ПРАКТИЧЕСКИЕ ЗАНЯТИЯ №11-12

Тема занятий. Изоморфизм групп. Смежные классы. Нормальные делители. Фактор-группы. Гомоморфизм. Задание группы образующими и определяющими соотношениями

1. **Изоморфизм групп**. Две группы G и G' с операциями $*$ и $\circ$ называются **изоморфными**, если существует биективное отображение $f : G \to G'$ такое, что $f(a * b) = f(a) \circ f(b) \quad \forall a, b \in G$.

Свойства изоморфизма.

1) Единица переходит в единицу. Действительно, пусть e - единичный элемент из G. Тогда $e*e = e$, откуда $b \circ b = b$, где $b = f(e)$, а следовательно, $b = b \circ b^{-1} = e'$ - единичный элемент в группе G'.

2) $f(a^{-1}) = [f(a)]^{-1}$. Действительно,

$$f(a) \circ f(a^{-1}) = f(a * a^{-1}) = f(e) = e',$$

откуда $f(a^{-1}) = [f(a)]^{-1}$.

3) $f^{-1} : G' \to G$ также является изоморфизмом. Действительно, f^{-1} - снова биекция. Пусть $a', b' \in G'$. Покажем, что $f^{-1}(a' \circ b') = f^{-1}(a') * f^{-1}(b')$. Рассмотрим элементы $a, b \in G$ такие, что $a' = f(a)$, $b' = f(b)$. Тогда $f(a * b) = f(a) \circ f(b)$, откуда $f(a * b) = a' \circ b'$, а следовательно, $a * b = f^{-1}(a' \circ b')$ или $f^{-1}(a') * f^{-1}(b') = f^{-1}(a' \circ b')$.

Пример 1. В качестве изоморфного отображения f мультипликативной группы $(\mathbb{R}_+, \cdot)$ положительных чисел на аддитивную группу $(\mathbb{R}, +)$ всех вещественных чисел может служить $f = \ln$. Действительно, $\forall a, b \in \mathbb{R}_+$ имеем $\ln ab = \ln a + \ln b$ (биективность очевидна). Обратным к f является отображение $x \longmapsto e^x$.

Утверждение 1. Все циклические группы одного и того же порядка (в том числе и бесконечного) изоморфны.

Утверждение 2 (Кэли). Любая конечная группа G порядка n изоморфна некоторой подгруппе H симметрической группы S_n.

При доказательстве утверждения 2 приводится конкретный вид изоморфного отображения L:

$$\forall a \in G \quad a \mapsto L_a = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ ag_1 & ag_2 & \cdots & ag_n \end{pmatrix} \in S_n.$$

Тогда $H = \{L_a \mid a \in G\}$ – подгруппа S_n, изоморфная G.

Задача I. Определить подгруппу H группы S_n, изоморфную группе G:

а) $G = (\{0 ; 1\}, +(\mathrm{mod}\, 2)), n = 2$;

б) $G = (\{0, 1, 2\}, +(\mathrm{mod}\, 3)), n = 3$;

в) $G = (\{0, 1, 2, 3\}, +(\mathrm{mod}\, 4)), n = 4$.

Решение. а) Имеем: $0 \mapsto L_0 = \begin{pmatrix} 0 & 1 \\ 0+0 & 0+1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = e$,

$1 \mapsto L_1 = \begin{pmatrix} 0 & 1 \\ 1+0 & 1+1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = (0\ 1)$,

откуда $H = \{e, (0\ 1)\}$;

б) имеем: $0 \mapsto L_0 = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} = e$;

$1 \mapsto L_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1+0 & 1+1 & 1+2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} = (0\ 1\ 2)$,

$2 \mapsto L_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2+0 & 2+1 & 2+2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} = (0\ 2\ 1)$,

откуда $H = \{e, (0\ 1\ 2), (0\ 2\ 1)\}$;

в) имеем: $0 \mapsto L_0 = e$,

$1 \mapsto L_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix} = (0\ 1\ 2\ 3)$,

$2 \mapsto L_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix} = (0\ 2)(1\ 3)$,

$3 \mapsto L_3 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 1 & 2 \end{pmatrix} = (0\ 3\ 2\ 1)$,

откуда $H = \{e, (0\ 1\ 2\ 3), (0\ 2)(1\ 3), (0\ 3\ 2\ 1)\}$.

Задача 2. Показать, что группа положительных рациональных чисел по умножению не изоморфна группе всех рациональных чисел по сложению.

Решение. Пусть существует изоморфное отображение f группы $(\mathbb{Q}_+, \cdot)$ на $(\mathbb{Q}, +)$. Обозначим $a = f^{-1}(f(2)/2)$. Очевидно, что $2 \in \mathbb{Q}_+ \Rightarrow f(2) \in \mathbb{Q} \Rightarrow f(2)/2 \in \mathbb{Q} \Rightarrow f^{-1}(f(2)/2) \in \mathbb{Q}_+$. С другой стороны $a^2 = f^{-1}(f(2)/2) \cdot f^{-1}(f(2)/2) =$ (см. свойство 3 изоморфизма) $= f^{-1}(f(2)/2 + f(2)/2) = f^{-1}(f(2)) = 2$, но уравнение $a^2 = 2$ не имеет решений на множестве рациональных чисел.

Задача 3. Пусть G – группа с операцией $*$, π – биекция из G в G. Введём операцию $\circ$ на G следующим образом $c \circ d = \pi(a * b)$, где $c, d \in G$, $a = \pi^{-1}(c)$, $b = \pi^{-1}(d)$. Показать, что группа $(G, *)$ изоморфна группе $(G, \circ)$.

Решение. $\forall a, b \in G$ имеем $a = \pi^{-1}(\pi(a))$, $b = \pi^{-1}(\pi(b))$, откуда по определению $\circ$ получаем $\pi(a) \circ \pi(b) = \pi(a * b)$.

Задача 4. Найти все с точностью до изоморфизма группы порядка 4.

Решение. Пусть $G = \{a, в, c, d\}$. В силу задачи 3 для определённости можно считать, что a - единичный элемент. Рассмотрим следующее дополнительное условие

(I) $b = b^{-1}$, $c = c^{-1}$, $d = d^{-1}$

(т.е. при выполнении (I) каждый элемент из G обратен к самому себе).

Пусть сначала условие (I) выполняется. Тогда в силу коммутативности любой группы четвёртого порядка (см. предыдущий семинар) таблица Кэли для рассматриваемой группы имеет вид

	a	в	c	d
a	a	в	c	d
в	в	a	x	y
c	c	x	a	z
d	d	y	z	a

, где x, y, z неизвестны.

Отметим следующее очевидное свойство таблицы Кэли: в каждую строку (в каждый столбец) этой таблицы входит любой элемент из группы G, причём ровно по одному разу. Из этого свойства следует, что $\{x, y\} = \{c, d\}$, $\{x, z\} = \{в, d\}$, откуда $x = d$, $y = c$, $z = в$. Таким образом, существует единственная с точностью до изоморфизма группа G такая, что выполняется (I) (заметим, что построенная группа изоморфна группе $\langle (1\ 2), (3\ 4) \rangle = \{ e, (1\ 2), (3\ 4), (1\ 2)(3\ 4) \} \subset S_4$; здесь, например, $f(a) = e$, $f(в) = (1\ 2)$, $f(c) = (3\ 4)$, $f(d) = (1\ 2)(3\ 4)$), где f - изоморфизм).

Пусть теперь условие (I) не выполняется и ,например, $в \neq в^{-1}$. Пусть, например, $в^{-1} = d$. Рассмотрим таблицу Кэли для рассматриваемого случая

	a	в	c	d
a	a	в	c	d
в	в	x	y	a
c	c	y	z	w
d	d	a	w	v

где x, y, z , w , v неизвестны. Из таблицы следует, что $\{x, y\} = \{c, d\}$.

Предположим, что $x = d$, тогда $y = c$, и при этом в третью строку таблицы Кэли дважды войдёт элемент c . Но тогда $x = c$, $y = d$, а следовательно, таблица Кэли имеет вид

	a	в	c	d
a	a	в	c	d
в	в	c	d	a
c	c	d	z	w
d	d	a	w	v

Из таблицы следует, что $\{z, w\} = \{a, в\}$, $\{w, v\} = \{c, в\}$, откуда $z = a$, $w = в$, $v = c$, т.е. таблица Кэли имеет вид

	a	в	c	d
a	a	в	c	d
в	в	c	d	a
c	c	d	a	в
d	d	a	в	c

+	0	I	2	3
0	0	I	2	3
I	I	2	3	0
2	2	3	0	I
3	3	0	I	2

Нетрудно видеть, что построенная группа изоморфна группе $(\{0, 1, 2, 3\}, +(\mathrm{mod}\ 4))$ (здесь $f(a) = 0$, $f(в) = 1$, $f(c) = 2$, $f(d) = 3$, где f - изоморфизм ; см. таблицы Кэли для этих групп).

Аналогично рассматривается случай $в^{-1} = c$, а также случай $c^{-1} = d$, в каждом из которых получаемая в результате группа изоморфна группе $\{(0, 1, 2, 3)\ , +(\mathrm{mod}\ 4)\}$, а следовательно, все эти группы изоморфны друг другу. Таким образом, существуют 2 группы с точностью до изоморфизма порядка 4 .

<u>Смежные классы по подгруппе</u>. Пусть H - подгруппа группы G . <u>Левым (правым) смежным классом</u> группы G по подгруппе H (коротко G по H) называется множество $gH = \{gh \mid h \in H\}$ $(Hg = \{hg \mid h \in H\})$. Элемент g называется <u>представителем</u> смежного класса.

<u>Утверждение 3</u>. Два левых (правых) смежных класса G по H либо совпадают либо не имеют общих элементов. Разбиение G на левые (правые) смежные классы по H определяет на G отношение эквивалентности: $a \sim в \iff \exists g \in G \mid a, b \in gH$ $(a \sim в \iff \exists g \in G \mid a, b \in Hg)$.

Множество всех левых смежных классов G по H обозначается символом

G/H. Пусть G – конечная группа. Тогда из того, что $(\forall g \in G)$ отображение $h \mapsto gh, h \in H$, является взаимнооднозначным $(gh_1 = gh_2 \Rightarrow g^{-1}gh_1 = g^{-1}gh_2 \Rightarrow h_1 = h_2$, а следовательно, $h_1 \neq h_2 \Rightarrow gh_1 \neq gh_2)$, получаем $\forall gH \in G/H \quad |gH| = |H|$, откуда в силу $G = \bigcup_{gH \in G/H} gH$; $g_1H, g_2H \in G/H$, $g_1H \neq g_2H \Rightarrow g_1H \cap g_2H = \emptyset$ (см. утверждение 3) имеем

(2) $|G| = |G/H|\,|H|$.

Следствием из (2) является

Теорема (Лагранж). Порядок конечной группы делится на порядок каждой своей подгруппы.

Следствие. Порядок любого элемента делит порядок группы. Группа простого порядка p всегда циклическая и с точностью до изоморфизма единственная (см. утверждение об изоморфизме циклических групп одного порядка).

Пример 2. Пусть $G = S_3$, $H = \langle(1\ 3\ 2)\rangle$. Определить множество всех левых и правых смежных классов G по H. Показать, что $\forall g \in G\ gH = Hg$.

Решение. Заметим, что $S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ (поскольку $|S_3| = 3! = 6$, то других элементов нет), $H = \{e, (1\ 3\ 2), (1\ 3\ 2)^2\} = \{e, (1\ 3\ 2), (1\ 2\ 3)\}$ (порядок элемента $(1\ 3\ 2)$ равен 3, а следовательно, $\langle(1\ 3\ 2)\rangle = \{e, (1\ 3\ 2)^1, (1\ 3\ 2)^2\}$). Найдём теперь gH для каждого $g \in S_3$:

1/ $eH = H$,

2/ $(1\ 2)H = \{(1\ 2)e, (1\ 2)(1\ 3\ 2), (1\ 2)(1\ 2\ 3)\} = \{(1\ 2), (1\ 3), (2\ 3)\}$,

3/ $(1\ 3)H$ очевидно, содержит $(1\ 3) \in (1\ 2)H$, а следовательно, $(1\ 3)H = (1\ 2)H$ (см. утверждение 3),

4/ $(2\ 3)H$ очевидно, содержит $(2\ 3) \in (1\ 2)H$, а следовательно, $(2\ 3)H = (1\ 2)H$,

5/ $(1\ 2\ 3)H$ содержит $(1\ 2\ 3) \in H$, а следовательно, $(1\ 2\ 3)H = H$,

6/ $(1\ 3\ 2)H$ содержит $(1\ 3\ 2) \in H$, а следовательно, $(1\ 3\ 2)H = H$.

Таким образом, $eH = (1\ 2\ 3)H = (1\ 3\ 2)H = H$, $(1\ 2)H = (1\ 3)H = (2\ 3)H$, т.е. множество левых смежных классов (S_3 по $H = \langle(1\ 3\ 2)\rangle$) состоит из H, $(1\ 2)H$.

Определим теперь Hg для каждого $g \in S_3$:

1/ $He = H$,

2/ $H(1\ 2) = \{e(1\ 2), (1\ 3\ 2)(1\ 2), (1\ 2\ 3)(1\ 2)\} = \{(1\ 2), (2\ 3), (1\ 3)\} = (1\ 2)H$, 3/ $H(1\ 3)$ содержит $(1\ 3) \in H(1\ 2)$, а следовательно, $H(1\ 3) = H(1\ 2) = (1\ 2)H = (1\ 3)H$,

4/ $H(2\ 3)$ содержит $(2\ 3) \in H(1\ 2)$, а следовательно, $H(2\ 3) = H(1\ 2) = (1\ 2)H = (2\ 3)H$,

5/ $H(1\ 2\ 3)$ содержит $(1\ 2\ 3) \in H$, а следовательно, $H(1\ 2\ 3) = H = (1\ 2\ 3)H$.

6/ $H(1\ 3\ 2)$ содержит $(1\ 3\ 2) \in H$, а следовательно, $H(1\ 3\ 2) = H = (1\,3\,2)H$.

<u>Задача 5</u>. Пусть $G = S_3$, $H = \langle (2\ 3) \rangle$. Определить множество всех левых и правых смежных классов G по H. При каких $g \in G$ $gH = Hg$?

<u>Решение</u>. Заметим, что $H = \{e, (2\ 3)\}$. Найдём gH для каждого элемента $g \in S_3$:

1/ $eH = H$,

2/ $(1\ 2)H = \{(1\ 2), (1\ 2)(2\ 3)\} = \{(1\ 2), (1\ 2\ 3)\}$,

3/ $(1\ 3)H = \{(1\ 3), (1\ 3)(2\ 3)\} = \{(1\ 3), (1\ 3\ 2)\}$,

4/ $(2\ 3)H$ содержит $(2\ 3) \in H$, а следовательно, $(2\ 3)H = H$,

5/ $(1\ 2\ 3)H$ содержит $(1\ 2\ 3) \in (1\ 2)H$, а следовательно, $(1\ 2\ 3)H = (1\ 2)H$,

6/ $(1\ 3\ 2)H$ содержит $(1\ 3\ 2) \in (1\ 3)H$, а следовательно, $(1\ 3\ 2)H = (1\ 3)H$.

Таким образом, $eH = (2\ 3)H = H$, $(1\ 2)H = (1\ 2\ 3)H$, $(1\ 3)H = (1\ 3\ 2)H$, т.е. множество левых смежных классов состоит из $H, (12)H, (1\ 3)H$.

Определим Hg для каждого $g \in S_3$:

1/ $He = H = eH$,

2/ $H(1\ 2) = \{(1\ 2), (2\ 3)(1\ 2)\} = \{(1\ 2), (1\ 3\ 2)\} \neq (1\ 2)H$,

3/ $H(1\ 3) = \{(1\ 3), (2\ 3)(1\ 3)\} = \{(1\ 3), (1\ 2\ 3)\} \neq (1\ 3)H$,

4/ $H(2\ 3)$ содержит $(2\ 3) \in H$, а следовательно, $H(2\ 3) = H = (2\ 3)H$,

5/ $H(1\ 2\ 3)$ содержит $(1\ 2\ 3) \in H(1\ 3)$, а следовательно, $H(1\ 2\ 3) = H(1\ 3) \neq (1\ 2\ 3)H$,

6/ $H(1\ 3\ 2)$ содержит $(1\ 3\ 2) \in H(1\ 2)$, а следовательно, $H(1\ 3\ 2) = H(1\ 2) \neq (1\ 3\ 2)H$.

Таким образом, множество правых смежных классов S_3 по $H = \langle (2\ 3) \rangle$ состоит из H, $H(1\ 2)$, $H(1\ 3)$.

<u>Замечание 1</u>. Очевидно, что в коммутативной группе G для любой подгруппы $H \subset G$ выполняется $\forall g \in G \quad gH = Hg$.

а следовательно, в коммутативных группах можно не различать левые и правые смежные классы и говорить просто о смежных классах.

Задача 6. Определить смежные классы группы $G = (\{0,1,2,3,4,5\}, +(\mathrm{mod}\, 6)\}$ по $H = \langle 3 \rangle$.

Решение. Заметим, что $H = \{0, 3\}$. Определим теперь $g + H$ для каждого $g \in G$:

1/ $0 + H = H$,

2/ $1 + H = \{1, 4\}$,

3/ $2 + H = \{2, 5\}$,

4/ $3 + H = H$,

5/ $4 + H = 1 + H$,

6/ $5 + H = 2 + H$.

Таким образом, $G/H = \{H, 1+H, 2+H\}$.

Задача 7. Доказать, что порядок любого элемента g конечной группы G делит порядок группы G.

Решение. Пусть q - порядок элемента g. Тогда

$\langle g \rangle = \{e, g, \dots, g^{q-1}\}$

(см. семинар №9), и по теореме Лагранжа получаем, что $|G|$ делится на $|\langle g \rangle|$, т.е. на q.

3. Нормальные подгруппы. Подгруппа H группы G называется нормальной, если

$$\forall g \in G \quad gH = Hg.$$

В случае, когда H - нормальная подгруппа, уже не имеет смысла различать левые и правые смежные классы, а говорят просто о смежных классах G по H. Множество смежных классов при этом обозначается символом G/H. В силу замечания 1 любая подгруппа коммутативной группы G является нормальной.

Пример 3. Пусть $G = S_3$, $H = \langle (1\ 3\ 2) \rangle$. Тогда H - нормальная подгруппа (см. пример 2), напротив, подгруппа $H = \langle (2\ 3) \rangle$ не является нормальной (см. задачу 5).

Пусть G - группа порядка $2n$. Тогда любая её подгруппа порядка n называется подгруппой индекса 2.

Задача 8. Доказать, что любая подгруппа индекса 2 является нормальной.

Решение. Пусть H - подгруппа группы G, $|G| = 2n$, $|H| = n$, $g \in G$. Покажем, что

$$(2) \qquad gH = Hg$$

Возможны случаи: а/ $g \in H$, б/ $g \notin H$. Рассмотрим сначала случай а/. Из того, что $g \in H$ имеем $gH = H = Hg$, а следовательно, в этом случае (2) выполняется. Рассмотрим теперь случай б). Из того, что $g \notin H$, имеем $gH \cap H = \varnothing$ (так как, если $gh_1 = h_2$, где $h_1, h_2 \in H$, то $g = h_2 h_1^{-1} \in H$), и при этом $|gH| = |H| = n$, а следовательно, $|gH \cup H| = |gH| + |H| = 2n$. Но тогда $gH \cup H = G$, а следовательно, $gH = G \setminus H$. Совершенно аналогично получаем, что $Hg = G \setminus H$, откуда и следует (2).

Задача 9. Доказать, что множество Z всех элементов группы G, каждый из которых перестановочен со всеми элементами этой группы, является нормальной подгруппой (центр группы G).

Решение. Покажем, что Z - подгруппа. Пусть $a_1, a_2 \in Z$. Тогда

$\forall g \in G \quad g(a_1 a_2) = (g a_1) a_2 = (a_1 g) a_2 = a_1 (g a_2) = a_1 (a_2 g) = (a_1 a_2) g$,

а следовательно, $a_1 a_2 \in Z$. Таким образом $a_1, a_2 \in Z \Rightarrow a_1 a_2 \in Z$. Очевидно, что $e \in Z$, так как $\forall g \in G \quad eg = ge$. Пусть теперь $a \in Z$, покажем, что $a^{-1} \in Z$. Действительно, $\forall g \in G \quad ga = ag$, откуда $\forall g \in G \quad a^{-1} g = g a^{-1}$, а следовательно, $a^{-1} \in Z$. Таким образом, Z - подгруппа, и при этом $\forall g \in G$ выполняется

$$gZ = \{ga \mid a \in Z\} = \{ag \mid a \in Z\} = Zg.$$

Задача 10. Элемент $aba^{-1}b^{-1}$ называется коммутатором элементов a и b в группе G. Доказать, что все коммутаторы и их произведения (с конечным числом сомножителей) — коммутант К гр. G образуют нормальную подгруппу.

Решение. Заметим, что $(aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1}$, т.е. элемент, обратный к коммутатору элементов a, b, является коммутатором элементов b, a. Пусть теперь $h = h_1 \dots h_k$, где h_i - коммутаторы, тогда $h^{-1} = h_k^{-1} \dots h_1^{-1}$, где h_i^{-1} - снова коммутаторы, т.е. h^{-1} также как и h является произведением коммутаторов. Заметим далее, что e - коммутатор элементов e и e. Но тогда множество K всех коммутаторов и их конечных произведений является подгруппой (по определению К имеем $h_1, h_2 \in K \Longrightarrow h_1 h_2 \in K$). Покажем, что К - нормальная подгруппа. Заметим, что

$$\forall g, a, b \in G \quad g a b a^{-1} b^{-1} = \tilde{a} \tilde{b} \tilde{a}^{-1} \tilde{b}^{-1} g,$$

где $\tilde{a} = g a g^{-1}$, $\tilde{b} = g b g^{-1}$ (действительно, $\tilde{a} \tilde{b} \tilde{a}^{-1} \tilde{b}^{-1} g = g a \underline{g^{-1} g}\, b \underline{g^{-1} g}\, a^{-1} \underline{g^{-1} g}\, b^{-1} \underline{g^{-1} g} = g a b a^{-1} b^{-1}$). Совершенно аналогично получаем $\forall\ g, a_1, b_1, \ldots, a_k, b_k \in G$

$$g a_1 b_1 a_1^{-1} b_1^{-1} \ldots a_k b_k a_k^{-1} b_k^{-1} = \tilde{a}_1 \tilde{b}_1 \tilde{a}_1^{-1} \tilde{b}_1^{-1} \ldots \tilde{a}_k \tilde{b}_k \tilde{a}_k^{-1} \tilde{b}_k^{-1} g,$$

где $\tilde{a}_i = g a_i g^{-1}$, $\tilde{b}_i = g b_i g^{-1}$, $i = 1, 2, \ldots, k$, $k \geq 1$, откуда следует, что любой элемент gh, где $g \in G$, $h \in K$ может быть представлен в виде $\tilde{h} g$, где $\tilde{h} \in K$, а следовательно, $gK \subseteq Kg$. Взяв в последнем включении вместо g элемент g^{-1}, имеем $g^{-1} K \subseteq K g^{-1}$ откуда $Kg \subseteq gK$, а следовательно, $\forall g \in G \quad gK = Kg$.

<u>Задача 11</u>. Доказать, что если пересечение двух нормальных подгрупп H_1 и H_2 группы G содержит лишь единицу e, то любой элемент $h_1 \in H_1$ перестановочен с любым элементом $h_2 \in H_2$.

<u>Решение</u>. Предположим, что для некоторых $h_1 \in H_1$, $h_2 \in H_2$ выполняется $h_1 h_2 \neq h_2 h_1$. Тогда $h = h_1 h_2 h_1^{-1} h_2^{-1} \neq e$. В силу того, что H_1, H_2 - нормальные подгруппы, имеем $\forall g \in G\ g H_1 g^{-1} = H_1$, $g H_2 g^{-1} = H_2$, а следовательно, $h \in H_1$ (так как $h_2 h_1^{-1} h_2^{-1} \in H$, $h_1 \in H_1$), $h \in H_2$ (так как $h_1 h_2 h_1^{-1} \in H_2$, $h_2^{-1} \in H_2$). Таким образом, $h \neq e$, $h \in H_1 \cap H_2$, что противоречит условиям задачи.

<u>Факторгруппа</u>. Пусть G - некоторая группа, H - нормальная подгруппа. Рассмотрим множество смежных классов G/H. Введём бинарную операцию на множествах из G:

$$AB = \{ab \mid a \in A, b \in B\}, \text{ где } A, B \subseteq G.$$

Ассоциативность в G влечёт ассоциативность введённой бинарной операции. Заметим, что если H - подгруппа, то $H^2 = H$ (так как $e \in H$ и композиция не выводит из H).

Произведением смежных классов aH, bH является множество $aH \cdot bH$. Заметим, что если H не является нормальным делителем, то последнее множество, вообще говоря, не обязано быть снова смежным классом. Так, например, в случае $H = \langle(1\ 2)\rangle = \{e, (1\ 2)\} \subset S_3$ имеем

$H\cdot(1\ 3)\ H = H\cdot\{(1\ 3),(1\ 3)(1\ 2)\} = H\cdot\{(1\ 3),(1\ 2\ 3)\} = \{(1\ 3),(1\ 2)(1\ 3),$ $(1\ 2\ 3),(1\ 2)(1\ 2\ 3)\} = \{(1\ 3),(1\ 3\ 2),(1\ 2\ 3),(2\ 3)\} = (1\ 3)\ H \cup (2\ 3)\ H$.

Очевидно, что $H\cdot(1\ 3)\ H$ уже не является левым смежным классом S_3 по H, так как любой левый смежный класс содержит ровно 2 элемента (так как $|H| = 2$), а $H\cdot(1\ 3)H$ содержит 4 элемента.

Однако, в случае, когда H – нормальный делитель, имеем

$$aH\cdot bH = a(Hb)H = a(bH)H = abH^2 = abH,$$

т.е. произведение смежных классов снова является смежным классом.

Очевидные свойства

$aH\cdot bH = abH$

$H\cdot aH = aH\cdot H = aH$

$a^{-1}H\cdot aH = aH\cdot a^{-1}H = eH = H$

показывают, что справедлива

Теорема. Если H – нормальная подгруппа в G , то операция умножения $aH\cdot bH = abH$ наделяет фактормножество G/H строением группы, называемой факторгруппой G по H . Смежный класс H служит единичным элементом в G/H , а $a^{-1}H = (aH)^{-1}$ – элементом, обратным к aH .

Замечание 2. В случае конечной группы G в силу (2) порядок факторгруппы G/H определяется по формуле

$$|G/H| = |G|/|H|.$$

Замечание 3. В случае аддитивно записываемых абелевых групп G вместо $aH\cdot bH = abH$ пишем

$$(a+H) + (b+H) = (a+b) + H.$$

В абелевых группах G/H часто называют группой G по модулю H , а в применении к паре $G = \mathbb{Z}$, $H = m\mathbb{Z}$ употребляется выражение "группа $\mathbb{Z}$ по модулю m " .

Пример 4. Пусть $G = (\mathbb{Z}, +)$, $H = 3\mathbb{Z} = \{0, \pm 3, \pm 6, \dots\}$. Тогда $G/H = \{H, 1+H, 2+H\}$ – факторгруппа, называемая группой целых чисел по модулю 3 .

Задача II. Доказать, что если H – нормальная подгруппа группы G , $a,b \in G$, то $\forall\ a_1 \in aH, \forall\ b_1 \in bH$ выполняется $a_1b_1H = abH$. Привести пример группы G и подгруппы $H \subset G$ таких, что для некоторых a, b, a_1 ,

$в_1 \in G$ таких, что $а_1 \in аН$, $в_1 \in вН$, выполняется $а_1 в_1 Н \neq авН$.

Решение. I. В силу $а_1 \in аН$, $в_1 \in вН$ имеем $а_1 Н = аН$, $в_1 Н = вН$, а следовательно, $а_1 в_1 Н = а_1 Н \cdot в_1 Н = аН \cdot вН = авН$.

2. Пусть $G = S_3$, $Н = \langle (I\ 2) \rangle = \{е\ , (I\ 2)\}$, $а = в = (I\ 3)$, $а_1 = в_1 = (I\ 2\ 3)$. Тогда $а_1 = в_1 \in аН = вН = \{(I\ 3), (I\ 2\ 3)\}$, $а_1 в_1 Н = (I\ 3\ 2)Н = \{(I\ 3\ 2), (I\ 3\ 2)(I\ 2)\} = \{(I\ 3\ 2), (2\ 3)\} \neq \{е\ , (I\ 2)\} = авН$.

Задача I2. Доказать, что если в группе G порядка n $\forall g \in G$ выполняется $g^2 = е$, то $n = 2^к$, где $к \geq 0$.

Решение. Возможны случаи: а) $G = \{е\}$; б) $(\exists g \in G)(g \neq е)$. В случае а) $|G| = n = I = 2^0$. Рассмотрим теперь случай б). Пусть $a \in G$, $a \neq е$. Тогда $\langle a \rangle = \{е\ , a\}$. Обозначим $Н_1 = \langle a \rangle$, $G_1 = G/Н_1$ - факторгруппа G по $Н_1$ (заметим, что $Н_1$ - нормальная подгруппа, поскольку группа G коммутативна, см. практические занятия №8-9, задача I5). В силу замечания 2 имеем

$$|G_1| = |G/H_1| = |G|/|H_1| = n/2.$$

Заметим, что $\forall a_1 \in G_1$ выполняется $а_I^2 = е_I$, где $е_I = Н_I$ - единичный элемент в группе G_1 (действительно, $а_I = g Н_I$, где g - некоторый элемент из G , а следовательно, $(g Н_I)^2 = g^2 Н_1 = еН_I = Н_1 = е_I$). Но тогда аналогично предыдущему либо $|G_1| = n/2 = I$ и тогда $n = 2^I$, либо мы перейдём к группе G_2 такой, что $|G_2| = |G_1|/2 = n/2^2$, $\forall a_2 \in G_2$ $а_2^2 = е_2$, где $е_2$ - единичный элемент группы G_2 . Поскольку n - конечное число, то продолжая указанный процесс последовательного перехода от группы G_i к некоторой группе G_{i+1}, мы при некотором номере $к$ получим $|G_k| = n/2^к = I$ и тогда $n = 2^к$.

Задача I3. Доказать, что факторгруппа $G/Н$ тогда и только тогда коммутативна, когда $Н$ содержит коммутант $К$ группы G (см. задачу I0).

Решение. Запишем формулу, выражающую коммутативность G/H

$$\forall a, b \in G \quad aH \cdot bH = bH \cdot aH,$$

откуда $\forall$ а,в $\in G$ $авН = ваН$, а следовательно, $\forall$ а,в $\in G$ $а^{-I}в^{-I}Н = в^{-I}а^{-I}Н$. Но тогда $\forall$ а,в $\in G$ $\exists h_1, h_2 \in Н$: $а^{-I}в^{-I} h_1 = в^{-I}а^{-I} h_2$, откуда $\forall$ а,в $\in G$ $ава^{-I}в^{-I} \in Н$. Таким образом, коммутативность $G/Н$ эквивалентна тому, что $Н$ содержит коммутатор любых элементов а,в $\in G$, откуда и следует справедливость доказываемого утверждения.

$\Rightarrow K \subseteq H$

<u>Задача I4</u>. Доказать, что факторгруппа некоммутативной группы G по её центру Z (см. задачу 9) не может быть циклической.

<u>Решение</u>. Предположим, что G/Z - циклическая группа. Тогда для некоторого элемента $a \in G$ выполняется $G/Z = \langle aH \rangle$, а следовательно, для любых двух элементов $g_1, g_2 \in G$ найдутся $n_1, n_2 \in \mathbb{Z}$ такие, что

$$g_1 H = (aH)^{n_1} = a^{n_1} H, \quad g_2 H = (aH)^{n_2} = a^{n_2} H,$$

откуда для некоторых элементов $h_1, h_2 \in Z$ выполняется $g_1 = a^{n_1} h_1, g_2 = a^{n_2} h_2$.
Используя теперь то, что $h_1, h_2 \in Z$, имеем

$$g_1 g_2 = (a^{n_1} h_1)(a^{n_2} h_2) = a^{n_1+n_2} h_1 h_2 = a^{n_2} a^{n_1} h_2 h_1 = (a^{n_2} h_2)(a^{n_1} h_1) = g_2 g_1,$$

а это противоречит тому, что группа G не является коммутативной.

<u>Гомоморфизмы</u>. Отображение $f : G \to G'$ группы $(G, *)$ в $(G', \circ)$ называется <u>гомоморфизмом</u>, если

$$f(a * b) = f(a) \circ f(b) \quad \forall a, b \in G.$$

<u>Ядром</u> гомоморфизма f называется множество

$$\operatorname{Ker} f = \{ g \in G \mid f(g) = e' \text{ - единичный элемент в } G' \}$$

Гомоморфное отображение группы в себя называется ещё <u>эндоморфизмом</u>. Если f - сюръективное отображение, то гомоморфизм называется <u>эпиморфизмом</u>. В случае, если f - инъективное отображение, гомоморфизм называется <u>мономорфизмом</u>. Если f - биективное отображение, то f - изоморфизм.

Свойства гомоморфизма:

I/ $f(e) = e'$ (см. доказательство аналогичного свойства изомофизма).

2/ $f(a^{-1}) = [f(a)]^{-1}$ (см. доказательство аналогичного свойства изоморфизма).

3/ $\operatorname{Ker} f$ - подгруппа в G. Это следует из 1/,2/.

4/ $\operatorname{Ker} f$ - нормальная подгруппа в G. Доказем это. Обозначим $H = \operatorname{Ker} f$. Тогда $\forall g \in G, \forall h \in H$ имеем (опускаем $*$, $\circ$)

$$f(g h g^{-1}) = f(g) f(h) [f(g)]^{-1} = f(g) e' [f(g)]^{-1} = e',$$

а следовательно, $g h g^{-1} \in H$, откуда $g H g^{-1} \subseteq H$. Заменив g на g^{-1} имеем $g^{-1} H g \subseteq H$, откуда $H \subseteq g H g^{-1}$, а следовательно, $g H g^{-1} = H$ или $gH = Hg$, т.е. H - нормальная подгруппа.

<u>Теорема</u> (основная теорема о гомоморфизмах). Пусть $f : G \to G'$ - гомоморфизм групп с ядром $H = \operatorname{Ker} f$. Тогда H - нормальная подгруппа в G и факторгруппа G/H изоморфна подгруппе $f(G)$ (образу G).

Обратно, если H - нормальная подгруппа в G , то отображение f : $G \to G/H$, определяемое формулой $\forall g\in G\ f(g) = gH$, есть эпиморфизм с ядром H .

Задача I5. Доказать, что если группа G гомоморфно отображается на группу G' , причём элемент a из G отображается на $a'\in G'$, то

а/ порядок a делится на порядок a' ;

б/ порядок G делится на порядок G' .

Решение. Пусть $H = \mathrm{Ker}\, f$, где f - гомомофное отображение G на G' (при этом $f(G) = G'$) . Тогда в силу основной теоремы о гомоморфизме группа G/H изоморфна G' , а следовательно, $|G/H| = |G'|$, откуда в силу того, что $|G/H| = |G|/|H|$, имеем $|G| = |H||G'|$, а следовательно, выполняется б/. Пусть q, q' - порядки элементов a , a' $(= f(a))$, соответственно. Тогда $(a')^q = f(a^q) = f(e) = e'$, откуда $q = l q'$, где $l \in \mathbb{Z}$, а следовательно, q делится на q' , т.е. выполняется а/.

Задача I6. Найти все гомоморфные отображения циклической группы $(G =)\langle a\rangle$ порядка I8 в циклическую группу $(G' =)\langle b\rangle$ порядка 6.

Решение. Гомоморфный образ G при отображении $f : G \to G'$ есть подгруппа группы G' (см. теор. о гом. ~~свойства гомоморфизма~~), ~~порядок которой делит порядок группы G' см. свойства гомоморфизма~~, порядок которой делит порядок группы G' (см. теорему Лагранжа), а также порядок группы G (см. задачу I5), т.е. делит числа 6 и I8 , а следовательно, $|f(G)|\in\{2 , 3 , 6\}$.

а/ Пусть $|f(G)| = 2$, тогда $f(G) = \langle b^3\rangle = \{e', b^3\}$ (каждому делителю d порядка циклической группы соответствует одна и только одна её циклическая подгруппа порядка d) , где $e' = в^0$. Верно! Обозначим $H = \mathrm{Ker}\, f$. Тогда по основной теореме о гомоморфизмах факторгруппа G/H изоморфна $f(G)$, т.е. имеет порядок 2 . Но тогда $|G/H| = |G|/|H| = 2$, а следовательно, $|H| = 9$, откуда $H = \langle a^2\rangle$. При этом, очевидно, $G/H = \{H , aH\}$, $f(H) = \{e\}$, $f(aH) = \{в^3\}$, т.е. отображение f полностью определено.

б/ Пусть $|f(G)| = 3$, тогда $f(G) = \langle в^2\rangle = \{e, в^2, в^4\} = \langle в^4\rangle$. Обозначим $H = \mathrm{Ker}\, f$. Тогда $|G/H| = |G|/|H| = |f(G)| = 3$, откуда $|H| = 6$, а следовательно, $H = \langle a^3 \rangle$. При этом, очевидно, $G/H = \{H, aH, a^2H\}$, $f(H) = \{e\}$, и возможны 2 случая: I/ $f(aH) = в^2$, $f(a^2H) = в^4$; 2/ $f(aH) = \{в^4\}$, $f(a^2H) = \{в^2\}$.

в/ Пусть $|f(G)| = 6$, тогда $f(G) = \langle в \rangle = \langle в^5 \rangle$. Обозначим $H = \mathrm{Ker}\, f$. Тогда $|G/H| = |G|/|H| = |f(G)| = 6$, откуда $|H| = 3$, а следовательно, $H = \langle a^6 \rangle$. При этом, очевидно, $G/H = \{H, aH, a^2H, a^3H, a^4H, a^5H\}$, и возможны два случая: I/ $f(a^kH) = \{в^k\}$, $k = \overline{0,5}$; 2/ $f(a^kH) = \{в^{5k}\} = \{в^{6-k}\}$, $k = \overline{0,5}$.

Задача I7. Найти все гомоморфные отображения циклической группы $G = \langle a \rangle$ порядка 6 в циклическую группу $G' = \langle в \rangle$ порядка I8.

Решение. Гомоморфный образ G при отображении $f: G \to G'$ есть подгруппа группы G', порядок которой делит порядки групп G', G (см. задачу I6), т.е. делит числа 18, 6, а следовательно, $|f(G)| \in \{2, 3, 6\}$.

а/ Пусть $|f(G)| = 2$. Тогда $f(G) = \langle в^9 \rangle$. Обозначим $H = \mathrm{Ker}\, f$. Тогда $|G/H| = |G|/|H| = |f(G)| = 2$, откуда $|H| = 3$, а следовательно, $H = \langle a^2 \rangle$. При этом, очевидно, $G/H = \{H, aH\}$, $f(H) = \{e\}$, $f(aH) = \{в^9\}$, т.е. отображение f полностью определено.

б/ Пусть $|f(G)| = 3$. Тогда $f(G) = \langle в^6 \rangle = \langle в^{I2} \rangle$. Обозначим $H = \mathrm{Ker}\, f$. Тогда $|G/H| = |G|/|H| = |f(G)| = 3$, откуда $|H| = 2$, а следовательно, $H = \langle a^3 \rangle$. При этом, очевидно, $G/H = \{H, aH, a^2H\}$, $f(H) = \{e\}$ и возможны 2 случая: I/ $f(aH) = \{в^6\}$, $f(a^2H) = \{в^{I2}\}$; 2/ $f(aH) = \{в^{I2}\}$, $f(a^2H) = \{в^6\}$.

в/ Пусть $|f(G)| = 6$. Тогда $f(G) = \langle в^3 \rangle = \langle в^{I5} \rangle$. Обозначим $H = \mathrm{Ker}\, f$. Тогда $|G/H| = |G|/|H| = |f(G)| = 6$, откуда $|H| = I$, а следовательно, $H = \{e\}$. При этом, очевидно, $G/H = G$ и возможны два случая: I/ $f(a^k) = в^{3k}$, $k = \overline{0,5}$; 2/ $f(a^k) = в^{I5k} = в^{I8-3k}$, $k = \overline{0,5}$.

Задача I8. Доказать, что группа G' тогда и только тогда является гомоморфным образом циклической группы $G = \langle a \rangle$, когда G' также циклическая группа и её порядок делит порядок группы G.

Решение. Необходимость. Пусть G' – гомоморфный образ группы G при отображении $f: G \to G'$. Тогда в силу задачи I5 порядок группы

т.е. f – эпиморфизм $G' = f(G) \sim G/H \Rightarrow$
$\Rightarrow |G'| = |G|/|H| \Rightarrow |G| = |G'||H|$ кон. л

G' делит порядок группы G. Покажем, что G' - циклическая группа. В силу основной теоремы о гомоморфизмах группа G' изоморфна факторгруппе G/H, где $H = \operatorname{Ker} f$. Заметим, что G/H - циклическая группа с образующей aH (действительно, $\forall g \in G$ имеем $g = a^k$, где $k \in \mathbb{Z}$, а следовательно, $gH = a^kH = (aH)^k$), а тогда циклической будет и изоморфная ей группа G'. (т.е. $G/H = \langle aH \rangle$)

Достаточность. Пусть G' - циклическая группа и её порядок делит порядок группы G. Выделим в группе G циклическую подгруппу H порядка $d = |G| / |G'|$. Это можно сделать, поскольку $|G|$ делится на d. Тогда G/H - циклическая группа (см. доказательство необходимости), причём $|G/H| = |G|/|H| = |G|/d = |G'|$. Таким образом, G' и G/H - циклические группы одного порядка, а следовательно, они изомофны, т.е. $\exists f : G/H \to G'$. В силу основной теоремы о гомоморфизмах отображение $\varphi : G \to G/H$ такое, что $\forall a \in G$ $\varphi(a) = aH$, есть эпиморфизм. Но тогда отображение $f \circ \varphi : G \to G'$ $\{((f\circ\varphi)(a) = f(\varphi(a)), a \in G)\}$ является также эпиморфизмом, а следовательно, G' является гомоморфным образом G при отображении $f \circ \varphi$.

Образующие и определяющие соотношения в группах. Пусть F_d - произвольная группа, порождённая d образующими $f_1, \ldots, f_d$. Тогда каждый элемент f записывается (в общем случае неоднозначно) в виде

(4) $$f = f_{i_1}^{s_1} f_{i_2}^{s_2} \ldots f_{i_k}^{s_k}, \; i_j \in \{1,2,\ldots,d\}, \; s_j \in \mathbb{Z},$$

где $i_j \neq i_{j+1}$, $j = 1,2,\ldots, k-1$. Это всегда достигается заменами

$$f_i^s f_i^t = f_i^{s+t}, \; f_i^0 = e, \; f_j e = e f_j = f_j.$$

Если $f = e \iff s_1 = \ldots = s_k = 0$ для каждого f, записанного в виде (4), то говорят, что F_d - свободная группа, порождённая d свободными образующими.

Элементы группы F_d обычно называются словами в алфавите $\{f_1, f_1^{-1}, \ldots$ $\ldots, f_d, f_d^{-1}\}$ (e - пустое слово). Несократимая запись (4) слова f и его длина $l(f) = |s_1| + \ldots + |s_k|$ однозначно определены, так как в противном случае слово $e = f f^{-1}$ имело бы длину > 0. При данном d две свободные группы F_d и G_d, порождённые свободными образующими $f_1, \dots, f_d$ и $g_1, \dots, g_d$ (соответственно) изоморфны: достаточно положить $\varphi(f_i) = g_i$ и для произвольного слова f вида (4) считать

$$\varphi(f) = g_{i_1}^{s_1} g_{i_2}^{s_2} \dots g_{i_k}^{s_k}.$$

Если G_d не является свободной группой, то φ - всего лишь эпиморфизм (так как $\varphi(F_d) = G_d$) с ядром $\mathrm{Ker}\ \Phi$, состоящим из тех слов, которые при подстановке $f_i \mapsto g_i$ переходят в единичный элемент группы G_d.

<u>Пример 5</u>. 1. $d = 1$, $F_1 = \langle 1 \rangle = (\mathbb{Z}, +)$.

2. $d = 2$, $F_2 = \langle (0, 1), (1, 0) \rangle = (\mathbb{Z}^2, +)$, где $\mathbb{Z}^2$ - множество пар вида (m, n), $m, n \in \mathbb{Z}$, $+$ - покоординатное сложение пар.

Пусть F_d - свободная группа с d свободными образующими $f_1, \dots, f_d$, $S = \{w_i, i \in I\}$ - некоторое множество элементов $w_i(f_1, \dots, f_d) \in F_d$, т.е. слов в алфавите $\{f_1, f_1^{-1}, \dots, f_d, f_d^{-1}\}$ и $K = \langle S^{F_d} \rangle$ - наименьшая нормальная подгруппа в F_d, содержащая S (пересечение всех нормальных подгрупп, содержащих S). Говорят, что группа G задана d образующими $a_1, \dots, a_d$ и соотношениями $w_i(a_1, \dots, a_d) = e$, $i \in I$, если $\exists$ эпиморфизм $\pi : F_d \longrightarrow G$ с ядром K такой, что $\pi(f_k) = a_k$, $1 \le k \le d$. При этом пишут

$$G = \langle a_1, \dots, a_d \mid w_i(a_1, \dots, a_d) = e, i \in I \rangle.$$

<u>Пример 6</u>. Пусть $d = 1$, $F_1 = \langle f_1 \rangle$, $S = \{w_1\}$, $w_1 = f_1^3$. Тогда $K = \{f_1^{3k}, k \in \mathbb{Z}\}$ - наименьшая нормальная подгруппа (циклическая группа коммутативна, а поэтому в ней всякая подгруппа является нормальной), содержащая f_1^3. Рассмотрим $G = \{e, a, a^2\}$, $\pi : F_1 \longrightarrow G$, где $\pi(f_1^n) = a^{n \,(\mathrm{mod}\, 3)}$. Тогда π - эпиморфизм с ядром $\mathrm{Ker}\ \pi = K$ и $\pi(f_1) = a$, а следовательно, $G = \langle a \mid a^3 = e \rangle$.

<u>Задача 19</u>. Пусть в группе $G = \langle u, v \rangle$ выполняются следующие соотношения $u^2 = e$, $v^5 = e$, $(uv)^4 = e$, $(uv^{-2}uv^2)^2 = e$. Доказать, что в группе G справедливы равенства а/ $(vu)^4 = e$; б/ $uv^{-2}uv^2 = v^{-2}uv^2u$; в/ $v^{-1}uv = v^3uv^{-1}uv^{-1}u$.

<u>Решение</u>. а/ В силу $(uv)^4 = e$ имеем

$$uv\,uv\,uv\,uv = e$$

Умножая это равенство слева на u^{-1}, а справа на u, имеем

$$u^{-1}u\,vu\,vu\,vu\,vu = u^{-1}u = e,$$

откуда $(vu)^4 = e$.

б/ Из $u^2 = e$, $(uv^{-2}uv^2)^2 = e$ имеем $u^{-1} = u$,

$$uv^{-2}uv^2 = (uv^{-2}uv^2)^{-1} = v^{-2}u^{-1}v^2u^{-1} = v^{-2}uv^2u.$$

в/ В силу $(uv)^4 = uv\,uv\,uv\,uv = e$ имеем

$v^{-1}u\,v^{-1}u\,v^{-1}u\,v^{-1}u = e$, откуда $uv^{-1}uv^{-1}u = vuv$, а следовательно, используя то, что $v^5 = e$ (откуда $v^4 = v^{-1}$), имеем

$$v^3uv^{-1}uv^{-1}u = v^4uv = v^{-1}uv.$$

Задача 20. Пусть в группе $G = \langle a, в \rangle$ выполняются соотношения

$$a^4 = в^3 = (aв)^2 = e.$$

Доказать, что элементы a^2, $в^{-1}a^2в$, $вa^2в^{-1}$ попарно перестановочны.

Решение. Покажем, что перестановочны элементы a^2, $в^{-1}a^2в$, т.е. что выполняется

(5) $$a^2в^{-1}a^2в = в^{-1}a^2вa^2$$

Обозначим $c = a^2в^{-1}a^2в$, тогда $c^{-1} = в^{-1}a^{-2}вa^{-2}$ или, используя то, что $a^4 = e$, а следовательно, $a^2 = a^{-2}$, имеем $c^{-1} = в^{-1}a^2вa^2$, откуда получаем, что (5) эквивалентно условию $c = c^{-1}$ или $c^2 = e$. Используя то, что $(aв)^2 = e$, имеем $aвaв = e$, откуда

(6) $$вa = a^{-1}в^{-1}, \quad a^{-1} = вaв.$$

Используя (6), имеем $c = a^2в^{-1}a^2в = a^{-2}в^{-1}a^2в = a^{-1}(a^{-1}в^{-1})a^2в = a^{-1}(вa)a^2в = a^{-1}вa^3в = a^{-1}вa^{-1}в = вaввaвв = вa^2в^2$, а следовательно, $c^2 = вa^2в^2вa^2в^2 = вa^2в^3a^2в^2 = вa^4в^2 = в^3 = e$, т.е. элементы a^2, $в^{-1}a^2в$ перестановочны.

Покажем, что перестановочны элементы a^2, $вa^2в^{-1}$, т.е. что выполняется

(7) $$a^2вa^2в^{-1} = вa^2в^{-1}a^2.$$

Обозначим $d = a^2вa^2в^{-1}$, тогда $d^{-1} = вa^2в^{-1}a^2$, откуда получаем, что (7) эквивалентно условию $d = d^{-1}$ или $d^2 = e$. Используя то, что $(aв)^2 = e$, имеем $aвaв = e$, откуда

(8) $\quad a = в^{-1}a^{-1}в^{-1}$, $в^{-1} = aвa$, $aв^{-1}a = a^2вa^2$.

Используя (8), имеем

$$d^2 = a^2вa^2\, в^{-1}\, a^2вa^2 в^{-1} = aв^{-1}aв^{-1}aв^{-1}aв^{-1} = в^{-1}a^{-1}в^{-1}\, в^{-1}\, в^{-1}a^{-1}в^{-1} \cdot$$
$$\cdot\, в^{-1}\, в^{-1}a^{-1}в^{-1}\, в^{-1}\, в^{-1}a^{-1}в^{-1}\, в^{-1} = в^{-1}a^{-1}в^{-3}a^{-1}в^{-3}a^{-1}в^{-3}a^{-1}в^{-2} = в^{-1}a^{-4}в^{-2} =$$
$$= в^{-3} = e\ .$$

Покажем теперь, что перестановочны элементы $в^{-1}a^2в$, $вa^2в^{-1}$, т.е. что выполняется $в^{-1}a^2в\, вa^2в^{-1} = вa^2в^{-1}\, в^{-1}a^2в$ или

(9) $$в^{-1}a^2в^{-1}a^2в^{-1} = вa^2вa^2в\ .$$

Обозначим $f = в^{-1}a^2в^{-1}a^2в^{-1}$, тогда $f^{-1} = вa^2вa^2в$, откуда получаем, что (9) эквивалентно условию $f = f^{-1}$ или $f^{-2} = e$. Используя то, что $(aв)^2 = e$, имеем $aвaв = e$, откуда $в = a^{-1}в^{-1}a^{-1}$, а следовательно,

$$f^{-1} = вa^2вa^2в = a^{-1}в^{-1}a^{-1}\, a^2\, a^{-1}в^{-1}a^{-1}\, a^2\, a^{-1}в^{-1}a^{-1} =$$
$$= a^{-1}в^{-1}\, a^{-1}a^2a^{-1}\, в^{-1}\, a^{-1}a^2a^{-1}\, в^{-1}a^{-1} = a^{-1}в^{-3}a^{-1} = a^{-2}\ ,$$

откуда $f^{-2} = a^{-4} = e$.

<u>Задача 2I</u>. Пусть мы находимся в условиях задачи 20. Показать, что подгруппа $\langle a^2, в \rangle$ является нормальной подгруппой группы G .

<u>Решение</u>. Заметим, что в силу (8) выполняется

(I0) $\quad aвa^{-1} = (aв)\, a^{-1} = (aв)a^3 = aвa^3 = (aвa)\, a^2 = в^{-1}a^2 \in \langle a^2, в \rangle$,

(II) $\quad aв^{-1}a^{-1} = (aвa^{-1})^{-1} = a^2в \in \langle a^2, в \rangle$,

(I2) $\quad a^{-1}вa = (a^{-1})вa = a^3вa = a^2\,(aвa) = a^2в^{-1} \in \langle a^2, в \rangle$,

(I3) $\quad a^{-1}в^{-1}a = (a^{-1}вa)^{-1} = вa^2 \in \langle a^2, в \rangle$.

Кроме того, очевидно, что

(I4) $\quad a\,(a^2)\,a^{-1} = a^{-1}(a^2)\,a = a\,(a^{-2})\,a^{-1} = a^{-1}(a^{-2})\,a = a^2 \in \langle a^2, в \rangle$,

(I5) $\quad вa^2в^{-1},\ в^{-1}a^2в\ ,\ вa^{-2}в^{-1}\ ,\ в^{-1}a^{-2}в \in \langle a^2, в \rangle$,

(I6) $\quad в\, в\, в^{-1} = в^{-1}\, в\, в = в \in \langle a^2, в \rangle,\ в\, в^{-1}в^{-1} = в^{-1}\, в^{-1}\, в = в^{-1} \in \langle a^2, в \rangle$,

Пусть теперь $h \in H \overset{df}{=\!=} \langle a^2, в \rangle$. Тогда

$h = h_1^{i_1} h_2^{i_2} \ldots h_l^{i_l}$, где $h_j \in \langle a^2, в \rangle$, $i_j \in \{1\ ;\ -1\}$, $j = \overline{1, к}$,

и в силу (I0), (II), (I4) выполняется

$$a h a^{-1} = (a h_1^{i_1} a^{-1})(a h_2^{i_2} a^{-1}) \ldots (a h_l^{i_l} a^{-1}) \in \langle a^2, b \rangle .$$

Аналогично в силу (I2)–(I6) справедливо $a^{-1}ha,\ bhb^{-1},\ b^{-1}hb \in \langle a^2, b \rangle$.

Таким образом,

(I7) $\quad \forall h \in H \quad aha^{-1}, a^{-1}ha, bhb^{-1}, b^{-1}hb \in H.$

Пусть теперь $g \in G = \langle a, в \rangle$. Тогда

$$g = g_1^{i_1} g_2^{i_2} \dots g_l^{i_l}, \text{ где } g_j \in \{a, в\}, \ i_j \in \{1; -1\}, \ j = \overline{1, l},$$

а следовательно, в силу (I7) $\forall h \in H$ имеем

$$g h g^{-1} = g_1^{i_1}(g_2^{i_2}(\dots(g_l^{i_l} h g_l^{-i_l})\dots) g_2^{-i_2}) g_1^{-i_1} \in H.$$

Таким образом, $\forall g \in G, \forall h \in H \quad g h g^{-1} \in H$, а следовательно,

(I8) $\qquad \forall g \in G \quad g H g^{-1} \subset H.$

Производя в (I8) замену g на g^{-1}, имеем $g^{-1} H g \subset H$, а следовательно, $H \subset g H g^{-1}$, откуда, учитывая (I8), получаем $g H g^{-1} = H$ или $gH = Hg \quad \forall g \in G$, т.е. H – нормальная подгруппа группы G.

МЦ НИЧ МАЙ. Заказ 4235 Тираж 4