Лекция 4.

Изоморфизм групп

Определение 1. Две группы G и G' изоморфны, если существует биекция $\varphi: G \to G'$, сохраняющая групповую операцию:

$$\varphi(g_1 \circ g_2) = \varphi(g_1) * \varphi(g_2),$$

$$g_1, g_2, g_1 \circ g_2 \in G, \quad \varphi(g_1 \circ g_2) \in G', \quad \varphi(g_1) \in G', \varphi(g_2) \in G'.$$

Пример 1. $G =< \mathbb{R}^+, *, 1 >, \quad G' =< \mathbb{R}, +, 0 >$

G и G' изоморфны: $\varphi(x) = \ln x$ – биекция

$$ln\, e^n \leftrightarrow n:$$

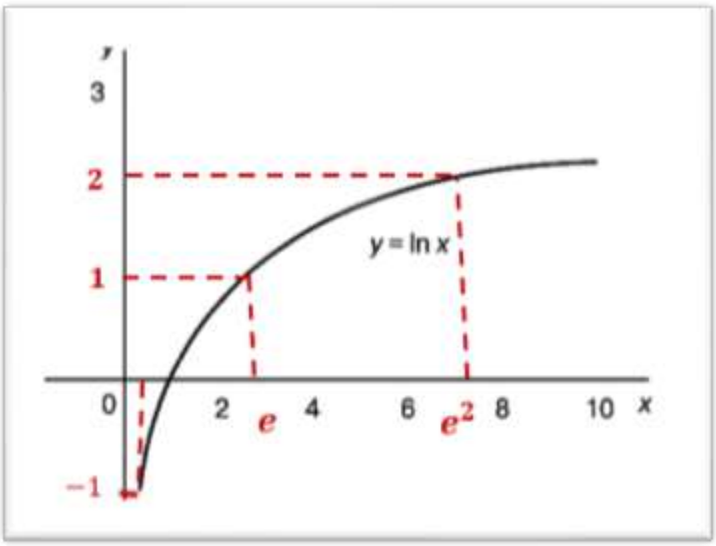
$$ln\, e^2 \leftrightarrow 2,$$

$$ln\, e^{-2} \leftrightarrow -2,$$

$$ln(e^2)^{-1} = -2$$

Единица переходит в единицу: $ln 1 \leftrightarrow 0 \qquad e_\times \to e_+ \quad 1 \to 0.$

Обратный элемент в обратный: $g^{-1} \in G \to \ln g^{-1} \in G'$.

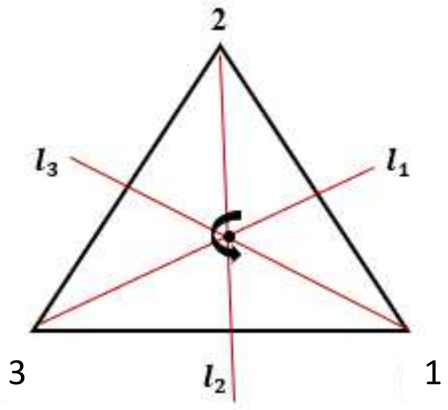


Пример 2. Рассмотрим группы G_{Δ} и S_3.

Покажем, что группа самосовмещений треугольника G_{Δ} и группа подстановок S_3 изоморфны. Установим взаимно-однозначное соответствие между элементами групп, сохраняющее групповую операцию.

$S_3 = \{\pi_0, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$.

$G_{\Delta} = \left\{\varphi_0, \varphi_1 = \varphi_{\frac{2\pi}{3}}, \varphi_2 = \varphi_{\frac{4\pi}{3}}, \psi_1, \psi_2, \psi_3\right\}$



$\circ$	φ_0	φ_1	φ_2	ψ_1	ψ_2	ψ_3
φ_0	φ_0	φ_1	φ_2	ψ_1	ψ_2	ψ_3
φ_1	φ_1	φ_2	φ_0	ψ_2	ψ_3	ψ_1
φ_2	φ_2	φ_0	φ_1	ψ_3	ψ_1	ψ_2
ψ_1	ψ_1	ψ_3	ψ_2	φ_0	φ_2	φ_1
ψ_2	ψ_2	ψ_1	ψ_3	φ_1	φ_0	φ_2
ψ_3	ψ_3	ψ_2	ψ_1	φ_2	φ_1	φ_0

1. Установим биекцию между элементами групп G_{Δ} и S_3 следующим образом:

$\varphi_0 \leftrightarrow \pi_0$

$\varphi_{\frac{2\pi}{3}} \leftrightarrow (1\ 2\ 3)$

$\varphi_{\frac{4\pi}{3}} \leftrightarrow (1\ 3\ 2)$

$\psi_1 \leftrightarrow (1\ 2)$

$\psi_2 \leftrightarrow (1\ 3)$

$\psi_3 \leftrightarrow (2\ 3)$

Легко убедиться, что единичный элемент переходит в единичный, а обратные группы G_{Δ} в обратные группы S_3.

$$\varphi_{\frac{2\pi}{3}}^{-1} = \varphi_{\frac{4\pi}{3}} \quad (1\ 2\ 3)^{-1} = (1\ 3\ 2) \qquad \psi_i^{-1} = \psi_i \quad (2\ 3)^{-1} = (2\ 3)\ \ldots$$

Проверим сохранение групповой операции.

$\varphi_{\frac{2\pi}{3}} \cdot \psi_1 = \psi_2 \quad \leftrightarrow \quad (1\ 2\ 3)(1\ 2) = (1\ 3)$

$\varphi_{\frac{2\pi}{3}} \cdot \psi_2 = \psi_3 \quad \leftrightarrow \quad (1\ 2\ 3)(1\ 3) = (2\ 3)$

$\varphi_{\frac{2\pi}{3}} \cdot \psi_3 = \psi_1 \quad \leftrightarrow \quad (1\ 2\ 3)(2\ 3) = (1\ 2)$

$\psi_1 \cdot \psi_2 = \varphi_{\frac{4\pi}{3}} \quad \leftrightarrow \quad (1\ 2)(1\ 3) = (1\ 3\ 2)$

$\psi_1 \cdot \psi_3 = \varphi_{\frac{2\pi}{3}} \quad \leftrightarrow \quad (1\ 2)(2\ 3) = (1\ 2\ 3)$

И т. д. Следует учесть, что группа не коммутативна.

Вывод: группы G_{Δ} и S_3 изоморфны.

2. Теперь попробуем установить биекцию по другому:

$\varphi_0 \leftrightarrow \pi_0$

$\varphi_{\frac{2\pi}{3}} \leftrightarrow (1\ 2\ 3)$

$\varphi_{\frac{4\pi}{3}} \leftrightarrow (1\ 3\ 2)$

$\psi_1 \leftrightarrow (1\ 3)$

$\psi_2 \leftrightarrow (1\ 2)$

$\psi_3 \leftrightarrow (2\ 3)$

Установленная таким образом биекция не позволяет сохранить групповую операцию:

$\varphi_{\frac{2\pi}{3}} \cdot \psi_1 = \boldsymbol{\psi_2} \quad \leftrightarrow \quad (1\ 2\ 3)(1\ 3) = (2\ 3) \leftrightarrow \boldsymbol{\psi_3}$.

Свойства изоморфизма

1. **Единичный элемент переходит в единичный**: $e \to e', \quad e \in G, e' \in G'$.

Доказательство.

Обозначим групповые операции, соответственно, $(G,\circ)$ и $(G',*)$.

$e' = \varphi(e)$, (по определению: $e \circ a = a \circ e = a$).

$\varphi(e) * \varphi(g) = \varphi(e \circ g) = \varphi(g) = \varphi(g \circ e) = \varphi(g) * \varphi(e)$ для $\forall g \in G$.

2. **Обратный элемент переходит в обратный**: $(\varphi(g))^{-1} = \varphi(g^{-1})$.

Доказательство.

(по определению: $a \circ a^{-1} = a^{-1} \circ a = e$).

$$\varphi(g^{-1}) * \varphi(g) = \varphi(g^{-1} \circ g) = \varphi(e) = e'$$

$$\varphi(g) * \varphi(g^{-1}) = \varphi(g \circ g^{-1}) = \varphi(e) = e'.$$

Количество групп второго, третьего и четвертого порядков с точностью до изоморфизма.

Утверждение 1. Групп второго порядка с точностью до изоморфизма одна, она циклическая: $a^2 = e$.

Доказательство. Составим таблицу Кэли

*	e	a
e	e	a
a	a	e

$a \cdot a \neq a$, т.к. $a \neq e \Rightarrow a \cdot a = e$, $G =< \text{a} >$ – группа циклическая.

Например, группа второго порядка $G =< \{0,1\},\ \sim,\ 1 >=< 0 >$. Каждый элемент сам себе обратный.

Утверждение 2. Групп третьего порядка с точностью до изоморфизма одна, она циклическая, порожденная любым не единичным элементом:

$$G =< a >= \{a, a^2 = b, a^3 = a \cdot b = e\} \quad G =< b >= \{b, b^2 = a, b^3 = b \cdot a = e\}.$$

Доказательство. Составим таблицу Кэли

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$a \cdot b \neq a,$ т.к. $b \neq e$ и $a \cdot b \neq b,$ т.к. $a \neq e \Rightarrow a \cdot b = e.$

Аналогично $b \cdot a = e$, следовательно, группа **коммутативна.**

$a \cdot a \neq a, \quad a \cdot a \neq e,$ т.к. $a^{-1} = b.$

Эта группа **циклическая**, так же, как и группа второго порядка.

Например, группы третьего порядка:

$G_{\varphi_\Delta} = \left\{\varphi_0, \varphi_{\frac{2\pi}{3}}, \varphi_{\frac{4\pi}{3}}\right\}$ – группа вращений треугольника с операцией композиция;

$C = \{C_0, C_1, C_2\}$ – группа классов вычетов по модулю 3 с операцией сложения.

Группы четвертого порядка

Утверждение 3. Любая группа четвертого порядка коммутативна.

Доказательство. Пусть $G = \{e, a, b, c\}$, и предположим, что какие-то два элемента не перестановочны: $b \cdot c \neq c \cdot b$. Имеем $b \cdot c \neq b$ и $b \cdot c \neq c$, т.к. $c \neq e, b \neq e \Rightarrow b \cdot c = a$ или $b \cdot c = e$: $b \cdot c \in \{a, e\}$. Аналогично получаем $c \cdot b \in \{a, e\}$. Пусть $b \cdot c = e$, а $c \cdot b = a$. Из того, что $b \cdot c = e$ следует, что $b^{-1} = c \Rightarrow c \cdot b = b^{-1} \cdot b = e$. А это противоречит предположению, что $c \cdot b = a$, следовательно, любая группа четвертого порядка коммутативна.

Утверждение 4. Групп четвертого порядка с точностью до изоморфизма две: **четвертная группа Клейна и циклическая.**

Доказательство.

1. Введем условие – все элементы группы сами себе обратные: $a^{-1} = a, b^{-1} = b, c^{-1} = c \Rightarrow a^2 = e, b^2 = e, c^2 = e$.

$*$	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

Воспользуемся тем, что в группе в каждой строке и в каждом столбце все элементы различны (легко доказать от противного), а также, что все группы 4-го порядка коммутативны.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	x	y
b	b	x	e	z
c	c	y	z	e

Из второй строки: $x, y \in \{b, c\}$. Из третьего столбца: $x, z \in \{a, c\}$. Следовательно, $x = c,\ y = b,\ z = a$.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Эта группа называется *четвертная группа Клейна*. Ее характерная особенность – все элементы сами себе обратны.

Пример четвертной **группы Клейна:**

группа самосовмещений прямоугольника.

Два поворота, две симметрии.

$$G_{\mathrm{W}} = \{\varphi_0, \varphi_\pi, \psi_1, \psi_2\}$$

$L \subseteq S_4$ – подгруппа перестановок, изоморфная группе самосовмещений прямоугольника: $L = \{\pi_0, (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2)(3\ 4)\}$.

$$\varphi_0 \to \pi_0, \varphi_\pi \to (1\ 3)(2\ 4), \psi_1 \to (1\ 4)(2\ 3), \psi_2 \to (1\ 2)(3\ 4)$$

2. Предположим, что не все элементы сами себе обратны. Пусть для определенности $a^{-1} = b$.

$*$	e	a	b	c
e	e	a	b	c
a	a		e	
b	b	e		
c	c			

Заполним таблицу Кэли, исходя из этого предположения и коммутативности группы четвертого порядка. Тогда $a \cdot b = e = b \cdot a$. (Предполагая перестановочность других элементов, аналогично получим так же, как и в этом случае, циклическую группу).

$*$	e	a	b	c
e	e	a	b	c
a	a	x	e	u
b	b	e	y	v
c	c	u	v	z

Из второй строки: $x, u \in \{b, c\}$. Из четвертого столбца: $u, v, z \in \{e, a, b\}$

Очевидно, что $u = b \Rightarrow x = c$. Из третьей строки: $y, v \in \{a, c\} \Rightarrow v = a, y = c$.

$*$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

$< a >= \{a, a^2 = c, a^3 = a \cdot c = b, a^4 = c^2 = e\}$ $\quad G =< a >$ – циклическая группа

$< b >= \{b, b^2 = c, b^3 = b \cdot c = a, b^4 = c^2 = e\}$ $\quad G =< b >$

$< c >= \{c, c^2 = e\}$ $\quad G \neq < c >$ – циклическая подгруппа группы G: $H =< c >$.

Например, циклические группы четвертого порядка**:**

- Группа вращений квадрата

$$G_{\mathrm{W}} = \left\{\varphi_0, \varphi_{\frac{\pi}{2}}, \varphi_\pi, \varphi_{\frac{3\pi}{2}}\right\} =< \varphi_{\frac{\pi}{2}} >=< \varphi_{\frac{3\pi}{2}} >.$$

Подгруппа $H =< \varphi_\pi >= \{\varphi_0, \varphi_\pi\}$.

- Группа классов вычетов по модулю 4

$$C = \{C_0, C_1, C_2, C_3\} =< C_1 >=< C_3 >,$$

Подгруппа $H =< C_2 >$.

Теорема 1. Все циклические группы одного порядка изоморфны.

Доказательство.

1. Рассмотрим произвольную циклическую группу бесконечного порядка

$$G = \{a^0, a^1, \dots, a^n, \dots\} =< a >.$$

Покажем, что она изоморфна аддитивной группе целых чисел

$$G_{\mathbb{Z}} =< \mathbb{Z}, +, 0 >=< 1 >,$$

т.е. существует биекция, сохраняющая групповую операцию.

$\exists \boldsymbol{\varphi}: \boldsymbol{G} \to \boldsymbol{G_{\mathbb{Z}}}$ **— биекция**:

$$a^n \in G: \quad \boldsymbol{a^n \leftrightarrow n.}$$

Сохраняется групповая операция:

$a^n \to n$, $a^m \to m$. Покажем, что $\varphi(a^n \cdot a^m) = \varphi(a^n) + \varphi(a^m)$.

$\varphi(a^n \cdot a^m) = \varphi(a^{n+m}) = n + m$

$\varphi(a^n) + \varphi(a^m) = n + m$

Ч.т.д.

Все циклические группы бесконечного порядка изоморфны между собой, т.к. они изоморфны группе $G_{\mathbb{Z}} =< \mathbb{Z}, +, 0 >$.

2. Теперь покажем, что все циклические группы одного и того же конечного порядка изоморфны. Рассмотрим произвольную циклическую группу G конечного порядка n. Докажем, что она *изоморфна* группе классов вычетов по модулю n.

$$G \to C: \qquad C = \{C_0, C_1, \dots, C_{n-1}\}$$

(Напомним, что, например, для $n = 4$ группа классов вычетов по модулю 4 содержит следующие элементы:

$C_0 = \{0, \pm 4, \pm 8, \dots\}$

$C_1 = \{\dots -7, -3, 1, 5, 9 \dots\}$

$C_2 = \{\ldots - 6, -2, 2, 6, 10 \ldots\}$

$C_3 = \{\ldots -5, -1, 3, 7, 11 \ldots\})$.

Рассмотрим группы: $G = \{a^0, a^1, \ldots, a^{n-1}\}$ и $C = \{C_0, C_1, \ldots, C_{n-1}\}$

Установим биекцию следующим образом:

$a^m \leftrightarrow C_m$ $(m = 0, \ldots, n-1)$.

Покажем, что при этом сохраняется групповая операция:

$\varphi(a^k \cdot a^m) = \varphi(a^k) + \varphi(a^m)$;

$\varphi(a^{k+m}) = C_{k+m} = C_r, \quad r = (k+m)(mod\, n)$;

$\varphi(a^k) + \varphi(a^m) = C_k + C_m = C_r, \quad r = (k+m)(\mathrm{mod}\, n)$.

Теорема доказана.

Пример 3.

Покажем, что группа вращений квадрата $G_W = \left\{\varphi_0, \varphi_{\frac{\pi}{2}}, \varphi_\pi, \varphi_{\frac{3\pi}{2}}\right\} =< \varphi_{\frac{\pi}{2}} >=< \varphi_{\frac{3\pi}{2}} >$ изоморфна группе классов вычетов по модулю 4.

1. Установим биекцию:

$$\varphi_0 \leftrightarrow C_0,$$
$$\varphi_{\frac{\pi}{2}} \leftrightarrow C_1,$$
$$\varphi_\pi \leftrightarrow C_2,$$
$$\varphi_{\frac{3\pi}{2}} \leftrightarrow C_3.$$

Убедимся, что она сохраняет групповую операцию:

$$\varphi_{\frac{\pi}{2}} \circ \varphi_\pi = \varphi_{\frac{3\pi}{2}} \leftrightarrow C_3 = C_1 + C_2$$
$$\varphi_{\frac{\pi}{2}} \circ \varphi_{\frac{3\pi}{2}} = \varphi_0 \leftrightarrow C_0 = C_1 + C_3$$

И т.д.

Теорема 2 (Кэли). Всякая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы S_n.

Доказательство.

$$G = \{g_1 = e, g_2, \dots, g_n\}$$

$$\exists \varphi: G \to L, \quad L \subseteq S_n$$

1) φ – биекция;

2) φ сохраняет групповую операцию.

Построим отображение φ (изоморфизм):

$$\boldsymbol{g_i \leftrightarrow L_{g_i} = \begin{pmatrix} g_1 & g_2 & \cdots g_n \\ g_i g_1 & g_i g_2 & \cdots g_i g_n \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & \dots n \\ i_1 & i_2 & i_3 & \dots\ i_n \end{pmatrix}}$$

(т.е. для всякого элемента $g_i \in G \quad L_{g_i}(g_k) = g_i g_k$).

Покажем, что L_{g_i} – подстановка, т.е. все элементы нижнего уровня различны. Предположим, что это не так: $g_i g_k = g_i g_t$, т.е. два элемента совпали. Но, т.к. G – группа, существуют обратные: $\exists g_i^{-1}: g_i^{-1} g_i g_k = g_i^{-1} g_i g_t \Rightarrow g_k = g_t$, а это по предположению различные элементы группы. Противоречие.

Покажем, что φ – биекция.

φ сюрьективно, т.к. у каждого L_{g_i} есть прообраз g_i.

φ инъективно: $g_i \neq g_j \Rightarrow L_{g_i} \neq L_{g_j}$. Единичный элемент переходит в различные элементы, т.к. $g_1 = e: e \to g_i, e \to g_j$. Следовательно, подстановки разные.

Таким образом, $L = \{L_{g_1} = L_e, \dots, L_{g_n}\}$

$$L_{g_1} = L_e; \qquad (L_{g_i})^{-1} = L_{g_i^{-1}}, \qquad \text{т. к.} \qquad L_{g_i g_i^{-1}} = L_{g_i^{-1} g_i} = L_e.$$

Покажем сохранение групповой операции: $\varphi(g_i g_k) = \varphi(g_i) \circ \varphi(g_k)$

$$L_{g_i g_k} = L_{g_i} \circ L_{g_k}$$

Равенство следует из ассоциативности групповой операции. $\forall g_t: (g_i g_k) g_t = g_i (g_k g_t)$:

$$L_{g_i g_k}(g_t) = (g_i g_k) g_t = g_i (g_k g_t) = L_{g_i}\left(L_{g_k}(g_t)\right).$$

Теорема доказана.

Пример 4.

Группа самосовмещений прямоугольника – группа Клейна. Два поворота, две симметрии.

$$G_{\mathrm{W}} = \{\varphi_0, \varphi_\pi, \psi_1, \psi_2\} \sim \{1, 2, 3, 4\}$$

Построим изоморфную ей подгруппу подстановок $L \subseteq S_4$.

$$\varphi_0 \leftrightarrow L_{\varphi_0} = \begin{pmatrix} \varphi_0 & \varphi_\pi & \psi_1 & \psi_2 \\ \varphi_0\varphi_0 & \varphi_0\varphi_\pi & \varphi_0\psi_1 & \varphi_0\psi_2 \end{pmatrix} = \begin{pmatrix} \varphi_0 & \varphi_\pi & \psi_1 & \psi_2 \\ \varphi_0 & \varphi_\pi & \psi_1 & \psi_2 \end{pmatrix} \sim \begin{pmatrix} 1\,2\,3\,4 \\ 1\,2\,3\,4 \end{pmatrix} = \pi_0$$

$$\varphi_\pi \leftrightarrow L_{\varphi_\pi} = \begin{pmatrix} \varphi_0 & \varphi_\pi & \psi_1 & \psi_2 \\ \varphi_\pi\varphi_0 & \varphi_\pi\varphi_\pi & \varphi_\pi\psi_1 & \varphi_\pi\psi_2 \end{pmatrix} = \begin{pmatrix} \varphi_0 & \varphi_\pi & \psi_1 & \psi_2 \\ \varphi_\pi & \varphi_0 & \psi_2 & \psi_1 \end{pmatrix} \sim \begin{pmatrix} 1\,2\,3\,4 \\ 2\,1\,4\,3 \end{pmatrix} = (1\;2)(3\;4)$$

$$\psi_1 \leftrightarrow L_{\psi_1} = \begin{pmatrix} \varphi_0 & \varphi_\pi & \psi_1 & \psi_2 \\ \psi_1\varphi_0 & \psi_1\varphi_\pi & \psi_1\psi_1 & \psi_1\psi_2 \end{pmatrix} = \begin{pmatrix} \varphi_0 & \varphi_\pi & \psi_1 & \psi_2 \\ \psi_1 & \psi_2 & \varphi_0 & \varphi_\pi \end{pmatrix} \sim \begin{pmatrix} 1\,2\,3\,4 \\ 3\,4\,1\,2 \end{pmatrix} = (1\;3)(2\;4)$$

$$\psi_2 \leftrightarrow L_{\psi_2} = \begin{pmatrix} \varphi_0 & \varphi_\pi & \psi_1 & \psi_2 \\ \psi_2\varphi_0 & \psi_2\varphi_\pi & \psi_2\psi_1 & \psi_2\psi_2 \end{pmatrix} = \begin{pmatrix} \varphi_0 & \varphi_\pi & \psi_1 & \psi_2 \\ \psi_2 & \psi_1 & \varphi_\pi & \varphi_0 \end{pmatrix} \sim \begin{pmatrix} 1\,2\,3\,4 \\ 4\,3\,2\,1 \end{pmatrix} = (1\;4)(2\;3)$$

$L = \{\pi_0, (1\;2)(3\;4), (1\;3)(2\;4), (1\;4)(2\;3)\}$