Арунова Маргарита БПМИ2011

Определение. *Бинарная операция* на M – это отображение $\circ : M \times M \to M,\ (a,b) \mapsto a \circ b$.

Определение.

1. $(M, \circ)$ является *группой*, если выполнены следующие три условия:
   (а) $(a \circ b) \circ c = a \circ (b \circ c)\ \ \forall\, a, b, c \in M$ *(ассоциативность)*
   (б) существует *нейтральный элемент*, то есть такой $e \in M$, что $e \circ a = a \circ e = a$
   (в) для всякого a существует *обратный элемент*, то есть такой $b \in M$, что $a \circ b = b \circ a = e$
2. $(M, \circ)$ является *полугруппой*, если выполнено только условие (а)
3. $(M, \circ)$ является *моноидом*, если выполнены только условия (а) и (б)

Определение. Подмножество H группы G называется *подгруппой*, если
(а) $e \in H$
(б) $a, b \in H \Rightarrow a \circ b \in H$
(в) $a \in H \Rightarrow a^{-1} \in H$

Для каждого $g \in G$ рассмотрим множество $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. Данное множество является подгруппой.
Определение. Подгруппа $\langle g \rangle$ называется *циклической подгруппой* в G, порождаемой g. Причём элемент g называется *образующим* или *порождающим* элементом для $\langle g \rangle$.

Пусть G – группа и $g \in G$. Рассмотрим множество $M(g) = \{n \in \mathbb{N} : g^n = e\}$.
Определение. *Порядок элемента g* – это величина

$$\operatorname{ord}(g) = \begin{cases} \min M(g),\ \text{если } M(g) \neq \varnothing \\ \infty,\ \text{если } M(g) = \varnothing \end{cases}$$

Определение. Множество $aH = \{ah \mid h \in H\}$ называется *левым смежным классом* элемента a по подгруппе H.
Определение. Множество $Ha = \{ha \mid h \in H\}$ называется *правым смежным классом* элемента a по подгруппе H.

Определение. *Индекс* подгруппы H в группе G – это число левых смежных классов G по H.
Обозначение: $[G : H]$.

Задание 1. Докажите, что формула $m \circ n = 3mn - 3m - 3n + 4$ задаёт бинарную операцию на множестве $\mathbb{Q} \setminus \{1\}$ и что $(\mathbb{Q} \setminus \{1\}, \circ)$ является группой.

1. Из определения бинарной операции на множестве следует, что для того, чтобы проверить, что формула $m \circ n$ задаёт бинарную операцию на множестве $\mathbb{Q} \setminus \{1\}$, достаточно проверить, что для любых $m, n \in \mathbb{Q} \setminus \{1\}$ элемент равный $m \circ n$ лежит в $\mathbb{Q} \setminus \{1\}$.

2. Известно, что произведение рациональных чисел – рациональное, сумма (разность) рациональных также рациональное ($\mathbb{Q}$ – поле):
   − $\forall a, b \in \mathbb{Q}$ выполнено $ab \in \mathbb{Q}$
   − $\forall a, b \in \mathbb{Q}$ выполнено $a \pm b \in \mathbb{Q}$
   Получаем, что для $m \in \mathbb{Q}, n \in \mathbb{Q}$ выполнено $3mn - 3m - 3n + 4 \in \mathbb{Q}$.

3. Осталось показать, что для любых $m \neq 1$ и $n \neq 1$ значение $m \circ n \neq 1$, то есть для любых $m \in \mathbb{Q} \setminus \{1\}$ и $n \in \mathbb{Q} \setminus \{1\}$ значение $m \circ n \in \mathbb{Q} \setminus \{1\}$:
$$3mn - 3m - 3n + 4 = 1 \Leftrightarrow 3m(n-1) - 3(n-1) = 0 \Leftrightarrow 3(m-1)(n-1) = 0 \Leftrightarrow$$
$$\Leftrightarrow m = 1 \vee n = 1, \text{ то есть нет решений в } \mathbb{Q} \setminus \{1\}$$

4. Последние два пункта говорят о том, что не существует таких $m, n \in \mathbb{Q} \setminus \{1\}$, что значение $m \circ n \notin \mathbb{Q} \setminus \{1\}$. Таким образом, для любых $m \in \mathbb{Q} \setminus \{1\}$ и $n \in \mathbb{Q} \setminus \{1\}$ значение $m \circ n \in \mathbb{Q} \setminus \{1\}$, значит, $m \circ n$ задаёт бинарную операцию на множестве $\mathbb{Q} \setminus \{1\}$.

5. По определению группы: $(\mathbb{Q} \setminus \{1\}, \circ)$ – группа $\overset{def}{\Leftrightarrow}$ выполнены следующие условия:
   (а) $\forall\, a, b, c \in \mathbb{Q} \setminus \{1\}$ выполняется $(a \circ b) \circ c = a \circ (b \circ c)$ *(ассоциативность)*
   (б) существует *нейтральный элемент*, т. е. такой $e \in \mathbb{Q} \setminus \{1\}$, что $e \circ a = a \circ e = a$, $\forall a \in \mathbb{Q} \setminus \{1\}$
   (в) $\forall a \in \mathbb{Q} \setminus \{1\}$ существует *обратный элемент*, т. е. такой $b \in \mathbb{Q} \setminus \{1\}$, что $a \circ b = b \circ a = e$

6. Проверим выполнение условия (а):
$$(a \circ b) \circ c = (3ab - 3a - 3b + 4) \circ c = 3 \cdot (3ab - 3a - 3b + 4) \cdot c - 3 \cdot (3ab - 3a - 3b + 4) - 3c + 4 =$$
$$= 9abc - 9ab - 9ac - 9bc + 9a + 9b + 9c - 8$$
$$a \circ (b \circ c) = a \circ (3bc - 3b - 3c + 4) = 3 \cdot a \cdot (3bc - 3b - 3c + 4) - 3a - 3 \cdot (3bc - 3b - 3c + 4) + 4 =$$
$$= 9abc - 9ab - 9ac - 9bc + 9a + 9b + 9c - 8$$
   Слагаемые и множители в выражениях можем переставлять, так как сложение и умножение в Q коммутативно и ассоциативно. Условие $(a \circ b) \circ c = a \circ (b \circ c)$ – выполнено.

7. Проверим выполнение условия (б). Если нейтральный элемент e существует, то для каждого элемента $a \in \mathbb{Q} \setminus \{1\}$ верно $e \circ a = a \circ e = a$.
$$a \circ e = 3ae - 3a - 3e + 4 = a$$
$$e \circ a = 3ea - 3e - 3a + 4 = a$$
$$a \circ e = 3ae - 3a - 3e + 4 = 3ea - 3e - 3a + 4 = e \circ a$$

Последнее верно в силу ассоциативности сложения и коммутативности умножения в $\mathbb{Q}$ (и как следствие в $\mathbb{Q} \setminus \{1\}$).

Найдём элемент e. Для этого решим уравнение $3ae - 3a - 3e + 4 = a \;\Leftrightarrow\; 3ea - 3e - 3a + 4 = a$.

$$3ea - 3e - 3a + 4 = a \;\Leftrightarrow\; 3ea - 3e - 4a + 4 = 0 \;\Leftrightarrow\; 3e(a-1) - 4(a-1) = 0 \;\Leftrightarrow$$

$$\Leftrightarrow\; (3e-4)(a-1) = 0 \;\Leftrightarrow\; \begin{cases} e \neq 1 \\ e = {}^4\!/_3 \end{cases} \;\Leftrightarrow\; e = \frac{4}{3}$$

В силу произвольности a элемент $e = {}^4\!/_3$ является нейтральным элементом в $\mathbb{Q} \setminus \{1\}$.

Таким образом, условие существования нейтрального элемента выполнено.

8. Проверим выполнение условия (в). Если обратный элемент b существует, то для каждого элемента $a \in \mathbb{Q} \setminus \{1\}$ верно $a \circ b = b \circ a = e$.

$$a \circ b = 3ab - 3a - 3b + 4 = e$$

$$b \circ a = 3ba - 3b - 3a + 4 = e$$

$$a \circ b = 3ab - 3a - 3b + 4 = 3ba - 3b - 3a + 4 = b \circ a$$

Последнее верно в силу ассоциативности сложения и коммутативности умножения в $\mathbb{Q}$ (и как следствие в $\mathbb{Q} \setminus \{1\}$).

Для каждого $a \in \mathbb{Q} \setminus \{1\}$ найдём элемент b. Для этого решим уравнение

$$3ab - 3a - 3b + 4 = e \;\Leftrightarrow\; 3ba - 3b - 3a + 4 = e$$

$$3ab - 3a - 3b + 4 = e \;\Leftrightarrow\; (3a-3)b = e + 3a \;\Leftrightarrow\; b = (e+3a)(3a-3)^{-1}$$

Нейтральный элемент существует (по доказанному в предыдущем пункте), значение $a \neq 1$, то есть $3a - 3 \in \mathbb{Q} \setminus \{0\} \Rightarrow$ существует $(3a-3)^{-1}$ ($\mathbb{Q}$ – поле). Значит, полученное значение b существует. Проверим, что оно не равно единице (ясно, что это значение лежит в $\mathbb{Q}$):

$$b = \frac{e+3a}{3a-3} = 1 \;\Leftrightarrow\; e + 3a = 3a - 3 \;\Leftrightarrow$$

$$\Leftrightarrow\; e = -3$$

Последнее выражение неверно, так как найденный в предыдущем пункте $e = {}^4\!/_3$, а нейтральный элемент единственный. Получаем, что для каждого $a \in \mathbb{Q} \setminus \{1\}$ существует обратный элемент $b \in \mathbb{Q} \setminus \{1\}$.

Таким образом, условие существования обратного элемента для каждого элемента рассматриваемого множества выполнено.

9. Все три условия выполнены, а значит, $(\mathbb{Q} \setminus \{1\}, \circ)$ по определению является группой.

Задание 2. Найдите все элементы порядка 18 в группе $(\mathbb{C} \setminus \{0\}, \times)$

1. По определению порядок элемента g группы G это величина
$$\operatorname{ord}(g) = \begin{cases} \min M(g), \text{ если } M(g) \neq \varnothing \\ \infty, \text{ если } M(g) = \varnothing \end{cases}, \text{ где } M(g) = \{n \in \mathbb{N} : g^n = e\}$$

2. В условии требуется найти такие $z = a + bi \in \mathbb{C} \setminus \{0\}$, что $\overbrace{z \cdot z \cdot \ldots \cdot z}^{18 \text{ раз}} = e$, причём $z^n \neq e$, где $n \in \mathbb{N}$, $n < 18$.

3. Любое комплексное представимо в виде $|r|(\cos\varphi + \sin\varphi)$, где $|r| = \sqrt{a^2 + b^2}$ – модуль комплексного числа, а $\varphi = \arg z$ – аргумент комплексного числа. При умножении двух комплексных чисел их модули перемножаются, а аргументы складываются. В частности:
$$z^n = \big(|r|(\cos\varphi + \sin\varphi)\big)^n = |r|^n(\cos n\varphi + \sin n\varphi)$$

4. Найдём нейтральный элемент в $(\mathbb{C} \setminus \{0\}, \times)$. Для любого $c = a + bi \in \mathbb{C} \setminus \{0\}$ должно выполняться
$$(a + bi) \cdot e = e \cdot (a + bi) = a + bi$$
Искомым e является единица, то есть $e = 1$. Действительно, верно следующее:
$$(a + bi) \cdot 1 = 1 \cdot (a + bi) = a + bi$$

5. Найдём такие $z \in \mathbb{C} \setminus \{0\}$, что $z \cdot z \cdot \ldots \cdot z = z^{18} = e = 1$. Другими словами, решим уравнение
$$z^{18} = 1 \;\Leftrightarrow\; z = \sqrt[18]{1} \;\Leftrightarrow\; z = \sqrt[18]{|1|} \cdot \left(\cos\frac{\varphi + 2\pi k}{18} + i \sin\frac{\varphi + 2\pi k}{18}\right),\; k = 0, 1, \ldots, 17 \overset{\varphi=0}{\Leftrightarrow}$$
$$\Leftrightarrow\; z_k = \cos\frac{\pi k}{9} + i \sin\frac{\pi k}{9},\; k = 0, 1, \ldots, 17$$
Таким образом, у найденных $z_k \in \mathbb{C} \setminus \{0\}$ порядок $\operatorname{ord} z_k \leqslant 18$.

6. Докажем следующее утверждение:
$$g^n = e \;\Leftrightarrow\; n \,\vdots\, \operatorname{ord}(g)$$
   - $\boxed{\Rightarrow}$ пусть $n \not\vdots\; m = \operatorname{ord}(g)$, тогда $n = qm + r$, $0 < r < m$
   $e = g^n = g^{qm+r} = (g^m)^q \cdot g^r = e^q \cdot g^r = g^r$, но $r < m = \operatorname{ord}(g) \Rightarrow$ противоречие
   - $\boxed{\Leftarrow}$ $n = q \cdot \operatorname{ord}(g) \Rightarrow g^n = g^{\operatorname{ord}(g) \cdot q} = (g^{\operatorname{ord}(g)})^q = e^q = e$

7. Исключим все такие найденные числа z_k, что $z_k^n = e$ для $n \in \mathbb{N}$ и $n < 18$. Из доказанного в предыдущем пункте следует, что описанные значения $n = \operatorname{ord}(z_k)$ – это делители числа 18.
Все возможные значения натурального числа $n < 18$ – это $\{1, 2, 3, 6, 9\}$. Найдём все такие рассматриваемые z_k, для которых существует $n \in \{1, 2, 3, 6, 9\} :\; z_k^n = 1$.
Будем последовательно рассматривать возможные значения порядка для элементов z_k (то есть возможные значения n). Если для заданного n число $z_k^n = 1$, то $\operatorname{ord}(z_k) \leqslant n < 18$ и z_k не входит в ответ.

- $n=1$:

$$z_k^1=\cos\frac{\pi k}{9}+i\sin\frac{\pi k}{9}=1 \Leftrightarrow \begin{cases}\cos\dfrac{\pi k}{9}=1\\ \sin\dfrac{\pi k}{9}=0\end{cases} \Leftrightarrow \begin{cases}\dfrac{\pi k}{9}=2\pi t\\ \dfrac{\pi k}{9}=\pi s\end{cases} \quad t,s\in\mathbb{Z} \Leftrightarrow$$

$$\Leftrightarrow\ k=18t,\ t\in\mathbb{Z} \Leftrightarrow\ k=0,\ \text{так как } k\in\{0,1,2,\dots,17\}$$

- $n=2$:

$$z_k^2=\cos\frac{2\pi k}{9}+i\sin\frac{2\pi k}{9}=1 \Leftrightarrow \begin{cases}\cos\dfrac{2\pi k}{9}=1\\ \sin\dfrac{2\pi k}{9}=0\end{cases} \Leftrightarrow \begin{cases}\dfrac{2\pi k}{9}=2\pi t\\ \dfrac{2\pi k}{9}=\pi s\end{cases} \quad t,s\in\mathbb{Z} \Leftrightarrow$$

$$\Leftrightarrow\ k=9t,\ t\in\mathbb{Z} \Leftrightarrow\ k=0,9 \text{ так как } k\in\{0,1,2,\dots,17\}$$

- $n=3$:

$$z_k^3=\cos\frac{3\pi k}{9}+i\sin\frac{3\pi k}{9}=1 \Leftrightarrow \begin{cases}\cos\dfrac{3\pi k}{9}=1\\ \sin\dfrac{3\pi k}{9}=0\end{cases} \Leftrightarrow \begin{cases}\dfrac{\pi k}{3}=2\pi t\\ \dfrac{\pi k}{3}=\pi s\end{cases} \quad t,s\in\mathbb{Z} \Leftrightarrow$$

$$\Leftrightarrow\ k=6t,\ t\in\mathbb{Z} \Leftrightarrow\ k=0,6,12 \text{ так как } k\in\{0,1,2,\dots,17\}$$

- $n=6$:

$$z_k^6=\cos\frac{6\pi k}{9}+i\sin\frac{6\pi k}{9}=1 \Leftrightarrow \begin{cases}\cos\dfrac{6\pi k}{9}=1\\ \sin\dfrac{6\pi k}{9}=0\end{cases} \Leftrightarrow \begin{cases}\dfrac{2\pi k}{3}=2\pi t\\ \dfrac{2\pi k}{3}=\pi s\end{cases} \quad t,s\in\mathbb{Z} \Leftrightarrow$$

$$\Leftrightarrow\ k=3t,\ t\in\mathbb{Z} \Leftrightarrow\ k=0,3,6,9,12,15 \text{ так как } k\in\{0,1,2,\dots,17\}$$

- $n=9$:

$$z_k^9=\cos\frac{9\pi k}{9}+i\sin\frac{9\pi k}{9}=1 \Leftrightarrow \begin{cases}\cos\dfrac{9\pi k}{9}=1\\ \sin\dfrac{9\pi k}{9}=0\end{cases} \Leftrightarrow \begin{cases}\pi k=2\pi t\\ \pi k=\pi s\end{cases} \quad t,s\in\mathbb{Z} \Leftrightarrow$$

$$\Leftrightarrow\ k=2t,\ t\in\mathbb{Z} \Leftrightarrow\ k=0,2,4,6,8,10,12,14,16 \text{ так как } k\in\{0,1,2,\dots,17\}$$

8. Получаем, что у найденных чисел $z_0,z_2,z_3,z_4,z_6,z_8,z_9,z_{10},z_{12},z_{14},z_{15},z_{16}$ порядок меньше 18, значит, такие числа не подходят. Порядок оставшихся чисел $z_1,z_5,z_7,z_{11},z_{13},z_{17}$ равен 18 (по построению) в силу доказанного в пункте 6 утверждения и того, что для каждого $n\in\{1,2,3,6,9\}$ $z_k^n\neq e$ при $k\in\{1,5,7,11,13,17\}$.

Ответ: $z_k=\cos\dfrac{\pi k}{9}+i\sin\dfrac{\pi k}{9}$ для $k=\{1,5,7,11,13,17\}$

Задание 3. Найдите все левые и правые смежные классы группы A_4 по подгруппе $\langle\sigma\rangle$, где

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

1. Найдём множество $\langle\sigma\rangle$, которое образует элемент σ. Разложим перестановку в произведение независимых циклов: $\sigma = (134)(2)$. Известно, что порядок перестановки равен НОК длин её независимых циклов, значит, $\operatorname{ord}(\sigma) = 3$. Рассмотрим следующие перестановки:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

$$\sigma^3 = \sigma^2 \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = id$$

Таким образом, $\langle\sigma\rangle = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \right\} = \{id,\ \sigma,\ \sigma^2\}$.

Всякий элемент из $\sigma^n \in \langle\sigma\rangle$ является элементом описанного множества:

- если $n \geqslant 0$, представим n в виде $n = 3q + r,\ 0 \leqslant r < 3$, тогда получаем следующее

$$\sigma^n = \sigma^{3q} \cdot \sigma^r = (\sigma^3)^q \cdot \sigma^r = (id)^q \cdot \sigma^r = \sigma^r \in \{id,\ \sigma,\ \sigma^2\}$$

- если $n < 0$, представим n в виде $|n| = 3q - r,\ 0 \leqslant r < 3$ (остаток равен $r = 3q - |n| = 3q + n$), тогда получаем следующее

$$\sigma^n = (id)^q \cdot \sigma^n = \sigma^{3q} \cdot \sigma^n = \sigma^{3q+n} = \sigma^r \in \{id,\ \sigma,\ \sigma^2\}$$

2. Докажем следующее утверждение: пусть $H \subseteq G$, $H = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$ и $\operatorname{ord}(a) = |\langle a \rangle| < \infty$; для любого $b \in G$ и $c \in bH$ выполняется $bH = cH$.

- По определению для $b \in G$ левый смежный класс этого элемента равен $bH = \{bh \mid h \in H\}$.
- Пусть $\operatorname{ord}(a) = |\langle a \rangle| = |H| = m < \infty$, тогда $H = \{e, a, \ldots, a^{m-1}\}$ и $bH = \{b, ba, \ldots, ba^{m-1}\}$. Возьмём произвольный элемент $c \in bH,\ c = ba^k$ и покажем, что его левый смежный класс по подгруппе H совпадает с bH.
- Получаем следующее

$$cH = \{c, ca, \ldots, ca^{m-1}\} = \{ba^k, ba^{k+1}, \ldots, ba^{m+k-1}\}$$

Пусть число $l > 0$ такое, что $k + l = m$ (ясно, что $k < m$), тогда

$$cH = \{ba^k, ba^{k+1}, \ldots, ba^{m+k-1}\} = \{ba^k, ba^{k+1}, \ldots, ba^{k+l}, ba^{k+l+1}, \ldots, ba^{k+l+k-1}\} =$$
$$= \{ba^k, ba^{k+1}, \ldots, be, ba^1, \ldots, ba^{k-1}\} = \{b, ba, \ldots, ba^{k-1}, ba^k, ba^{k+1}\} = bH$$

Таким же образом доказывается аналогичное утверждение для правых смежных классов.

3. Опишем все левые смежные классы элементов группы A_4 по подгруппе $\langle\sigma\rangle$. Утверждение, доказанное в предыдущем пункте, позволяет уменьшить перебор по чётным перестановкам.
   - Для перестановок id, σ, σ^2 левый смежный класс по подгруппе $\langle\sigma\rangle$ равен самой подгруппе $\langle\sigma\rangle$. Легко убедится в этом, найдя левый смежный класс для id: это множество
   $$\{id \cdot \pi \mid \pi \in \langle\sigma\rangle\}$$
   Перестановки σ и σ^2 лежат в этом классе, а значит, их левые смежные классы по доказанному утверждению такие же.
   - Рассмотрим перестановку $\pi \in A_4$, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ и найдём её левый смежный класс:
   $$\pi \cdot id = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$
   $$\pi \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$
   $$\pi \cdot \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$
   Для $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ левый смежный класс равен
   $$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \right\}$$
   - Рассмотрим перестановку $\pi \in A_4$, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ и найдём её левый смежный класс:
   $$\pi \cdot id = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$
   $$\pi \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$
   $$\pi \cdot \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$
   Для $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ левый смежный класс равен
   $$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \right\}$$

– Рассмотрим перестановку $\pi \in A_4$, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ и найдём её левый смежный класс:

$$\pi \cdot id = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\pi \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

$$\pi \cdot \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

Для $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ левый смежный класс равен

$$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \right\}$$

4. Опишем все правые смежные классы элементов группы A_4 по подгруппе $\langle\sigma\rangle$. Утверждение, доказанное в пункте 2, позволяет уменьшить перебор по чётным перестановкам.

– Для перестановок id, σ, σ^2 правый смежный класс по подгруппе $\langle\sigma\rangle$ равен самой подгруппе $\langle\sigma\rangle$. Легко убедится в этом, найдя правый смежный класс для id: это множество

$$\{\pi \cdot id \mid \pi \in \langle\sigma\rangle\}$$

Перестановки σ и σ^2 лежат в этом классе, а значит, их правые смежные классы по доказанному утверждению такие же.

– Рассмотрим перестановку $\pi \in A_4$, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ и найдём её правый смежный класс:

$$id \cdot \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

$$\sigma \cdot \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$\sigma^2 \cdot \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

Для $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$ правый смежный класс равен

$$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \right\}$$

– Рассмотрим перестановку $\pi \in A_4$, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ и найдём её правый смежный класс:

$$id \cdot \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

$$\sigma \cdot \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

$$\sigma^2 \cdot \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Для $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ правый смежный класс равен

$$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \right\}$$

– Рассмотрим перестановку $\pi \in A_4$, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ и найдём её правый смежный класс:

$$id \cdot \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\sigma \cdot \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

$$\sigma^2 \cdot \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

Для $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ правый смежный класс равен

$$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \right\}$$

5. Таким образом, найдены все левые и правые смежные классы.
6. Также заметим, что равенство порядка A_4 произведению индекса подгруппы $\langle\sigma\rangle$ в A_4 и порядка подгруппы $\langle\sigma\rangle$ выполняется:

$$|A_4| = |\langle\sigma\rangle| \cdot |A_4 : \langle\sigma\rangle| = \mathrm{ord}(\sigma) \cdot 4 = 12$$

Это говорит о том, что найденное множество левых (правых) смежных классов состоит из правильного числа элементов.

Ответ:

– левые смежные классы группы A_4:

$$\left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}\right\}$$
$$\left\{\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}\right\}$$
$$\left\{\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\right\}$$
$$\left\{\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}\right\}$$

– правые смежные классы группы A_4:

$$\left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}\right\}$$
$$\left\{\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}\right\}$$
$$\left\{\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\right\}$$
$$\left\{\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}\right\}$$

Задание 4. Докажите, что всякая подгруппа циклической группы является циклической.

1. Пусть $G = \langle g \rangle$ – циклическая группа с образующим элементом g и $H \subseteq G$.

2. Первый случай: $H = \{e\}$. В данном случае всё выполнено: подгруппа $H = \{e\} = \langle e \rangle$ – циклическая подгруппа в G, порождаемая элементом e.

3. Второй случай: $H \neq \{e\}$. Так как все элементы G имеют вид $g^k \ (k \in \mathbb{Z})$, а $H \subseteq G$, в рассматриваемой подгруппе H лежат только элементы вида $g^k \ (k \in \mathbb{Z})$.

   Возьмём $g^m \in H$ с минимальным положительным m. Такой элемент с заданным m найдётся:
   - $H \neq \{e\}$, значит, существует $n \neq 0 : \ g^n \in H$
   - если $n > 0$, то в H есть элемент g^n с положительной степенью
   - если $n < 0$, то, взяв обратный к g^n элемент g^{-n}, получим элемент с положительной степенью; обратный элемент всегда существует по определению подгруппы

   Докажем, что $H = \langle g^m \rangle$, то есть все элементы в H имеют вид $g^{mt} \ (t \in \mathbb{Z})$.
   - предположим противное: пусть в H есть элемент g^n, $n \neq 0$ и $n \not\vdots\, m$
   - из неделимости n на m следует, что $0 < \text{НОД}(n, m) = d < m$
   - рассмотрим следующее диофантово уравнение
   $$ma + nb = d$$
   - такое уравнение имеет решение в целых числах по построению: $\text{НОД}(m, n) = d$; пусть числа a_0, b_0 – какое-то частное решение этого уравнения
   - получаем следующее:
   $$(g^m)^{a_0} \cdot (g^n)^{b_0} = g^{ma_0} \cdot g^{nb_0} = g^{ma_0 + nb_0} = g^d \in H$$
   элементы $(g^m)^{a_0}$, $(g^n)^{b_0}$ и $(g^m)^{a_0} \cdot (g^n)^{b_0}$ лежат в подгруппе H по определению
   - из предположения число $d < m \ \Rightarrow$ получаем противоречие с тем, что m – описанное минимальное положительное число
   - таким образом, если $g^n \in H$, $n \neq 0$, то $n \,\vdots\, m$, то есть $n = mt$, $t \in \mathbb{Z} \setminus \{0\}$

   Все элементы H имеют вид g^{mt}, $t \in \mathbb{Z}$, значит, $H = \langle g^m \rangle$, то есть циклическая.