

Примерни задачи за групи по Висша алгебра 1

специалност Математика

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 $x_0 \pmod{\frac{n}{d}}$ е единственото решение на редуцираното сравнение $\left(\frac{a}{d}\right)x \equiv \left(\frac{b}{d}\right) \pmod{\frac{n}{d}}$ 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 $a(x_0 + i\frac{n}{d}) = b + ny_0 + ai\frac{n}{d} \equiv b \pmod{n}$ и $x_i \equiv x_0 + i\frac{n}{d} \pmod{\frac{n}{d}}$ 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 $x_1 \pmod{\frac{n}{d}} \equiv x_0 \pmod{\frac{n}{d}}$ е единственото решение на сравнението $\left(\frac{a}{d}\right)x \equiv \left(\frac{b}{d}\right) \pmod{\frac{n}{d}}$. Но условието $x_1 \equiv x_0 \pmod{\frac{n}{d}}$ 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) $6x \equiv 3 \pmod{9}$.

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

$$x = \frac{5y + 3}{2} = 2y + 1 + \frac{y + 1}{2}. \quad (1)$$

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 $2x \equiv 3 \pmod{5}$ има единствено решение $x \equiv -1 \pmod{5}$.

(ii) Сравнението $2x \equiv 1 \pmod{4}$ 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 $6x \equiv 3 \pmod{9}$ има три решения, защото коефициентът 6 на неизвестния остатък $x \pmod{9}$ 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

$$x = \frac{3y + 1}{2} = y + \frac{y + 1}{2}. \quad (2)$$

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

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

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

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,

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

съвпада с

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

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

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

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

на общата линейна група

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

са подгрупи, а подмножеството

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

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 $f : (\mathbb{C}^*, \cdot) \rightarrow (\mathbb{R}^*, \cdot)$ 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 $f(z_1 z_2) = \frac{1}{|z_1 z_2|} = \frac{1}{|z_1| \cdot |z_2|} = f(z_1) f(z_2)$ 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) Въз основа 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 $f(z_1 z_2) = 1 = 1 \cdot 1 = f(z_1) f(z_2)$ за $\forall z_1, z_2 \in \mathbb{C}^*$ постоянното изображение $f(z) = 1$ е хомоморфизъм на \mathbb{C}^* в \mathbb{R}^* .

(vii) Съгласно $f(z_1 z_2) = 2 = \frac{1}{2} \cdot 2 \cdot 2 = \frac{1}{2} f(z_1) f(z_2) \neq f(z_1) f(z_2)$ 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

$$\varphi_1 : H_1 = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R} \right\} \longrightarrow (\mathbb{R}, +),$$

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

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

(ii) изображението

$$\varphi_2 : H_2 = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R}^*, b \in \mathbb{R} \right\} \longrightarrow (\mathbb{R}^*, \cdot),$$

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

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

(iii) изображението

$$\varphi_3 : H_3 = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{R}^*, b \in \mathbb{R} \right\} \longrightarrow (\mathbb{R}^*, \cdot),$$

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

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

(iv) изображението

$$\varphi_4 : H_2 = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R}^*, b \in \mathbb{R} \right\} \longrightarrow (\mathbb{R}, +),$$

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

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

Решение: (i) Съгласно

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

изображението φ_1 е хомоморфизъм на групи.

(ii) От

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

следва, че φ_2 е хомоморфизъм на групи.

(iii) Вземайки предвид, че

$$\begin{aligned} \varphi_3 \left(\left(\begin{array}{cc} a_1 & b_1 \\ 0 & c_1 \end{array} \right) \left(\begin{array}{cc} a_2 & b_2 \\ 0 & c_2 \end{array} \right) \right) &= \varphi_3 \left(\begin{array}{cc} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{array} \right) = c_1 c_2 = \\ &= \varphi_3 \left(\begin{array}{cc} a_1 & b_1 \\ 0 & c_1 \end{array} \right) \varphi_3 \left(\begin{array}{cc} a_2 & b_2 \\ 0 & c_2 \end{array} \right) \quad \text{за } \forall a_i, c_i \in \mathbb{R}^*, \forall b_i \in \mathbb{R}, \end{aligned}$$

стигаме до извода, че φ_3 е хомоморфизъм на групи.

(iv) От

$$\begin{aligned} \varphi_4 \left(\left(\begin{array}{cc} a_1 & b_1 \\ 0 & 1 \end{array} \right) \left(\begin{array}{cc} a_2 & b_2 \\ 0 & 1 \end{array} \right) \right) &= \varphi_4 \left(\begin{array}{cc} a_1 a_2 & a_1 b_2 + b_1 \\ 0 & 1 \end{array} \right) = a_1 b_2 + b_1 \neq b_1 + b_2 = \\ \varphi_4 \left(\begin{array}{cc} a_1 & b_1 \\ 0 & 1 \end{array} \right) + \varphi_4 \left(\begin{array}{cc} a_2 & b_2 \\ 0 & 1 \end{array} \right) &\quad \text{за } \forall a_1 \in \mathbb{R}^* \setminus \{1\}, \forall a_2 \in \mathbb{R}^*, \forall b_1 \in \mathbb{R}, \forall b_2 \in \mathbb{R}^* \end{aligned}$$

следва, че φ_4 не е хомоморфизъм на групи.

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

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

(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 $g = -\frac{\sqrt{3}}{2} + \frac{1}{2}i = \cos\left(\frac{5\pi}{6}\right) + i \sin\left(\frac{5\pi}{6}\right) \in (\mathbb{C}^*, \cdot)$ 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, $H = \langle h_1, \dots, h_m \rangle \neq G$ е собствена подгрупа на G , породена от елементите $h_1, \dots, h_m \in G$, т.е.

$$H = \{h_{i_1}^{k_1} h_{i_2}^{k_2} \dots h_{i_s}^{k_s} \mid s \in \mathbb{N}, 1 \leq i_j \leq m, k_j \in \mathbb{Z}\}$$

е подмножеството на G , съставено от думите с крайна дължина $\sum_{j=1}^s |k_j| \in \mathbb{N}$ в азбу-

ката $h_1, h_1^{-1}, \dots, h_m, h_m^{-1}$. Да се докаже, че:

(i) ако за всяко $g \in G$ е в сила $h_1 g = g h_2, h_2 g = g h_3, \dots, h_{m-1} g = g h_m, h_m g = g h_1$, то H е нормална подгрупа на G ;

(ii) ако за всяко $g \in G$ е в сила $h_1 g = g h_2^2, h_2 g = g h_3^2, \dots, h_{m-1} g = g h_m^2, h_m g = g h_1^2$, то H е нормална подгрупа на G ;

(iii) ако за всяко $g \in G$ е в сила $h_1 g = g^m h_1, h_2 g = g^{m-1} h_2, \dots, h_{m-1} g = g^2 h_{m-1}, h_m g = g h_m$ и $m \geq 2$, то H не е нормална подгрупа на G ;

(iv) ако за всяко $g \in G$ е в сила $h_1 g = g^2 h_2, h_2 g = g^2 h_3, \dots, h_{m-1} g = g^2 h_m, h_m g = g^2 h_1$, то H не е нормална подгрупа на G .

Решение: Подгрупата $H \leq G$ е нормална тогава и само тогава, когато се изобразява в себе си при спрягане с произволно $g \in G$, т.е. $g^{-1} h g \in H$ за $\forall g \in G, \forall h \in H$. Когато подгрупата $H = \langle h_1, \dots, h_m \rangle$ е породена от h_1, \dots, h_m , достатъчно е $g^{-1} h_i g \in H$ за $\forall g \in G, \forall 1 \leq i \leq m$, защото тогава

$$g^{-1} (h_{i_1}^{k_1} h_{i_2}^{k_2} \dots h_{i_s}^{k_s}) g = (g^{-1} h_{i_1} g)^{k_1} (g^{-1} h_{i_2} g)^{k_2} \dots (g^{-1} h_{i_s} g)^{k_s} \in H$$

за $\forall g \in G, \forall h_{i_1}^{k_1} h_{i_2}^{k_2} \dots h_{i_s}^{k_s} \in H$.

(i) Условијата $h_i g = g h_{i+1}$ за $\forall 1 \leq i \leq m-1, \forall g \in G$ и $h_m g = g h_1$ за $\forall g \in G$ са еквивалентни на $g^{-1} h_i g = h_{i+1} \in H$ за $\forall 1 \leq i \leq m-1, \forall g \in G$ и $g^{-1} h_m g = h_1 \in H$ за $\forall g \in G$. Следователно H е нормална подгрупа.

(ii) От $h_i g = g h_{i+1}^2$ за $\forall 1 \leq i \leq m-1, \forall g \in G$ и $h_m g = g h_1^2$ за $\forall g \in G$ следва $g^{-1} h_i g = h_{i+1}^2 \in H$ за $\forall 1 \leq i \leq m-1, \forall g \in G$ и $g^{-1} h_m g = h_1^2 \in H$ за $\forall g \in G$. Подгрупата H е нормална.

(iii) Ако $h_i g = g^{m+1-i} h_i$ за $\forall 1 \leq i \leq m, \forall g \in G$, то $g^{-1} h_i g = g^{m-i} h_i \notin H$ за $i = m-1$ и $\forall g \in G \setminus H$. Следователно $H \neq G$ не може да е нормална подгрупа.

(iv) Ако $h_i g = g^2 h_{i+1}$ за $\forall 1 \leq i \leq m-1, \forall g \in G$ и $h_m g = g^2 h_1$ за $\forall g \in G$, то $g^{-1} h_i g = g h_{i+1} \notin H$ за $\forall g \in G \setminus H, \forall 1 \leq i \leq m-1$. Подгрупата $H \neq G$ със сигурност не е нормална.

Задача 9. 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 10. Дадена е подгрупата

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

на общата линейна група. Да се докаже, че

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

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

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

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

$$\begin{aligned} \ker(\det) &= \left\{ \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \in G \mid \det \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} = ab = 1 \right\} = \\ &= \left\{ \begin{pmatrix} a & c \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{Q}^*, c \in \mathbb{Q} \right\} = N \end{aligned}$$

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

Изображението

$$\varphi : G \longrightarrow (\mathbb{Q}^*, \cdot),$$

$$\varphi \left(\begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \right) = ab^2$$

е хомоморфизъм на групи съгласно

$$\begin{aligned} \varphi \left(\left(\begin{pmatrix} a_1 & c_1 \\ 0 & b_1 \end{pmatrix} \right) \left(\begin{pmatrix} a_2 & c_2 \\ 0 & b_2 \end{pmatrix} \right) \right) &= \varphi \left(\begin{pmatrix} a_1 a_2 & a_1 c_2 + c_1 b_2 \\ 0 & b_1 b_2 \end{pmatrix} \right) = (a_1 a_2)(b_1 b_2)^2 = \\ &= (a_1 b_1^2)(a_2 b_2^2) = \varphi \left(\begin{pmatrix} a_1 & c_1 \\ 0 & b_1 \end{pmatrix} \right) \varphi \left(\begin{pmatrix} a_2 & c_2 \\ 0 & b_2 \end{pmatrix} \right). \end{aligned}$$

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

$$\begin{aligned} \ker \varphi &= \left\{ \left(\begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \in G \mid \varphi \left(\begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \right) = ab^2 = 1 \right\} = \\ &= \left\{ \left(\begin{pmatrix} b^{-2} & c \\ 0 & b \end{pmatrix} \mid b \in \mathbb{Q}^*, c \in \mathbb{Q} \right\} = H \end{aligned}$$

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

Задача 11. В множеството

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

на наредените тройки реални числа въвеждаме бинарна операция

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

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

$$\begin{aligned} A &= (a_1 + a_2, \quad b_1 + a_1 c_2 + b_2, \quad c_1 + c_2) \circ (a_3, b_3, c_3) = \\ &= ((a_1 + a_2) + a_3, \quad (b_1 + a_1 c_2 + b_2) + (a_1 + a_2) c_3 + b_3, \quad (c_1 + c_2) + c_3) = \\ &= (a_1 + a_2 + a_3, \quad b_1 + b_2 + b_3 + a_1 c_2 + a_1 c_3 + a_2 c_3, \quad c_1 + c_2 + c_3) \end{aligned}$$

и

$$\begin{aligned} B &= (a_1, b_1, c_1) \circ (a_2 + a_3, b_2 + a_2c_3 + b_3, c_2 + c_3) = \\ &= (a_1 + (a_2 + a_3), b_1 + a_1(c_2 + c_3) + (b_2 + a_2c_3 + b_3), c_1 + (c_2 + c_3)) = \\ &= (a_1 + a_2 + a_3, b_1 + b_2 + b_3 + a_1c_2 + a_1c_3 + a_2c_3, c_1 + c_2 + c_3). \end{aligned}$$

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

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

По-точно,

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

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

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

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 $(a, b, c)^{-1} = (-a, ac - b, -c) \in G$ относно \circ и (G, \circ) е група.

(б) Изображението

$$\begin{aligned} \varphi : G &\longrightarrow (\mathbb{R}^2, +), \\ \varphi(a, b, c) &= (a, c) \end{aligned}$$

е хомоморфизъм на групи съгласно

$$\begin{aligned} \varphi((a_1, b_1, c_1) \circ (a_2, b_2, c_2)) &= \varphi(a_1 + a_2, b_1 + a_1c_2 + b_2, c_1 + c_2) = (a_1 + a_2, c_1 + c_2) = \\ &= (a_1, c_1) + (a_2, c_2) = \varphi(a_1, b_1, c_1) + \varphi(a_2, b_2, c_2). \end{aligned}$$

Още повече, φ е епиморфизъм на групи, защото $\forall (a, c) \in \mathbb{R}^2$ е от вида $\varphi(a, 0, c) = (a, c) \in \text{im}\varphi$. 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 $\text{im}\varphi = (\mathbb{R}^2, +)$.

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 12. Кои от следните двойки пермутации от S_6 са спрегнати:

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

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

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

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

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

Решение: Ако $\sigma = \zeta_k \dots \zeta_1$ 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.

Задача 14. Нека S_4 е симетричната група от степен 4, а $H = \{\sigma \in S_4 \mid \sigma(4) = 4\}$. Да се докаже, че:

(i) H е подгрупа на S_4 , изоморфна на S_3 ;

(ii) подгрупата H на S_4 не е нормална;

(iii) $S_4 = H \cup (1, 2)(3, 4)H \cup (1, 3)(2, 4)H \cup (1, 4)(2, 3)H$ е разлагане на S_4 в непресичащо се обединение от леви съседни класове на S_4 по H .

(iv) при умножението на различни представители на съседни класове aH и bH се получават различни съседни класове относно H . Например, за $a = (1, 2)(3, 4)$, $b = (1, 4)(2, 3)$ и $h = (1, 3) \in e$ в сила $(ah)bH \neq abH$.

Решение: (i) Изображението

$$\rho : H \longrightarrow S_3,$$

$$\rho(\sigma) = \begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix} \quad \text{за } \forall \sigma \in H,$$

съпоставящо на $\sigma : \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}$ неговото ограничение

$$\rho(\sigma) : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$$

е хомоморфизъм на групи, защото последователното прилагане на $\tau, \sigma \in H$ върху числата от 1 до 4, последвано от ограничение върху 1, 2, 3 съвпада с последователното прилагане на ограниченията на τ и σ върху 1, 2, 3. Съответствието ρ е взаимно-еднозначно, така че $\rho : H \rightarrow S_3$ е изоморфизъм на групи.

(ii) Подгрупа H на симетрична група S_n е нормална точно когато заедно с всеки свой елемент $h \in H \setminus \{\varepsilon\}$ съдържа всички $\sigma \in S_n$, които имат еднакъв цикличен строеж с h . В случая, подгрупата H съдържа тройните цикли (123) и (132) от S_4 , но не и тройните цикли (4ij) за $1 \leq i \neq j \leq 3$. Следователно H не е нормална подгрупа на S_4 . Същият извод се получава и от това, че H съдържа транспозициите (ij) $\in S_4$ за $1 \leq i < j \leq 3$, но не и транспозициите (4k) $\in S_4$ за $1 \leq k \leq 3$.

(iii) Съгласно Теоремата на Лагранж, индексът $|S_4 : H| = \frac{|S_4|}{|H|} = \frac{4!}{3!} = 4$. Достатъчно е да проверим, че $H, (12)(34)H, (13)(24)H$ и $(14)(23)H$ са различни съседни класове, за да твърдим, че $S_4 = H \cup (1,2)(3,4)H \cup (1,3)(2,4)H \cup (1,4)(2,3)H$ е разлагането на S_4 в непресичащо се обединение от леви съседни класове относно H . За произволна пермутация ijk на 234, левият съседен клас $(1i)(jk)H$ е различен от H , защото $(1i)(jk) \notin H$. Ако допуснем, че $(1i)(jk)H = (1j)(ik)H$, то $\sigma = [(1j)(ik)]^{-1}(1i)(jk) \in H$. Но $\sigma = (ik)^{-1}(1j)^{-1}(1i)(jk) = (ik)(1j)(1i)(jk) = (1k)(ij) \notin H$, така че и $(12)(34)H, (13)(24)H, (14)(23)H$ са два по два различни леви съседни класове на S_4 по H .

(iv) По-точно, $ab = (12)(34)(14)(23) = (13)(24)$ и $(ah)b = [(12)(34)(13)](14)(23) = (13)$ пораждаат различни съседни класове $(ah)bH = (13)H = H \neq (13)(24)H = abH$.

Задача 15. Да разгледаме елементите $a = (1, 2, 3, 4), b = (1, 3), c = (1, 2)$ на симетричната група S_4 със съотношенията

$$(ca)^k c(ca)^{-k} = (1, k+2) \quad \text{за } 1 \leq k \leq 2,$$

$$(i, j) = (1, i)(1, j)(1, i) \quad \text{за } \forall 2 \leq i < j \leq 4,$$

$$ba = a^3b, \quad ab = ba^3.$$

Да се докаже, че подгрупата $D = \langle a, b \rangle$ на S_4 , породена от a, b съвпада с множествата

$$M_1 = \{a^i b^j \mid 0 \leq i \leq 3, 0 \leq j \leq 1\} \quad \text{и} \quad M_2 = \{b^i a^j \mid 0 \leq i \leq 1, 0 \leq j \leq 3\},$$

а $G = \langle a, c \rangle$ съвпада с S_4 .

Решение: (i) Съотношението $ba = a^3b$ позволява да представим всеки елемент на D във вида $a^i b^j$. Съгласно $a^4 = \varepsilon, b^2 = \varepsilon$ за тъждествената пермутация $\varepsilon \in S_4$, групата D се съдържа, а оттам и съвпада с множеството M_1 . От $ab = ba^3$ получаваме $D \subseteq M_2$ и $D = M_2$.

(ii) Всяка пермутация $\sigma \in S_4$ се представя като произведение на транспозиции (i, j) за $1 \leq i < j \leq 4$. Съгласно $(i, j) = (1, i)(1, j)(1, i)$ за $\forall 2 \leq i < j \leq 4$, групата $S_4 = \langle (1, 2), (1, 3), (1, 4) \rangle$ се поражда от транспозициите $(1, k)$ с $2 \leq k \leq 4$. От $(1, k+2) = (ca)^k c(ca)^{-k} \in \langle a, c \rangle = G$ за $\forall 0 \leq k \leq 2$ следва, че $S_4 \subseteq G$ и $S_4 = G$.

Задача 16. Нека G е група, а H е подгрупа на G с индекс n . Да се докаже, че:

(i) съответствието

$$G \times G/H \longrightarrow G/H,$$

$$(g, xH) \mapsto gxH \quad \text{за } \forall g \in G, \quad \forall xH \in G/H$$

е действие на групата G върху множеството на левите съседни класове на G по H ;

(ii) ядрото $\ker(\Phi)$ на асоцирания с това действие хомоморфизъм $\Phi : G \rightarrow S_n$ е сечението $\ker(\Phi) = \bigcap_{x \in G} xHx^{-1}$ на всички спрегнати с H подгрупи xHx^{-1} на G .

Задача 17. Да се докаже, че ако група G има подгрупа с индекс $[G : H] = n$, то G има нормална подгрупа N , съдържаща се в H , чийто индекс $[G : N]$ се дели на n и дели $n!$.

Упътване: Изберете $N = \ker(\Phi)$ за хомоморфизма Φ от задача 16.