 \leqslant x+y < 1$ и $0 \leqslant y+z < 1$.

У овом случају важи $(x \oplus y) \oplus z = (x+y) \oplus z$ и $x \oplus (y \oplus z) = x \oplus (y+z)$. Вредност претходних израза зависи од $x+y+z$. Како је $x+y < 1$ и $z < 1$, то је $0 \leqslant x+y+z < 2$, па је довољно размотрити случајеве $0 \leqslant x+y+z < 1$ и $x+y+z \geqslant 1$.

- Ако је $0 \leqslant x+y+z < 1$, тада важи $(x+y) \oplus z = x+y+z$ и $x \oplus (y+z) = x+y+z$, па је $(x \oplus y) \oplus z = x \oplus (y \oplus z)$.
- Ако је $x+y+z \geqslant 1$, тада важи $(x+y) \oplus z = x+y+z-1$ и $x \oplus (y+z) = x+y+z-1$, па је опет $(x \oplus y) \oplus z = x \oplus (y \oplus z)$.

Случај 2. $0 \leqslant x+y < 1$ и $y+z \geqslant 1$.

У овом случају важи $(x \oplus y) \oplus z = (x+y) \oplus z$ и $x \oplus (y \oplus z) = x \oplus (y+z-1)$. Како је $x+y < 1$ и $z < 1$, то је $x+y+z < 2$, а како је $y+z \geqslant 1$ и $x \geqslant 0$, то је и $1 \leqslant x+y+z$. Дакле, важи $(x+y) \oplus z = x+y+z-1$ и $x \oplus (y+z-1) = x+y+z-1$ (јер је $0 \leqslant x+y+z-1 < 1$), па је $(x \oplus y) \oplus z = x \oplus (y \oplus z)$.

Случај 3. $x+y \geqslant 1$ и $0 \leqslant y+z < 1$.

Овај случај разматрамо као претходни.

Случај 4. $x+y \geqslant 1$ и $y+z \geqslant 1$.

У овом случају важи $(x \oplus y) \oplus z = (x+y-1) \oplus z$ и $x \oplus (y \oplus z) = x \oplus (y+z-1)$. Како је $x+y \geqslant 1$, то је $x+y+z \geqslant 1$, а како је $x, y, z < 1$, то је $x+y+z < 3$. Размотримо засебно случајеве: $1 \leqslant x+y+z < 2$ и $2 \leqslant x+y+z < 3$.

- Ако је $1 \leqslant x+y+z < 2$, тада је $0 \leqslant x+y+z-1 < 1$, па важи $(x+y-1) \oplus z = x+y-1+z$ и $x \oplus (y+z-1) = x+y+z-1$, а самим тим и $(x \oplus y) \oplus z = x \oplus (y \oplus z)$.
- Ако је $2 \leqslant x+y+z < 3$, тада је $x+y+z-1 \geqslant 1$, па важи $(x+y-1) \oplus z = x+y-1+z-1 = x+y+z-2$ и $x \oplus (y+z-1) = x+y+z-1-1 = x+y+z-2$, а самим тим и $(x \oplus y) \oplus z = x \oplus (y \oplus z)$.

Напомена. Асоцијативност операције смо могли краће доказати користећи својства функција $[x]$ (цео део од x) и $\{x\}$ (разломљени део од x), где је x реалан број.

Сигурно је свима позната функција $[x]$. Подсетимо се да је за $x \in \mathbb{R}$ цео део од x, тј. $[x]$ јединствени цео број за који важи: $[x] \leqslant x < [x]+1$. Ово је еквивалентно са $x-1 < [x] \leqslant x$. Приметимо да важи следеће: $[x+1] = [x]+1$. Наиме, из $x-1 < [x] \leqslant x$ добијамо $(x+1)-1 < [x]+1 \leqslant x+1$. Како је $[x+1]$ једини цео број за који важи $(x+1)-1 < [x+1] \leqslant x+1$, то мора бити $[x+1] = [x]+1$.

Разломљени део броја x, у ознаци $\{x\}$ дефинише се са: $\{x\} := x - [x]$. Приметимо да је ова функција периодична са периодом 1: $\{x+1\} = (x+1) - [x+1] = (x+1) - ([x]+1) = x - [x]$. Стога је и $\{x+m\} = \{x\}$ за све $m \in \mathbb{Z}$.

Зашто уопште причамо о овим функцијама? Разлог је једноставан, ако су $x, y \in G$, $x \oplus y$ није ништа друго до $\{x+y\}$. Наиме, ако је $x + y < 1$, онда је (обратите пажњу да $x, y \geqslant 0$) $[x+y] = 0$ и стога је $\{x+y\} = x + y - [x+y] = x + y$, а ако је $x + y \geqslant 1$, тада је $[x+y] = 1$ (знамо да је сигурно $x + y < 2$), па је $\{x+y\} = x + y - [x+y] = x + y - 1$.

Сада је лако показати да је операција $\oplus$ асоцијативна. Наиме:

$$(x \oplus y) \oplus z = \{\{x+y\} + z\} = \{x + y - [x+y] + z\} = \{x + y + z - [x+y]\} = \{x+y+z\},$$

а

$$x \oplus (y \oplus z) = \{x + \{y+z\}\} = \{x + y + z - [y+z]\} = \{x+y+z\}.$$

Наставимо са провером да је G група. Докажимо да је 0 неутрал операције $\oplus$. Заиста, ако је $x \in G$, тада важи $0 \leqslant 0 + x < 1$, па је $x \oplus 0 = x$ и $0 \oplus x = x$.

Одредимо инверз x' елемента $x \in G$, тј. елемент такав да важи $x \oplus x' = x' \oplus x = 0$. Увидом у дефиницију операције $\oplus$, јасно је да ове једнакости важе за $x' = 1 - x$ ако је $x \neq 0$, односно $x' = 0$ ако је $x = 0$.

Јасно је да је група G Абелова и да је бесконачна. Докажимо још да је сваки елемент из G коначног реда.

Нека је $\frac{m}{n} \in G$. Тада је $\frac{m}{n} = m\frac{1}{n}$ (приметимо да је $m < n$), па је довољно доказати да је елемент $\frac{1}{n}$ коначног реда. Но, то је лако доказати, пошто је јасно да је

$$\underbrace{\frac{1}{n} \oplus \cdots \oplus \frac{1}{n}}_{n-1} = \frac{n-1}{n},$$

а

$$\frac{n-1}{n} \oplus \frac{1}{n} = \frac{n-1}{n} + \frac{1}{n} - 1 = 0,$$

те је $n\frac{1}{n} = 0$, тј. ред елемента $\frac{1}{n}$ је заправо n.

7. Нека је

$$SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc = 1 \right\}.$$

Доказати да је $SL_2(\mathbb{Z})$ група у односу на множење матрица. Ако су матрице $A, B \in SL_2(\mathbb{Z})$ задате са:

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix},$$

одредити редове елемената A, B, AB и BA.

Решење: Приметимо да је $SL_2(\mathbb{Z})$ скуп матрица из $M_2(\mathbb{Z})$ чија је детерминанта једнака 1.

Нека је $A, B \in SL_2(\mathbb{Z})$. Тада је $AB \in M_2(\mathbb{Z})$, тј. сви елементи матрице AB су цели бројеви. Како је по Бине-Кошијевој теореми $\det(AB) = \det(A)\det(B)$, то је и $\det(AB) = 1$, па важи $AB \in SL_2(\mathbb{Z})$.

Као у претходном задатку закључујемо да је операција асоцијативна и да је њен неутрал E (јер је $E \in SL_2(\mathbb{Z})$).

Докажимо и да матрица $A \in SL_2(\mathbb{Z})$ има инверз у $SL_2(\mathbb{Z})$. Нека је $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Знамо да инверз матрице, тј. A^{-1}, можемо одредити по формули

$$A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A),$$

па како је $\det(A) = 1$, то је

$$A^{-1} = \operatorname{adj}(A) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Дакле, $A^{-1} \in M_2(\mathbb{Z})$, па како је $\det(A^{-1}) = da - (-b)(-c) = \det(A) = 1$, закључујемо да важи $A^{-1} \in SL_2(\mathbb{Z})$.

Директним рачуном добијамо да је

$$A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},$$

а одавде следи да је $A^4 = E$. Из последње једнакости закључујемо да ред елемента A дели 4, но, како $A^2 \neq E$, закључујемо да је ред елемента A једнак 4 (наравно, могли смо израчунати и A^3 и проверити да је $A^3 \neq E$).

Опет директним рачуном добијамо да је:

$$B^2 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}, \qquad B^3 = E,$$

те је ред елемента B једнак 3.

$$C = AB = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

Индукцијом није тешко показати да је

$$C^n = \begin{bmatrix} 1 & n \\ 0 & 0 \end{bmatrix}.$$

Наиме, видимо да је та једнакост тачна за $n = 1$. Из претпоставке да је

$$C^n = \begin{bmatrix} 1 & n \\ 0 & 0 \end{bmatrix}.$$

добијамо

$$C^{n+1} = C^n C = \begin{bmatrix} 1 & n+1 \\ 0 & 0 \end{bmatrix}.$$

Стога видимо да је $C^n \neq E$ за све $n \geq 1$, па је елемент $C = AB$ бесконачног реда.

Елемент BA је заправо коњугован елементу AB:

$$BA = A^{-1}(AB)A,$$

па је стога истог реда као и AB, тј. и он је бесконачног реда.

8. Наћи све подгрупе група $\mathbb{Z}_4$, $\mathbb{Z}_7$, $\mathbb{Z}_{12}$, $\mathbb{D}_4$ и $\mathbb{D}_5$.

Решење: Подгрупе цикличних група није тешко одредити. Ми знамо да свака циклична група има тачно једну подгрупу реда k за сваки k који је делилац реда те група.

Јединe подгрупе групе $\mathbb{Z}_4$ су реда 1, 2 и 4 и то су заправо подгрупе $\{0\}$, $\{0, 2\}$, $\mathbb{Z}_4$.

Како је 7 прост број, то су јединe подгрупе групе $\mathbb{Z}_7$ реда 1 и 7, односно то је тривијална подгрупа $\{0\}$ и цела група $\mathbb{Z}_7$.

Подгрупе групе $\mathbb{Z}_{12}$ су реда 1, 2, 3, 4, 6 и 12. То су редом подгрупе: $\{0\}$, $\{0, 6\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$ и $\mathbb{Z}_{12}$.

Како је $|\mathbb{D}_4| = 8$, по Лагранжовој теореми свака подгрупа групе $\mathbb{D}_4$ има 1, 2, 4 или 8 елемената. Јасно, једина подгрупа са једним елементом је $\{\varepsilon\}$. Подгрупе са 2 елемента одговарају елементима реда 2 групе $\mathbb{D}_4$, а то су $\sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3, \rho^2$, па су $\{\varepsilon, \sigma\}$, $\{\varepsilon, \sigma\rho\}$, $\{\varepsilon, \sigma\rho^2\}$, $\{\varepsilon, \sigma\rho^3\}$ и $\{\varepsilon, \rho^2\}$ све подгрупе реда 2 групе $\mathbb{D}_4$.

Одредимо сада све подгрупе реда 4 групе $\mathbb{D}_4$. Приметимо да је $\langle\rho\rangle = \langle\rho^3\rangle = \{\varepsilon, \rho, \rho^2, \rho^3\}$, па је $\{\varepsilon, \rho, \rho^2, \rho^3\}$ једина подгрупа реда 4 групе $\mathbb{D}_4$ која садржи ρ или ρ^3. Нека је зато H подгрупа реда

4 таква да $\rho, \rho^3 \notin H$. Ова подгрупа садржи барем две симетрије $\sigma\rho^i$ и $\sigma\rho^j$, $0 \leqslant i < j \leqslant 3$ (јер поред симетрија може садржати још само ε и ρ^2), па важи

$$H \ni \sigma\rho^i\sigma\rho^j = \sigma\sigma\rho^{n-i}\rho^j = \rho^{j-i} \neq \varepsilon.$$

Дакле, H садржи барем једну ротацију, а како је ρ^2 једина ротација коју H може садржати закључујемо да је $j - i = 2$ (јер је $0 < j - i \leqslant 3$). Дакле, имамо две могућности за H, а то су $\{\varepsilon, \rho^2, \sigma, \sigma\rho^2\}$ и $\{\varepsilon, \rho^2, \sigma\rho, \sigma\rho^3\}$. Приметимо да су сви елементи ових скупова реда 1 или 2, па је сваки од њих једнак свом инверзу. Такође, није тешко проверити да су ови скупови затворени за операцију, па јесу подгрупе групе $\mathbb{D}_4$.

Коначно, једина подгрупа реда 8 је баш $\mathbb{D}_4$, тако да су све подгрупе групе $\mathbb{D}_4$

$$\{\varepsilon\}, \{\varepsilon, \sigma\}, \{\varepsilon, \sigma\rho\}, \{\varepsilon, \sigma\rho^2\}, \{\varepsilon, \sigma\rho^3\}, \{\varepsilon, \rho^2\},$$

$$\{\varepsilon, \rho^2, \sigma, \sigma\rho^2\}, \{\varepsilon, \rho^2, \sigma\rho, \sigma\rho^3\}, \{\varepsilon, \rho, \rho^2, \rho^3\} \text{ и } \mathbb{D}_4.$$

Како је $|\mathbb{D}_5| = 10$, по Лагранжовој теореми свака подгрупа групе $\mathbb{D}_5$ има 1, 2, 5 или 10 елемената. Јасно, једина подгрупа са једним елементом је $\{\varepsilon\}$, а слично као у делу под в) закључујемо да су све подгрупе са 2 елемента $\{\varepsilon, \sigma\}$, $\{\varepsilon, \sigma\rho\}$, $\{\varepsilon, \sigma\rho^2\}$, $\{\varepsilon, \sigma\rho^3\}$ и $\{\varepsilon, \sigma\rho^4\}$.

Одредимо подгрупе реда 5 групе $\mathbb{D}_5$. Како је $\langle\rho\rangle = \langle\rho^2\rangle = \langle\rho^3\rangle = \langle\rho^4\rangle = \{\varepsilon, \rho, \rho^2, \rho^3, \rho^4\}$, закључујемо да је $\{\varepsilon, \rho, \rho^2, \rho^3, \rho^4\}$ једина подгрупа реда 5 која садржи неки од елемената $\rho, \rho^2, \rho^3, \rho^4$. Претпоставимо да постоји и нека друга подгрупа H групе $\mathbb{D}_5$ која је реда 5. Тада H садржи неке две симетрије $\sigma\rho^i$ и $\sigma\rho^j$, $0 \leqslant i < j \leqslant 4$, па као у претходном делу закључујемо да $H \ni \sigma\rho^i\sigma\rho^j = \rho^{j-i}$, што је контрадикција.

Једина подгрупа реда 10 је $\mathbb{D}_5$, тако да су све подгрупе групе $\mathbb{D}_5$

$$\{\varepsilon\}, \{\varepsilon, \sigma\}, \{\varepsilon, \sigma\rho\}, \{\varepsilon, \sigma\rho^2\}, \{\varepsilon, \sigma\rho^3\}, \{\varepsilon, \sigma\rho^4\}, \{\varepsilon, \rho, \rho^2, \rho^3, \rho^4\} \text{ и } \mathbb{D}_5.$$

9. Одредити подгрупу од $\mathbb{D}_n$ генерисану елементима ρ^2 и $\rho^2\sigma$; посебно дискутовати случај парног, а посебно непарног n.

Решење: Приметимо да је $\sigma = (\rho^2)^{-1}(\rho^2\sigma)$, па σ припада тој подгрупи. Но, $\rho^2\sigma$ је производ елемената ρ^2 и σ, па $\rho^2\sigma$ припада подгрупи генерисаној са ρ^2 и σ. Закључујемо да је

$$\langle\rho^2, \rho^2\sigma\rangle = \langle\rho^2, \sigma\rangle,$$

па ћемо у даљем испитивати подгрупу $\langle\rho^2, \sigma\rangle$.

Одредимо ред елемента ρ^2. Знамо да је $\omega(\rho) = n$.

n је непаран број. У овом случају је

$$\omega(\rho^2) = \frac{n}{\text{NZD}(2, n)} = \frac{n}{1} = n.$$

Заправо је $\langle\rho^2\rangle = \langle\rho\rangle$, и стога је $\langle\rho^2, \sigma\rangle = \mathbb{D}_n$.

n је паран број. Нека је $n = 2k$. Тада је

$$\omega(\rho^2) = \frac{2k}{\text{NZD}(2, 2k)} = \frac{2k}{2} = k.$$

Заправо је $\langle\rho^2\rangle = \{\varepsilon, \rho^2, \ldots, \rho^{2k-2}\}$, те је

$$\{\varepsilon, \rho^2, \ldots, \rho^{2k-2}, \sigma, \sigma\rho^2, \ldots, \sigma\rho^{2k-2}\} \subseteq \langle\rho^2, \sigma\rangle$$

и $\rho \notin \langle\rho^2, \sigma\rangle$. Дакле, добили смо да наведена подгрупа има бар $2k$ елемената и да она није једнака целој групи која има $4k$ елемената. Закључујемо да је та подгрупа заправо једнака

$$\{\varepsilon, \rho^2, \ldots, \rho^{2k-2}, \sigma, \sigma\rho^2, \ldots, \sigma\rho^{2k-2}\}.$$

Није тешко уверити се да је та подгрупа изоморфна групи $\mathbb{D}_k$.

10. Нека је G Абелова група и H скуп свих елемената коначног реда у G. Доказати да је H подгрупа од G.

Решење: Нека су x и y произвољни елементи подгрупе H. Како је група G Абелова користићемо адитивну нотацију. Уколико је $\omega(x) = m$ и $\omega(y) = n$, то је $mx = 0$ и $ny = 0$. Тада је

$$mn(x - y) = mnx - mny = n(mx) - m(ny) = n0 - m0 = 0,$$

па је ред елемента $x - y$ коначан, тј. $x - y \in H$. Уз чињеницу да је $0 \in H$, те $H \neq \emptyset$, то нам показује да је H заиста подгрупа групе G.

11. Доказати да Абелова група $\mathbb{Q}$ НЕМА коначан скуп генератора.

Решење: Претпоставимо да група $\mathbb{Q}$ има коначан скуп генератора. Нека су то бројеви $\frac{r_1}{s_1}, \frac{r_2}{s_2}, \ldots, \frac{r_k}{s_k}$. То значи да је сваки рационалан број облика

$$n_1\frac{r_1}{s_1} + n_2\frac{r_2}{s_2} + \cdots + n_k\frac{r_k}{s_k},$$

за неке целе бројеве $n_1, n_2, \ldots, n_k$. Свођењем на заједнички именилац добијамо да је сваки рационалан број облика

$$\frac{m}{s_1 s_2 \cdots s_k},$$

за неки цео број m. Нека је p било који прост број који не дели ниједан од бројева $s_1, s_2, \ldots, s_k$. Јасно је да такав постоји пошто је скуп свих простих бројева бесконачан, а сваки од бројева s_i је дељив коначним бројем простих бројева. Тако бисмо добили да је

$$\frac{1}{p} = \frac{m}{s_1 s_2 \cdots s_k},$$

за неки цео број m, те је

$$s_1 s_2 \cdots s_k = pm.$$

Закључујемо да $p \mid s_1 s_2 \cdots s_k$, а како је p прост број, добијамо да $p \mid s_j$ за неко j, што противречи избору простог броја p. Према томе, Абелова група $\mathbb{Q}$ нема коначан скуп генератора.

12. Пермутације $(4\,5\,6\,8)(1\,2\,4\,5)$ и $(6\,2\,4)(2\,5\,3)(8\,7\,6)(4\,5)$ из $\mathbb{S}_8$ представити као производ дисјунктних циклуса и одредити њихов ред.

Решење: Директно добијамо да је

$$(4\,5\,6\,8)(1\,2\,4\,5) = (1\,2\,5)(4\,6\,8), \quad (6\,2\,4)(2\,5\,3)(8\,7\,6)(4\,5) = (2\,5\,6\,8\,7)(3\,4)$$

те је

$$\omega((4\,5\,6\,8)(1\,2\,4\,5)) = \text{NZS}(3,3) = 3, \quad \omega((6\,2\,4)(2\,5\,3)(8\,7\,6)(4\,5)) = \text{NZS}(5,2) = 10.$$

13. Показати да је $H = \{\pi \in \mathbb{S}_8 : \pi(2) = 2, \pi(3) = 3, \pi(6) = 6\}$ подгрупа групе $\mathbb{S}_8$ (у односу на композицију пермутација) и одредити ред те подгрупе.

Решење: Јасно је да идентична пермутација задовољава наведени услов, те $H \neq \emptyset$.

Претпоставимо да $\sigma, \pi \in H$. Покажимо да тада и $\sigma\pi^{-1} \in H$. Како $\pi \in H$, то је $\pi(2) = 2$, па је и $\pi^{-1}(2) = 2$. Слично важи и за бројеве 3 и 6. Стога, ако $k \in \{2, 3, 6\}$:

$$(\sigma\pi^{-1})(k)) = \sigma(\pi^{-1}(k)) = \sigma(k) = k$$

и закључујемо да заиста $\sigma\pi^{-1} \in H$.

Ред подгрупе H није тешко одредити. Наиме, свака пермутација из H фиксира елементе $2, 3$ и 6, док слободно пермутује елементе $1, 4, 5, 7, 8$. Дакле, елемената у H има колико и пермутација ових 5 елемената, тј. $|H| = 5!$. Заправо је $H \cong \mathbb{S}_{\{1,4,5,7,8\}}$.

14. Наћи све подгрупе од $\mathbb{S}_4$ које имају 6 елемената.

Решење: Приметимо најпре да у $\mathbb{S}_4$ не постоји елемент реда 6. Наиме, свака неидентична пермутација у $\mathbb{S}_4$ је или 3-цикл, или 4-цикл, или 2-цикл, или је производ два дисјунктна 2-цикла. Дакле, сваки елемент сем неутрала је реда 2, 3 или 4. У подгрупи реда 6 не може бити елемената реда 4, јер $4 \nmid 6$.

Ако погледамо претходни задатак, није тешко да уочимо неколико подгрупа од $\mathbb{S}_4$ које су реда 6. Наиме, то су подгрупе H_i, где $i \in \{1,2,3,4\}$ одређене са:

$$H_i := \{\pi \in \mathbb{S}_4 : \pi(i) = i\}.$$

Покажимо да су то и једине подгрупе групе $\mathbb{S}_4$ које су реда 6.

У ту сврху, нека је $H \leqslant \mathbb{S}_4$ и $|H| = 6$. На основу Кошијеве теореме у њој постоји елемент реда 3. Сваки елемент реда 3 у групи $\mathbb{S}_4$ је један 3-цикл. Нека је, на пример, $(2\,3\,4)$ тај 3-цикл који се налази у H. Тада је $\{(1), (2\,3\,4), (2\,4\,3)\} \subset H$. У H се мора налазити и неки елемент σ реда 2. Но, тада је заправо

$$H = \{(1), (2\,3\,4), (2\,4\,3), \sigma, \sigma(2\,3\,4), \sigma(2\,4\,3)\}.$$

Наиме, сви ови елементи морају бити у H, а лако се показује да су они сви различити. Но, у H се мора налазити и елемент

$$(2\,3\,4)\sigma.$$

Лако се види (погледати у скриптама како се описују групе реда 6) да

$$(2\,3\,4)\sigma \notin \{(1), (2\,3\,4), (2\,4\,3), \sigma\}.$$

Уколико би важила једнакост

$$(2\,3\,4)\sigma = \sigma(2\,3\,4),$$

из чињенице да је

$$\langle(2\,3\,4)\rangle \cap \langle\sigma\rangle = \{(1), (2\,3\,4), (2\,4\,3)\} \cap \{(1), \sigma\} = \{(1)\}$$

добили бисмо да је $(2\,3\,4)\sigma$ елемент реда 6, а већ смо констатовали да у $\mathbb{S}_4$ нема елемената реда 6.

Стога мора бити

$$(2\,3\,4)\sigma = \sigma(2\,4\,3).$$

Добијамо да је

$$(2\,3\,4) = \sigma(2\,3\,4)\sigma^{-1} = (\sigma(2)\,\sigma(3)\,\sigma(4)),$$

те је $\{\sigma(2), \sigma(3), \sigma(4)\} = \{2,3,4\}$, те мора бити $\sigma(1) = 1$. Тако добијамо да сваки елемент $\pi \in H$ испуњава услов да је $\pi(1) = 1$, те можемо закључити да је $H = H_1$.

15. Ако $\pi, \sigma \in \mathbb{S}_n$, доказати да $\pi\sigma\pi^{-1}\sigma^{-1} \in \mathbb{A}_n$.

Решење: Представимо π и σ у облику производа транспозиција:

$$\pi = \tau_1\tau_2\cdots\tau_k, \quad \sigma = \theta_1\theta_2\cdots\theta_l.$$

Тада је

$$\begin{aligned}
\pi\sigma\pi^{-1}\sigma^{-1} &= \tau_1\tau_2\cdots\tau_k\theta_1\theta_2\cdots\theta_l(\tau_1\tau_2\cdots\tau_k)^{-1}(\theta_1\theta_2\cdots\theta_l)^{-1} \\
&= \tau_1\tau_2\cdots\tau_k\theta_1\theta_2\cdots\theta_l\tau_k^{-1}\cdots\tau_2^{-1}\tau_1^{-1}\theta_l^{-1}\cdots\theta_2^{-1}\theta_1^{-1} \\
&= \tau_1\tau_2\cdots\tau_k\theta_1\theta_2\cdots\theta_l\tau_k\cdots\tau_2\tau_1\theta_l\cdots\theta_2\theta_1
\end{aligned}$$

Дакле, број транспозиција у овом приказу пермутације $\pi\sigma\pi^{-1}\sigma^{-1}$ је $k+l+k+l = 2(k+l)$ те је у питању парна пермутација, тј. $\pi\sigma\pi^{-1}\sigma^{-1} \in \mathbb{A}_n$.

16. Ако је n непаран број, доказати да $(1\,2\,3)$ и $(1\,2\,\ldots\,n)$ генеришу $\mathbb{A}_n$. Ако је n паран број, доказати да $(1\,2\,3)$ и $(2\,3\cdots n)$ генеришу $\mathbb{A}_n$.

Решење: а) Како је n непаран број важи $(1\,2\,\ldots\,n)\in\mathbb{A}_n$, па је

$$\langle(1\,2\,3),(1\,2\,\ldots\,n)\rangle\subseteq\mathbb{A}_n.$$

У скриптама смо доказали да је подгрупа $\mathbb{A}_n$ генерисана циклусима облика $(1\,a\,b)$, где је $a,b\in\{2,3,\ldots,n\}$ и $a\neq b$. Стога је довољно доказати да се у $\langle(1\,2\,3),(1\,2\,\ldots\,n)\rangle$ налазе сви циклуси тог облика. Означимо $G=\langle(1\,2\,3),(1\,2\,\ldots\,n)\rangle$ и $\pi=(1\,2\,\ldots\,n)$.

Докажимо прво да је $(i\;i+1\;i+2)\in G$ за све $1\leqslant i\leqslant n-2$. Ово доказујемо индукцијом по i. За $i=1$ тврђење важи (јер је $(1\,2\,3)\in G$). Претпоставимо зато да тврђење важи за неко $i\leqslant n-3$ и докажимо га за $i+1$. Користећи познату формулу добијамо

$$\pi\,(i\;i+1\;i+2)\,\pi^{-1}=(\pi(i)\;\pi(i+1)\;\pi(i+2))=(i+1\;i+2\;i+3),$$

па како је $\pi\in G$ и $(i\;i+1\;i+2)\in G$ (по индуктивној претпоставци), то је и $(i+1\;i+2\;i+3)=\pi\,(i\;i+1\;i+2)\,\pi^{-1}\in G$.

Докажимо сада да је $(1\;i\;i+1)\in G$ за све $2\leqslant i\leqslant n-1$. Доказ изводимо индукцијом по i. За $i=2$ тврђење важи (јер је $(1\,2\,3)\in G$). Претпоставимо зато да тврђење важи за неко $i\leqslant n-2$ и докажимо га за $i+1$. Користећи исту формулу као и горе добијамо

$$(i\;i+1\;i+2)(1\;i\;i+1)(i\;i+1\;i+2)^{-1}=(1\;i+1\;i+2),$$

па како је $(i\;i+1\;i+2)\in G$ (доказано у претходном пасусу) и $(1\;i\;i+1)\in G$ (по индуктивној претпоставци), то је $(1\;i+1\;i+2)\in G$.

Коначно, докажимо да је $(1\;i\;i+k)\in G$ за све i,k такве да је $2\leqslant i<i+k\leqslant n$. Доказ изводимо индукцијом по k. За $k=1$ тврђење важи по претходном пасусу. Претпоставимо зато да тврђење важи за $k\geqslant 1$ (и све i такве да је $2\leqslant i<i+k\leqslant n$) и докажимо га за $k+1$ (и све i такве да је $2\leqslant i<i+k+1\leqslant n$). По претходном пасусу је $(1\;i+k\;i+k+1)\in G$, па је $(1\;i+k+1\;i+k)=(1\;i+k\;i+k+1)^{-1}\in G$. Поновном применом формуле добијамо

$$(1\;i+k+1\;i+k)(1\;i\;i+k)(1\;i+k+1\;i+k)^{-1}=(i+k+1\;i\;1),$$

па је $(i+k+1\;i\;1)\in G$, а самим тим и $(1\;i\;i+k+1)=(i+k+1\;i\;1)^{-1}\in G$.

Дакле, $(1\;i\;i+k)\in G$ за све i,k такве да је $2\leqslant i<i+k\leqslant n$, па је и $(1\;i+k\;i)=(1\;i\;i+k)^{-1}\in G$. Како је сваки циклус $(1\,a\,b)$, где је $a,b\in\{2,3,\ldots,n\}$ и $a\neq b$, једног од ова два облика, доказ је завршен.

б) Како је n паран број важи $(2\,3\,\ldots\,n)\in\mathbb{A}_n$, па је

$$\langle(1\,2\,3),(2\,3\,\ldots\,n)\rangle\subseteq\mathbb{A}_n.$$

Слично као у делу под а) довољно је доказати да $\langle(1\,2\,3),(2\,3\,\ldots\,n)\rangle$ садржи све циклусе облика $(1\,a\,b)$, где је $a,b\in\{2,3,\ldots,n\}$ и $a\neq b$. Означимо $G=\langle(1\,2\,3),(2\,3\,\ldots\,n)\rangle$ и $\pi=(2\,3\,\ldots\,n)$.

Докажимо прво да је $(1\;i\;i+1)\in G$ за све $2\leqslant i\leqslant n-1$. Ово доказујемо индукцијом по i. За $i=2$ тврђење важи (јер је $(1\,2\,3)\in G$). Претпоставимо зато да тврђење важи за неко $i\leqslant n-2$ и докажимо га за $i+1$. Имамо да је

$$\pi\,(1\;i\;i+1)\,\pi^{-1}=(\pi(1)\;\pi(i)\;\pi(i+1))=(1\;i+1\;i+2),$$

па како су $\pi\in G$ и $(1\;i\;i+1)\in G$ (по индуктивној претпоставци), то је и $(1\;i+1\;i+2)\in G$.

Докажимо сада да је $(i\;i+1\;i+2)\in G$ за све $1\leqslant i\leqslant n-2$. Доказ изводимо индукцијом по i. За $i=1$ тврђење важи (јер је $(1\,2\,3)\in G$). Претпоставимо зато да тврђење важи за неко $i\leqslant n-3$ и докажимо га за $i+1$. Важи да је

$$(1\;i+1\;i+2)(1\;i\;i+1)(i\;i+1\;i+2)^{-1}=(i+1\;i\;i+2)=(i\;i+2\;i+1),$$

па како је $(1\;i\;i+1)$ и $(1\;i+1\;i+2)$ у G (доказано у претходном пасусу), то је $(i\;i+2\;i+1)\in G$. Одавде је $(i\;i+1\;i+2)=(i\;i+2\;i+1)^{-1}\in G$, што је требало доказати.

Доказ сада можемо завршити као у делу под а).

17. Показати да $\mathbb{A}_4$ садржи подгрупу изоморфну групи симетрија правоугаоника који није квадрат.

Решење: Означимо темена квадрата бројевима од 1 до 4. Знамо да је Клајнова група $V = \{\varepsilon, \mathcal{S}_p, \mathcal{S}_q, \mathcal{S}_O\}$, где је са $\mathcal{S}_p$ означена осна рефлексија у односу на праву p, која је симетрала страница 12 и 34, са $\mathcal{S}_q$ осна рефлексија у односу на праву q која је симетрала страница 14 и 23 и са $\mathcal{S}_O$ централна симетрија у односу на тачку O која је пресек правих p и q.

Сваки елемент Клајнове групе пермутује темена правоугаоника. Посматрајмо подгрупу V' групе $\mathbb{A}_4$ задату са $V' = \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. Ако сваком елементу групе V придружимо пермутацију темена коју тај елемент врши, видимо да ε одговара идентичној пермутацији, $\mathcal{S}_p$ одговара пермутацији $(1\,2)(3\,4)$, $\mathcal{S}_q$ пермутацији $(1\,4)(2\,3)$ и $\mathcal{S}_O$ пермутацији $(1\,3)(2\,4)$. Тако смо добили бијекцију између V и V', но како је у оба случаја операција у групи заправо композиција пресликавања, а придруживање је заправо рестрикција пресликавања на скуп темена, јасно је да се та бијекција слаже са операцијама, тј. задаје изоморфизам група V и V'.

18. Показати да бројеви 1, 2, 4, 5, 7, 8 чине групу у односу на множење по модулу 9 и да је та група изоморфна групи $\mathbb{Z}_6$

Решење: Нека је $G = \{1, 2, 4, 5, 7, 8\}$. Посматрајмо таблицу множења у овом скупу при чему је операција $\cdot_9$:

$\cdot_9$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Знамо да је множење по модулу n, где је n било који природан број већи од 1 комутативна и асоцијативна операција. Такође је јасно и да је 1 неутрал за ову операцију. Горња таблица нам показује и да сваки елемент из G има инверз у односу на ту операцију, те је G заиста група (заправо Абелова група).

Да бисмо показали да је ова група изоморфна групи $\mathbb{Z}_6$ довољно је показати да је она циклична, с обзиром да је свака циклична група реда 6 изоморфна групи $\mathbb{Z}_6$. Дакле, треба наћи генератор за групу G. Директним рачуном добијамо да је то елемент 2. Наиме:

$$2^0 = 1, \quad 2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 7, \quad 2^5 = 5,$$

па је заиста $\langle 2 \rangle = G$.

19. Показати да бројеви 1, 3, 7, 9, 11, 13, 17, 19 чине групу у односу на множење по модулу 20 и да та група НИЈЕ изоморфна групи $\mathbb{Z}_8$.

Решење: Нека је $G = \{1, 3, 7, 9, 11, 13, 17, 19\}$. Формирајмо таблицу множења.

$\cdot_{20}$	1	3	7	9	11	13	17	19
1	1	3	7	9	11	13	17	19
3	3	9	1	7	13	19	11	17
7	7	1	9	3	17	11	19	13
9	9	7	3	1	19	17	13	11
11	11	13	17	19	1	3	7	9
13	13	19	11	17	3	9	1	7
17	17	11	19	13	7	1	9	3
19	19	17	13	11	9	7	3	1

Из таблице видимо да заиста сваки елемент из G има инверз у G и, као у претходном задатку, закључујемо да је $(G, \cdot_{20})$ Абелова група.

Да бисмо доказали да ова група није изоморфна групи $\mathbb{Z}_8$ довољно је доказати да $(G, \cdot_{20})$ није циклична група. Знамо да је нека група циклична ако и само ако садржи елемент чији је ред једнак

реду групе, тако да је довољно доказати да у G нема елемената реда 8. Следећа табела доказује ову тврдњу:

n	1	3	7	9	11	13	17	19
$\omega(n)$	1	4	4	2	2	4	4	2

.

20. Нека је G група. Доказати да је $f : G \to G$, дефинисано са $f(x) = x^{-1}$ изоморфизам ако и само ако је група G Абелова.

Решење: С обзиром да је јасно да је f бијекција, f је изоморфизам ако и само ако је :

$$f(xy) = f(x)f(y)$$

за све $x, y \in G$. Другим речима, f је изоморфизам ако и само ако за све $x, y \in G$ важи:

$$(xy)^{-1} = x^{-1}y^{-1}.$$

С обзиром да је $(xy)^{-1} = y^{-1}x^{-1}$, добијамо да је f изоморфизам акко за све $x, y \in G$ важи:

$$y^{-1}x^{-1} = x^{-1}y^{-1}.$$

Множењем слева најпре са x, а потом са y добијамо да је та релација еквивалентна са:

$$yxy^{-1}x^{-1} = e.$$

Множење здесна најпре са x, а потом са y добијамо еквивалентну релацију

$$yx = xy,$$

што и показује да је f изоморфизам ако и само ако је група G комутативна.

21. Доказати да је подгрупа групе $\mathbb{S}_6$, која је генерисана циклусима $(1\,2\,3\,4)$ и $(5\,6)$ изоморфна групи из 19. задатка.

Решење: Нека је $\pi = (1\,2\,3\,4)$, а $\sigma = (5\,6)$. С обзиром да су ово дисјунктни циклуси знамо да је $\pi\sigma = \sigma\pi$. Означимо са H подгрупу од $\mathbb{S}_6$ генерисану циклусима π и σ. С обзиром да π и σ комутирају и да је $\omega(\pi) = 4$, а $\omega(\sigma) = 2$, имамо да је

$$H = \{(1), \pi, \pi^2, \pi^3, \sigma, \sigma\pi, \sigma\pi^2, \sigma\pi^3\}.$$

Ако са H_1 означимо подгрупу генерисану са π, а са H_2 подгрупу генерисану са σ, видимо да су испуњени услови за примену става о раставу на директан производ, те је

$$H \cong H_1 \times H_2 \cong \mathbb{Z}_4 \times \mathbb{Z}_2.$$

Дакле, сада треба да покажемо да је и група G из 19. задатка изоморфна истом производу. Означимо са G_1 подгрупу генерисану елементом 3, а са G_2 подгрупу генерисану елементом 11. Како је $G_1 = \{1, 3, 9, 7\}$, $G_2 = \{1, 11\}$, видимо да је $G_1 \cap G_2 = \emptyset$. Такође се директно може проверити да је $G_1G_2 = G$, а знамо и да је G комутативна група. Стога је

$$G \cong G_1 \times G_2 \cong \mathbb{Z}_4 \times \mathbb{Z}_2,$$

те добијамо да је заиста $H \cong G$.

22. Доказати да је подгрупа од $\mathbb{S}_4$, генерисана елементима $(1\,2\,3\,4)$ и $(2\,4)$ изоморфна групи $\mathbb{D}_4$.

Решење: Нека је $\pi = (1\,2\,3\,4)$, а $\theta = (2\,4)$. Тада је

$$\theta\pi = (2\,4)(1\,2\,3\,4) = (1\,4)(2\,3)$$

С обзиром да је $\pi^3 = (1\,4\,3\,2)$, добијамо да је

$$\pi^3\theta = (1\,4\,3\,2)(2\,4) = (1\,4)(2\,3).$$

Дакле, $\theta\pi = \pi^3\theta$. С обзиром да је $\omega(\pi) = 4$ и $\omega(\theta) = 2$, видимо да ови елементи испуњавају исте услове као и елементи ρ и σ у групи $\mathbb{D}_4$. Према томе, ако са G означимо подгрупу од $\mathbb{S}_4$ генерисану елементима π и θ, имамо да је $G = \{(1), \pi, \pi^2, \pi^3, \theta, \theta\pi, \theta\pi^2, \theta\pi^3\}$ и да је $f\colon \mathbb{D}_4 \to G$ задато са $f(\sigma^i\rho^j) = \theta^i\pi^j)$, где је $0 \leqslant i \leqslant 1$, $0 \leqslant j \leqslant 3$ изоморфизам група.

23. Одредити $Z(\mathbb{S}_n)$, $Z(\mathbb{A}_n)$, $Z(\mathbb{D}_n)$.

Решење: а) Ако је $n \leqslant 2$, тада група $\mathbb{S}_n$ група има највише 2 елемента, па је Абелова и важи $Z(\mathbb{S}_n) = \mathbb{S}_n$. Нека је зато $n \geqslant 3$.

Нека је $\pi \in Z(\mathbb{S}_n)$. Претпоставимо да $\pi \neq (1)$. То значи да за неко $a \in \{1, \ldots, n\}$ важи $b = \pi(a) \neq a$. Узмимо елемент $c \notin \{a, b\}$. Он постоји пошто је $n \geqslant 3$. Како π припада центру групе $\mathbb{S}_n$, то мора бити $\pi(a\,c) = (a\,c)\pi$, тј.

$$\pi(a\,c)\pi^{-1} = (a\,c).$$

Како је $\pi(a\,c)\pi^{-1} = (\pi(a)\,\pi(c))$, то је $(\pi(a)\,\pi(c)) = (a\,c)$ те следи да је $\{\pi(a), \pi(c)\} = \{a, c\}$, што није могуће, јер $b = \pi(a)$ не припада подскупу $\{a, c\}$ на основу избора елемента c. Закључујемо да мора бити $\pi = (1)$, тј. $Z(\mathbb{S}_n) = \{(1)\}$.

б) Ако је $n \leqslant 3$, тада група $\mathbb{A}_n$ има највише три елемента, па је Абелова и важи $Z(\mathbb{A}_n) = \mathbb{A}_n$. Нека је зато $n \geqslant 4$. У наставку поступамо као у делу под а).

Нека је $\pi \in Z(\mathbb{A}_n)$. Претпоставимо да $\pi \neq (1)$. То значи да за неко $a \in \{1, \ldots, n\}$ важи $b = \pi(a) \neq a$. Изаберимо два различита елемента c и d из $\{1, \ldots, n\}$, који не припадају подскупу $\{a, b\}$. То је могуће учинити, јер је $n \geqslant 4$. Како π припада центру групе $\mathbb{S}_n$, то мора бити $\pi(a\,c\,d) = (a\,c\,d)\pi$, тј.

$$\pi(a\,c\,d)\pi^{-1} = (a\,c\,d).$$

Како је $\pi(a\,c\,d)\pi^{-1} = (\pi(a)\,\pi(c)\,\pi(d))$, то је $(\pi(a)\,\pi(c)\,\pi(d)) = (a\,c\,d)$ те следи да је $\{\pi(a), \pi(c), \pi(d)\} = \{a, c, d\}$, што није могуће, јер $b = \pi(a)$ не припада подскупу $\{a, c, d\}$ на основу избора елемената c и d. Закључујемо да мора бити $\pi = (1)$, тј. $Z(\mathbb{A}_n) = \{(1)\}$.

в) Знамо да је $\mathbb{D}_n = \{\varepsilon, \rho, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \ldots, \sigma\rho^{n-1}\}$, где је наравно σ осна рефлексија, а ρ ротација.

Испитајмо најпре да ли неки елемент облика $\sigma\rho^k$ за $0 \leqslant k \leqslant n-1$ може припадати центру. У том случају би важила једнакост

$$(\sigma\rho^k)\rho = \rho(\sigma\rho^k).$$

Знамо да је $\rho\sigma = \sigma\rho^{n-1} = \sigma\rho^{-1}$. Уколико то применимо на горњу једнакост добијамо

$$\sigma\rho^k\rho = \sigma\rho^{-1}\rho^k.$$

Одавде следи да је

$$\rho^{k+1} = \rho^{k-1},$$

односно да је

$$\rho^2 = \varepsilon.$$

С обзиром да је $\omega(\rho) = n > 2$, ово није могуће. Закључујемо да елементи облика $\sigma\rho^k$ не припадају центру.

Посматрајмо сада ротације, тј. елементе облика ρ^k за $1 \leqslant k \leqslant n-1$ (јасно је да је ε у центру). С обзиром да ρ^k комутира са ρ, закључујемо да ρ^k припада центру ако и само ако је

$$\rho^k\sigma = \sigma\rho^k.$$

Но, знамо да је $\sigma\rho^k = \rho^{n-k}\sigma = \rho^{-k}\sigma$, па је горња једнакост еквивалентна са

$$\rho^k\sigma = \rho^{-k}\sigma,$$

тј. са

$$\rho^{2k} = \varepsilon.$$

С обзиром да је $\omega(\rho) = n$, добијамо да $n \mid 2k$. Уколико је n непаран број, то би значило да $n \mid k$, али то није могуће с обзиром да је $1 \leqslant k \leqslant n-1$. Закључујемо да је $Z(\mathbb{D}_n) = \{\varepsilon\}$ уколико је n непаран број.

Уколико је n паран број добијамо да $\frac{n}{2} \mid k$. Како је $1 \leqslant k \leqslant n-1$, мора бити заправо $\frac{n}{2} = k$. Дакле, у случају да је n паран број $Z(\mathbb{D}_n) = \{\varepsilon, \rho^{n/2}\}$.

24. Ако је група $G \times H$ циклична, доказати да су и G и H цикличне групе.

Решење: Претпоставимо да је $G \times H$ циклична група и нека је (g_0, h_0) генератор те групе. Покажимо да је g_0 генератор групе G. У ту сврху, нека је $g \in G$ ма који елемент из G. Уколико је e неутрал у G, а ε неутрал у H, тада је (g, ε) елемент у $G \times H$. С обзиром да је (g_0, h_0) генератор групе $G \times H$, то постоји $m \in \mathbb{Z}$ такав да је $(g, \varepsilon) = (g_0, h_0)^m = (g_0^m, h_0^m)$. Дакле, $g = g_0^m$ и видимо да је g_0 заиста генератор групе G. На исти начин се добија и да је h_0 генератор групе H, те су и G и H цикличне групе.

25. Доказати да група $\mathbb{Z} \times \mathbb{Z}$ НИЈЕ изоморфна групи $\mathbb{Z}$.

Решење: Уколико би група $\mathbb{Z} \times \mathbb{Z}$ била изоморфна групи $\mathbb{Z}$ она би била циклична група. Покажимо да $\mathbb{Z} \times \mathbb{Z}$ није циклична група.

Претпоставимо да она јесте циклична и нека је (x_0, y_0) генератор. Како је $(1, 0) \in \mathbb{Z} \times \mathbb{Z}$, то постоји $m \in \mathbb{Z}$ тако да је

$$m(x_0, y_0) = (1, 0).$$

Дакле,

$$mx_0 = 1, \quad my_0 = 0.$$

Из $mx_0 = 1$ следи да је $m \neq 0$, па $my_0 = 0$ повлачи да је $y_0 = 0$. Но, и $(0, 1) \in \mathbb{Z} \times \mathbb{Z}$, па мора постојати $k \in \mathbb{Z}$ тако да је

$$(0, 1) = k(x_0, y_0) = (kx_0, ky_0) = (kx_0, 0).$$

Но, тако добијамо да је $1 = 0$ и ова контрадикција нам показује да група $\mathbb{Z} \times \mathbb{Z}$ није циклична, па стога није изоморфна групи $\mathbb{Z}$.

26. Ако је $A \leqslant G$ и $B \leqslant H$, доказати да је $A \times B \leqslant G \times H$. Наћи подгрупу од $\mathbb{Z} \times \mathbb{Z}$, која није овог облика.

Решење: Како је $A \leqslant G$ и $B \leqslant H$, то је јасно да је $A \times B \neq \emptyset$.

Претпоставимо да су (a_1, b_1) и (a_2, b_2) елементи из $A \times B$. Покажимо да $(a_1, b_1)(a_2, b_2)^{-1} \in A \times B$:

$$(a_1, b_1)(a_2, b_2)^{-1} = (a_1, b_1)(a_2^{-1}, b_2^{-1}) = (a_1 a_2^{-1}, b_1 b_2^{-1}).$$

С обзиром да је $A \leqslant G$ и да $a_1, a_2 \in A$, важи да је $a_1 a_2^{-1} \in A$. На сличан начин закључујемо да $b_1 b_2^{-1} \in B$, те $(a_1 a_2^{-1}, b_1 b_2^{-1}) \in A \times B$ и на основу познатог критеријума закључујемо да је $A \times B \leqslant G \times H$.

Нека је $D = \{(m, m) : m \in \mathbb{Z}\}$. Јасно је да $D \neq \emptyset$. Претпоставимо да су (r, r) и (s, s) два елемента из D. Тада је $(r, r) - (s, s) = (r - s, r - s) \in D$. Стога је D заиста подгрупа групе $\mathbb{Z} \times \mathbb{Z}$, а јасно је да она није облика $A \times B$ за неке $A, B \subseteq \mathbb{Z}$.

27. Испитати које су од следећих група изоморфне једна другој:

$$\mathbb{Z}_{24}, \quad \mathbb{D}_4 \times \mathbb{Z}_3, \quad \mathbb{D}_{12}, \quad \mathbb{A}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{D}_6, \quad \mathbb{S}_4, \quad \mathbb{Z}_{12} \times \mathbb{Z}_2.$$

Решење: Ако су групе G и H изоморфне, тада су њихови редови исти, једна је комутативна ако и само ако је и друга, максималан ред њихових елемената је исти, за свако k имају исти број елемената реда k, итд. Дакле, ако је за групе G и H барем једна од ових „особина" различита онда оне нису изоморфне (међутим, ако су за групе G и H све од наведених „особина" исте ипак не можемо закључити да су оне изоморфне, била би потребна даља анализа).

Свака од наведених група је реда 24 (проверите ово!), па на основу реда не можемо закључити да неке две од датих група нису изоморфне. Групе $\mathbb{Z}_{24}$ и $\mathbb{Z}_{12} \times \mathbb{Z}_2$ су комутативне, док преостале нису. Дакле, групе $\mathbb{Z}_{24}$ и $\mathbb{Z}_{12} \times \mathbb{Z}_2$ нису изоморфне са неком од преосталих група, па је довољно проверити да ли су оне изоморфне. Но, $\mathbb{Z}_{24}$ је циклична група док група $\mathbb{Z}_{12} \times \mathbb{Z}_2$ није циклична (присетимо се да је $\mathbb{Z}_m \times \mathbb{Z}_n$ циклична група акко су m и n узајамно прости бројеви), те ове две групе нису изоморфне.

Како је сваки елемент у S_4, сем идентичне пермутације, или 2-циклус, или производ два дисјунктна 2-циклуса, или 3-циклус, или 4-циклус, то видимо да је максималан ред елемента у $\mathbb{S}_4$ једнак 4.

Но, све остале групе имају елементе вишег реда. У $\mathbb{D}_{12}$ је то основна ротација, која је реда 12. У $\mathbb{D}_4 \times \mathbb{Z}_3$ је то елемент $(\rho, 1)$ (где смо са ρ означили базну ротацију). Наиме,

$$(\rho, 1) = (\rho, 0) * (\varepsilon, 1),$$

где смо са $*$ означили операцију у $\mathbb{D}_4 \times \mathbb{Z}_3$ (операција у $\mathbb{D}_4$ је заправо композиција пресликавања, а у $\mathbb{Z}_3$ је то сабирање по модулу 3, па смо увели посебну ознаку да означимо операцију у овом директном производу). Но,

$$(\rho, 0) * (\varepsilon, 1) = (\varepsilon, 1) * (\rho, 0),$$

$$\omega((\rho, 0)) = \omega(\rho) = 4, \quad \omega((\varepsilon, 1)) = \omega(1) = 3$$

и

$$\langle(\rho, 0)\rangle \cap \langle(\varepsilon, 1)\rangle = \{(\varepsilon, 0), (\rho, 0), (\rho^2, 0), (\rho^3, 0)\} \cap \{(\varepsilon, 0), (\varepsilon, 1), (\varepsilon, 2)\} = \{(\varepsilon, 0)\},$$

па на основу познатог резултата закључујемо да је

$$\omega((\rho, 1)) = \omega((\rho, 0) * (\varepsilon, 1)) = \text{NZS}(4, 3) = 12.$$

Како је сваки елемент у $\mathbb{A}_4$, сем идентичне пермутације, или 3-цикл, или производ два дисјунктна 2-цикла, то је сваки елемент који није неутрал овде реда 2 или 3. На исти начин као и у горњој анализи добијамо да је

$$\omega((1\,2\,3), 1)) = \omega((1\,2\,3), 0) * (0, 1)) = \text{NZS}(3, 2) = 6$$

и то је заправо максималан ред неког елемента у $\mathbb{A}_4 \times \mathbb{Z}_2$. Дакле, ни ова група није изоморфна групи $\mathbb{S}_4$. Но, она није ни изоморфна групама $\mathbb{D}_4 \times \mathbb{Z}_3$ и $\mathbb{D}_{12}$ јер у њој нема елемента реда 12. Но, није се тешко уверити да ни у $\mathbb{Z}_2 \times \mathbb{D}_6$ нема елемената реда 12. Наиме, у групи $\mathbb{D}_6$ имамо осне рефлексије које су све реда 2, и ротације чији ред дели 6. Но, ако је $f \in \mathbb{D}_6$ произвољан елемент, онда је у $\mathbb{Z}_2 \times \mathbb{D}_6$

$$\omega((1, f)) = \text{NZS}(2, \omega(f))$$

(погледати горњу анализу) и овај број је или 2, или 6.

Остало је да проверимо само да ли је $\mathbb{D}_{12} \cong \mathbb{D}_4 \times \mathbb{Z}_3$ и да ли је $\mathbb{A}_4 \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{D}_6$.

Знамо да у $\mathbb{D}_{12}$ имамо 12 рефлексија које су све реда 2. С друге стране, нека је $(f, x) \in \mathbb{D}_4 \times \mathbb{Z}_3$ реда 2. Тада је

$$(\varepsilon, 0) = (f, x) * (f, x) = (f^2, 2x).$$

Но, уколико је $x \in \mathbb{Z}_3$ такав да је $2x = 0$, онда мора бити заправо $x = 0$, те је елемент $(f, x) \in \mathbb{D}_4 \times \mathbb{Z}_3$ реда 2 акко је $f \in \mathbb{D}_4$ реда 2 и $x = 0$. Но, у $\mathbb{D}_4$ имамо 4 рефлексије које су све реда 2 и једну ротацију која је реда 2. Дакле, у $\mathbb{D}_4 \times \mathbb{Z}_3$ имамо 5 елемената реда 2, док у $\mathbb{D}_{12}$ имамо заправо 13 елемената реда 2 — 12 рефлексија и једна ротација. Како се при изоморфизму елементи реда 2 сликају у елементе реда 2, закључујемо да групе $\mathbb{D}_{12}$ и $\mathbb{D}_4 \times \mathbb{Z}_3$ нису изоморфне.

Посматрајмо сада групе $\mathbb{A}_4 \times \mathbb{Z}_2$ и $\mathbb{D}_6 \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{D}_6$. Нека је G било која група и нека је $(g, x) \in G \times \mathbb{Z}_2$ елемент реда 3. Тада је

$$(e, 0) = (g, x)^3 = (g^3, 3x) = (g^3, x),$$

те следи да је $x = 0$. Закључујемо да у $G \times \mathbb{Z}_2$ има онолико елемената реда 3 колико их има у групи G.

У групи $\mathbb{D}_6$ имамо 6 рефлексија и све су оне реда 2. Једино ротације могу бити реда 3, но заправо имамо само две ротације реда 3 — ρ^2 и ρ^4 (где је ρ основна ротација). Но, у групи $\mathbb{A}_4$ имамо више елемената реда 3 — сви 3-цикли су реда 3: $(1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3)$. Дакле, како у групи $\mathbb{A}_4 \times \mathbb{Z}_2$ има осам елемената реда 3, а у групи $\mathbb{D}_6 \times \mathbb{Z}_2$ их има два, закључујемо да ове две групе нису изоморфне.

Да резимирамо: показали смо заправо да међу наведеним групама нема међусобно изоморфних.

28. Нека су H и K коначне подгрупе неке групе G и нека су редови тих подгрупа узајамно прости бројеви. Доказати да је $H \cap K = \{e\}$.

Решење: По Лагранжовој теореми знамо да ред подгрупе дели ред групе. Стога $|H \cap K| \mid |H|$ и $|H \cap K| \mid |K|$. По претпоставци је $\mathrm{NZD}(|H|, |K|) = 1$ те следи да је $|H \cap K| = 1$, тј. $H \cap K = \{e\}$.

29. Нека је $H \leqslant \mathbb{S}_n$ и нека $H \not\subseteq \mathbb{A}_n$. Доказати да тачно половину елемената из H чине парне пермутације.

Решење: $H = (H \cap \mathbb{A}_n) \sqcup (H \cap \mathbb{A}_n^c)$. С обзиром да $H \not\subseteq \mathbb{A}_n$, оба ова подскупа су непразна и нека је $\sigma \in H \cap \mathbb{A}_n^c$ ма која непарна пермутација из H. Пресликавање

$$F \colon H \cap \mathbb{A}_n \to H \cap \mathbb{A}_n^c$$

задато са $F(\pi) = \sigma\pi$ је коректно задато, јер, како је H подгрупа, из чињенице да $\pi \in H$ следи да $\sigma\pi \in H$, а с обзиром да је σ непарна пермутација из чињенице да је π парна пермутација следи да је $\sigma\pi$ непарна пермутација. Није тешко уверити се да је F бијекција. Наиме, уколико је $F(\pi_1) = F(\pi_2)$ добијамо да је $\sigma\pi_1 = \sigma\pi_2$, а онда, множењем слева са σ^{-1} следи да је $\pi_1 = \pi_2$. Дакле, F је „1–1". Уколико је $\theta \in H \cap \mathbb{A}_n^c$, онда је $\sigma^{-1}\theta \in H \cap \mathbb{A}_n$, а $F(\sigma^{-1}\theta) = \theta$, па је F и „на". Дакле, F је бијекција и добијамо да је $|H \cap \mathbb{A}_n| = |H \cap \mathbb{A}_n^c|$, те је

$$|H| = |H \cap \mathbb{A}_n| + |H \cap \mathbb{A}_n^c| = |H \cap \mathbb{A}_n| + |H \cap \mathbb{A}_n| = 2|H \cap \mathbb{A}_n|,$$

тј. $|H \cap \mathbb{A}_n| = \frac{1}{2}|H|$, а то је оно што је и тражено.

30. Доказати да је свака Абелова група реда pq, где су p и q различити прости бројеви, циклична.

Решење: Нека је A Абелова група реда pq. На основу Кошијеве теореме, постоји у A елемент x реда p и елемент y реда q. Покажимо да је елемент $x + y$ реда pq. Јасно је да је

$$(pq)(x + y) = (pq)x + (pq)y = q(px) + p(qy) = q0 + p0 = 0,$$

па $\omega(x + y) \mid pq$. Како је $x + y \neq 0$ (ако је $x = -y$, онда је $p = \omega(x) = \omega(-y) = \omega(y) = q$ што је контрадикција), онда $\omega(x + y) \in \{p, q, pq\}$. Но, уколико би било $\omega(x + y) = p$, имали бисмо

$$0 = p(x + y) = px + py = 0 + py = py,$$

па би $q \mid p$. Уколико претпоставимо да је $\omega(x + y) = q$, добили бисмо да $p \mid q$. Стога $\omega(x + y) \notin \{p, q\}$, па мора бити $\omega(x + y) = pq$. Но, с обзиром да је група A реда pq закључујемо да је $\langle x + y \rangle = A$, те је група A циклична.

31. Доказати да је свака Абелова група реда $p_1 \cdots p_n$, где су p_i различити прости бројеви, циклична.

Решење: Претходни задатак је заправо овај за случај $n = 2$. Нека је A Абелова група реда $p_1 \cdots p_n$, где су p_i различити прости бројеви. Нека су x_i елементи групе A који су реда p_i а који постоје на основу Кошијеве теореме. Докажимо да је елемент $x_1 + \cdots + x_n$ реда $p_1 \cdots p_n$. Нека је $a = p_1 \cdots p_n$. Покажимо да $\frac{a}{p_i}(x_1 + \cdots + x_n) \neq 0$ за све i. Наиме, ако је $j \neq i$, онда је

$$\frac{a}{p_i}x_j = \frac{a}{p_i p_j}p_j x_j = \frac{a}{p_i p_j}0 = 0.$$

Дакле,

$$\frac{a}{p_i}(x_1 + \cdots + x_n) = \frac{a}{p_i}x_1 + \cdots + \frac{a}{p_i}x_n = \frac{a}{p_i}x_i.$$

Но, ако би било $\frac{a}{p_i}x_i = 0$, како је $\omega(x_i) = p_i$, добили бисмо да $p_i \mid \frac{a}{p_i}$. Но, ово није могуће, јер је $\frac{a}{p_i}$ производ преосталих простих бројева и тај производ није дељив са p_i.

Дакле, за све i је $\frac{a}{p_i}(x_1 + \cdots + x_n) \neq 0$. Знамо да $\omega(x_1 + \cdots + x_n) \mid |A|$, тј. $\omega(x_1 + \cdots + x_n) \mid p_1 \cdots p_n$. Уколико $\omega(x_1 + \cdots + x_n) \neq p_1 \cdots p_n$, тај ред би био производ неких од ових простих бројева у коме се не појављује бар један од $p_1, \ldots, p_n$. Рецимо, нека је то број p_k. Тада $\omega(x_1 + \cdots + x_n) \mid \frac{a}{p_k}$, па би морало бити $\frac{a}{p_k}(x_1 + \cdots + x_n) = 0$, а видели смо да то није тачно. Стога је $\omega(x_1 + \cdots + x_n) = p_1 \cdots p_n$ и група A је циклична са генератором $x_1 + \cdots + x_n$.

32. Испитати да ли у групи $\mathbb{S}_7$ постоји елемент реда 12.

Решење: Ово није тешко показати. Наиме, елемент $(1\,2\,3\,4)(5\,6\,7)$ је производ два дисјунктна циклуса и његов ред је $\mathrm{NZS}(4,3) = 12$.

33. Испитати да ли у групи $\mathbb{S}_7$ постоји елемент реда 8.

Решење: Претпоставимо да је $\pi \in \mathbb{S}_7$ реда 8. Пермутацију π можемо да представимо у облику производа дисјунктних циклуса:

$$\pi = \sigma_1 \cdots \sigma_k.$$

Тада је

$$\omega(\pi) = \mathrm{NZS}(n_1, \ldots, n_k),$$

где је n_i дужина циклуса σ_i. Тако бисмо добили да су n_i природни бројеви за које важи

$$\mathrm{NZS}(n_1, \ldots, n_k) = 8.$$

Но, 8 је степен простог броја 2 и ово је могуће једино уколико је неки од бројева n_i једнак баш 8. Но, у $\mathbb{S}_7$ не постоји циклус дужине 8, те закључујемо да у $\mathbb{S}_7$ нема елемената реда 8.

34. Одредити елемент максималног реда у групи $\mathbb{S}_9$.

Решење: Као и у претходном задатку, свака пермутација π у $\mathbb{S}_9$ се може представити у облику производа дисјунктних циклуса:

$$\pi = \sigma_1 \cdots \sigma_k.$$

Тада је

$$\omega(\pi) = \mathrm{NZS}(n_1, \ldots, n_k),$$

где је n_i дужина циклуса σ_i. Овде је такође

$$n_1 + \cdots + n_k = 9,$$

уколико у запису узимамо и циклусе дужине 1 (а то је заправо идентична пермутација). Дакле, проблем је следећи: наћи

$$\max \mathrm{NZS}(n_1, \ldots, n_k),$$

при услову

$$n_1 + \cdots + n_k = 9.$$

Наравно, број k се такође може мењати. У случају да је $k = 1$, имамо само један циклус дужине 9 и његов ред је 9.

У случају $k = 2$ имамо више могућности:

$$8 + 1 = 7 + 2 = 6 + 3 = 5 + 4.$$

Наравно, $4 + 5$ нам даје исто што и $5 + 4$. Јасно је да се највећи ред добија баш у том случају — добијамо елемент реда 20.

У случају $k = 3$ имамо још више могућности.

$$7 + 1 + 1 = 6 + 2 + 1 = 5 + 3 + 1 = 5 + 2 + 2 = 4 + 3 + 2 = 3 + 3 + 3.$$

Одговарајући редови елемената су редом: 7, 6, 15, 10, 12.

Случај $k = 4$ даје:

$$6 + 1 + 1 + 1 = 5 + 2 + 1 + 1 = 4 + 2 + 2 + 1 = 4 + 3 + 1 + 1 = 3 + 3 + 2 + 1.$$

Редови елемената су: 6, 10, 4, 12, 6. За $k = 5$ имамо:

$$5 + 1 + 1 + 1 + 1 = 4 + 2 + 1 + 1 + 1 = 3 + 2 + 2 + 1 + 1 = 3 + 3 + 1 + 1 + 1$$

и редове: 5, 4, 6, 3. За $k = 6$ имамо:

$$4 + 1 + 1 + 1 + 1 + 1 = 3 + 2 + 1 + 1 + 1 + 1$$

и редове 4 и 6. За $k = 7$ имамо само случајеве

$$3+1+1+1+1+1+1 = 2+2+1+1+1+1+1$$

и ред елемената 3 и 2. $k = 8$ даје само случај $2+1+1+1+1+1+1+1$ и ред елемента је 2, док за $k = 9$ добијамо само идентичну пермутацију.

Дакле, максималан резултат добијамо уколико имамо производ два дисјунктна циклуса од којих је један дужине 5, а други дужине 4 и максималан ред елемента у $\mathbb{S}_9$ је 20.

35. Нека су H и K подгрупе групе G. Доказати да је HK подгрупа ако и само ако је $HK = KH$.

Решење: $\Longrightarrow$: Дакле, по претпоставци је $HK \leqslant G$. Узмимо било који елемент $hk \in HK$. Тада и $(hk)^{-1} \in HK$, те је $(hk)^{-1} = h_1k_1$ за неки $h_1 \in H$ и неки $k_1 \in K$. Добијамо

$$hk = ((hk)^{-1})^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH,$$

јер су H и K подгрупе од G и садрже инверзе својих елемената. Тако смо добили да је $HK \subseteq KH$. Да бисмо показали обратну инклузију, узмимо ма који елемент $kh \in KH$. Но, $k = ek \in HK$, а и $h = he \in HK$. Дакле, $k, h \in HK$, па, како је $HK \leqslant G$ мора и $kh \in HK$, те смо показали и да је $KH \subseteq HK$.

$\Longleftarrow$: Најпре можемо да констатујемо да $HK \neq \emptyset$, јер је $e = ee \in HK$. Узмимо нека два елемента x и y из HK: $x = h_1k_1$ и $y = h_2k_2$. Треба показати да и $xy^{-1} \in HK$. Но,

$$xy^{-1} = (h_1k_1)(h_2k_2)^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1}) = h_1(k_1k_2^{-1})h_2^{-1}.$$

Како је $K \leqslant G$, а $k_1, k_2 \in K$, то $k_1k_2^{-1} \in K$, а како је $H \leqslant G$, а $h_2 \in H$, то и $h_2^{-1} \in H$. Дакле,

$$(k_1k_2^{-1})h_2^{-1} \in KH.$$

По претпоставци је $KH = HK$, па постоје $h_3 \in H$ и $k_3 \in H$ такви да је

$$(k_1k_2^{-1})h_2^{-1} = h_3k_3.$$

Стога је

$$xy^{-1} = h_1(h_3k_3) = (h_1h_3)k_3.$$

Како је $H \leqslant G$, а $h_1, h_3 \in H$, то $h_1h_3 \in H$. Знамо и да $k_3 \in K$, па је

$$xy^{-1} = (h_1h_3)k_3 \in HK.$$

На основу познатог критеријума закључујемо да је $HK \leqslant G$.

36. Наћи све нормалне подгрупе у групама $\mathbb{D}_4$ и $\mathbb{D}_5$.

Решење: У задатку 8 смо одредили све подгрупе група $\mathbb{D}_4$ и $\mathbb{D}_5$. Сада можемо то искористити да нађемо које су међу њима нормалне подгрупе. Наравно, цела група и тривијална подгрупа $\{\varepsilon\}$ су нормалне подгрупе. Концентрисаћемо се на остале подгрупе.

Посматрајмо најпре групу $\mathbb{D}_4$. Знамо да је свака подгрупа индекса 2 нормална. Стога имамо већ три нормалне подгрупе:

$$\{\varepsilon, \rho^2, \sigma, \sigma\rho^2\}, \{\varepsilon, \rho^2, \sigma\rho, \sigma\rho^3\} \text{ и } \{\varepsilon, \rho, \rho^2, \rho^3\}.$$

Остале су нам подгрупе реда 2. Знамо да је $Z(\mathbb{D}_4) = \{\varepsilon, \rho^2\}$, а центар је увек нормална подгрупа.

Приметимо да, ако је H нормална подгрупа од $\mathbb{D}_4$ и ако је $\sigma\rho^i \in H$, онда у H мора бити и елемент:

$$\sigma(\sigma\rho^i)\sigma^{-1} = \rho^i\sigma = \sigma\rho^{4-i}.$$

Стога је јасно да подгрупе $\{\varepsilon, \sigma\rho\}$ и $\{\varepsilon, \sigma\rho^3\}$ нису нормалне подгрупе. Остале су нам подгрупе $\{\varepsilon, \sigma\}$ и $\{\varepsilon, \sigma\rho^2\}$. Но,

$$\rho\{\varepsilon, \sigma\}\rho^{-1} = \{\varepsilon, \rho\sigma\rho^{-1}\} = \{\varepsilon, \sigma\rho^3\rho^{-1}\} = \{\varepsilon, \sigma\rho^2\}, \quad \rho\{\varepsilon, \sigma\rho^2\}\rho^{-1} = \{\varepsilon, \rho\sigma\rho^2\rho^{-1}\} = \{\varepsilon, \sigma\rho^3\rho\} = \{\varepsilon, \sigma\},$$

те видимо да оне нису нормалне. Дакле, нормалне подгрупе групе $\mathbb{D}_4$ су:

$$\{\varepsilon\}, \quad \mathbb{D}_4, \quad \{\varepsilon, \rho^2\}, \quad \{\varepsilon, \rho^2, \sigma, \sigma\rho^2\}, \quad \{\varepsilon, \rho^2, \sigma\rho, \sigma\rho^3\} \quad \text{и} \quad \{\varepsilon, \rho, \rho^2, \rho^3\}.$$

Што се групе $\mathbb{D}_5$ тиче, нормалне су $\{\varepsilon\}$, $\mathbb{D}_5$ и подгрупа $\{\varepsilon, \rho, \rho^2, \rho^3, \rho^4\}$, која је индекса 2. Релација

$$\rho(\sigma\rho^i)\rho^{-1} = \sigma\rho^{-1}\rho^{i-1} = \sigma\rho^{i-2}$$

нам показује да ниједна подгрупа реда 2 није нормална.

37. Нека је H нормална подгрупа групе G и K нормална подгрупа од H. Примером показати да K не мора бити нормална подгрупа од G.

Решење: Посматрајмо групу $\mathbb{S}_4$ и њене подгрупе $V' = \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$, $H = \{(1), (1\,2)(3\,4)\}$. V' је комутативна група и стога је свака њена подгрупа нормална, те је $H \triangleleft V'$. Осим тога, како је

$$\pi(a\,b)(c\,d)\pi^{-1} = (\pi(a\,b)\pi^{-1})(\pi(c\,d)\pi^{-1}) = (\pi(a)\,\pi(b))(\pi(c)\,\pi(d))$$

за сваку пермутацију $\pi \in \mathbb{S}_4$, закључујемо да је $V' \triangleleft \mathbb{S}_4$. Но, јасно је да H није нормална подгрупа од $\mathbb{S}_4$:

$$(1\,3)((1\,2)(3\,4))(1\,3)^{-1} = (3\,2)(1\,4) \notin H.$$

38. Нека су H и K нормалне подгрупе групе G и нека је $H \cap K = \{e\}$. Доказати: $(\forall x \in H)(\forall y \in K)xy = yx$.

Решење: Нека је $x \in H$ и $y \in K$. Знамо да је $xy = yx$ акко је $xyx^{-1}y^{-1} = e$. Покажимо да је ово тачно. Како је K нормална подгрупа и $y \in K$, закључујемо да је и $xyx^{-1} \in K$, те је и $xyx^{-1}y^{-1} \in K$. Слично, како је $x \in H$, а H нормална подгрупа, $yxy^{-1} \in H$, те $xyx^{-1}y^{-1} \in H$. Према томе, $xyx^{-1}y^{-1} \in H \cap K = \{e\}$, те је $xyx^{-1}y^{-1} = e$.

39. Ако је H ЦИКЛИЧНА нормална подгрупа групе G, доказати да је свака подгрупа од H такође нормална подгрупа групе G.

Решење: Нека је $H = \langle a \rangle$. Нека је $K \leqslant H$. Знамо да мора бити $K = \langle a^r \rangle$ за неко $r \geqslant 1$. Треба показати да је K нормална подгрупа од G. У ту сврху, нека је $g \in G$. С обзиром да је $H \triangleleft G$, мора бити $gag^{-1} = a^t$ за неко $t \in \mathbb{Z}$. Уколико је x произвољан елемент из K, онда је $x = (a^r)^s = a^{rs}$ за неко $s \in \mathbb{Z}$, па је

$$gxg^{-1} = ga^{rs}g^{-1} = (gag^{-1})^{rs} = (a^t)^{rs} = a^{trs} = (a^r)^{ts} \in K.$$

Дакле, $K \triangleleft G$.

40. Доказати да је сваки елемент количничке групе $\mathbb{Q}/\mathbb{Z}$ коначног реда, док у количничкој групи $\mathbb{R}/\mathbb{Q}$ ниједан елемент (сем неутрала) нема коначан ред.

Решење: Елемент из $\mathbb{Q}/\mathbb{Z}$ је облика $\frac{m}{n} + \mathbb{Z}$, за неко $m \in \mathbb{Z}$ и неки природан број $n \geqslant 1$. Но, тада је

$$n\left(\frac{m}{n} + \mathbb{Z}\right) = \left(n\frac{m}{n} + \mathbb{Z}\right) = m + \mathbb{Z} = \mathbb{Z} = 0_{\mathbb{Q}/\mathbb{Z}},$$

те је $\frac{m}{n} + \mathbb{Z}$ коначног реда.

Уколико је $r + \mathbb{Q} \neq 0_{\mathbb{R}/\mathbb{Q}}$, тј. уколико је $r \in \mathbb{R} \setminus \mathbb{Q}$, онда је, за свако $n \geqslant 1$:

$$n\,(r + \mathbb{Q}) \neq 0_{\mathbb{R}/\mathbb{Q}}.$$

Наиме, уколико је

$$n\,(r + \mathbb{Q}) = nr + \mathbb{Q} = 0_{\mathbb{R}/\mathbb{Q}} = \mathbb{Q},$$

то би значило да је $nr \in \mathbb{Q}$, па бисмо добили да и $r \in \mathbb{Q}$, што није тачно.

41. Нека је A нормална подгрупа групе G и B нормална подгрупа групе H. Доказати да је $A \times B$ нормална подгрупа групе $G \times H$, као и да је $(G \times H)/(A \times B) \cong (G/A) \times (H/B)$.

Решење: У задатку 26 смо показали да је $A \times B \leqslant G \times H$. Докажимо да је та подгрупа нормална. У ту сврху, нека је $(a, b) \in A \times B$ и $(g, h) \in G \times H$. Тада је

$$(g, h)(a, b)(g, h)^{-1} = (ga, hb)(g^{-1}, h^{-1}) = (gag^{-1}, hbh^{-1}).$$

С обзиром да је $A \triangleleft G$ и $B \triangleleft H$, добијамо да $gag^{-1} \in A$, $hbh^{-1} \in B$, те заиста $(gag^{-1}, hbh^{-1}) \in A \times B$.

Покажимо да је пресликавање

$$\phi\colon (G \times H)/(A \times B) \to (G/A) \times (H/B)$$

задато са:

$$\phi\left((g, h)(A \times B)\right) : = (gA, hB)$$

изоморфизам група. Проверимо да је оно добро дефинисано. Дакле, нека је $(g, h)(A \times B) = (g_1, h_1)(A \times B)$. Треба показати да је $(gA, hB) = (g_1A, h_1B)$. Из $(g, h)(A \times B) = (g_1, h_1)(A \times B)$ следи да је $(g, h)^{-1}(g_1, h_1) \in A \times B$, па је $(g^{-1}g_1, h^{-1}h_1) \in A \times B$ и добијамо да је $g^{-1}g_1 \in A$ и $h^{-1}h_1 \in B$. Стога је $gA = g_1A$ и $hB = h_1B$, те је и $(gA, hB) = (g_1A, h_1B)$.

Доказ да је пресликавање ϕ '1–1' изводи се слично. Нека је $\phi((g, h)(A \times B)) = \phi((g_1, h_1)(A \times B)$. То значи да је $(gA, hB) = (g_1A, h_1B)$, те је $gA = g_1A$ и $hB = h_1B$. Добијамо да је $g^{-1}g_1 \in A$ и $h^{-1}h_1 \in B$, те је $(g, h)^{-1}(g_1, h_1) = (g^{-1}g_1, h^{-1}h_1) \in A \times B$ и следи да је $(g, h)(A \times B) = (g_1, h_1)(A \times B)$.

Јасно је да је пресликавање ϕ 'на'. Покажимо још да се слаже са операцијама.

$$\phi((g, h)(A \times B)(g_1, h_1)(A \times B)) = \phi((gg_1, hh_1)(A \times B)) = ((gg_1)A, (hh_1)B) = ((gA)(g_1A), (hB)(h_1B))$$

$$= (gA, hB)(g_1A, h_1B) = \phi((g, h)(A \times B))\phi((g_1, h_1)(A \times B)).$$

Дакле, ϕ је изоморфизам те је $(G \times H)/(A \times B) \cong (G/A) \times (H/B)$.

42. Доказати да је $f : G \to H$ хомоморфизам ако и само ако је $\{(x, f(x)) : x \in G\}$ подгрупа од $G \times H$.

Решење: Нека је $\Gamma(f) = \{(x, f(x)) : x \in G\}$.

$\Longrightarrow$: Како је $f(e) = \varepsilon$, где је са ε означен неутрал у H имамо да $(e, \varepsilon) \in \Gamma(f)$, па $\Gamma(f) \neq \emptyset$. Претпоставимо да $(g, f(g)), (g_1, f(g_1)) \in \Gamma(f)$. Како је f хомоморфизам:

$$(g, f(g))^{-1}(g_1, f(g_1)) = (g^{-1}, f(g)^{-1})(g_1, f(g_1)) = (g^{-1}, f(g^{-1}))(g_1, f(g_1))$$

$$= (g^{-1}g_1, f(g^{-1})f(g_1)) = (g^{-1}g_1, f(g^{-1}g_1)) \in \Gamma(f).$$

$\Longleftarrow$: Нека су $g, g_1 \in G$. Треба показати да је $f(gg_1) = f(g)f(g_1)$. Како $(g, f(g)), (g_1, f(g_1)) \in \Gamma(f)$ и како је $\Gamma(f) \leqslant G \times H$, добијамо да $(g, f(g))(g_1, f(g_1)) \in \Gamma(f)$, тј. $(gg_1, f(g)f(g_1)) \in \Gamma(f)$. Но, по дефиницији $\Gamma(f)$ мора тада бити $f(g)f(g_1) = f(gg_1)$.

43. Означимо са $f_{a,b} : \mathbb{R} \to \mathbb{R}$, где је $a \in \mathbb{R} \setminus \{0\}$, $b \in \mathbb{R}$ функције задате са $f_{a,b}(x) = ax + b$. Нека је $G = \{f_{a,b} : a \in \mathbb{R} \setminus \{0\}, b \in \mathbb{R}\}$ и $H = \{f_{1,b} : b \in \mathbb{R}\}$. Показати да је G група у односу на композицију функција, да је H нормална подгрупа групе G, као и да је $G/H \cong (\mathbb{R} \setminus \{0\}, \cdot)$.

Решење: Најпре, $f_{1,0}(x) = x$, те можемо закључити да $\mathrm{id}_{\mathbb{R}} \in G$. Нека $f_{a,b}, f_{a_1,b_1} \in G$. Тада је

$$(f_{a,b} \circ f_{a_1,b_1})(x) = f_{a,b}(f_{a_1,b_1}(x)) = f_{a,b}(a_1x + b_1) = a(a_1x + b_1) + b = aa_1x + ab_1 + b = f_{aa_1,ab_1+b}.$$

Како из $a \neq 0$ и $a_1 \neq 0$ следи да $aa_1 \neq 0$, добијамо да је $f_{aa_1,ab_1+b} \in G$ и закључујемо да је скуп G затворен у односу на композицију пресликавања. С обзиром да је композиција пресликавања асоцијативна, потребно је још само да докажемо да је инверз сваког елемента у G такође у G.

Но, ако је f_{a_1,b_1} инверз од $f_{a,b}$, онда је

$$f_{a,b} \circ f_{a_1,b_1} = \mathrm{id}_{\mathbb{R}},$$

те је

$$f_{aa_1,ab_1+b} = f_{1,0},$$

тј. $aa_1 = 1$, $ab_1 + b = 0$. Добијамо да је $f_{1/a,-b/a}$ инверз од $f_{a,b}$, а $f_{1/a,-b/a} \in G$ те је G заиста група.

Нека је $f_{1,b} \in H$ и $f_{a_1,b_1} \in G$. Тада је

$$f_{a_1,b_1} \circ f_{1,b} \circ f_{a_1,b_1}^{-1} = f_{a_1,a_1b+b_1} \circ f_{1/a_1,-b_1/a_1} = f_{a_1 \frac{1}{a_1}, a_1(-\frac{b_1}{a_1})+a_1b+b_1} = f_{1,a_1b} \in H.$$

Да бисмо показали да је $G/H \cong (\mathbb{R} \setminus \{0\}, \cdot)$ посматрајмо пресликавање $\phi\colon G \to \mathbb{R} \setminus \{0\}$ задато са:

$$\phi(f_{a,b}) = a.$$

Ово пресликавање је хомоморфизам групе G у групу $(\mathbb{R} \setminus \{0\}, \cdot)$:

$$\phi(f_{a,b} \circ f_{a_1,b_1}) = \phi(f_{aa_1,ab_1+b}) = aa_1 = \phi(f_{a,b})\phi(f_{a_1,b_1}).$$

Јасно је да је ϕ 'на' — ако је $a \neq 0$, онда $f_{a,0} \in G$ и $\phi(f_{a,0}) = a$. Одредимо језгро хомоморфизма ϕ:

$$f_{a,b} \in \mathrm{Ker}(\phi) \text{ акко } \phi(f_{a,b}) = 1 \text{ акко } a = 1.$$

Дакле, $\mathrm{Ker}(\phi) = \{f_{a,b} \in G : a = 1\} = H$. На основу прве теореме о изоморфизму за групе закључујемо да је $G/H \cong (\mathbb{R} \setminus \{0\}, \cdot)$.

44. Нека је G подгрупа групе $\mathbb{S}_8$ генерисана елементима $(1\,2\,3)(4\,5)$ и $(7\,8)$. Нека G дејствује као група пермутација скупа $X = \{1, 2, \ldots, 8\}$. Одредити орбиту и стабилизатор сваког елемента из X.

Решење: Нека је $\pi = (1\,2\,3)(4\,5)$ и $\sigma = (7\,8)$. Како је $\pi\sigma = \sigma\pi$, а $\omega(\pi) = \mathrm{NZS}(3, 2) = 6$ и $\omega(\sigma) = 2$, то је

$$G = \{\mathrm{id}, \pi, \pi^2, \pi^3, \pi^4, \pi^5, \sigma, \sigma\pi, \sigma\pi^2, \sigma\pi^3, \sigma\pi^4, \sigma\pi^5\}.$$

Стога је орбита елемента k:

$$\Omega(k) = \{\mathrm{id}(k), \pi(k), \pi^2(k), \pi^3(k), \pi^4(k), \pi^5(k), \sigma(k), (\sigma\pi)(k), (\sigma\pi^2)(k), (\sigma\pi^3)(k), (\sigma\pi^4)(k), (\sigma\pi^5)(k)\}.$$

Овде смо са id, а не са (1) означили идентичну пермутацију. Делује компликовано, али није тешко одредити ове орбите. Приметимо да елементе 1, 2 и 3 пермутује једино пермутација цикл $(1\,2\,3)$ и добијамо да је

$$\Omega(1) = \Omega(2) = \Omega(3) = \{1, 2, 3\}.$$

Слично елементе 4 и 5 пермутује једино цикл $(4\,5)$ и

$$\Omega(4) = \Omega(5) = \{4, 5\}.$$

Лако добијамо и

$$\Omega(7) = \Omega(8) = \{7, 8\}.$$

Док елемент 6 фиксирају и π и σ, па је $\Omega(6) = \{6\}$. Приметимо да заправо ове орбите одговарају дисјунктним циклусима који се појављују овде.

Одредимо сада стабилизаторе елемената из $\{1, 2, \ldots, 8\}$. Кренимо од елемента 1. Приметимо да је $\sigma(1) = 1$ и да је

$$(\sigma\pi^k)(1) = 1 \text{ акко } (\sigma\sigma\pi^k)(1) = \sigma(1) \text{ акко } \pi^k(1) = 1.$$

Дакле, $\sigma \in \Sigma_1$ и треба још проверити који степени од π не померају 1. Но, јасно је да је то само $\pi^3 = (4\,5)$. Дакле, Σ_x је подгрупа од G генерисана елементима σ и π^3, тј.

$$\Sigma_x = \{\mathrm{id}, (4\,5), (7\,8), (4\,5)(7\,8)\}.$$

Подсетимо се да мора важити једнакост $|\Omega(1)| = [G : \Sigma_1]$. И заиста,

$$|\Omega(1)| = 3, \quad [G : \Sigma_1] = \frac{|G|}{|\Sigma_1|} = \frac{12}{4} = 3.$$

Знамо из теорије да су стабилизатори елемената из исте орбите конјуговане подгрупе. Но, група G је комутативна и стога су сваке две конјуговане подгрупе заправо једнаке. Стога је

$$\Sigma_2 = \Sigma_3 = \Sigma_1 = \{\mathrm{id}, (4\,5), (7\,8), (4\,5)(7\,8)\}.$$

Дакле, знамо и да је $\Sigma_4 = \Sigma_5$. Одредимо ову подгрупу. Као и у претходном случају σ јесте у Σ_4, само треба проверити који степени од π припадају Σ_4. Како је $\pi^k = (1\,2\,3)^k(4\,5)^k$ и да би $\pi^k(4) = 4$ потребно је, а и довољно да је $(4\,5)^k = \mathrm{id}$. Дакле, то су парни степени од π и добијамо да је

$$\Sigma_4 = \Sigma_5 = \{\mathrm{id}, \pi^2, \pi^4, \sigma, \sigma\pi^2, \sigma\pi^4\}.$$

Приметимо да је

$$|\Omega(4)| = 2 = \frac{12}{6} = \frac{|G|}{|\Sigma_4|} = [G : \Sigma_4].$$

Знамо да је $\Sigma_7 = \Sigma_8$. Приметимо да је $\pi \in \Sigma_7$, но да $\sigma \notin \Sigma_7$. Заправо је јасно да је Σ_7 подгрупа генерисана са π, тј.

$$\Sigma_7 = \Sigma_8 = \{\mathrm{id}, \pi, \pi^2, \pi^3, \pi^4, \pi^5\}.$$

Имамо и

$$|\Omega(7)| = 2 = \frac{12}{6} = \frac{|G|}{|\Sigma_7|} = [G : \Sigma_7].$$

На крају, видимо да сваки елемент из G фиксира 6, те је $\Sigma_6 = G$ и

$$|\Omega(6)| = 1 = \frac{12}{12} = \frac{G}{|\Sigma_6|} = [G : \Sigma_6].$$

45. Нека је G група и $x \in G$. Показати да подскуп $C(x) = \{g \in G : xg = gx\}$ чини подгрупу групе G (ова подгрупа се назива централизатор елемента x). Одредити везу те подгрупе и броја елемената у класи конјугованости елемента x. Показати да уколико у G постоји класа конјугованости са тачно два елемента, група G не може бити проста.

Решење: Приметимо да $e \in C(x)$, за свако $x \in G$, те је $C(x) \neq \emptyset$ за све $x \in G$.

Нека је $x \in G$ и нека су $g, h \in C(x)$. Како $h \in C(x)$, то је $xh = hx$. Множењем слева са h^{-1} и здесна са h добијамо да је $h^{-1}x = xh^{-1}$. Тада је

$$x(gh^{-1}) = (xg)h^{-1} = (gx)h^{-1} = g(xh^{-1}) = g(h^{-1}x) = (gh^{-1})x.$$

Закључујемо да $gh^{-1} \in C(x)$, те је заиста $C(x) \leqslant G$.

Група G делује на скупу G на следећи начин:

$$g \bullet x \colon = gxg^{-1}.$$

При том дејству је $\Omega(x) = \{gxg^{-1} : g \in G\}$, те је орбита заправо класа конјугованости елемента x, док је

$$\Sigma_x = \{g \in G : g \bullet x = x\} = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} = C(x).$$

Дакле, на основу везе између броја елемената у орбити и реда стабилизатора добијамо да је број елемената у класи конјугованости елемента x једнак индексу подгрупе $C(x)$ у групи G.

Претпоставимо да постоји класа конјугованости са тачно два елемента. Нека је то класа конјугованости елемента x. Према управо показаном добијамо да је $[G : C(x)] = 2$, а знамо да је свака подгрупа индекса 2 нормална и стога група G није проста.

46. Нека група G дејствује на скуповима X и Y. Показати да је са $g \cdot (x, y) := (g \cdot x, g \cdot y)$ дефинисано једно дејство групе G на скупу $X \times Y$ (ово дејство се назива ДИЈАГОНАЛНО ДЕЈСТВО). Одредити везу између стабилизатора елемената x, y и (x, y).

Решење: Најпре је $e \cdot (x, y) = (e \cdot x, e \cdot y) = (x, y)$. Нека $g, h \in G$. Тада:

$$(gh) \cdot (x, y) = ((gh) \cdot x, (gh) \cdot y) = (g \cdot (h \cdot x), g \cdot (h \cdot y)) = g \cdot (h \cdot x, h \cdot y) = g \cdot (h \cdot (x, y)).$$

Докажимо да је $\Sigma_{(x,y)} = \Sigma_x \cap \Sigma_y$.

$\subseteq$: Нека је $g \in \Sigma_{(x,y)}$. То значи да је $g \cdot (x,y) = (x,y)$. Но, како је $g \cdot (x,y) = (g \cdot x, g \cdot y)$ добијамо да је $(g \cdot x, g \cdot y) = (x,y)$, те је $g \cdot x = x$ и $g \cdot y = y$, тј. $g \in \Sigma_x \cap \Sigma_y$.

$\supseteq$: Нека $g \in \Sigma_x \cap \Sigma_y$. То значи да је $g \cdot x = x$ и $g \cdot y = y$. Но, тада је $g \cdot (x,y) = (g \cdot x, g \cdot y) = (x,y)$, те закључујемо да $g \in \Sigma_{(x,y)}$.

47. Нека је $X = \{1,2,3,4\}$ и G подгрупа од $\mathbb{S}_4$ генерисана елементима $(1\,2\,3\,4)$ и $(2\,4)$. Одредити орбите и стабилизаторе за дијагонално дејство G на $X \times X$.

Решење: Из задатка 22 знамо да је подгрупа G изоморфна групи $\mathbb{D}_4$ и да је, ако је $\pi = (1\,2\,3\,4)$ и $\sigma = (2\,4)$, $G = \{\mathrm{id}, \pi, \pi^2, \pi^3, \sigma, \sigma\pi, \sigma\pi^2, \sigma\pi^3\}$.

Знамо да је $|X \times X| = 16$. Одредимо најпре орбиту елемента $(1,1)$. Како је $\pi \cdot (1,1) = (2,2), \pi^2 \cdot (1,1) = (3,3), \pi^3 \cdot (1,1) = (4,4)$ то је $\{(1,1),(2,2),(3,3),(4,4)\} \subseteq \Omega((1,1))$. Но, јасно је да $(x,y) \notin \Omega((1,1))$ ако је $x \neq y$. Дакле, $\Omega((1,1)) = \{(1,1),(2,2),(3,3),(4,4)\}$.

Да бисмо наставили даље, корисно је да одредимо стабилизаторе елемената из X при дејству G на X. То није тешко урадити (подсетити се задатка 44). Добијамо:

$$\Sigma_1 = \Sigma_3 = \langle \sigma \rangle, \quad \Sigma_2 = \Sigma_4 = \langle \sigma\pi^2 \rangle.$$

Одредимо сада орбиту елемента $(1,2)$. Како је $\Sigma_1 \cap \Sigma_2 = \{\mathrm{id}\}$, то је

$$|\Omega((1,2))| = [G : \Sigma_{(1,2)}] = [G : \Sigma_1 \cap \Sigma_2] = 8.$$

Дакле, у овој орбити имамо 8 елемената, тачно колико имамо и у подгрупи G, јер је стабилизатор тривијална група и различити елементи групе дају различите елементе у орбити. Директном провером добијамо

$$\pi \cdot (1,2) = (2,3), \quad \pi^2 \cdot (1,2) = (3,4), \quad \pi^3 \cdot (1,2) = (4,1).$$

Користећи ово добијамо

$$(\sigma\pi) \cdot (1,2) = (4,3), \quad (\sigma\pi^2) \cdot (1,2) = (3,2), \quad (\sigma\pi^3) \cdot (1,2) = (2,1).$$

У орбити су наравно и елементи $(1,2)$ и $(1,4) = \sigma \cdot (1,2)$. Коначно

$$\Omega((1,2)) = \{(1,2),(1,4),(2,3),(3,4),(4,1),(4,3),(3,2),(2,1)\}.$$

Одредимо сада орбиту елемента $(1,3)$. Приметимо да је

$$|\Omega((1,3))| = [G : \Sigma_{(1,3)}] = [G : \Sigma_1 \cap \Sigma_3] = [G : \langle \sigma \rangle] = 8/2 = 4.$$

С обзиром да је $|X \times X| = 16$ и $|\Omega((1,1))| + |\Omega((1,2))| = 4 + 8 = 12$, то добијамо да се у $\Omega(1,3)$ налазе сви преостали елементи, те мора бити $\Omega((1,3)) = \{(1,3),(2,4),(4,2),(3,1)\}$.

48. Нека је p прост број. Показати да скуп матрица

$$G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a,b,c \in \mathbb{Z}_p \right\}$$

чини некомутативну групу реда p^3 у односу на множење матрица.

Решење: Приметимо да је детерминанта сваке матрице из G једнака 1, те су све оне инвертибилне. Осим тога, јединична матрица је у G (њу добијамо за $a = b = c = 0$). Знамо да је множење матрица асоцијативно. Само треба проверити да ли је производ две матрице из G такође у G и да је инверз сваке матрице из G у G. Није тешко показати да је производ две матрице из G такође у G:

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a_1 + a & b_1 + ac_1 + b \\ 0 & 1 & c_1 + c \\ 0 & 0 & 1 \end{bmatrix}$$

За налажење инверза матрице

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

решимо систем једначина

$$\begin{aligned} a_1 + a &= 0 \\ b_1 + ac_1 + b &= 0 \\ c_1 + c &= 0. \end{aligned}$$

Но, то није тешко. Добијамо да је $a_1 = -a$, $c_1 = -c$, $b_1 = ac - b$. Дакле,

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} \in G.$$

Ова група није комутативна, на пример:

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

49. Рођенданска торта је подељена на 8 једнаких парчића. На колико различитих начина се могу поређати црвене и плаве свећице које се постављају у центар сваког парчета (тако да добијемо истински различито украшене торте).

Решење: Замислимо да смо означили парчиће торте бројевима од 1 до 8. Ако са X означимо такву 'означену' торту, узимајући у обзир да се на сваком парчету може поставити црвена или плава свећица, број могућих украшавања тако означене торте је 2^8. Но, јасно је да то није оно што се тражи — ротацијом торте се добија иста торта. Зато ми посматрамо дејство цикличне групе G реда 8 чији је генератор ротација ρ за угао $\frac{360^\circ}{8}$. Можемо је видети и као подгрупу ротација групе $\mathbb{D}_8$ (али не користимо и рефлекције, јер торту не можемо да преврћемо!).

Дакле, треба одредити број орбита при овом дејству. Ако са X/G означимо скуп свих орбита, онда је

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$

где је са X^g означен скуп свих фиксних тачака од g при дејству на скуп X. Знамо да је $|X^g| = |X^h|$, ако су g и h конјуговани и то понекад скраћује рачун, но овде нам то не помаже пошто је група G циклична, те је комутативна и два различита елемента никада нису конјугована. Дакле, у нашем случају је

$$|X/G| = \frac{1}{8}\left(|X^\varepsilon| + |X^\rho| + |X^{\rho^2}| + |X^{\rho^3}| + |X^{\rho^4}| + |X^{\rho^5}| + |X^{\rho^6}| + |X^{\rho^7}|\right).$$

Знамо да је $|X^\varepsilon| = |X| = 2^8$. Колико је $|X^\rho|$? Ако је на једно парче постављена црвена свећица, да би тако означена торта била фиксирана при дејству ротације ρ и на све остале парчиће мора бити постављена црвена свећица. Исто и ако је постављена плава свећица. Дакле, имамо само две могућности — све су црвене свећице или су све плаве свећице, тј. $|X^\rho| = 2$. Но, исто добијамо ако посматрамо $|X^{\rho^3}|$, $|X^{\rho^5}|$ и $|X^{\rho^7}|$. Наиме сви непарни степени од ρ генеришу целу групу. Погледајмо шта се дешава у случају ρ^3. Ако је на парчету 1 постављена црвена свећица, онда црвена свећица мора бити и на парчету 4 и на парчету 7 и на парчету 10... Пардон, не постоји парче 10, то је заправо парче 2. Па онда и на парчету 5 и на парчету 8 и на парчету 3 и на парчету 6. Дакле, на свим. Слично је и за ρ^5 и ρ^7. Добијамо да је $|X^{\rho^3}| = |X^{\rho^5}| = |X^{\rho^7}| = 2$.

За елемент ρ^2 имамо већи скуп фиксних тачака. Наиме, исте боје морају бити свећице на парчићима 1, 3, 5, 7, као и парчићима 2, 4, 6, 8, али не мора постојати веза између боје свећице на парчету 1 и парчету 2. Дакле, овде је $|X^{\rho^2}| = 2 \cdot 2 = 4$. Није тешко уверити се (слична анализа као за непарне степене ρ) да је и $|X^{\rho^6}| = 4$. У случају ρ^4 имамо 4 групе парчића које бојимо независно, те је $|X^{\rho^4}| = 2^4$. Коначно, број украшавања је:

$$\frac{1}{8}(2^8 + 2 + 4 + 2 + 16 + 2 + 4 + 2) = \frac{288}{8} = 36.$$

50. Одредити колико различито обојених правилних тетраедара има уколико бојимо сваку ивицу тог тетраедра са једном од 4 могуће боје.

Решење: Поступићемо слично примеру из скрипти. Овде ће за нас X бити скуп свих могућих означених тетраедара чије су ивице обојене са једном од 4 боје. Како имамо 6 ивица и 4 боје, то је $|X| = 4^6 = 4096$. Користићемо исту формулу као у скриптама и тражени број ће бити једнак:

$$\frac{1}{12}\left(|X^{(1\,2\,3)}|\cdot 4 + |X^{(1\,3\,2)}|\cdot 4 + |X^{(1\,2)(3\,4)}|\cdot 3 + |X^{(1)}|\cdot 1\right)$$

(подсетите се примера). За одређивање $|X^{(1\,2\,3)}|$ можемо да констатујемо да све ивице у основи тетраедра морају бити обојене истом бојом, као и да све ивице које спајају теме 4 са осталим теменима морају бити обојене истом бојом (која може бити и различита од боје којом смо бојили ивице у основи). Дакле, $|X^{(1\,2\,3)}| = 4\cdot 4 = 16$. На исти начин добијамо да је и $|X^{(1\,3\,2)}| = 4\cdot 4 = 16$.

За одређивање $|X^{(1\,2)(3\,4)}|$ приметимо да ивица $[1,2]$, као и ивица $[3,4]$ може бити обојена ма којом бојом, док ивице $[1,4]$ и $[2,3]$ морају бити обојене истом бојом, као и ивице $[1,3]$ и $[2,4]$. Дакле,

$$|X^{(1\,2)(3\,4)}| = \underbrace{4}_{\text{ивица }[1,2]} \cdot \underbrace{4}_{\text{ивица }[3,4]} \cdot \underbrace{4}_{\text{ивице }[1,4]\text{ и }[2,3]} \cdot \underbrace{4}_{\text{ивице }[1,3]\text{ и }[2,4]} = 256.$$

Наравно, $|X^{(1)}| = |X| = 4096$. Дакле, укупан број различито обојених тетраедара је:

$$\frac{1}{12}\left(16\cdot 4 + 16\cdot 4 + 256\cdot 3 + 4096\right) = \frac{1}{12}4992 = 416.$$

51. Одредити нормалну форму за Абелове групе задате генераторима x_1, x_2, x_3, x_4 и релацијама

(а)

$$\begin{aligned} 9x_1 + 6x_2 + 5x_3 + 4x_4 &= 0\\ 6x_1 + 5x_2 - 3x_3 + 11x_4 &= 0\\ 3x_1 + 2x_2 - x_3 + 4x_4 &= 0; \end{aligned}$$

(б)

$$\begin{aligned} 4x_1 + 2x_2 + 3x_3 + 7x_4 &= 0\\ 5x_1 + x_2 - x_3 + 12x_4 &= 0\\ 2x_1 + 4x_2 + 11x_3 - 3x_4 &= 0; \end{aligned}$$

(в)

$$\begin{aligned} 7x_1 - x_2 - x_3 + 2x_4 &= 0\\ 9x_1 + 3x_2 - 3x_3 &= 0\\ 2x_1 + 4x_2 - 2x_4 &= 0; \end{aligned}$$

(г)

$$\begin{aligned} 5x_1 + 3x_2 - 3x_4 &= 0\\ 2x_1 + 4x_2 - 2x_3 &= 0\\ 7x_1 + 7x_2 - 2x_3 - 3x_4 &= 0. \end{aligned}$$

Решење: (а) Формирајмо матрицу:

$$A = \begin{bmatrix} 9 & 6 & 5 & 4\\ 6 & 5 & -3 & 11\\ 3 & 2 & -1 & 4 \end{bmatrix}.$$

Најпре ћемо -1 да 'доведемо' на позицију $(1,1)$. Заменом прве и треће врсте добијамо еквивалентну матрицу:

$$A_1 = \begin{bmatrix} 3 & 2 & -1 & 4 \\ 6 & 5 & -3 & 11 \\ 9 & 6 & 5 & 4 \end{bmatrix}.$$

Сада заменом прве и треће колоне добијамо еквивалентну матрицу:

$$A_2 = \begin{bmatrix} -1 & 2 & 3 & 4 \\ -3 & 5 & 6 & 11 \\ 5 & 6 & 9 & 4 \end{bmatrix}.$$

Другој врсти додајемо прву помножену са -3, а трећој врсти додајемо прву врсту помножену са 5. Тако добијамо еквивалентну матрицу:

$$A_3 = \begin{bmatrix} -1 & 2 & 3 & 4 \\ 0 & -1 & -3 & -1 \\ 0 & 16 & 24 & 24 \end{bmatrix}.$$

Другој колони додајемо прву колону помножену са 2, трећој колони додајемо прву колону помножену са 3 и четвртој колони додајемо прву колону помножену са 4. Добијамо еквивалентну матрицу:

$$A_4 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & -3 & -1 \\ 0 & 16 & 24 & 24 \end{bmatrix}.$$

Трећој врсти додајемо другу помножену са 16:

$$A_5 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & -3 & -1 \\ 0 & 0 & -24 & 8 \end{bmatrix}.$$

Трећој колони додајемо другу колону помножену са -3 и четвртој колони додајемо другу колону помножену са -1:

$$A_6 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -24 & 8 \end{bmatrix}.$$

Како $8 \mid (-24)$ видимо да смо при крају. Најпре заменимо трећу и четврту колону:

$$A_7 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 8 & -24 \end{bmatrix}.$$

Потом додајемо четвртој колони трећу колону помножену са 3:

$$A_8 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 8 & 0 \end{bmatrix}.$$

Коначно, помножимо и прву и другу врту са -1:

$$A_9 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 8 & 0 \end{bmatrix}.$$

Уколико су y_1, y_2, y_3, y_4 нови генератори видимо да међу њима важе релације:

$$\begin{aligned} y_1 &= 0 \\ y_2 &= 0 \\ 8y_3 &= 0. \end{aligned}$$

Дакле, $y_1 = y_2 = 0$, y_3 генерише цикличну подгрупу реда 8, а y_4 генерише бесконачну цикличну подгрупу. Нормална форма за нашу групу је $\mathbb{Z}_8 \times \mathbb{Z}$.

(б) Формирајмо матрицу:

$$B = \begin{bmatrix} 4 & 2 & 3 & 7 \\ 5 & 1 & -1 & 12 \\ 2 & 4 & 11 & -3 \end{bmatrix}.$$

Доведимо најпре 1 на позицију $(1,1)$. Најпре заменимо прву и другу врсту и добијемо еквивалентну матрицу:

$$B_1 = \begin{bmatrix} 5 & 1 & -1 & 12 \\ 4 & 2 & 3 & 7 \\ 2 & 4 & 11 & -3 \end{bmatrix},$$

а затим заменимо прву и другу колону:

$$B_2 = \begin{bmatrix} 1 & 5 & -1 & 12 \\ 2 & 4 & 3 & 7 \\ 4 & 2 & 11 & -3 \end{bmatrix}.$$

Другој врсти додајемо прву врсту помножену са -2, а трећој врсти додајемо прву врсту помножену са -4. Добијамо еквивалентну матрицу:

$$B_3 = \begin{bmatrix} 1 & 5 & -1 & 12 \\ 0 & -6 & 5 & -17 \\ 0 & -18 & 15 & -51 \end{bmatrix}.$$

Сада додајмо другој колони прву колону помножену са -5, трећој колони прву колону и четвртој колони прву колону помножену са -12:

$$B_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -6 & 5 & -17 \\ 0 & -18 & 15 & -51 \end{bmatrix}.$$

Приметимо да је највећи заједнички делилац елемената који се налазе у подматрици формата 2×3 коју формирају елементи на позицијама (i,j) за $2 \leqslant i \leqslant 3$, $2 \leqslant j \leqslant 4$ једнак 1. Додајмо другој колони трећу колону:

$$B_5 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 5 & -17 \\ 0 & -3 & 15 & -51 \end{bmatrix}.$$

Нисмо баш добили 1, али је и -1 довољно добро ☺. Сада додајмо трећој врсти другу врсту помножену са -3:

$$B_6 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 5 & -17 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Занимљиво, добили смо нула врсту. То нам смањује даљи рад. Сада додајмо трећој колони другу колону помножену са 5 и четвртој колони другу колону помножену са -17:

$$B_7 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

На крају, помножимо другу врсту са -1:

$$B_8 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Ако су y_1, y_2, y_3, y_4 нови генератори видимо да међу њима важе релације

$$y_1 = 0$$
$$y_2 = 0$$

Дакле, $y_1 = y_2 = 0$, док су y_3 и y_4 слободни генератори. Стога је нормална форма за нашу групу: $\mathbb{Z} \times \mathbb{Z}$.

(в) Формирајмо матрицу (обратите пажњу на то који су коефицијенти једнаки нули):

$$C = \begin{bmatrix} 7 & -1 & -1 & 2 \\ 9 & 3 & -3 & 0 \\ 2 & 4 & 0 & -2 \end{bmatrix}.$$

Заменимо прве две колоне:

$$C_1 = \begin{bmatrix} -1 & 7 & -1 & 2 \\ 3 & 9 & -3 & 0 \\ 4 & 2 & 0 & -2 \end{bmatrix}.$$

Другој врсти додајмо прву врсту помножену са 3, а трећој врсти додајмо прву врсту помножену са 4:

$$C_2 = \begin{bmatrix} -1 & 7 & -1 & 2 \\ 0 & 30 & -6 & 6 \\ 0 & 30 & -4 & 6 \end{bmatrix}.$$

Другој колони додајмо прву колону помножену са 7, трећој колони додајмо прву колону помножену са -1 и четвртој колони додајмно прву колону помножену са 2:

$$C_3 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 30 & -6 & 6 \\ 0 & 30 & -4 & 6 \end{bmatrix}.$$

Другој врсти додајмо трећу помножену са -1:

$$C_4 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 30 & -6 & 6 \end{bmatrix}.$$

Заменимо другу и трећу колону:

$$C_5 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & -6 & 30 & 6 \end{bmatrix}.$$

Трећој врсти додајмо другу врсту помножену са -3:

$$C_6 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 30 & 6 \end{bmatrix}.$$

Заменимо трећу и четврту колону:

$$C_7 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 6 & 30 \end{bmatrix}.$$

Четвртој колони додајмо трећу помножену са -5:

$$C_8 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 6 & 0 \end{bmatrix}.$$

На крају, помножимо прву и другу врсту са -1:

$$C_7 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 6 & 0 \end{bmatrix}.$$

Ако су y_1, y_2, y_3, y_4 нови генератори видимо да међу њима важе релације

$$\begin{aligned} y_1 &= 0 \\ 2y_2 &= 0 \\ 6y_3 &= 0. \end{aligned}$$

Дакле, $y_1 = 0$, y_2 генерише цикличну групу реда 2, y_3 генерише цикличну групу реда 6, док је y_4 слободни генератор. Нормална форма за нашу групу је: $\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}$.

(г) Формирајмо матрицу:

$$D = \begin{bmatrix} 5 & 3 & 0 & -3 \\ 2 & 4 & -2 & 0 \\ 7 & 7 & -2 & -3 \end{bmatrix}.$$

Додајмо првој врсти другу врсту помножену са -2:

$$D_1 = \begin{bmatrix} 1 & -5 & 4 & -3 \\ 2 & 4 & -2 & 0 \\ 7 & 7 & -2 & -3 \end{bmatrix}.$$

Сада другој врсти додајмо прву врсту помножену са -2 и трећој врсти додајмо прву врсту помножену са -7:

$$D_2 = \begin{bmatrix} 1 & -5 & 4 & -3 \\ 0 & 14 & -10 & 6 \\ 0 & 42 & -30 & 18 \end{bmatrix}.$$

Другој колони додајмо прву колону помножену са 5, трећој колони додајмо прву колону помножену са -4 и четвртој колони додајмо прву колону помножену са 3:

$$D_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 14 & -10 & 6 \\ 0 & 42 & -30 & 18 \end{bmatrix}.$$

Трећој врсти додајмо другу врсту помножену са -3:

$$D_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 14 & -10 & 6 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Приметимо да је $\mathrm{NZD}(14, -10, 6) = 2$. Другој колони додајмо четврту колону помножену са -2:

$$D_5 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & -10 & 6 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Најзад, трећој колони додајмо другу колону помножену са 5 и четвртој колони додајмо другу колону помножену са -3:

$$D_6 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Ако су y_1, y_2, y_3, y_4 нови генератори видимо да међу њима важе релације

$$y_1 = 0$$
$$2y_2 = 0.$$

Дакле, $y_1 = 0$, y_2 генерише цикличну подгрупу реда 2, док су y_3 и y_4 слободни генератори. Стога је нормална форма за нашу групу: $\mathbb{Z}_2 \times \mathbb{Z} \times \mathbb{Z}$.

52. Одредити инваријантне делитеље за групе

$$\mathbb{Z}_{10} \times \mathbb{Z}_{15} \times \mathbb{Z}_{20}; \quad \mathbb{Z}_{28} \times \mathbb{Z}_{42}; \quad \mathbb{Z}_9 \times \mathbb{Z}_{14} \times \mathbb{Z}_6 \times \mathbb{Z}_{16}.$$

Решење:

$$\mathbb{Z}_{10} \times \mathbb{Z}_{15} \times \mathbb{Z}_{20} \cong \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \cong \mathbb{Z}_5 \times (\mathbb{Z}_2 \times \mathbb{Z}_5) \times (\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5) \cong \mathbb{Z}_5 \times \mathbb{Z}_{10} \times \mathbb{Z}_{60},$$

те су инваријантни делитељи $d_1 = 5$, $d_2 = 10$, $d_3 = 60$.

$$\mathbb{Z}_{28} \times \mathbb{Z}_{42} \cong \mathbb{Z}_4 \times \mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \cong (\mathbb{Z}_2 \times \mathbb{Z}_7) \times (\mathbb{Z}_4 \times \ \mathbb{Z}_3 \times \mathbb{Z}_7) \cong \mathbb{Z}_{14} \times \mathbb{Z}_{84},$$

те су инваријантни делитељи $d_1 = 14$, $d_2 = 84$.

$$\mathbb{Z}_9 \times \mathbb{Z}_{14} \times \mathbb{Z}_6 \times \mathbb{Z}_{16} \cong \mathbb{Z}_9 \times \mathbb{Z}_2 \times \mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{16} \cong \mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_3) \times (\mathbb{Z}_{16} \times \mathbb{Z}_9 \times \mathbb{Z}_7) \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{1008},$$

те су инваријантни делитељи $d_1 = 2$, $d_2 = 6$ и $d_3 = 1008$.

53. Доказати да свака Абелова група реда 100 има елемент реда 10. Одредити инваријантне делитеље у случају да у таквој групи нема елемената реда већег од 10.

Решење: На основу Кошијеве теореме у групи реда 100 увек постоји елемент x реда 2 и елемент y реда 5. Како је група комутативна лако се показује да је елемент $x+y$ реда 10 (видети став о реду производа два елемента, или неке од претходних задатака).

Ако су $d_1, \ldots, d_k$ инваријантни делитељи за Абелову групу реда 100, онда је $d_1 \cdots d_k = 100$ и $d_i \mid d_{i+1}$ за $1 \leqslant i \leqslant k-1$. Како је $100 = 2^2 \cdot 5^2 = 2 \cdot 2 \cdot 5 \cdot 5$, то и нема много могућности за инваријантне делитеље. Уколико је $k = 1$, онда имамо цикличну групу изоморфну са $\mathbb{Z}_{100}$, но у њој има елемената реда знатно већег од 10. Уколико је $k = 2$, имамо следеће могућности: $d_1 = 2, d_2 = 50$; $d_1 = 10, d_2 = 10$ и $d_1 = 5, d_2 = 20$. У првом случају бисмо имали групу изоморфну са $\mathbb{Z}_2 \times \mathbb{Z}_{50}$ но у њој имамо елементе реда 50. У другом случају је наша група изоморфна са $\mathbb{Z}_{10} \times \mathbb{Z}_{10}$ и у њој заиста нема елемената реда већег од 10. У трећем случају имамо групу изоморфну са $\mathbb{Z}_5 \times \mathbb{Z}_{20}$ и у њој има елемената реда 20. Случајеви $k \geqslant 3$ нису могући.

Стога закључујемо да су за Абелову групу реда 100 у којој нема елемената реда већег од 10 инваријантни делитељи $d_1 = d_2 = 10$.

54. Класификовати све Абелове групе реда 81, 144 и 216.

Решење: Приметимо да је $81 = 3^4$, дакле појављује се само један прост број у факторизацији. Свака Абелова група реда 81 изоморфна је тачно једној од група:

$$\mathbb{Z}_{81}, \quad \mathbb{Z}_3 \times \mathbb{Z}_{27}, \quad \mathbb{Z}_9 \times \mathbb{Z}_9, \quad \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9, \quad \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3.$$

Видимо да је $144 = 2^4 \cdot 3^2$. Разматрајући могућности за инваријантне делитеље, закључујемо да је свака Абелова група реда 144 изоморфна тачно једној од група:

$$\mathbb{Z}_{144}, \quad \mathbb{Z}_2 \times \mathbb{Z}_{72}, \quad \mathbb{Z}_3 \times \mathbb{Z}_{48}, \quad \mathbb{Z}_4 \times \mathbb{Z}_{36}, \quad \mathbb{Z}_6 \times \mathbb{Z}_{24}, \quad \mathbb{Z}_{12} \times \mathbb{Z}_{12}, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{36}, \quad \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{12}$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{18}, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_6.$$

Имамо факторизацију $216 = 2^3 \cdot 3^3$. Свака Абелова група реда 216 изоморфна је тачно једној од група:

$$\mathbb{Z}_{216}, \quad \mathbb{Z}_2 \times \mathbb{Z}_{108}, \quad \mathbb{Z}_3 \times \mathbb{Z}_{72}, \quad \mathbb{Z}_6 \times \mathbb{Z}_{36}, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{54}, \quad \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{24}, \quad \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{18}$$

$$\mathbb{Z}_3 \times \mathbb{Z}_6 \times \mathbb{Z}_{12}, \quad \mathbb{Z}_6 \times \mathbb{Z}_6 \times \mathbb{Z}_6.$$

55. Нека је p прост број и нека Абелова група реда p^n има $p-1$ елемената реда p. Доказати да је та група циклична.

Решење: Јасно је да је група циклична ако је она реда p. Дакле, претпоставимо да је $n \geqslant 2$. Уколико та Абелова група, означимо је са A, није циклична, онда она има бар два инваријантна фактора. Нека има k инваријантних фактора, где је $k \geqslant 2$. Тада је

$$A \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k},$$

при чему је $1 < d_1$ и $d_i \mid d_{i+1}$ за све $1 \leqslant i \leqslant k-1$. Но, $|A| = p^n$ и стога су сви d_i степени простог броја p. Како свака циклична група чији је број елемената степен броја p има цикличну подгрупу реда p, то A садржи подгрупу

$$C_1 \times \cdots \times C_k \cong \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p.$$

Но, јасно је да сваки елемент, сем неутрала, у групи $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ има ред p, те у A има бар $p^k - 1$ елемената реда p, а то противречи претпоставци, јер је $p^k - 1 \geqslant p^2 - 1 > p - 1$.

56. Нека је G коначна Абелова група реда 360, која не садржи елементе реда 12, као ни елементе реда 18. Одредити инваријантне делитеље за G. Одредити број елемената реда 6 у групи G.

Решење: Приметимо да је $360 = 2^3 \cdot 3^2 \cdot 5$. Дакле, у елементарној факторизацији појављују се степени простих бројева 2, 3 и 5. С обзиром да у групи G нема елемената реда 12, у факторизацији се не сме појавити ни фактор $\mathbb{Z}_4$ ни фактор $\mathbb{Z}_8$. Наиме, тада би у групи постојао елемент реда 4, а како сигурно постоји и елемент реда 3, њихов збир би био елемент реда 12. Слично, у факторизацији се не сме појавити ни фактор $\mathbb{Z}_9$, јер би то значило да у групи постоји елемент реда 9 и уз елемент реда 2 добили бисмо и елемент реда 18. Закључујемо да је

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{30},$$

те су инваријантни фактори $d_1 = 2$, $d_2 = 6$, $d_3 = 30$.

За одређивање броја елемената реда 6 можемо користити елементарну факторизацију, тј. одредићемо број елемената реда 6 у групи $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$. Нека је $(x_1, x_2, x_3, x_4, x_5, x_6)$ неки елемент те групе. Уколико је $6(x_1, x_2, x_3, x_4, x_5, x_6) = (0, 0, 0, 0, 0, 0)$, то би значило да је $6x_6 = 0$. Но, како је $x_6 \in \mathbb{Z}_5$, то је $5x_6 = 0$ и добијамо да је $x_6 = 0$.

Дакле, проблем се своди на одређивање броја елемената реда 6 у групи $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. Како је $6x = 0$ за све x из ове групе, то су у њој, сем неутрала, искључиво елементи реда 2, 3 и 6. Нека је $(x_1, x_2, x_3, x_4, x_5)$ елемент реда 2. То значи да је $2(x_1, x_2, x_3, x_4, x_5) = 0$. Но, добијамо да је тада $2x_4 = 0 = 2x_5$. Како $x_4, x_5 \in \mathbb{Z}_3$, то повлачи да је $x_3 = x_4 = 0$. Дакле, елемент реда 2 је облика $(x_1, x_2, x_3, 0, 0)$ при чему нису сви x_i једнаки 0. Стога имамо 7 елемената реда 2. На сличан начин су сви елементи реда 3 облика $(0, 0, 0, x_4, x_5)$ при чему бар један од x_i није 0. Те имамо 8 елемената реда 3. Све у свему у групи $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, која је реда 72, имамо неутрал, 7 елемената реда 2 и 8 елемената реда 3. Дакле, имамо $72 - (1 + 7 + 8) = 56$ елемената реда 6. До овог закључка смо могли да дођемо и тако да приметимо да је збир ма ког елемента реда 2 и ма ког елемента реда 3 (у Абеловој групи наравно) елемент реда 6. Па елемената реда 6 има (број елемената реда 2) $\cdot$ (број елемената реда 3) $= 7 \cdot 8 = 56$.

57. Доказати да је свака коначно генерисана нетривијална подгрупа групе $(\mathbb{R} \setminus \{0\}), \cdot)$ изоморфна или групи $\mathbb{Z}_2$, или групи $\mathbb{Z}^s$ или групи $\mathbb{Z}_2 \times \mathbb{Z}^s$, за неко $s \geqslant 1$.

Решење: Овај задатак можда делује теже него што заправо јесте. Најпре, приметимо да је група $(\mathbb{R} \setminus \{0\}, \cdot)$ Абелова група и то је и свака њена коначно генерисана подгрупа. Но, знамо да је свака коначно генерисана Абелова група производ цикличних група. Посматрајмо подгрупу коју чине елементи коначног реда. Једино што ми треба да покажемо је да је та група или тривијална или је изоморфна са $\mathbb{Z}_2$. Но, то није тешко. Наиме, ако је $x \in \mathbb{R} \setminus \{0\}$ такав реалан број да је, за неко $n \geqslant 2$, $x^n = 1$, онда врло добро знамо да ако је n непаран број, мора бити $x = 1$, а ако је n паран број, онда је $x \in \{-1, 1\}$. Дакле, једини елемент реда n, за неко $n > 1$, у групи $(\mathbb{R} \setminus \{0\}, \cdot)$ је елемент -1 и он је реда 2. Дакле, у факторизацији од коначних фактора се може појављивати само $\mathbb{Z}_2$, а то је и требало показати.

У свим наредним задацима претпостављамо да су сви прстени са којима радимо комутативни прстени са јединицом, мада можда то експлицитно није наглашено.

58. Нека је p прост број и $R = \{\frac{m}{n} \in \mathbb{Q} : p \nmid n\}$. Доказати да је R потпрстен од $\mathbb{Q}$.

Решење: Приметимо најпре да $1 \in R$. Претпоставимо да су $\frac{m_1}{n_1}$ и $\frac{m_2}{n_2}$ из R. Тада је

$$\frac{m_1}{n_1} - \frac{m_2}{n_2} = \frac{m_1 n_2 - n_1 m_2}{n_1 n_2}.$$

Но, како је p прост број, уколико би $p \mid n_1 n_2$ важило би да $p \mid n_1$ или $p \mid n_2$, а знамо да то није тачно. Дакле $\frac{m_1}{n_1} - \frac{m_2}{n_2} \in R$.
Слично, како је

$$\frac{m_1}{n_1} \cdot \frac{m_2}{n_2} = \frac{m_1 m_2}{n_1 n_2},$$

а $p \nmid n_1 n_2$, добијамо да је и $\frac{m_1}{n_1} \cdot \frac{m_2}{n_2} \in R$.

Напомена: Није лоше знати да се овај потпрстен означава са $\mathbb{Z}_{(p)}$.

59. Нека је R комутативан прстен. За елемент x кажемо да је нилпотентан уколико је за неко $n \geqslant 1$ испуњено $x^n = 0_R$. Доказати да скуп свих нилпотентних елемената чини идеал.

Решење: Јасно је да је 0_R нилпотентан елемент. Претпоставимо да су x и y нилпотентни елементи и нека је $x^m = 0_R$ и $y^n = 0_R$ за неке природне бројеве m и n. Како је R комутативан прстен, важи биномна формула

$$(x+y)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} x^k y^{m+n-k}.$$

Посматрајмо производе $x^k y^{m+n-k}$ за $0 \leqslant k \leqslant m+n$. Уколико је $k \geq m$, онда је

$$x^k y^{m+n-k} = x^m x^{k-m} y^{m+n-k} = 0_R x^{k-m} y^{m+n-k} = 0_R.$$

Но, уколико је $k < m$, онда је $m - k > 0$, па је

$$x^k y^{m+n-k} = x^k y^{m-k} y^n = x^k y^{m-k} 0_R = 0_R.$$

Дакле, сви производи су једнаки нули, па је онда и $(x+y)^{m+n} = 0_R$ те је елемент $x+y$ нилпотентан.

Нека је x нилпотентан те је $x^m = 0_R$ за неки природан број m. Ако је $r \in R$ произвољан елемент онда је, због комутативности прстена $(rx)^m = r^m x^m = r^m 0_R = 0_R$, те је и rx нилпотентан.

Тиме смо показали да је скуп свих нилпотентних елемената један идеал у R.

60. Ако је x нилпотентан елемент комутативног прстена са јединицом R доказати да је елемент $1 - x$ инвертибилан.

Решење: Нека је x нилпотентан елемент. Стога је $x^m = 0_R$ за неки природан број m. Тада је

$$(1-x)(1 + x + \cdots + x^{m-1}) = 1 - x^m = 1,$$

те је $1 + x + \cdots + x^{m-1}$ инверз елемента $1 - x$.

61. Нека је $R = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Показати да је R потпрстен од $\mathbb{C}$ у коме је сваки елемент различит од 0 инвертибилан.

Решење: Нека је $a + b\sqrt{2} = 0$, где $a, b \in \mathbb{Q}$. Ако је $b \neq 0$, добијамо да је $\sqrt{2} = -\frac{a}{b} \in \mathbb{Q}$, а знамо да $\sqrt{2}$ није рационалан број. Стога мора бити $b = 0$, а онда и $a = 0$. Дакле, ако је $a + b\sqrt{2} \neq 0$, овај елемент сигурно има инверз у скупу реалних, па и комплексних бројева. Само треба показати да је његов инверз такође у R. Но,

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2} \in R,$$

јер је јасно да $\frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in \mathbb{Q}$ пошто $a, b \in \mathbb{Q}$.

62. Нека је $R = I + J$ за неке идеале I, J прстена R. Доказати да је тада и $I^2 + J^2 = R$ ($I^2 = I \cdot I$).

Решење: Докажимо да заправо из $I + J = R$ следи да је и $I^2 + J = R$. Наравно, ми све време радимо са прстенима са јединицом. Стога је $I + J = R$ акко $1_R \in I + J$ (подсетимо се да је $I + J$ увек идеал и да је идеал једнак целом прстену акко он садржи јединицу прстена). Дакле, из $I + J = R$ следи да постоји $x \in I$ и $y \in J$ тако да је $x + y = 1_R$. Тада је $x = (1_R - y)$. Следи да је $x^2 = 1_R - 2y + y^2$, па је $x^2 + (2y - y^2) = 1_R$. Но, јасно је да $x^2 \in I^2$ и да је $2y - y^2 = y(2-y) \in J$, па добијамо да је $1_R \in I^2 + J$, те је $I^2 + J = R$. Но, сада из $I^2 + J = R$, на исти начин добијамо да је $I^2 + J^2 = R$, а то се и тражило.

63. Нека је S потпрстен прстена R и I идеал у R. Доказати или оповргнути: $S+I$ је потпрстен од R.

Како је S потпрстен од R, то $1_R \in S$. А како је I идеал у R, то $0_R \in I$. Стога $1_R = 1_R + 0_R \in S+I$.

Узмимо два елемента из $S+I$: $s+x$, за неки $s \in S$ и $x \in I$ и $t+y$ за неки $t \in S$ и $y \in I$. Тада је

$$(s+x)-(t+y) = (s-t)+(x-y).$$

Како је S потпрстен од R, знамо да $s-t \in S$, а како је I идеал у R мора бити и $x-y \in I$. Стога $(s+x)-(t+y) \in S+I$.

$$(s+x)\cdot(t+y) = st + (sy+xt+xy).$$

Како је S потпрстен од R имамо да је $st \in S$. С обзиром да је I идеал у R и да $x, y \in I$, то и $sy, xt, xy \in I$, па и $sy+xt+xy \in I$, те $(s+x)(t+y) \in S+I$.

Закључујемо да је $S+I$ потпрстен од R.

64. Показати да је пресек два потпрстена увек потпрстен, као и да унија не мора бити потпрстен.

Решење: Нека је A прстен и S, T потпрстени од A. Јасно је да $1_R \in S \cap T$. Уколико $a, b \in S \cap T$, онда је и $a-b \in S$, јер је S потпрстен, али и $a-b \in T$, јер је T потпрстен, па $a-b \in S \cap T$. Јасно је и да $ab \in S \cap T$, па је $S \cap T$ заиста потпрстен.

Посматрајмо прстен $\mathbb{Q}[X]$. Тада је $S = \mathbb{Z}[X]$ његов потпрстен: разлика два полинома са целобројним коефицијентима је полинома са целобројним коефицијентима, а и производ два полинома са целобројним коефицијентима је полином са целобројним коефицијентима. Наравно и $1 \in S$. Такође је и $\mathbb{Q}$ потпрстен од $\mathbb{Q}[X]$. Но, $\mathbb{Z}[X] \cup \mathbb{Q}$ није потпрстен од $\mathbb{Q}[X]$: $\frac{1}{2}, X \in \mathbb{Z}[X] \cup \mathbb{Q}$, но $\frac{1}{2} + X$ није ни рационалан број ни полином са целобројним коефицијентима.

65. Одредити идеал $I \lhd \mathbb{Z}$ задат са: $I = (\langle 45\rangle + \langle 36\rangle) \cap \langle 12\rangle$.

Решење: Знамо да је у $\mathbb{Z}$: $\langle a\rangle + \langle b\rangle = \langle \mathrm{NZD}(a,b)\rangle$, док је $\langle a\rangle \cap \langle b\rangle = \langle \mathrm{NZS}(a,b)\rangle$. Стога је

$$(\langle 45\rangle + \langle 36\rangle) \cap \langle 12\rangle = \langle \mathrm{NZD}(45,36)\rangle \cap \langle 12\rangle = \langle 9\rangle \cap \langle 12\rangle = \langle \mathrm{NZS}(9,12)\rangle = \langle 36\rangle.$$

66. Одредити праве делитеље нуле у прстенима $\mathbb{Z}_{21}$ и $\mathbb{Z}_{16}$.

Решење: Ако је $k \in \mathbb{Z}_{21} \setminus \{0\}$ облика $3l$ за неко l, онда је јасно да је k прави делитељ нуле: $7 \cdot_{21} k = 7 \cdot_{21} 3l = 0$. Слично, ако је $k = 7s$ за неко s, опет је прави делитељ нуле, јер је $3 \cdot_{21} k = 3 \cdot_{21} 7s = 0$. Но, уколико k није дељив ни са 3 ни са 7, онда из $k \cdot_{21} t = 0$ за неко $t \in \mathbb{Z}_{21}$ следи да $21 \mid k \cdot t$ у $\mathbb{Z}$. Но, како $3 \nmid k$ и $7 \nmid k$, то је $\mathrm{NZD}(21,k) = 1$, па $21 \mid t$, те је заправо $t = 0$. Дакле, прави делитељи нуле у $\mathbb{Z}_{21}$ чине скуп $\{3,6,9,12,15,18,7,14\}$.

Уколико је $k \in \mathbb{Z}_{16} \setminus \{0\}$ паран број, јасно је да је k прави делитељ нуле, јер је тада $k \cdot_{16} 8 = 0$. Но, ако је $k \in \mathbb{Z}_{16} \setminus \{0\}$ непаран број, онда из $k \cdot_{16} t$ за неко $t \in \mathbb{Z}_{16}$ следи да $16 \mid k \cdot t$ у $\mathbb{Z}$ и како је тада $\mathrm{NZD}(16,k) = 1$, добијамо да $16 \mid t$, тј. $t = 0$. Према томе, скуп правих делитеља нуле у $\mathbb{Z}_{16}$ је скуп $\{2,4,6,8,10,12,14\}$.

67. Одредити инвертибилне елементе у прстенима $\mathbb{Z}_{15}$ и $\mathbb{Z}_{36}$ и наћи њихове инверзе.

Решење: У коначном прстену је елемент или делитељ нуле или је инвертибилан. Но, ми заправо знамо да су инвертибилни елементи у $\mathbb{Z}_n$ заправо они $k \in \mathbb{Z}_n \setminus \{0\}$ који су узајамно прости са n.

Стога је скуп инвертибилних елемената у $\mathbb{Z}_{15}$ скуп $\{1,2,4,7,8,11,13,14\}$, а

$$2^{-1} = 8, \quad 8^{-1} = 2, \quad 4^{-1} = 4, \quad 7^{-1} = 13, \quad 13^{-1} = 7, \quad 11^{-1} = 11, \quad 14^{-1} = 14.$$

Наравно, нисмо наводили инверз неутрала 1.

Скуп инвертибилних елемената у $\mathbb{Z}_{36}$ је $\{1,5,7,11,13,17,19,23,25,29,31,35\}$ и

$$5^{-1} = 29, \quad 29^{-1} = 5, \quad 7^{-1} = 31, \quad 31^{-1} = 7, \quad 11^{-1} = 23, \quad 23^{-1} = 11,$$
$$13^{-1} = 25, \quad 25^{-1} = 13, \quad 19^{-1} = 19, \quad 35^{-1} = 35.$$

68. Одредити све идеале у прстенима $\mathbb{Z}_{24}$ и $\mathbb{Z}_{16}$.

Решење: Знамо да је сваки идеал у прстену $\mathbb{Z}_n$ главни, тј. генерисан је једним елементом. Но, знамо да је идеал адитивна подгрупа групе $\mathbb{Z}_n$ (а она је наравно циклична) и за сваки делитељ елемента n постоји тачно једна циклична подгрупа тог реда. Но, заправо је свака адитивна подгрупа групе $\mathbb{Z}_n$ идеал у $\mathbb{Z}_n$. Наиме, нека је $(A, +_n)$ нека подгрупа групе $(\mathbb{Z}_n, +_n)$. Треба показати да је она идеал у прстену $(\mathbb{Z}_n, +_n, \cdot_n)$, а за то треба само показати да, ако је $k \in \mathbb{Z}_n$ и $a \in A$, онда је $k \cdot_n a \in A$. Но,

$$k \cdot_n a = \underbrace{a +_n \cdots +_n a}_{k},$$

а овај елемент је наравно у A.

Дакле, ми знамо како да одредимо ове идеале. У случају прстена $\mathbb{Z}_{24}$ посматрамо делитеље броја 24. То су бројеви $1, 2, 3, 4, 6, 8, 12, 24$. Подгрупа реда k генерисана је, као што смо већ имали прилике да разматрамо, елементом $24/k$. Другим речима идеали у $\mathbb{Z}_{24}$ су:

$$\{0\}, \quad \langle 12\rangle, \quad \langle 8\rangle, \quad \langle 6\rangle, \quad \langle 4\rangle, \quad \langle 3\rangle, \quad \langle 2\rangle, \quad \mathbb{Z}_{24}.$$

У случају прстена $\mathbb{Z}_{16}$ посматрамо делитеље броја 16, тј. бројеве $1, 2, 4, 8, 16$. Стога су сви идеали у прстену $\mathbb{Z}_{16}$:

$$\{0\}, \quad \langle 8\rangle, \quad \langle 4\rangle, \quad \langle 2\rangle, \quad \mathbb{Z}_{16}.$$

69. Испитати да ли је са $f(x) = \rho(x, 9)$ дефинисан један хомоморфизам $f\colon \mathbb{Z}_{36} \to \mathbb{Z}_9$ прстена са јединицом и у потврдном случају наћи $\mathrm{Ker}(f)$.

Решење: Јасно је да је $f(1) = 1$. Треба испитати да ли важи следеће: за $k, l \in \mathbb{Z}_{36}$:

$$\rho(k +_{36} l, 9) = \rho(k, 9) +_9 \rho(l, 9), \qquad \rho(k \cdot_{36} l, 9) = \rho(k, 9) \cdot_9 \rho(l, 9).$$

Доказ ћемо извршити за сабирање, а за множење се доказ изводи на аналогни начин. Подсетимо се да $\rho(m, n)$ означава остатак при дељењу m са n. Доказаћемо да је

$$\rho(k +_{36} l, 9) = \rho(k + l, 9) = \rho(k, 9) +_9 \rho(l, 9).$$

Подсетимо се да је $k +_{36} l = \rho(k + l, 36)$, те је

$$\rho(k +_{36} l, 9) = \rho(\rho(k + l, 36), 9).$$

Дакле, ми најпре тражимо остатак при дељењу $k + l$ са 36, а потом остатак при дељењу тог остатка са 9:

$$k + l = 36q + r, \quad 0 \leqslant r < 36, \tag{1}$$

$$r = 9q_1 + r_1, \quad 0 \leqslant r_1 < 9. \tag{2}$$

Према томе, због јединствености који имамо при еуклидском дељењу,

$$r = \rho(k + l, 36), \qquad r_1 = \rho(\rho(k + l, 36), 9) = \rho(k +_{36} l, 9).$$

Но, из (1) и (2) добијамо:

$$k + l = 36q + r = 36q + 9q_1 + r_1 = 9(4q + q_1) + r_1.$$

Како је $0 \leqslant r_1 < 9$. јединственост остатка при еуклидском дељењу нам казује да је $r_1 = \rho(k + l, 9)$.

Подсетимо се да је $\rho(k, 9) +_9 \rho(l, 9) = \rho(\rho(k, 9) + \rho(l, 9), 9)$. Дакле, ако је

$$k = 9q_2 + r_2, \qquad 0 \leqslant r_2 < 9, \tag{3}$$

$$l = 9q_3 + r_3, \qquad 0 \leqslant r_3 < 9, \tag{4}$$

тј. $r_2 = \rho(k, 9)$ и $r_3 = \rho(l, 9)$, тада је $\rho(k, 9) +_9 \rho(l, 9) = \rho(r_2 + r_3, 9)$.

$$r_2 + r_3 = 9q_4 + r_4, \qquad 0 \leqslant r_4 < 9, \tag{5}$$

те је $r_4 = \rho(r_2 + r_3, 9) = \rho(k, 9) +_9 \rho(l, 9)$. Но, из (3), (4) и (5) добијамо:

$$k + l = 9q_2 + r_2 + 9q_3 + r_3 = 9(q_2 + q_3) + r_2 + r_3 = 9(q_2 + q_3) + 9q_4 + r_4 = 9(q_2 + q_3 + q_4) + r_4.$$

Како је $0 \leqslant r_4 < 9$, јединственост остатка при еуклидском дељењу нам даје: $r_4 = \rho(k + l, 9)$. Према томе $r_1 = r_4$ и добили смо да је заиста

$$\rho(k +_{36} l, 9) = r_1 = r_4 = \rho(k, 9) +_9 \rho(l, 9),$$

као што смо и најавили. Дакле, $f\colon \mathbb{Z}_{36} \to \mathbb{Z}_9$ је заиста хомоморфизам.

Језгро није тешко наћи:

$$\mathrm{Ker}(f) = \{k \in \mathbb{Z}_{36} : f(x) = 0\} = \{k \in \mathbb{Z}_{36} : 9 \mid k\} = \{0, 9, 18, 27\}.$$

Приметимо да је $\mathrm{Ker}(f) = \langle 9 \rangle \cong \mathbb{Z}_4$.

70. Испитати да ли је са $f(x) = \rho(x, 6)$ дефинисан један хомоморфизам $f\colon \mathbb{Z}_{36} \to \mathbb{Z}_6$ и у потврдном случају наћи $\mathrm{Ker}(f)$.

Решење: Доказ да је f хомоморфизам се изводи као у претходном задатку, док је

$$\mathrm{Ker}(f) = \{k \in \mathbb{Z}_{36} : f(x) = 0\} = \{k \in \mathbb{Z}_{36} : 6 \mid k\} = \{0, 6, 12, 18, 24, 30\}.$$

Приметимо да је $\mathrm{Ker}(f) = \langle 6 \rangle \cong \mathbb{Z}_6$.

Напомена. Наведимо пример када на овај начин не добијамо хомоморфизам. Ако се посматра пресликавање $f\colon \mathbb{Z}_{32} \to \mathbb{Z}_6$, дефинисано са $f(x) = \rho(x, 6)$, онда f није хомоморфизам. Наиме, имамо да је $15 +_{32} 17 = 0$ у $\mathbb{Z}_{32}$, те је и $f(15 +_{32} 17) = f(0) = 0$, а $f(15) +_6 f(17) = 3 +_6 5 = 2 \neq 0$. Размислите када је $f : \mathbb{Z}_m \to \mathbb{Z}_n$ задато са $f(x) = \rho(x, n)$ хомоморфизам.

71. Решити системе конгруенција:

(а) $x \equiv 3 \pmod 7$, $\quad x \equiv 5 \pmod 8$;

(б) $x \equiv 1 \pmod{11}$, $\quad x \equiv 5 \pmod{15}$;

(в) $x \equiv -4 \pmod{16}$, $\quad x \equiv 5 \pmod 7$;

(г) $x \equiv 5 \pmod{13}$, $\quad x \equiv -1 \pmod 8 \quad x \equiv 4 \pmod 7$;

(д) $x \equiv 5 \pmod{23}$, $\quad x \equiv 3 \pmod{18} \quad x \equiv 2 \pmod{17}$;

(ђ) $x \equiv 3 \pmod 5$, $\quad x \equiv 1 \pmod 8 \quad x \equiv -4 \pmod{11}$.

Решење: (а) Како је $\mathrm{NZD}(7, 8) = 1$ из Кинеске теореме о остацима закључујемо да је решење јединствено по модулу $7 \cdot 8 = 56$.

Конгруенција $x \equiv 3 \pmod 7$ еквивалентна је са $x = 7k + 3$ за неко $k \in \mathbb{Z}$. Тада је $x \equiv 5 \pmod 8$ еквивалентно са $7k + 3 \equiv 5 \pmod 8$, тј. са $7k \equiv 2 \pmod 8$. Но, $7^{-1} = 7$ у $\mathbb{Z}_8$ и добијамо да је претходна конгруенција еквивалентна са $7 \cdot 7k \equiv 7 \cdot 2 \pmod 8$, тј. са $k \equiv 6 \pmod 8$.

Дакле, решење конгруенције су сви цели бројеви x облика $x = 7k + 2 = 7(8l + 6) + 2 = 56l + 44$, где је $l \in \mathbb{Z}$.

(б) Како је $\mathrm{NZD}(11, 15) = 1$ из Кинеске теореме о остацима закључујемо да је решење јединствено по модулу $11 \cdot 15 = 165$.

Конгруенција $x \equiv 5 \pmod{15}$ еквивалентна је са $x = 15k + 5$, за неко $k \in \mathbb{Z}$. Тада је $x \equiv 1 \pmod{11}$ еквивалентно са $15k + 5 \equiv 1 \pmod{11}$, тј. са $4k \equiv 7 \pmod{11}$. Но, $4^{-1} = 3$ у $\mathbb{Z}_{11}$, па је претходна конгруенција еквивалентна са $3 \cdot 4k \equiv 3 \cdot 7 \pmod{11}$, тј. са $k \equiv 10 \pmod{11}$.

Дакле, решење конгруенције су сви цели бројеви x облика $x = 15k + 5 = 15(11l + 10) + 5 = 165l + 155$, где је $l \in \mathbb{Z}$.

(в) Како је $\mathrm{NZD}(16, 7) = 1$ из Кинеске теореме о остацима закључујемо да је решење јединствено по модулу $16 \cdot 7 = 112$.

Конгруенција $x \equiv -4 \pmod{16}$ еквивалентна је са $x = 16k - 4$, за неко $k \in \mathbb{Z}$. Тада је $x \equiv 5 \pmod 7$ еквивалентно са $16k - 4 \equiv 5 \pmod 7$, тј. са $2k \equiv 2 \pmod 7$. Но, $2^{-1} = 4$ у $\mathbb{Z}_7$, па је претходна конгруенција еквивалентна са $4 \cdot 2k \equiv 4 \cdot 2 \pmod 7$, тј. са $k \equiv 1 \pmod 7$.

Дакле, решење конгруенције су сви цели бројеви x облика $x = 16k - 4 = 16(7l + 1) - 4 = 112l + 12$, где је $l \in \mathbb{Z}$.

(г) Како је $\text{NZD}(13, 8) = \text{NZD}(8, 7) = \text{NZD}(13, 7)$ из Кинеске теореме о остацима закључујемо да је решење јединствено по модулу $13 \cdot 8 \cdot 7 = 728$.

Конгруенција $x \equiv 5 \pmod{13}$ еквивалентна је са $x = 13k + 5$, за неко $k \in \mathbb{Z}$. Тада је $x \equiv -1 \pmod 8$ еквивалентно са $13k + 5 \equiv -1 \pmod 8$, тј. са $5k \equiv 2 \pmod 8$. Но, $5^{-1} = 5$ у $\mathbb{Z}_8$, па је претходна конгруенција еквивалентна са $5 \cdot 5k \equiv 5 \cdot 2 \pmod 8$, тј. са $k \equiv 2 \pmod 8$. Дакле, $x = 13k + 5 = 13(8l+2)+5 = 104l+31$, за неко $l \in \mathbb{Z}$. Тада је конгруенција $x \equiv 4 \pmod 7$ еквивалентна са $104l+31 \equiv 4 \pmod 7$, тј. са $6l \equiv 1 \pmod 7$. Како је $6^{-1} = 6$ у $\mathbb{Z}_7$, то је претходна конгруенција еквивалентна са $6 \cdot 6l \equiv 6 \cdot 1 \pmod 7$, тј. са $l \equiv 6 \pmod 7$.

Коначно, решење конгруенције су сви бројеви x облика $x = 104l + 31 = 104(7m + 6) + 31 = 728m + 655$, где је $m \in \mathbb{Z}$.

(д) Као и у претходном примеру, како су бројеви 23, 18 и 17 пар по пар међусобно прости, на основу Кинеске теореме о остацима можемо да закључимо да је решење јединствено по модулу $23 \cdot 18 \cdot 17 = 7038$.

Конгруенција $x \equiv 5 \pmod{23}$ еквивалентна је са $x = 23k + 5$, за неко $k \in \mathbb{Z}$. Тада је $x \equiv 3 \pmod{18}$ еквивалентно са $23k + 5 \equiv 3 \pmod{18}$, тј. са $5k \equiv 16 \pmod{18}$. Приметимо да је $7 \cdot_{18} 5 = 35 = -1$ у $\mathbb{Z}_{18}$, те је $5^{-1} = -7 = 11$ у $\mathbb{Z}_{18}$. Стога је конгруенција $5k \equiv 16 \pmod{18}$ еквивалентна са $11 \cdot 5k \equiv 11 \cdot 16 \pmod{18}$, тј. са $k \equiv 14 \pmod{18}$. Дакле, $x = 23k + 5 = 23(18l + 14) + 5 = 414l + 327$, за неко $l \in \mathbb{Z}$. Тада је конгруенција $x \equiv 2 \pmod{17}$ еквивалентна са $414l + 327 \equiv 2 \pmod{17}$, тј. са $6l \equiv 15 \pmod{17}$. Но, $6^{-1} = 3$ у $\mathbb{Z}_{17}$, па је претходна конгруенција еквивалентна са $3 \cdot 6l \equiv 3 \cdot 15 \pmod{17}$, тј. са $l \equiv 11 \pmod{17}$.

Коначно, решење конгруенције су сви бројеви x облика $x = 414l + 327 = 414(17m + 11) + 327 = 7038m + 4881$, где је $m \in \mathbb{Z}$.

(ђ) Као и у претходном примеру, како су бројеви 5, 8 и 11 пар по пар међусобно прости, на основу Кинеске теореме о остацима можемо да закључимо да је решење јединствено по модулу $5 \cdot 8 \cdot 11 = 440$.

Конгруенција $x \equiv -4 \pmod{11}$ еквивалентна је са $x = 11k - 4$ за неки $k \in \mathbb{Z}$. Тада је конгруенција $x \equiv 1 \pmod 8$ еквивалентна са $11k - 4 \equiv 1 \pmod 8$, тј. са $3k \equiv 5 \pmod 8$. Како је $3^{-1} = 3$ у $\mathbb{Z}_8$, то је претходна конгруенција еквивалентна са $3 \cdot 3k \equiv 3 \cdot 5 \pmod 8$, тј. са $k \equiv 7 \pmod 8$. Дакле, $x = 11k - 4 = 11(8l + 7) - 4 = 88l + 73$, за неко $l \in \mathbb{Z}$. Тада је конгруенција $x \equiv 3 \pmod 5$ еквивалентна са $88l + 73 \equiv 3 \pmod 5$, тј. са $3l \equiv 0 \pmod 5$. Како је $3^{-1} = 2$ у $\mathbb{Z}_5$, то је претходна конгруенција еквивалентна са $2 \cdot 3l \equiv 2 \cdot 0 \pmod 5$, тј. са $l \equiv 0 \pmod 5$.

Коначно, решење конгруенције су сви бројеви x облика $x = 88l + 73 = 88 \cdot 5m + 73 = 440m + 73$, где је $m \in \mathbb{Z}$.

72. Испитати да ли решење постоји и уколико постоји наћи сва решења наведених конгруенција:

(а) $3x \equiv 4 \pmod 7$;

(б) $4x \equiv 2 \pmod 6$;

(в) $15x \equiv 4 \pmod{10}$;

(г) $12x \equiv 21 \pmod{15}$;

Решење:

(а) Како је 7 прост број и $7 \nmid 3$, то је 3 инвертибилан у $\mathbb{Z}_7$. Заправо је његов инверз једнак 5: $5 \cdot_7 3 = 1$. Стога је $3x \equiv 4 \pmod 7$ еквивалентно са $x \equiv 5 \cdot_7 4 \pmod 7$, тј. са $x \equiv 6 \pmod 7$ што је и решење конгруенције, тј. решења су сви бројеви облика $7k + 6$, за $k \in \mathbb{Z}$.

(б) Како 4 није инвертибилан у $\mathbb{Z}_6$, морамо поступити пажљивије. Приметимо да је $4x \equiv 2 \pmod 6$ акко $6 \mid (4x - 2)$ у $\mathbb{Z}$, тј. акко $3 \mid (2x - 1)$ у $\mathbb{Z}$. Дакле,

$$4x \equiv 2 \pmod 6 \quad \text{акко} \quad 2x \equiv 1 \pmod 3.$$

Но, како је 2 инвертибилан у $\mathbb{Z}_3$ и инверз му је 2, множењем са 2 добијамо еквивалентну конгруенцију $x \equiv 2 \pmod 3$, што је и решење почетне конгруенције, тј. решења су сви цели бројеви облика $3k+2$, за $k \in \mathbb{Z}$.

(в) Дата конгруенција еквивалентна је услову $10 \mid (15x-4)$. Како су и 10 и 4 парни бројеви, видимо да и x мора бити паран број. Нека је $x = 2y$. Добијамо да је почетна конгруенција еквивалентна услову $10 \mid (30y-4)$, те и услову $5 \mid (15y-2)$. Но, $5 \mid 15y$, па је последњи услов еквивалентан са $5 \mid (-2)$, што није тачно. Закључујемо да наведена конгруенција нема решења.

(г) Наведена конгруенција еквивалентна је услову $15 \mid (12x-21)$, те и услову $5 \mid (4x-7)$ што је еквивалентно са $5 \mid (4x-2)$. Дакле, имамо еквивалентну конгруенцију $4x \equiv 2 \pmod 5$. Како је инверз од 4 у $\mathbb{Z}_5$ једнак 4, множењем са 4 добијамо еквивалентну конгруенцију $x \equiv 4 \cdot_5 2 \pmod 5$, тј. конгруенцију $x \equiv 3 \pmod 5$. Према томе, решења почетне конгруенције су сви бројеви облика $5k+3$, за $k \in \mathbb{Z}$.

73. Наћи бар један примитивни корен r модуло 11 и помоћу таблице за ind_r одредити све примитивне корене модуло 11. Испитати да ли следеће конгруенције имају решење и у потврдном случају наћи сва решења:

(а) $4x \equiv 3 \pmod{11}$, (б) $x^2 \equiv 3 \pmod{11}$, (в) $x^3 \equiv 2 \pmod{11}$, (г) $x^4 \equiv -3 \pmod{11}$.

Решење: Приметимо да у $\mathbb{Z}_{11}$ имамо:

$$\begin{aligned} 2^1 &= 2 \\ 2^2 &= 4 \\ 2^3 &= 8 \\ 2^4 &= 5 \\ 2^5 &= 10 \\ 2^6 &= 9 \\ 2^7 &= 7 \\ 2^8 &= 3 \\ 2^9 &= 6 \end{aligned}$$

Закључујемо да је 2 један примитивни корен модуло 11. Подсетимо се да је

$$\mathrm{ind}_r(a) = x \text{ акко } r^x = a,$$

уколико је r примитивни корен. Та функција ind_r је заправо дискретна верзија логаритма.

Формирајмо тражену таблицу:

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{ind}_2(a)$	0	1	8	2	4	9	7	3	6	5

По дефиницији функције ind_r у овом нашем случају она успоставља изоморфизам

$$\mathrm{ind}_r \colon (\mathbb{Z}_{11} \setminus \{0\}, \cdot_{11}) \to (\mathbb{Z}_{10}, +_{10}).$$

Дакле a је примитивни корен акко је $\mathrm{ind}_r(a)$ генератор групе $(\mathbb{Z}_{10}, +_{10})$, а ово је тачно акко је $\mathrm{NZD}(\mathrm{ind}_r(a), 10) = 1$. Дакле, скуп свих примитивних корена модуло 11 је: $\{2, 6, 7, 8\}$.

Решимо сада наведене конгруенције.

(а) Наравно да ову конгруенцију можемо да решимо као и раније конгруенције. Но, решимо је помоћу функције ind_2. Јасно је да је довољно ову конгруенцију решити сматрајући да је $x \in \mathbb{Z}_{11}$, пошто се из тог решења лако добијају сва решења у $\mathbb{Z}$. Применимо овде функцију ind_2. На основу својстава те функције, конгруенција $4x \equiv 3 \pmod{11}$ еквивалентна је једначини

$$\mathrm{ind}_2(4) +_{10} \mathrm{ind}_2(x) = \mathrm{ind}_2(3)$$

у $\mathbb{Z}_{10}$, те је $\mathrm{ind}_2(x) = 6$. Закључујемо да је $x = 9$, те су решења почетне конгруенције сви цели бројеви x облика $x = 11k + 9$, где је $k \in \mathbb{Z}$.

(б) Као и у претходном примеру, претпостављамо да је $x \in \mathbb{Z}_{11}$. Конгруенција $x^2 \equiv 3 \pmod{11}$ еквивалентна је једначини

$$2\,\mathrm{ind}_2(x) = \mathrm{ind}_2(3)$$

у $\mathbb{Z}_{10}$. Како је $\mathrm{ind}_2(3) = 8$, добијамо једначину

$$2\,\mathrm{ind}_2(x) = 8$$

у $\mathbb{Z}_{10}$. Ово је еквивалентно услову $10 \mid (2\,\mathrm{ind}_2(x) - 8)$ у $\mathbb{Z}$, односно услову $5 \mid (\mathrm{ind}_2(x) - 4)$. Проверавајући таблицу за ind_2, видимо да је ово могуће за $\mathrm{ind}_2(x) \in \{4, 9\}$, тј. $x = 5$ или $x = 6$ у $\mathbb{Z}_{11}$. Закључујемо да су решења конгруенције сви бројеви x облика $11k+5$, где је $k \in \mathbb{Z}$, као и сви бројеви облика $11k + 6$, где је $k \in \mathbb{Z}$.

Краће: решења су сви бројеви облика $11k \pm 5$, где је $k \in \mathbb{Z}$.

(в) Као и у претходним примерима, разматрајмо $x \in \mathbb{Z}_{11}$. Конгруенција $x^3 \equiv 2 \pmod{11}$ еквивалентна је једначини

$$3\,\mathrm{ind}_2(x) = \mathrm{ind}_2(2),$$

у $\mathbb{Z}_{10}$, тј.

$$3\,\mathrm{ind}_2(x) = 1.$$

Како је $3^{-1} = 7$ у $\mathbb{Z}_{10}$, добијамо да је

$$\mathrm{ind}_2(x) = 7.$$

Из таблице добијамо да је $x = 7$, па су сва решења цели бројеви x облика $x = 11k + 7$, где је $k \in \mathbb{Z}$.

(г) Конгруенција $x^4 \equiv -3 \pmod{11}$ еквивалентна је конгруенцији $x^4 \equiv 8 \pmod{11}$, те једначини

$$4\,\mathrm{ind}_2(x) = \mathrm{ind}_2 8$$

у $\mathbb{Z}_{10}$, тј. једначини

$$4\,\mathrm{ind}_2(x) = 3$$

у $\mathbb{Z}_{10}$. Но, то значи да $10 \mid (4\,\mathrm{ind}_2(x) - 3)$. Посебно, то би значило да је $4\,\mathrm{ind}_2(x) - 3$ паран број, но то није тачно. Закључујемо да почетна конгруенција нема решења.

74. Наћи бар један примитивни корен r модуло 17 и помоћу таблице за ind_r одредити све примитивне корене модуло 17. Испитати да ли следеће конгруенције имају решење и у потврдном случају наћи сва решења:

(а) $7x \equiv 3 \pmod{17}$, (б) $x^2 \equiv -2 \pmod{17}$, (в) $x^3 \equiv 3 \pmod{17}$, (г) $x^4 \equiv 3 \pmod{17}$.

Решење: Овај пут нам провера показује да 2 није примитиван корен модуло 17, но 3 јесте:

$$3^1 = 3$$
$$3^2 = 9$$
$$3^3 = 10$$
$$3^4 = 13$$
$$3^5 = 5$$
$$3^6 = 15$$
$$3^7 = 11$$
$$3^8 = 16$$
$$3^9 = 14$$
$$3^{10} = 8$$
$$3^{11} = 7$$
$$3^{12} = 4$$
$$3^{13} = 12$$
$$3^{14} = 2$$
$$3^{15} = 6.$$

Таблица за ind_3:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{ind}_3(a)$	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Дакле, a је примитиван корен модуло 17 акко је $\mathrm{NZD}(\mathrm{ind}_3(a), 16) = 1$, тј. акко је $\mathrm{ind}_3(a)$ непаран број. Стога је скуп свих примитивних корена модуло 17: $\{3, 5, 6, 7, 10, 11, 12, 14\}$.

(а) Дата конгруенција еквивалентна је једначини

$$\mathrm{ind}_3(7) +_{16} \mathrm{ind}_3(x) = \mathrm{ind}_3(3)$$

у $\mathbb{Z}_{16}$. тј. једначини

$$11 +_{16} \mathrm{ind}_3(x) = 1$$

у $\mathbb{Z}_{16}$. Дакле, $\mathrm{ind}_3(x) = 6$ и из таблице добијамо да је $x = 15$. Дакле, решења почетне конгруенције су сви цели бројеви x облика $17k + 15$, где је $k \in \mathbb{Z}$.

(б) Дата конгруенција еквивалентна је конгруенцији

$$x^2 \equiv 15 \pmod{17},$$

те једначини

$$2\,\mathrm{ind}_3(x) = 6$$

у $\mathbb{Z}_{16}$ ($\mathrm{ind}_3(15) = 6$). Дакле, $16 \mid (2\,\mathrm{ind}_3(x) - 6)$, те $8 \mid (\mathrm{ind}_3(x) - 3)$. Из таблице закључујемо да мора бити $x = 10$, или $x = 7$ те су сва решења почетне конгруенције цели бројеви x облика $x = 17k \pm 10$, где је $k \in \mathbb{Z}$.

(в) Дата конгруенција еквивалентна је једначини

$$3\,\mathrm{ind}_3(x) = 1$$

у $\mathbb{Z}_{16}$. Како је $3^{-1} = 11$ у $\mathbb{Z}_{16}$, добијамо да је $\mathrm{ind}_3(x) = 11$, па је $x = 7$. Решења почетне конгруенције су сви цели бројеви x облика $x = 17k + 7$, где је $k \in \mathbb{Z}$.

(г) Дата конгруенција еквивалентна је једначини

$$4\,\mathrm{ind}_3(x) = 1$$

у $\mathbb{Z}_{16}$. Дакле,$16 \mid (4\,\mathrm{ind}_3(x) - 1)$, а јасно је да ово није могуће, јер је $4\,\mathrm{ind}_3(x) - 1$ непаран број.

75. Наћи бар један примитивни корен r модуло 7 и помоћу таблице за ind_r одредити све примитивне корене модуло 7. Испитати да ли следеће конгруенције имају решење и у потврдном случају наћи сва решења:

(а) $4x \equiv 3 \pmod 7$, (б) $x^2 \equiv 2 \pmod 7$, (в) $x^3 \equiv 2 \pmod 7$, (г) $x^4 \equiv 3 \pmod 7$.

Решење: Провера нам даје да је 3 један примитивни корен модуло 7:

$$3^1 = 3$$
$$3^2 = 2$$
$$3^3 = 6$$
$$3^4 = 4$$
$$3^5 = 5$$

Таблица за ind_3:

a	1	2	3	4	5	6
$\mathrm{ind}_3(a)$	0	2	1	4	5	3

Примитивни корени су они a за које је $\mathrm{NZD}(\mathrm{ind}_3(a), 6) = 1$. Дакле, скуп примитивних корена је $\{3, 5\}$.

(а) Конгруенција $4x \equiv 3 \pmod 7$, где је $x \in \mathbb{Z}_7$, еквивалентна је једначини

$$\mathrm{ind}_3(4) + \mathrm{ind}_3(x) = \mathrm{ind}_3(3),$$

тј. једначини

$$4 + \mathrm{ind}_3(x) = 1$$

у $\mathbb{Z}_6$. Дакле, $\mathrm{ind}_3(x) = 3$, те је $x = 6$. Стога је решење почетне конгруенције сваки цео број x облика $7k + 6$, где је $k \in \mathbb{Z}$.

(б) Конгруенција $x^2 \equiv 2 \pmod 7$, где је $x \in \mathbb{Z}_7$, еквивалентна је једначини

$$2\,\mathrm{ind}_3(x) = \mathrm{ind}_3(2),$$

односно једначини

$$2\,\mathrm{ind}_3(x) = 2$$

у $\mathbb{Z}_6$. То значи да $6 \mid 2(\mathrm{ind}_3(x) - 1)$, те $3 \mid (\mathrm{ind}_3(x) - 1)$. Из таблице видимо да је то испуњено за $x = 3$ и $x = 4$. Стога је решење почетне конгруенције сваки цео број x облика $x = 7k + 3$, као и сваки цео број x облика $7k + 4$, где је $k \in \mathbb{Z}$.

(в) Конгруенција $x^3 \equiv 2 \pmod 7$, где је $x \in \mathbb{Z}_7$, еквивалентна је једначини

$$3\,\mathrm{ind}_3(x) = \mathrm{ind}_3(2),$$

односно једначини

$$3\,\mathrm{ind}_3(x) = 2$$

у $\mathbb{Z}_6$. Дакле, $6 \mid (3\,\mathrm{ind}_3(x) - 2)$. Јасно је да то није могуће, јер број $3\,\mathrm{ind}_3(x) - 2$ није дељив са 3. Закључујемо да почетна конгруенција нема решења.

(г) Конгруенција $x^4 \equiv 3 \pmod 7$, где је $x \in \mathbb{Z}_7$, еквивалентна је једначини

$$4\,\mathrm{ind}_3(x) = \mathrm{ind}_3(3),$$

односно једначини

$$4\,\mathrm{ind}_3(x) = 1$$

у $\mathbb{Z}_6$. Дакле, $6 \mid (4\,\mathrm{ind}_3(x) - 1)$. Но, јасно је да то није могуће јер је број $4\,\mathrm{ind}_3(x) - 1$ непаран. Закључујемо да почетна конгруенција нема решења.

76. Доказати да поља $\mathbb{Q}(\sqrt{2})$ и $\mathbb{Q}(\sqrt{3})$ нису изоморфна.

Решења: Претпоставимо да постоји изоморфизам $f\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$. Знамо да мора бити $f(1) = 1$. Но, тада се индукцијом лако показује да је $f(n) = n$, за све $n \in \mathbb{N}$: из претпоставке да је $f(n) = n$ добијамо да је $f(n+1) = f(n) + f(1) = n + 1$. Наравно, пошто је $f(-n) = -f(n)$, добијамо да је $f(m) = m$ за све $m \in \mathbb{Z}$. Такође, $f(1) = f(n \cdot n^{-1}) = f(n) \cdot f(n^{-1})$, па је и $f(n^{-1}) = (f(n))^{-1}$. Одавде лако следи да је $f\left(\frac{m}{n}\right) = \frac{m}{n}$ за све $m \in \mathbb{Z}$ и све $n \in \mathbb{N}$, те је $f(q) = q$ за све $q \in \mathbb{Q}$.

Како је $2 = (\sqrt{2})^2$, то је

$$2 = f(2) = f\left(\left(\sqrt{2}\right)^2\right) = \left(f\left(\sqrt{2}\right)\right)^2.$$

Дакле, ако је $f\left(\sqrt{2}\right) = a + b\sqrt{3}$ за неке $a, b \in \mathbb{Q}$, тада је

$$(a + b\sqrt{3})^2 = 2.$$

Добијамо да је

$$a^2 + 3b^2 + 2ab\sqrt{3} = 2,$$

тј.

$$ab\sqrt{3} = \frac{1}{2}(2 - a^2 - 3b^2) \in \mathbb{Q}.$$

Знамо да $\sqrt{3} \notin \mathbb{Q}$, па мора бити $ab = 0$, те је $a = 0$ или $b = 0$.

Претпоставимо да је $a = 0$. Тада је $3b^2 = 2$. Нека је $b = \frac{m}{n}$, где је $\frac{m}{n}$ 'нескратив' разломак, тј. $\mathrm{NZD}(m, n) = 1$. Добијамо да је

$$3m^2 = 2n^2,$$

те $2 \mid 3m^2$. Како је 2 прост број и $2 \nmid 3$, мора бити $2 \mid m^2$, те $2 \mid m$. Дакле, $m = 2m_1$ за неки $m_1 \in \mathbb{Z}$ и добијамо

$$12m_1^2 = 2n^2,$$

те је

$$6m_1^2 = n^2.$$

Но, из овога следи да $2 \mid n^2$, те $2 \mid n$, а то, заједно са $2 \mid m$ противречи претпоставци да је $\mathrm{NZD}(m, n) = 1$. Тиме смо добили контрадикцију и закључујемо да је $a \neq 0$.

Остала је могућност да је $b = 0$. Тада добијамо да је $a^2 = 2$ те бисмо добили да је $\sqrt{2} \in \mathbb{Q}$. Ова контрадикција завршава задатак — поља $\mathbb{Q}(\sqrt{2})$ и $\mathbb{Q}(\sqrt{3})$ нису изоморфна.

77. Конструисати поља са 8 и 9 елемената.

Решење: За конструкцију поља од 8 елемената потребан нам је нерастављив полином степена 3 из $\mathbb{Z}_2[X]$ (подсетите се теоријског материјала из скрипти). То није тешко наћи, полином $a(X) = X^3 + X + 1 \in \mathbb{Z}_2[X]$ је нерастављив. Наиме, пошто је то полином трећег степена, једино се може раставити у облику производа једног полинома првог степена и једног полинома другог степена, но то би значило да он има нулу у $\mathbb{Z}_2$. Но, како је $a(0) = 0$ и $a(1) = 1$, то није тачно. Дакле, $F = \mathbb{Z}_2[X]/\langle a(X)\rangle$ је тражено поље. Ако је $\mu = X + \langle a(X)\rangle$, онда је

$$F = \{0, 1, \mu, \mu^2, 1+\mu, 1+\mu^2, \mu+\mu^2, 1+\mu+\mu^2\}.$$

Како је $1 + 1 = 0$ у $\mathbb{Z}_2$, то је и $1 + 1 = 0$ у F, па је и $\alpha + \alpha = \alpha \cdot 1 + \alpha \cdot 1 = \alpha \cdot (1 + 1) = \alpha \cdot 0 = 0$, за све $\alpha \in F$. Стога је лако написати таблицу сабирања за F:

$+$	0	1	μ	μ^2	$1+\mu$	$1+\mu^2$	$\mu+\mu^2$	$1+\mu+\mu^2$
0	0	1	μ	μ^2	$1+\mu$	$1+\mu^2$	$\mu+\mu^2$	$1+\mu+\mu^2$
1	1	0	$1+\mu$	$1+\mu^2$	μ	μ^2	$1+\mu+\mu^2$	$\mu+\mu^2$
μ	μ	$1+\mu$	0	$\mu+\mu^2$	1	$1+\mu+\mu^2$	μ^2	$1+\mu^2$
μ^2	μ^2	$1+\mu^2$	$\mu+\mu^2$	0	$1+\mu+\mu^2$	1	μ	$1+\mu$
$1+\mu$	$1+\mu$	μ	1	$1+\mu+\mu^2$	0	$\mu+\mu^2$	$1+\mu^2$	μ^2
$1+\mu^2$	$1+\mu^2$	μ^2	$1+\mu+\mu^2$	1	$\mu+\mu^2$	0	$1+\mu$	μ
$\mu+\mu^2$	$\mu+\mu^2$	$1+\mu+\mu^2$	μ^2	μ	$1+\mu^2$	$1+\mu$	0	1
$1+\mu+\mu^2$	$1+\mu+\mu^2$	$\mu+\mu^2$	$1+\mu^2$	$1+\mu$	μ^2	μ	1	0

За таблицу множења нам је важно да знамо да је $\mu^3+\mu+1=0$, те је $\mu^3=1+\mu$.

$\cdot$	0	1	μ	μ^2	$1+\mu$	$1+\mu^2$	$\mu+\mu^2$	$1+\mu+\mu^2$
0	0	0	0	0	0	0	0	0
1	0	1	μ	μ^2	$1+\mu$	$1+\mu^2$	$\mu+\mu^2$	$1+\mu+\mu^2$
μ	0	μ	μ^2	$1+\mu$	$\mu+\mu^2$	1	$1+\mu+\mu^2$	$1+\mu^2$
μ^2	0	μ^2	$1+\mu$	$\mu+\mu^2$	$1+\mu+\mu^2$	μ	$1+\mu^2$	1
$1+\mu$	0	$1+\mu$	$\mu+\mu^2$	$1+\mu+\mu^2$	$1+\mu^2$	μ^2	1	μ
$1+\mu^2$	0	$1+\mu^2$	1	μ	μ^2	$1+\mu+\mu^2$	$1+\mu$	$\mu+\mu^2$
$\mu+\mu^2$	0	$\mu+\mu^2$	$1+\mu+\mu^2$	$1+\mu^2$	1	$1+\mu$	μ	μ^2
$1+\mu+\mu^2$	0	$1+\mu+\mu^2$	$1+\mu^2$	1	μ	$\mu+\mu^2$	μ^2	$1+\mu$

За конструкцију поља са 9 елемената, треба нам нерастављив полином из $\mathbb{Z}_3[X]$ степена 2. На пример, полином $b(X)=X^2+1$ је такав. Наиме, $b(0)=1$, $b(1)=2$, те $b(X)$ нема нуле у $\mathbb{Z}_3$ и пошто је степена 2 закључујемо да је нерастављив. Дакле, тражено поље је $E=\mathbb{Z}_3[X]/\langle b(X)\rangle$. Ако је $\xi=X+\langle b(X)\rangle$, онда је

$$E=\{0,1,2,\xi,2\xi,1+\xi,2+\xi,1+2\xi,2+2\xi\}.$$

Како је $3=0$ у $\mathbb{Z}_3$, то је и $3\alpha=0$ у E за све $\alpha\in E$. То нам помаже да саставимо таблицу сабирања:

$+$	0	1	2	ξ	2ξ	$1+\xi$	$2+\xi$	$1+2\xi$	$2+2\xi$
0	0	1	2	ξ	2ξ	$1+\xi$	$2+\xi$	$1+2\xi$	$2+2\xi$
1	1	2	0	$1+\xi$	$1+2\xi$	$2+\xi$	ξ	$2+2\xi$	2ξ
2	2	0	1	$2+\xi$	$2+2\xi$	ξ	$1+\xi$	2ξ	$1+2\xi$
ξ	ξ	$1+\xi$	$2+\xi$	2ξ	0	$1+2\xi$	$2+2\xi$	1	2
2ξ	2ξ	$1+2\xi$	$2+2\xi$	0	ξ	1	2	$1+\xi$	$2+\xi$
$1+\xi$	$1+\xi$	$2+\xi$	ξ	$1+2\xi$	1	$2+2\xi$	2ξ	2	0
$2+\xi$	$2+\xi$	ξ	$1+\xi$	$2+2\xi$	2	2ξ	$1+2\xi$	0	1
$1+2\xi$	$1+2\xi$	$2+2\xi$	2ξ	1	$1+\xi$	2	0	$2+\xi$	ξ
$2+2\xi$	$2+2\xi$	2ξ	$1+2\xi$	2	$2+\xi$	0	1	ξ	$1+\xi$

За таблицу множења је важно да приметимо да је $\xi^2+1=0$, те је $\xi^2=2$.

$\cdot$	0	1	2	ξ	2ξ	$1+\xi$	$2+\xi$	$1+2\xi$	$2+2\xi$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	ξ	2ξ	$1+\xi$	$2+\xi$	$1+2\xi$	$2+2\xi$
2	0	2	1	2ξ	ξ	$2+2\xi$	$1+2\xi$	$2+\xi$	$1+\xi$
ξ	0	ξ	2ξ	2	1	$2+\xi$	$2+2\xi$	$1+\xi$	$1+2\xi$
2ξ	0	2ξ	ξ	1	2	$1+2\xi$	$1+\xi$	$2+2\xi$	$2+\xi$
$1+\xi$	0	$1+\xi$	$2+2\xi$	$2+\xi$	$1+2\xi$	2ξ	1	2	ξ
$2+\xi$	0	$2+\xi$	$1+2\xi$	$2+2\xi$	$1+\xi$	1	ξ	2ξ	2
$1+2\xi$	0	$1+2\xi$	$2+\xi$	$1+\xi$	$2+2\xi$	2	2ξ	ξ	1
$2+2\xi$	0	$2+2\xi$	$1+\xi$	$1+2\xi$	$2+\xi$	ξ	2	1	2ξ

78. Показати да је $\alpha=i+\sqrt{3}$ алгебарски над $\mathbb{Q}$. Наћи минимални полином за α и одредити $\frac{1}{\alpha^2-2}$ у облику $p(\alpha)$, где је $p(X)$ полином из $\mathbb{Q}[X]$.

Решење: Из $\alpha=i+\sqrt{3}$ квадрирањем добијамо

$$\alpha^2=-1+2i\sqrt{3}+3,$$

те је

$$\alpha^2-2=2i\sqrt{3}.$$

Поновним квадрирањем добијамо

$$\alpha^4-4\alpha^2+4=-12.$$

Стога је $\alpha^4-4\alpha^2+16=0$ и видимо да је α алгебарски над $\mathbb{Q}$. Покажимо да је $\mu_\alpha=X^4-4X^2+16$ минимални полином за α. Ово ће следити из чињенице да је тај полином нерастављив над $\mathbb{Q}$. Покажимо да он јесте нерастављив над $\mathbb{Q}$.

Пошто је X^4-4X^2+16 полином четвртог степена он се може раставити само на два начина у облику производа полинома мањег степена: као производ полинома степена 1 и полинома степена 3 или као производ два полинома степена 2.

У првом случају би полином имао једну нулу у $\mathbb{Q}$. Нека је то број $\frac{m}{n}$, где је $m \in \mathbb{Z}$, $n \in \mathbb{N}$ и $\mathrm{NZD}(m,n)=1$. Дакле

$$\left(\frac{m}{n}\right)^4 - 4\left(\frac{m}{n}\right)^2 + 16 = 0.$$

Добијамо да је

$$m^4 - 4m^2n^2 + 16n^4 = 0.$$

Уколико је $n \neq 1$, то постоји неки прост број p такав да $p \mid n$. Но, тада из горње једнакости следи да $p \mid m^4$ и како је p прост број добијамо да $p \mid m$ што противречи чињеници да је $\frac{m}{n}$ нескратив разломак.

Дакле, $n=1$. Сада добијамо

$$m^4 - 4m^2 + 16 = 0.$$

Закључујемо да m мора бити паран број: $m = 2m_1$. Дакле

$$16m_1^4 - 16m_1^2 + 16 = 0,$$

те је

$$m_1^4 - m_1^2 + 1 = 0.$$

Но, $m_1^4 - m_1^2 = m_1^2(m_1^2-1) = m_1^2(m_1-1)(m_1+1)$ и видимо да је $m_1^4 - m_1^2$ паран број и он не може бити једнак -1. Закључујемо да полином $X^4 - 4X^2 + 16$ нема нулу у $\mathbb{Q}$.

Остаје друга могућност — да је X^4-4X^2+16 производ два полинома степена 2 који су оба у $\mathbb{Q}[X]$. Можемо претпоставити да су оба монична. Наиме, ако је

$$X^4 - 4X^2 + 16 = (pX^2 + qX + r)(sX^2 + tX + u),$$

где $p,q,r,s,t,u \in \mathbb{Q}$ онда је $ps = 1$, а

$$(pX^2 + qX + r)(sX^2 + tx + u) = \left(X^2 + \frac{q}{p}X + \frac{r}{p}\right)\left(psX^2 + ptX + pu\right) = (X^2 + aX + b)(X^2 + cX + d),$$

где $a,b,c,d \in \mathbb{Q}$. Дакле, претпоставимо да је

$$X^4 - 4X^2 + 16 = (X^2 + aX + b)(X^2 + cX + d) = X^4 + (a+c)X^3 + (b + ac + d)X^2 + (ad + bc)X + ad,$$

где $a,b,c,d \in \mathbb{Q}$. Тада важе следеће једнакости:

$$\begin{aligned} a + c &= 0 \\ b + ac + d &= -4 \\ ad + bc &= 0 \\ bd &= 16 \end{aligned}$$

Из прве једначине добијамо да је $c = -a$, те је:

$$\begin{aligned} b - a^2 + d &= -4 \\ a(d-b) &= 0 \\ bd &= 16 \end{aligned}$$

Из $a(d-b) = 0$ следи да је $a = 0$ или $d = b$.

Претпоставимо да је $a = 0$. Добијамо

$$\begin{aligned} b + d &= -4 \\ bd &= 16 \end{aligned}$$

Ако је $b = -2 - t$ за неки $t \in \mathbb{Q}$, онда из прве једнакости добијамо да је $d = -2 + t$, а из друге онда да је $(-2-t)(-2+t) = 16$, те је $4 - t^2 = 16$ и мора бити $t^2 = -12$, што није могуће, јер је t реалан број. Закључујемо да је $a \neq 0$.

Остаје могућност $d = b$. Добијамо

$$\begin{aligned} 2b - a^2 &= -4 \\ b^2 &= 16 \end{aligned}$$

Дакле, $b \in \{-4, 4\}$. Уколико је $b = -4$ из прве једнакости добијамо да је $-8 - a^2 = -4$, па је $a^2 = -4$, што није могуће јер је $a \in \mathbb{Q} \subseteq \mathbb{R}$. Остаје могућност $b = 4$. Тада је $8 - a^2 = -4$, па је $a^2 = 12$, те је $(a/2)^2 = 3$ и добили бисмо да је $\sqrt{3} \in \mathbb{Q}$.

Закључујемо да полином $X^4 - 4X^2 + 16$ није растављив над $\mathbb{Q}$, те је он заиста минимални полином за елемент α.

Из теоријског дела знамо да постоје јединствено одређени рационални бројеви a, b, c, d такви да је

$$\frac{1}{\alpha^2 - 2} = a + b\alpha + c\alpha^2 + d\alpha^3.$$

Тада је

$$(a + b\alpha + c\alpha^2 + d\alpha^3)(\alpha^2 - 2) = 1.$$

Добијамо да је

$$d\alpha^5 + c\alpha^4 + (b - 2d)\alpha^3 + (a - 2c)\alpha^2 - 2b\alpha - 2a - 1 = 0.$$

Из једнакости $\alpha^4 = 4\alpha^2 - 16$ добијамо $\alpha^5 = 4\alpha^3 - 16\alpha$. Заменом у горњој једнакости добијамо:

$$d(4\alpha^3 - 16\alpha) + c(4\alpha^2 - 16) + (b - 2d)\alpha^3 + (a - 2c)\alpha^2 - 2b\alpha - 2a - 1 = 0.$$

Сређивањем се добија:

$$(b + 2d)\alpha^3 + (a + 2c)\alpha^2 + (-2b - 16d)\alpha + (-2a - 16c - 1) = 0.$$

Добијамо систем једначина

$$\begin{aligned} b + 2d &= 0 \\ a + 2c &= 0 \\ -2b - 16d &= 0 \\ -2a - 16c - 1 &= 0 \end{aligned}$$

Приметимо да се он састоји од два система по две непознате

$$\begin{aligned} b + 2d &= 0 \\ -2b - 16d &= 0 \end{aligned}$$

и

$$\begin{aligned} a + 2c &= 0 \\ -2a - 16c &= 1 \end{aligned}$$

Ови системи се лако решавају: $b = d = 0$, $a = \frac{1}{6}$, $c = -\frac{1}{12}$. Дакле,

$$\frac{1}{\alpha^2 - 2} = \frac{1}{6} - \frac{1}{12}\alpha^2.$$

У школи су нас учили да на крају треба проверити резултат ☺ :

$$\begin{aligned} \left(\frac{1}{6} - \frac{1}{12}\alpha^2\right)(\alpha^2 - 2) &= \frac{1}{6}\alpha^2 - \frac{1}{3} - \frac{1}{12}\alpha^4 + \frac{1}{6}\alpha^2 \\ &= \frac{1}{6}\alpha^2 - \frac{1}{3} - \frac{1}{12}(4\alpha^2 - 16) + \frac{1}{6}\alpha^2 \\ &= \left(\frac{1}{6} - \frac{4}{12} + \frac{1}{6}\right)\alpha^2 + \left(-\frac{1}{3} + \frac{16}{12}\right) \\ &= 1. \end{aligned}$$

79. Урадити све из претходног задатка за елемент $\alpha = \sqrt{5} - \sqrt{3}$.

Решење: У овом решењу нећемо толико детаљно све образлагати.

$$\alpha^2 = (\sqrt{5} - \sqrt{3})^2 = 5 - 2\sqrt{15} + 3 = 8 - 2\sqrt{15}$$

Дакле

$$\alpha^2 - 8 = -2\sqrt{15}.$$

Квадрирањем добијамо:

$$\alpha^4 - 16\alpha^2 + 64 = 60,$$

те је

$$\alpha^4 - 16\alpha^2 + 4 = 0.$$

Дакле, α је заиста алгебарски над $\mathbb{Q}$. Покажимо да је $X^4 - 16X^2 + 4$ минимални полином за α над $\mathbb{Q}$. Наравно, то се своди на то да покажемо да је овај полином нерастављив.

Уколико је $\frac{m}{n}$, где је $m \in \mathbb{Z}$, $n \in \mathbb{N}$ и $\mathrm{NZD}(m, n) = 1$, нула полинома $X^4 - 16X^2 + 4$, онда је

$$\frac{m^4}{n^4} - 16\frac{m^2}{n^2} + 4 = 0,$$

те је

$$m^4 - 16m^2n^2 + 4n^2 = 0.$$

Уколико је $n > 1$, постоји прост број p који дели n. Но, из последње једнакости се тада добија да $p \mid m$, што противречи чињеници да је $\mathrm{NZD}(m, n) = 1$.

За $n = 1$ добијамо да је

$$m^4 - 16m^2 + 4 = 0.$$

Дакле, m^4 је паран број, па онда мора то бити и m: $m = 2m_1$ за неки $m_1 \in \mathbb{Z}$ и добијамо:

$$16m_1^4 - 64m_1^2 + 4 = 0.$$

Одавде следи да је

$$4m_1^4 - 16m_1^2 + 1 = 0,$$

што је очигледно немогуће, јер је број $4m_1^4 - 16m_1^2$ паран.

Претпоставимо да $X^4 - 16X^2 + 4$ има факторизацију у облику производа два полинома степена 2 из $\mathbb{Q}[X]$:

$$X^4 - 16X^2 + 4 = (X^2 + aX + b)(X^2 + cX + d).$$

Тада је

$$\begin{aligned} a + c &= 0 \\ b + ac + d &= -16 \\ ad + bc &= 0 \\ bd &= 4. \end{aligned}$$

Дакле, $c = -a$ и

$$\begin{aligned} b - a^2 + d &= -16 \\ a(d - b) &= 0 \\ bd &= 4. \end{aligned}$$

Ако је $a = 0$ онда је

$$\begin{aligned} b + d &= -16 \\ bd &= 4. \end{aligned}$$

Уколико је $b = -8 - t$ за неки $t \in \mathbb{Q}$, онда је $d = -8 + t$ и $(-8 - t)(-8 + t) = 4$, тј. $64 - t^2 = 4$, те је $t^2 = 60$ и $(t/2)^2 = 15$. Добили бисмо тако да $\sqrt{15} \in \mathbb{Q}$.

Нека је $\sqrt{15} = \frac{m}{n}$, где $m \in \mathbb{Z}$, $n \in \mathbb{N}$, при чему је $\text{NZD}(m,n) = 1$. Тада је $m^2 = 15n^2$, те $3 \mid m^2$ и пошто је 3 прост број, закључујемо да $3 \mid m$. Дакле, $m = 3m_1$ за неки $m_1 \in \mathbb{Z}$ и $9m_1^2 = 15n^2$, те је $3m_1^2 = 5n^2$. Дакле, $3 \mid 5n^2$ те мора бити $3 \mid n$. Но, уз $3 \mid m$, добијамо да m и n нису узајамно прости и ова контрадикција показује да $\sqrt{15} \notin \mathbb{Q}$.

Дакле, $a \neq 0$, па мора бити $d = b$. Добијамо

$$2b - a^2 = -16$$
$$b^2 = 4.$$

Уколико је $b = 2$, из прве једнакости се добија да је $a^2 = 20$, те је $(a/2)^2 = 5$ и следило би да је $\sqrt{5} \in \mathbb{Q}$. Покажите да ово није тачно.

Уколико је $b = -2$, из прве једнакости се добија да је $a^2 = 12$, те је $(a/2)^2 = 3$ и добили бисмо да је $\sqrt{3} \in \mathbb{Q}$, што није тачно.

Дакле, добили смо заиста да $X^4 - 16X^2 + 4$ није растављив над $\mathbb{Q}$, те је то минимални полином елемента α.

Да бисмо одредили $\frac{1}{\alpha^2-2}$ у облику $p(\alpha)$ можемо поступити као и у претходном примеру, али можемо то урадити и другачије.

Приметимо да је $(\alpha^2-2)^2 = \alpha^4 - 4\alpha^2 + 4$, а ми знамо да је $\alpha^4 - 16\alpha^2 + 4 = 0$. Из ове две једнакости добијамо да је

$$(\alpha^2-2)^2 = 12\alpha^2,$$

те је

$$\frac{12\alpha^2}{\alpha^2-2} = \alpha^2 - 2.$$

Дакле,

$$\alpha^2 - 2 = \frac{12\alpha^2}{\alpha^2-2} = \frac{12\alpha^2 - 12\cdot 2 + 12\cdot 2}{\alpha^2-2} = 12 + \frac{24}{\alpha^2-2}.$$

Дакле,

$$\frac{24}{\alpha^2-2} = \alpha^2 - 14,$$

те је

$$\frac{1}{\alpha^2-2} = \frac{1}{24}(\alpha^2 - 14).$$

Провера:

$$\frac{1}{24}(\alpha^2-14)\cdot(\alpha^2-2) = \frac{1}{24}(\alpha^4 - 14\alpha^2 - 2\alpha^2 + 28) = \frac{1}{24}(\alpha^4 - 16\alpha^2 + 28) = \frac{1}{24}(\underbrace{\alpha^4 - 16\alpha^2 + 4}_{=0} + 24) = \frac{24}{24} = 1.$$

80. Урадити све из претходног задатка за елемент $\alpha = \sqrt{2+\sqrt{3}}$.

Решење:

$$\alpha^2 = 2 + \sqrt{3}$$
$$(\alpha^2-2)^2 = 3$$

Дакле, $\alpha^4 - 4\alpha^2 + 1 = 0$, те је α алгебарски над $\mathbb{Q}$. Доказујемо да је полином $X^4 - 4X^2 + 1$ нерастављив над $\mathbb{Q}$. Уколико је $\frac{m}{n}$ нерастављив разломак који је нула полинома $X^4 - 4X^2 + 1$, добијамо

$$\frac{m^4}{n^4} - 4\frac{m^2}{n^2} + 1 = 0,$$

те је

$$m^4 - 4m^2n^2 + n^4 = 0.$$

Уколико је $n > 1$ и p прост број који дели n, онда $p \mid m$ што противречи претпоставци да је $\frac{m}{n}$ нескратив разломак. Дакле, наведени полином нема нулу у $\mathbb{Q}$.

Уколико је

$$X^4 - 4X^2 + 1 = (X^2 + aX + b)(X^2 + cX + d),$$

за неке $a, b, c, d \in \mathbb{Q}$, добијамо да је

$$\begin{aligned} a + c &= 0 \\ b + ac + d &= -4 \\ ad + bc &= 0 \\ bd &= 1. \end{aligned}$$

Дакле, $c = -a$ и

$$\begin{aligned} b - a^2 + d &= -4 \\ a(d - b) &= 0 \\ bd &= 1. \end{aligned}$$

Ако је $a = 0$, онда је

$$\begin{aligned} b + d &= -4 \\ bd &= 1. \end{aligned}$$

Ако је $b = -4 - t$ за неки $t \in \mathbb{Q}$, онда је $d = -4 + t$, па је $1 = bd = (-4 - t)(-4 + t) = 16 - t^2$. Стога је $t^2 = 15$, што није могуће за рационалан број t. Наиме, ако је $t = \frac{m}{n}$ нескратив разломак, добија се да је $m^2 = 15n^2$. Како $3 \mid 15n^2$, то $3 \mid m^2$, па $3 \mid m$. Дакле, $m = 3m_1$ за неки $m_1 \in \mathbb{Z}$. Сада је $9m_1^2 = 15n^2$, те је $3m_1^2 = 5n^2$ и $3 \mid 5n^2$. Како је 3 прост број, добијамо да $3 \mid n$, што противречи претпоставци да је разломак $\frac{m}{n}$ нескратив.

Остаје могућност да је $d = b$. Тада је

$$\begin{aligned} 2b - a^2 &= -4 \\ b^2 &= 1. \end{aligned}$$

Уколико је $b = 1$, добијамо да је $a^2 = 6$. Као и у претходним случајевима, лако се показује да то није могуће за $a \in \mathbb{Q}$. Уколико је $b = -1$, добија се да је $a^2 = 2$, па би $\sqrt{2}$ био рационалан број.

Дакле, полином $X^4 - 4X^2 + 1$ је нерастављив над $\mathbb{Q}$, те је он минимални полином елемента α.

Знамо да је $\alpha^4 - 4\alpha^2 + 1 = 0$. Стога је

$$(\alpha^2 - 2)^2 = \alpha^4 - 4\alpha^2 + 4 = (\alpha^4 - 4\alpha^2 + 1) + 3 = 3.$$

Одавде непосредно добијамо да је

$$\frac{1}{\alpha^2 - 2} = \frac{1}{3}(\alpha^2 - 2).$$

81. Наћи α тако да је $\mathbb{Q}(i, \sqrt{5}) = \mathbb{Q}(\alpha)$.

Решење: Покажимо да је $\alpha = i + \sqrt{5}$ тражени елемент.

$$\begin{aligned} \alpha^3 &= i^3 + 3i^2\sqrt{5} + 3i(\sqrt{5})^2 + (\sqrt{5})^3 \\ &= -i - 3\sqrt{5} + 15i + 5\sqrt{5} \\ &= 14i + 2\sqrt{5} \\ &= 2(i + \sqrt{5}) + 12i \\ &= 2\alpha + 12i. \end{aligned}$$

Добијамо да је

$$i = \frac{1}{12}(\alpha^3 - 2\alpha) \in \mathbb{Q}(\alpha).$$

Но, тада је и

$$\sqrt{5} = \alpha - i = \alpha - \frac{1}{12}(\alpha^3 - 2\alpha) \in \mathbb{Q}(\alpha).$$

Дакле, како $i, \sqrt{5} \in \mathbb{Q}(\alpha)$, добијамо да је $\mathbb{Q}(i, \sqrt{5}) \subseteq \mathbb{Q}(\alpha)$. Обратна инклузија је јасна, јер је

$$\alpha = i + \sqrt{5} \in \mathbb{Q}(i, \sqrt{5}),$$

па је и $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(i, \sqrt{5})$.

82. Наћи α тако да је $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\alpha)$.

Решење: Показаћемо да за $\alpha = \sqrt{5} + \sqrt{7}$ важи: $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\alpha)$. Како $\alpha \in \mathbb{Q}(\sqrt{5}, \sqrt{7})$, инклузија $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{5}, \sqrt{7})$ јесте испуњена.

$$\begin{aligned}
\alpha^3 &= (\sqrt{5})^3 + 3(\sqrt{5})^2\sqrt{7} + 3\sqrt{5}(\sqrt{7})^2 + (\sqrt{7})^3 \\
&= 5\sqrt{5} + 15\sqrt{7} + 21\sqrt{5} + 7\sqrt{7} \\
&= 26\sqrt{5} + 22\sqrt{7} \\
&= 22(\sqrt{5} + \sqrt{7}) + 4\sqrt{5} \\
&= 22\alpha + 4\sqrt{5}.
\end{aligned}$$

Дакле,

$$\sqrt{5} = \frac{1}{4}(\alpha^3 - 22\alpha) \in \mathbb{Q}(\alpha).$$

Тада је и

$$\sqrt{7} = \alpha - \sqrt{5} = \alpha - \frac{1}{4}(\alpha^3 - 22\alpha) \in \mathbb{Q}(\alpha).$$

Како $\sqrt{5}, \sqrt{7} \in \mathbb{Q}(\alpha)$, добијамо да је и $\mathbb{Q}(\sqrt{5}, \sqrt{7}) \subseteq \mathbb{Q}(\alpha)$.

83. Наћи коренско поље K полинома $X^4 + 2X^2 - 15 \in \mathbb{Q}[X]$ и одредити елемент α за који је $K = \mathbb{Q}(\alpha)$.

Решење:

$$\begin{aligned}
X^4 + 2X^2 - 15 &= (X^2 + 1)^2 - 1 - 15 \\
&= (X^2 + 1)^2 - 16 \\
&= (X^2 + 1)^2 - 4^2 \\
&= (X^2 + 1 - 4)(X^2 + 1 + 4) \\
&= (X^2 - 3)(X^2 + 5) \\
&= (X - \sqrt{3})(X + \sqrt{3})(X - i\sqrt{5})(X + i\sqrt{5})
\end{aligned}$$

Закључујемо да је коренско поље $K = \mathbb{Q}(\sqrt{3}, i\sqrt{5})$. Покажимо да је $\alpha = \sqrt{3} + i\sqrt{5}$ такав елемент да је $K = \mathbb{Q}(\alpha)$. Урадићемо то нешто другачије него у претходним примерима. Приметимо да је

$$\alpha \cdot \overline{\alpha} = |\alpha^2| = (\sqrt{3})^2 + (\sqrt{5})^2 = 8 \in \mathbb{Q}.$$

Дакле, $\overline{\alpha} = \frac{8}{\alpha} \in \mathbb{Q}(\alpha)$. Но, из чињенице да $\alpha, \overline{\alpha} \in \mathbb{Q}(\alpha)$, следи да и

$$\sqrt{3} = \frac{1}{2}(\alpha + \overline{\alpha}) \in \mathbb{Q}(\alpha),$$

$$i\sqrt{5} = \frac{1}{2}(\alpha - \overline{\alpha}) \in \mathbb{Q}(\alpha),$$

Дакле, $\sqrt{3}$, $i\sqrt{5} \in \mathbb{Q}(\alpha)$, па је онда и $K = \mathbb{Q}(\sqrt{3}, i\sqrt{5}) \subseteq \mathbb{Q}(\alpha)$. Но, јасно је да је $\alpha \in K$, те закључујемо да је заиста $K = \mathbb{Q}(\alpha)$.

84. Наћи коренско поље K полинома $X^4 - 12X^2 + 9$ и одредити елемент α за који је $K = \mathbb{Q}(\alpha)$.

Решење:

$$\begin{aligned} X^4 - 12X^2 + 9 &= (X^2 - 6)^2 - 36 + 9 \\ &= (X^2 - 6)^2 - 27 \\ &= (X^2 - 6)^2 - (3\sqrt{3})^2 \\ &= (X^2 - 6 - 3\sqrt{3})(X^2 - 6 + 3\sqrt{3}) \\ &= (X^2 - (6 + 3\sqrt{3}))(X^2 - (6 - 3\sqrt{3})) \\ &= \left(X^2 - \left(\sqrt{6 + 3\sqrt{3}}\right)^2\right)\left(X^2 - \left(\sqrt{6 - 3\sqrt{3}}\right)^2\right). \end{aligned}$$

Коначно

$$X^4 - 12X^2 + 9 = \left(X - \sqrt{6 + 3\sqrt{3}}\right)\left(X + \sqrt{6 + 3\sqrt{3}}\right)\left(X - \sqrt{6 - 3\sqrt{3}}\right)\left(X + \sqrt{6 - 3\sqrt{3}}\right).$$

Дакле, коренско поље K је дато са: $K = \mathbb{Q}\left(\sqrt{6 + 3\sqrt{3}}, \sqrt{6 - 3\sqrt{3}}\right)$. Но, приметимо да је

$$\sqrt{6 + 3\sqrt{3}} \cdot \sqrt{6 - 3\sqrt{3}} = \sqrt{36 - (3\sqrt{3})^2} = \sqrt{36 - 27} = 9.$$

Стога је

$$\sqrt{6 - 3\sqrt{3}} = \frac{9}{\sqrt{6 + 3\sqrt{3}}} \in \mathbb{Q}\left(\sqrt{6 + 3\sqrt{3}}\right),$$

те можемо да закључимо да је $K = \mathbb{Q}\left(\sqrt{6 + 3\sqrt{3}}\right)$.