Примерни задачи за групи по Висша Алгебра 1

Теорема 1. *(i) Ако $a \in \mathbb{Z} \setminus \{0\}$ и $n \in \mathbb{N} \setminus \{1\}$ са взаимно прости, то сравнението $ax \equiv b \pmod{n}$ има единствено решение $x \equiv x_0 \pmod{n}$ за някое $0 \leq x_0 \leq n-1$.*

(ii) Ако най-големият общ делител $d = (a, n) \in \mathbb{N} \setminus \{1\}$ на $a \in \mathbb{Z} \setminus \{0\}$ и $n \in \mathbb{N} \setminus \{1\}$ не дели $b \in \mathbb{Z}$, то сравнението $ax \equiv b \pmod{n}$ няма решение.

(iii) Ако най-големият общ делител $d = (a, n) \in \mathbb{N} \setminus \{1\}$ на $a \in \mathbb{Z} \setminus \{0\}$ и $n \in \mathbb{N} \setminus \{1\}$ дели $b \in \mathbb{Z}$, то сравнението $ax \equiv b \pmod{n}$ има d решения $x_i \equiv x_0 + i\frac{n}{d} \pmod{n}$, $0 \leq i \leq d-1$, където $x_0 \left(\bmod \ \frac{n}{d}\right)$ е единственото решение на редуцираното сравнение $\left(\frac{a}{d}\right) x \equiv \left(\frac{b}{d}\right) \left(\bmod \frac{n}{d}\right)$ с $\left(\frac{a}{d}, \frac{n}{d}\right) = 1$.

Доказателство: (i) По Тъждеството на Безу съществуват $u, v \in \mathbb{Z}$, така че $au + nv = 1$. След почленно умножение с b получаваме $abu + bnv = b$. Тогава $x \equiv bu \pmod{n}$ е решение на $ax \equiv b \pmod{n}$.

Произволно решение $x_1 \pmod{n}$ на $ax \equiv b \pmod{n}$ дава решение $x_1 - bu \pmod{n}$ на хомогенното линейно сравнение $ax \equiv 0 \pmod{n}$. Съгласно взаимната простота на a и n, от равенството $a(x_1 - bu) = nz$ за някое $z \in \mathbb{Z}$ следва, че n дели $x_1 - bu$ или $x_1 \equiv bu \pmod{n}$. С други думи, $bu \pmod{n}$ е единственото решение на $ax \equiv b \pmod{n}$.

(ii) Ако съществува $x_0 \in \mathbb{Z}$ с $ax_0 \equiv b \pmod{n}$, то $ax_0 - b = ny_0$ за някое $y_0 \in \mathbb{Z}$. Затова $d = (a, n)$ трябва да дели $b = ax_0 - ny_0$.

(iii) Ако $\frac{a}{d}x_0 - \frac{b}{d} = \frac{n}{d}y_0$ за някои $x_0, y_0 \in \mathbb{Z}$, то за всяко $0 \leq i \leq d-1$ е в сила $a\left(x_0 + i\frac{n}{d}\right) = b + ny_0 + ai\frac{n}{d} \equiv b \pmod{n}$ и $x_i \equiv x_0 + i\frac{n}{d} \left(\bmod \ \frac{n}{d}\right)$ са решения на сравнението $ax \equiv b \pmod{n}$. Тези решения са различни, защото n не дели $(i-j)\frac{n}{d}$ за $\forall 0 \leq i < j \leq d-1$.

Обратно, ако $ax_1 - b = ny_1$ за някои $x_1, y_1 \in \mathbb{Z}$, то $\left(\frac{a}{d}\right) x_1 - \frac{b}{d} = \frac{n}{d}y_1$ или $x_1 \left(\bmod \ \frac{n}{d}\right) \equiv x_0 \left(\bmod \ \frac{n}{d}\right)$ е единственото решение на сравнението $\left(\frac{a}{d}\right) x \equiv \left(\frac{b}{d}\right) \left(\bmod \ \frac{n}{d}\right)$. Но условието $x_1 \equiv x_0 \left(\bmod \ \frac{n}{d}\right)$ е еквивалентно на $x_1 - x_0 = \frac{n}{d}z$ за някое $z \in \mathbb{Z}$ и остатъкът на $\frac{n}{d}z$ при деление с n зависи точно от остатъка на z при деление с d. По този начин, $x_1 \equiv x_0 + \frac{n}{d}z \pmod{n}$ за някое $0 \leq z \leq d-1$.

Задача 2. *Да се решат сравненията*

(i) $2x \equiv 3 \pmod{5}$*;*

(ii) $2x \equiv 1 \pmod{4}$*;*

(iii) $6x \equiv 3 \pmod{9}$*;*

(iv) $11x \equiv 7 \pmod{15}$.

Решение: (i) По метода на Ойлер, остатъкът $x \pmod{5}$ е решение на $2x \equiv 3 \pmod{5}$ точно когато съществува $y \in \mathbb{Z}$, така че $2x - 3 = 5y$. Коефициентът 2 на неизвестното x е по-малък по модул от коефициента 5 на неизвестното y и затова представяме уравнението във вида

$$x = \frac{5y+3}{2} = 2y + 1 + \frac{y+1}{2}. \tag{1}$$

Оттук 2 дели $y+1$ или $y = 2z - 1$ за $z \in \mathbb{Z}$ е нечетно цяло число. Замествайки в (1) получаваме $x = 5z - 1$ или $2x \equiv 3 (\bmod\ 5)$ има единствено решение $x \equiv -1 (\bmod\ 5)$.

(ii) Сравнението $2x \equiv 1 (\bmod\ 4)$ е еквивалентно на уравнението $2x - 1 = 4y$ с две неизвестни x и y, което се свежда до $1 = 2x - 4y = 2(x - 2y)$ и няма решение в цели числа.

(iii) Сравнението $6x \equiv 3 (\bmod\ 9)$ има три решения, защото коефициентът 6 на неизвестния остатък $x (\bmod\ 9)$ и модулът 9 имат най-голям общ делител $(6, 9) = 3$, който дели свободния член 3. Решаваното сравнение се свежда до уравнението $6x - 3 = 9y$. След съкращаване на 3 получаваме $2x - 1 = 3y$ или

$$x = \frac{3y+1}{2} = y + \frac{y+1}{2}. \tag{2}$$

Оттук $y + 1$ е четно или $y = 2z - 1$ е нечетно. Замествайки в (2) получаваме $x = 3z - 1$ или $x \equiv -1 + k\frac{9}{3} = 3k - 1 (\bmod\ 9)$ за $0 \leq k \leq 2$. С други думи, решенията на сравнението $6x \equiv 3 (\bmod\ 9)$ са $x_1 \equiv -1 (\bmod\ 9)$, $x_2 \equiv 2 (\bmod\ 9)$ и $x_3 \equiv 5 (\bmod\ 9)$.

(iv) Ако $11x - 7 = 15y$ за цяло число y, то

$$x = \frac{15y+7}{11} = y + 1 + \frac{4y-4}{11}.$$

Полагаме

$$z := \frac{4y-4}{11}$$

и изразяваме

$$y = \frac{11z+4}{4} = 3z + 1 - \frac{z}{4}.$$

Ако

$$t := \frac{z}{4} \in \mathbb{Z},$$

то $z = 4t$, $y = 11t + 1$, $x = 15t + 2$. Единственото решение на $11x \equiv 7 (\bmod\ 15)$ е $x \equiv 2 (\bmod\ 15)$.

Задача 3. *В множеството* $\mathbb{R}^2$ *на наредените двойки реални числа е зададена операцията*

$$(x_1, y_1) \circ (x_2, y_2) = (x_1 + x_2, \quad y_1 e^{-x_2} + y_2 e^{x_1}).$$

Да се докаже, че $(\mathbb{R}^2, \circ)$ *е група.*

Решение: Асоциативният закон за $\circ$ гласи, равенството на наредените двойки реални числа $A = [(x_1, y_1) \circ (x_2, y_2)] \circ (x_3, y_3)$ и $B = (x_1, y_1) \circ [(x_2, y_2) \circ (x_3, y_3)]$ за $\forall (x_i, y_i) \in \mathbb{R}^2$. Наистина,

$$A = (x_1 + x_2, \ \ y_1 e^{-x_2} + y_2 e^{x_1}) \circ (x_3, y_3) = ((x_1 + x_2) + x_3, \ \ (y_1 e^{-x_2} + y_2 e^{x_1}) e^{-x_3} + y_3 e^{x_1 + x_2}) =$$

$$= (x_1 + x_2 + x_3, \ \ y_1 e^{-x_2 - x_3} + y_2 e^{x_1 - x_3} + y_3 e^{x_1 + x_2})$$

съвпада с

$$B = (x_1, y_1) \circ (x_2 + x_3, \ \ y_2 e^{-x_3} + y_3 e^{x_2}) = (x_1 + (x_2 + x_3), \ \ y_1 e^{-(x_2 + x_3)} + (y_2 e^{-x_3} + y_3 e^{x_2}) e^{x_1}) =$$

$$= (x_1 + x_2 + x_3, \quad y_1 e^{-x_2 - x_3} + y_2 e^{x_1 - x_3} + y_3 e^{x_1 + x_2}).$$

Търсим неутрален елемент $(r, s) \in (\mathbb{R}^2, \circ)$, така че

$$(x, y) \circ (r, s) = (x, y) = (r, s) \circ (x, y) \quad \text{за} \quad \forall (x, y) \in \mathbb{R}^2.$$

Вземайки предвид, че $(a_1, b_1) = (a_2, b_2)$ за $(a_i, b_i) \in \mathbb{R}^2$ е изпълнено точно когато поотделно $a_1 = a_2$ и $b_1 = b_2$ са равни, получаваме

$$x + r = x = r + x \quad \text{и} \quad ye^{-r} + se^{x} = y = se^{-x} + ye^{r} \quad \text{за} \quad \forall (x, y) \in \mathbb{R}^2.$$

Оттук следва, че $r = 0 \in \mathbb{R}$, $s = 0$ и $(0, 0) \in \mathbb{R}^2$ е неутралният елемент на $(\mathbb{R}^2, \circ)$.

За произволен елемент $(x, y) \in \mathbb{R}^2$ търсим $(x, y)^{-1} = (z, t) \in \mathbb{R}^2$, така че

$$(x, y) \circ (z, t) = (0, 0) = (z, t) \circ (x, y).$$

С други думи,

$$x + z = 0 = z + x \quad \text{и} \quad ye^{-z} + te^{x} = 0 = te^{-x} + ye^{z},$$

откъдето $z = -x$, $t = -y$ и $(x, y)^{-1} = (-x, -y)$. Следователно $(\mathbb{R}^2, \circ)$ е група.

Задача 4. *Да се докаже, че подмножествата*

$$G_1 = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in \mathbb{R} \right\} \quad \text{\textit{и}}$$

$$G_2 = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \;\middle|\; a \in \mathbb{R}, \quad b \in \mathbb{R}^* \right\}$$

на общата линейна група

$$GL_2(\mathbb{R}) = \left\{ A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \;\middle|\; a_{ij} \in \mathbb{R}, \quad \det A \neq 0 \right\}$$

са подгрупи, а подмножеството

$$G_3 = \left\{ \begin{pmatrix} -1 & a \\ 0 & -1 \end{pmatrix} \;\middle|\; a \in \mathbb{R} \right\} \subset GL_2(\mathbb{R})$$

не е подгрупа.

Решение: Подмножеството $G_i \subset GL_2(\mathbb{R})$ е подгрупа тогава и само тогава, когато за $\forall A_1, A_2 \in G_i$ е в сила $A_1^{-1}, A_1 A_2 \in G_i$.

От

$$\begin{pmatrix} 1 & a_1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a_1 \\ 0 & 1 \end{pmatrix} \in G_1, \quad \begin{pmatrix} 1 & a_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_1 + a_2 \\ 0 & 1 \end{pmatrix} \in G_1$$

за $\forall a_i \in \mathbb{R}$ следва, че G_1 е подгрупа на $GL_2(\mathbb{R})$.

Съгласно

$$\begin{pmatrix} 1 & a_1 \\ 0 & b_1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -\frac{a_1}{b_1} \\ 0 & \frac{1}{b_1} \end{pmatrix} \in G_2, \quad \begin{pmatrix} 1 & a_1 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} 1 & a_2 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} 1 & a_2 + a_1 b_2 \\ 0 & b_1 b_2 \end{pmatrix} \in G_2$$

за $\forall a_i \in \mathbb{R}$, $\forall b_i \in \mathbb{R}^*$, подмножеството $G_2 \subset GL_2(\mathbb{R})$ е подгрупа.

От

$$\begin{pmatrix} -1 & a_1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & a_2 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -a_1 - a_2 \\ 0 & 1 \end{pmatrix} \notin G_4$$

за произволни $a_i \in \mathbb{R}$ получаваме, че G_3 не е подгрупа на $GL_2(\mathbb{R})$.

Задача 5. *Да се определи кои от изображенията $f : (\mathbb{C}^*, .) \to (\mathbb{R}^*,)$ са хомоморфизми на групи:*

(i) $f(z) = |z|$;

(ii) $f(z) = 2|z|$;

(iii) $f(z) = \frac{1}{|z|}$;

(iv) $f(z) = 1 + |z|$;

(v) $f(z) = |z|^2$;

(vi) $f(z) = 1$;

(vii) $f(z) = 2$.

Решение: (i) От $f(z_1 z_2) = |z_1 z_2| = |z_1||z_2| = f(z_1) f(z_2)$ за $\forall z_1, z_2 \in \mathbb{C}^*$ следва, че $f(z) = |z|$ е хомоморфизъм на $\mathbb{C}^*$ в $\mathbb{R}^*$.

(ii) Понеже $f(z_1) f(z_2) = (2|z_1|)(2|z_2|) = 2(2|z_1 z_2|) = 2f(z_1 z_2) \neq f(z_1 z_2) \in \mathbb{R}^*$ за някои (всъщност, за всички) $z_1, z_2 \in \mathbb{C}^*$, изображението $f(z) = 2|z|$ не е хомоморфизъм на групи.

(iii) Съгласно $f(z_1 z_2) = \frac{1}{|z_1 z_2|} = \frac{1}{|z_1|} . \frac{1}{|z_2|} = f(z_1) f(z_2)$ за $\forall z_1, z_2 \in \mathbb{C}^*$ функцията $f(z) = \frac{1}{|z|}$ е хомоморфизъм на $\mathbb{C}^*$ в $\mathbb{R}^*$.

(iv) От $f(z_1) f(z_2) = (1 + |z_1|)(1 + |z_2|) = 1 + |z_1 z_2| + |z_1| + |z_2| = f(z_1 z_2) + |z_1| + |z_2| > f(z_1 z_2)$ за някои (всъщност, за всички) $z_1, z_2 \in \mathbb{C}^*$ получаваме, че $f(z) = 1 + |z|$ не е хомоморфизъм на $\mathbb{C}^*$ в $\mathbb{R}^*$.

(v) Възоснова на $f(z_1 z_2) = |z_1 z_2|^2 = |z_1|^2 |z_2|^2 = f(z_1) f(z_2)$ за $\forall z_1, z_2 \in \mathbb{C}^*$ функцията $f(z) = |z|^2$ е хомоморфизъм на $\mathbb{C}^*$ в $\mathbb{R}^*$.

(vi) Поради $f(z_1 z_2) = 1 = 1.1 = f(z_1) f(z_2)$ за $\forall z_1, z_2 \in \mathbb{C}^*$ постоянното изображение $f(z) = 1$ е хомоморфизъм на $\mathbb{C}^*$ в $\mathbb{R}^*$.

(vii) Съгласно $f(z_1 z_2) = 2 = \frac{1}{2}.2.2 = \frac{1}{2} f(z_1) f(z_2) \neq f(z_1) f(z_2)$ за за някои (всъщност, за всички) $z_1, z_2 \in \mathbb{C}^*$, постоянното изображение $f(z) = 2$ не е хомоморфизъм на $\mathbb{C}^*$ в $\mathbb{R}^*$.

Задача 6. *Да се докаже, че:*

(i) изображението

$$\varphi_1 : H_1 = \left\{ \left(\begin{array}{cc} 1 & a \\ 0 & 1 \end{array} \right) \quad \middle| \quad a \in \mathbb{R} \right\} \longrightarrow (\mathbb{R}, +),$$

$$\varphi_1 \left(\begin{array}{cc} 1 & a \\ 0 & 1 \end{array} \right) = a$$

на подгрупата H_1 *на* $GL_2(\mathbb{R})$ *в адитивната група на реалните числа е хомоморфизъм на групи;*

(ii) изображението

$$\varphi_2 : H_2 = \left\{ \left(\begin{array}{cc} a & b \\ 0 & 1 \end{array} \right) \quad \middle| \quad a \in \mathbb{R}^*, \quad b \in \mathbb{R} \right\} \longrightarrow (\mathbb{R}^*, .),$$

$$\varphi_2 \left(\begin{array}{cc} a & b \\ 0 & 1 \end{array} \right) = a$$

на подгрупата H_2 *на* $GL_2(\mathbb{R})$ *в мултипликативната група на ненулевите реални числа е хомоморфизъм на групи;*

(iii) изображението

$$\varphi_3 : H_3 = \left\{ \left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \quad \middle| \quad a, c \in \mathbb{R}^*, \quad b \in \mathbb{R} \right\} \longrightarrow (\mathbb{R}^*, .),$$

$$\varphi_3 \left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) = c$$

на подгрупата H_3 *на* $GL_2(\mathbb{R})$ *в мултипликативната група на ненулевите реални числа е хомоморфизъм на групи;*

(iv) изображението

$$\varphi_4 : H_2 = \left\{ \left(\begin{array}{cc} a & b \\ 0 & 1 \end{array} \right) \quad \middle| \quad a \in \mathbb{R}^*, \quad b \in \mathbb{R} \right\} \longrightarrow (\mathbb{R}, +),$$

$$\varphi_4 \left(\begin{array}{cc} a & b \\ 0 & 1 \end{array} \right) = b$$

на подгрупата H_2 *на* $GL_2(\mathbb{R})$ *в адитивната група на реалните числа не е хомоморфизъм на групи.*

Решение: (i) Съгласно

$$\varphi_1 \left(\left(\begin{array}{cc} 1 & a_1 \\ 0 & 1 \end{array} \right) \left(\begin{array}{cc} 1 & a_2 \\ 0 & 1 \end{array} \right) \right) = \varphi_1 \left(\begin{array}{cc} 1 & a_1 + a_2 \\ 0 & 1 \end{array} \right) = a_1 + a_2 =$$

$$= \varphi_1 \left(\begin{array}{cc} 1 & a_1 \\ 0 & 1 \end{array} \right) + \varphi_1 \left(\begin{array}{cc} 1 & a_2 \\ 0 & 1 \end{array} \right) \quad \text{за} \quad \forall a_i \in \mathbb{R},$$

изображението φ_1 е хомоморфизъм на групи.

(ii) От

$$\varphi_2\left(\begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix}\right) = \varphi_2\begin{pmatrix} a_1a_2 & a_1b_2+b_1 \\ 0 & 1 \end{pmatrix} = a_1a_2 =$$

$$= \varphi_2\begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix}\varphi_2\begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix} \quad \text{за} \quad \forall a_i \in \mathbb{R}^*, \quad \forall b_i \in \mathbb{R}$$

следва, че φ_2 е хомоморфизъм на групи.

(iii) Вземайки предвид, че

$$\varphi_3\left(\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}\right) = \varphi_3\begin{pmatrix} a_1a_2 & a_1b_2+b_1c_2 \\ 0 & c_1c_2 \end{pmatrix} = c_1c_2 =$$

$$= \varphi_3\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}\varphi_3\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} \quad \text{за} \quad \forall a_i, c_i \in \mathbb{R}^*, \quad \forall b_i \in \mathbb{R},$$

стигаме до извода, че φ_3 е хомоморфизъм на групи.

(iv) От

$$\varphi_4\left(\begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix}\right) = \varphi_4\begin{pmatrix} a_1a_2 & a_1b_2+b_1 \\ 0 & 1 \end{pmatrix} = a_1b_2+b_1 \neq b_1+b_2 =$$

$$\varphi_4\begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} + \varphi_4\begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix} \quad \text{за} \quad \forall a_1 \in \mathbb{R}^* \setminus \{1\}, \quad \forall a_2 \in \mathbb{R}^*, \quad \forall b_1 \in \mathbb{R}, \quad \forall b_2 \in \mathbb{R}^*$$

следва, че φ_4 не е хомоморфизъм на групи.

Задача 7. *Да се намери реда на елемента g на групата G, ако:*

(а) $g = -\frac{\sqrt{3}}{2} + \frac{1}{2}i$ *и* $G = (\mathbb{C}^*, .)$*;*

(б) $g = -\frac{\sqrt{3}}{2} + \frac{1}{2}i$ *и* $G = (\mathbb{C}, +)$*;*

(в) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$ *и* $G = S_5$*;*

(г) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix}$ *и* $G = S_6$*;*

(д) $g = \begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix}$ *и* $G = GL_2(\mathbb{C})$*;*

(е) $g = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ *и* $G = GL_4(\mathbb{R})$.

Решение: Редът на $g \in G$ е минималното естествено число r с $g^r = e$ за неутралния елемент e на G.

(а) Елементът $g = -\frac{\sqrt{3}}{2} + \frac{1}{2}i = \cos\left(\frac{5\pi}{6}\right) + i\sin\left(\frac{5\pi}{6}\right) \in (\mathbb{C}^*, .)$ е от ред 12, защото $g^m = \cos\left(\frac{5\pi m}{6}\right) + i\sin\left(\frac{5\pi m}{6}\right) = 1$ тогава и само тогава, когато $\frac{5\pi m}{6} = 2k\pi$ за $k \in \mathbb{Z}$. Последното е равносилно на това 12 да дели m, а минималното естествено кратно на 12 е 12.

(б) Същото комплексно число $g = -\frac{\sqrt{3}}{2} + \frac{1}{2}i$ има безкраен ред в $(\mathbb{C}, +)$, защото за $\forall l \in \mathbb{Z} \setminus \{0\}$ е в сила $lg \neq 0$.

(в) След разлагане $g = (45)(123) \in S_5$ в произведение от независими цикли, пресмятаме реда на g като най-малкото общо кратно 6 на дължините 2 и 3 на участващите в разлагането на g цикли.

(г) Пермутацията $g = (12345) \in S_6$ е от ред 5 като цикъл с дължина 5.

(д) От $g^2 = \begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E_2$ следва, че матрицата $E_2 \neq g = \begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix} \in Gl_2(\mathbb{C})$ е елемент от ред 2.

(е) Непосредствено пресмятаме, че

$$g^2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \neq E_4, \quad g^3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \neq E_4,$$

$$g^4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = E_4,$$

така че $g = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \in Gl_4(\mathbb{R})$ е елемент от ред 4.

Задача 8. *Нека G е група, а H е нормална подгрупа на G с индекс $n-1$. Да се докаже, че всеки елемент $g \in G$ от ред n принадлежи на H.*

Решение: Ако $g \in G$ е от ред n, то $g^n = e$ за неутралния елемент $e \in G$. От друга страна фактор-групата G/H е от ред $n-1$, така че $(gH)^{n-1} = g^{n-1}H = H$. В резултат, $g^{n-1} = h \in H$ и $g = (g^{n-1})^{-1} = h^{-1} \in H$.

Задача 9. *Дадена е подгрупата*

$$G = \left\{ \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{Q}^*, \, c \in \mathbb{Q} \right\} < GL_2(\mathbb{Q})$$

на общата линейна група. Да се докаже, че

$$N = \left\{ \begin{pmatrix} a & c \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{Q}^*, \, c \in \mathbb{Q} \right\} \quad \textit{и}$$

$$H=\left\{\left(\begin{array}{cc} b^{-2} & c \\ 0 & b \end{array}\right) \mid b\in\mathbb{Q}^*,\, c\in\mathbb{Q}\right\},$$

са нормални подгрупи на G с фактор-групи $G/N\simeq\mathbb{Q}^*$, $G/H\simeq\mathbb{Q}^*$.

Решение: Детерминантата $\det : G \longrightarrow (\mathbb{Q}^*,.)$ е хомоморфизъм на групи съгласно Теоремата за умножение на детерминанти $\det(AB)=\det(A)\det(B)$ за $\forall A,B\in G$. Образът $\mathrm{im}(\det)=\mathbb{Q}^*$, защото за $\forall q\in\mathbb{Q}^*$ съществува $A(q)=\left(\begin{array}{cc} q & 0 \\ 0 & 1 \end{array}\right)\in G$ с $\det(A(q))=q$. Следователно $\det : G\to(\mathbb{Q}^*,.)$ е епиморфизъм на групи. Съгласно Теоремата за епиморфизмите на групи, ядрото

$$\ker(\det)=\left\{\left(\begin{array}{cc} a & c \\ 0 & b \end{array}\right)\in G \;\middle|\; \det\left(\begin{array}{cc} a & c \\ 0 & b \end{array}\right)=ab=1\right\}=$$

$$=\left\{\left(\begin{array}{cc} a & c \\ 0 & a^{-1} \end{array}\right) \;\middle|\; a\in\mathbb{Q}^*,\quad c\in\mathbb{Q}\right\}=N$$

е нормална подгрупа на G с фактор-група G/N, изоморфна на образа $\mathbb{Q}^*$ на $\det$.

Изображението

$$\varphi : G\longrightarrow(\mathbb{Q}^*,.),$$
$$\varphi\left(\begin{array}{cc} a & c \\ 0 & b \end{array}\right)=ab^2$$

е хомоморфизъм на групи съгласно

$$\varphi\left(\left(\begin{array}{cc} a_1 & c_1 \\ 0 & b_1 \end{array}\right)\left(\begin{array}{cc} a_2 & c_2 \\ 0 & b_2 \end{array}\right)\right)=\varphi\left(\begin{array}{cc} a_1a_2 & a_1c_2+c_1b_2 \\ 0 & b_1b_2 \end{array}\right)=(a_1a_2)(b_1b_2)^2=$$

$$=(a_1b_1^2)(a_2b_2^2)=\varphi\left(\begin{array}{cc} a_1 & c_1 \\ 0 & b_1 \end{array}\right)\varphi\left(\begin{array}{cc} a_2 & c_2 \\ 0 & b_2 \end{array}\right).$$

Образът $\mathrm{im}\varphi=(\mathbb{Q}^*,.)$, защото за $\forall q\in\mathbb{Q}^*$ съществува $A(q)=\left(\begin{array}{cc} q & 0 \\ 0 & 1 \end{array}\right)\in G$ с $\varphi(A(q))=q.1^2=q$. Следователно φ е епиморфизъм на групи. Съгласно Теоремата за епиморфизмите на групи, ядрото

$$\ker\varphi=\left\{\left(\begin{array}{cc} a & c \\ 0 & b \end{array}\right)\in G \;\middle|\; \varphi\left(\begin{array}{cc} a & c \\ 0 & b \end{array}\right)=ab^2=1\right\}=$$

$$=\left\{\left(\begin{array}{cc} b^{-2} & c \\ 0 & b \end{array}\right) \;\middle|\; b\in\mathbb{Q}^*, c\in\mathbb{Q}\right\}=H$$

нормална подгрупа на G и фактор-групата G/H е изоморфна на $\mathrm{im}\varphi=(\mathbb{Q}^*,.)$.

Задача 10. *В множеството*

$$G=\{\,(a,b,c)\mid a,b,c\,\in\mathbb{R}\,\}$$

на наредените тройки реални числа въвеждаме бинарна операция

$$(a_1,b_1,c_1)\circ(a_2,b_2,c_2)=(a_1+a_2,\quad b_1+a_1c_2+b_2,\quad c_1+c_2).$$

Да се докаже, че:

(а) G е група относно $\circ$;

(б) $H = \{\, (0,b,0) \mid b \in \mathbb{R}\,\}$ е нормална подгрупа на G, изоморфна на $(\mathbb{R},+)$, а фактор-групата G/H е изоморфна на адитивната група $(\mathbb{R}^2,+)$ на линейното пространство $\mathbb{R}^2$ на наредените двойки реални числа.

Упътване: (а) Асоциативността на $\circ$ гласи, съвпадението на наредените тройки $A = [(a_1,b_1,c_1)\circ(a_2,b_2,c_2)]\circ(a_3,b_3,c_3)$ и $B = (a_1,b_1,c_1)\circ[(a_2,b_2,c_2)\circ(a_3,b_3,c_3)]$. Това е в сила съгласно

$$A = (a_1+a_2, \quad b_1+a_1c_2+b_2, \quad c_1+c_2)\circ(a_3,b_3,c_3) =$$

$$= ((a_1+a_2)+a_3, \quad (b_1+a_1c_2+b_2)+(a_1+a_2)c_3+b_3, \quad (c_1+c_2)+c_3) =$$

$$= (a_1+a_2+a_3, \quad b_1+b_2+b_3+a_1c_2+a_1c_3+a_2c_3, \quad c_1+c_2+c_3)$$

и

$$B = (a_1,b_1,c_1)\circ(a_2+a_3, \quad b_2+a_2c_3+b_3, \quad c_2+c_3) =$$

$$= (a_1+(a_2+a_3), \quad b_1+a_1(c_2+c_3)+(b_2+a_2c_3+b_3), \quad c_1+(c_2+c_3)) =$$

$$= (a_1+a_2+a_3, \quad b_1+b_2+b_3+a_1c_2+a_1c_3+a_2c_3, \quad c_1+c_2+c_3).$$

Неутралният елемент $e = (e_1,e_2,e_3) \in G$ изпълнява равенствата

$$(a,b,c)\circ(e_1,e_2,e_3) = (a,b,c) = (e_1,e_2,e_3)\circ(a,b,c) \quad \text{за} \quad \forall (a,b,c)\in\mathbb{R}^3.$$

По-точно,

$$\left| \begin{array}{c} a+e_1 = a = e_1+a \\ b+ae_3+e_2 = b = e_2+e_1c+b \\ c+e_3 = c = e_3+c \end{array} \right. .$$

От първото и третото равенство получаваме $e_1 = e_3 = 0$. Заместваме във второто равенство и извеждаме, че $e_2 = 0$. Следователно неутралният елемент на $(G,\circ)$ е $e = (0,0,0)$.

За $\forall (a,b,c)\in G$ търсим $(a,b,c)^{-1} = (x,y,z)\in G$, така че

$$(a,b,c)\circ(x,y,z) = e = (0,0,0) = (x,y,z)\circ(a,b,c).$$

Получаваме системата

$$\left| \begin{array}{c} a+x = 0 = x+a \\ b+az+y = 0 = y+xc+b \\ c+z = 0 = z+c \end{array} \right.$$

за $x,y,z\in\mathbb{R}$. Оттук $x=-a$, $z=-c$ и $b-ac+y=0$ или $y = ac-b$. По този начин, $\forall (a,b,c)\in G$ има обратен $(a,b,c)^{-1} = (-a, \quad ac-b, \quad -c)\in G$ относно $\circ$ и $(G,\circ)$ е група.

(б) Изображението

$$\varphi : G \longrightarrow (\mathbb{R}^2,+),$$

$$\varphi(a,b,c) = (a,c)$$

е хомоморфизъм на групи съгласно

$$\varphi((a_1,b_1,c_1)\circ(a_2,b_2,c_2)) = \varphi(a_1+a_2,\quad b_1+a_1c_2+b_2,\ c_1+c_2) = (a_1+a_2, c_1+c_2) =$$

$$= (a_1,c_1)+(a_2,c_2) = \varphi(a_1,b_1,c_1)+\varphi(a_2,b_2,c_2).$$

Още повече, φ е епиморфизъм на групи, защото $\forall(a,c)\in\mathbb{R}^2$ е от вида $\varphi(a,0,c) = (a,c)\in \mathrm{im}\varphi$. Съгласно Теоремата за епиморфизмите на групи, ядрото

$$\ker\varphi = \{(a,b,c)\in G \mid \varphi(a,b,c)=(a,c)=(0,0)\} = \{(0,b,0)\mid b\in\mathbb{R}\} = H$$

е нормална подгрупа на $(G,\circ)$ с фактор-група G/H, изоморфна на $\mathrm{im}\varphi = (\mathbb{R}^2,+)$.

Съответствието $\psi : H \longrightarrow (\mathbb{R},+)$, $\psi(0,b,0) = b$ за $b\in\mathbb{R}$ е взаимно-еднозначен хомоморфизъм на групи, съгласно

$$\psi((0,b_1,0)\circ(0,b_2,0)) = \psi(0,b_1+b_2,0) = b_1+b_2 = \psi(0,b_1,0)+\psi(0,b_2,0).$$

Задача 11. *Кои от следните двойки пермутации от S_6 са спрегнати:*

(а) $\sigma = \begin{pmatrix} 1&2&3&4&5&6\\ 2&5&4&3&1&6\end{pmatrix}$ *и* $\tau = \begin{pmatrix} 1&2&3&4&5&6\\ 6&5&3&2&4&1\end{pmatrix}$;

(б) $\sigma = \begin{pmatrix} 1&2&3&4&5&6\\ 3&4&1&2&5&6\end{pmatrix}$ *и* $\tau = \begin{pmatrix} 1&2&3&4&5&6\\ 4&6&3&5&1&2\end{pmatrix}$;

Решение: Две пермутации $\sigma,\tau\in S_6$ са спрегнати в S_6 тогава и само тогава, когато имат еднакъв цикличен строеж. Това означава наличие на един и същи брой цикли с една и съща дължина в разлаганията на σ и τ като произведения от независими цикли.

(а) $\sigma = (34)(125)$ и $\tau = (254)(16)$ са спрегнати в S_6 като произведения на два независими цикъла с дължини 2 и 3.

(б) $\sigma = (24)(13)$ и $\tau = (26)(145)$ не са спрегнати в S_6, защото σ е произведение на две независими транспозиции, а τ е произведение на троен цикъл с независима от него транспозиция.

Задача 12. *Да се определи кои от следните пермутации $\sigma\in S_6$ са нечетни:*

(а) $\sigma = \begin{pmatrix} 1&2&3&4&5&6\\ 2&3&1&6&5&4\end{pmatrix}$;

(б) $\sigma = \begin{pmatrix} 1&2&3&4&5&6\\ 1&4&3&2&6&5\end{pmatrix}$;

Решение: Ако $\sigma = \zeta_k\ldots\zeta_1$ е разлагането на σ в произведение от независими цикли ζ_i, то четността на σ съвпада с четността на броя на циклите ζ_i с четна дължина. Причина за това е, че циклите с нечетна дължина са четни пермутации, докато циклите с четна дължина са нечетни пермутации.

(а) Разлагането $\sigma = (46)(123)$ на σ в произведение от независими цикли съдържа единствен цикъл с четна дължина, така че $\sigma\in S_6\setminus A_6$ е нечетна пермутация.

(б) Разлагането $\sigma = (56)(24)$ на σ в произведение от независими цикли се състои от два цикъла с четна дължина, така че $\sigma\in A_6$ е четна пермутация.