Лекция 2

Определение 1. Пусть $(G, *)$ и $(H, \circ)$ – две группы. Отображение $\varphi\colon G \to H$ называется *гомоморфизмом*, если $\varphi(g_1 * g_2) = \varphi(g_1) \circ \varphi(g_2)$.

На самом деле, чтобы определить гомоморфизм нам не нужно, чтобы G и H были группами. Достаточно, чтобы на них были заданы некие операции (т.е., чтобы они были группоидами).

Докажем следующие элементарные свойства гомоморфизма.

Лемма 1. *Пусть $\varphi\colon (G, *) \to (H, \circ)$ – гомоморфизм групп. Обозначим через e_G и e_H единицы группы G и H соответственно. Тогда*

1) $\varphi(e_G) = e_H$,

2) $\varphi(g^{-1}) = \varphi(g)^{-1}$. (В левой части обратный берется в группе G, а в правой – в H.)

Доказательство. 1) Поскольку e_G – единица группы G. Тогда $e_G * e_G = e_G$, а значит,

$$\varphi(e_G) \circ \varphi(e_G) = \varphi(e_G * e_G) = \varphi(e_G).$$

В группе H есть обратный к $\varphi(e_G)$ элемент. Умножим на него обе части. Получим

$$\varphi(e_G) = e_H.$$

2) $e_H = \varphi(e_G) = \varphi(g * g^{-1}) = \varphi(g) \circ \varphi(g^{-1})$. Следовательно, $\varphi(g^{-1}) = \varphi(g)^{-1}$. □

.

Определение 2. Биективный гомоморфизм $\varphi\colon G \to H$ называется *изоморфизмом*, а группы G и H при наличии изоморфизма между ними называются *изоморфными*.

Изоморфные группы имеют одинаковую алгебраическую структуру. Более строго любой алгебраический факт (то есть формулирующийся только в терминах операции) верный в одной из них, верен и в другой. Поэтому в дальнейшем мы будем отождествлять изоморфные группы и будем изучать группы с точностью до изоморфизма.

Пример 1. *Рассмотрим две группы: $(\mathbb{R}, +)$ и $(\mathbb{R}_{>0}, \cdot)$. Вторая группа состоит из всех положительных вещественных чисел с операцией умножения. Рассмотрим отображение $\varphi\colon \mathbb{R} \to \mathbb{R}_{>0}$, $\varphi(x) = 2^x$. Легко видеть, что φ – изоморфизм.*

Пример 2. *Группа $\mathrm{GL}_n(\mathbb{C})$ изоморфна группе невырожденных линейных преобразований векторного пространства $\mathbb{C}^n$ с операцией композиции. Чтобы получить изоморфизм между этими группами нужно выбрать некоторый базис в $\mathbb{C}^n$ и отобразить линейное преобразование в его матрицу в этом базисе.*

На самом деле изоморфизм (биективное соответствие, переводящее умножение одной группы в умножение другой) можно задать в случае, когда про одну из структур не известно, группа это или нет. Тогда вторая структура будет автоматически группой.

Теорема 1. *Пусть G – группа, а H – группоид. И пусть $\varphi\colon G \to H$ – биекция и гомоморфизм (то есть $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$. (Можно сказать, что φ – изоморфизм группоидов.) Тогда H – также группа и φ – изоморфизм групп.*

Доказательство. Докажем, что H – группа. Проверим ассоциативность. Пусть $h_1, h_2, h_3 \in H$. Обозначим $g_i = \varphi^{-1}(h_i)$, $i = 1, 2, 3$. Тогда

$$\begin{aligned} h_1(h_2h_3) &= \varphi(g_1)(\varphi(g_2)\varphi(g_3)) = \varphi(g_1)\varphi(g_2g_3) = \\ &= \varphi(g_1(g_2g_3)) = \varphi((g_1g_2)g_3) = \varphi(g_1g_2)\varphi(g_3) = (\varphi(g_1)\varphi(g_2))\varphi(g_3) = (h_1h_2)h_3. \end{aligned}$$

Проверим, что $l = \varphi(e)$ – нейтральный элемент. Действительно, пусть $h = \varphi(g)$. Тогда $hl = \varphi(g)\varphi(e) = \varphi(ge) = \varphi(g) = h$ и $lh = \varphi(e)\varphi(g) = \varphi(eg) = \varphi(g) = h$.

Теперь проверим наличие обратного к элементу $h = \varphi(g)$. Докажем, что это $f = \varphi(g^{-1})$. Действительно, $hf = \varphi(g)\varphi(g^{-1}) = \varphi(e) = l$ и $fh = \varphi(g^{-1})\varphi(g) = \varphi(e) = l$.

Итак, мы проверили, что H – группа. Таким образом φ – биективный гомоморфизм групп, то есть изоморфизм. □

Теорема 2. *Отношение изоморфности – это отношение эквивалентности.*

Доказательство. Нужно проверить, что отношение изоморфности удовлетворяет свойствам рефлексивности, симметричности и транзитивности. В самом деле. Тождественное преобразование задает изоморфизм любой группы с собой. Рефлексивность доказана. Если $\varphi\colon G \to H$ – изоморфизм, то в частности это биекция. Тогда существует обратное отображение φ^{-1}. Оно также является гомоморфизмом. В самом деле, пусть $a, b \in H$, в силу сюръективности φ, имеем $a = \varphi(u)$, $b = \varphi(v)$ для некоторых $u, v \in G$. Тогда $\varphi^{-1}(ab) = \varphi^{-1}(\varphi(u)\varphi(v)) = \varphi^{-1}(\varphi(uv)) = uv = \varphi^{-1}(a)\varphi^{-1}(b)$. Таким образом, φ^{-1} – изоморфизм. Симметричность доказана. Докажем, что композиция двух изоморфизмов – изоморфизм. Пусть $\varphi\colon G \to H$ и $\psi\colon H \to F$ – два гомоморфизма. Тогда

$$\psi \circ \varphi(g_1 g_2) = \psi(\varphi(g_1 g_2)) = \psi(\varphi(g_1)\varphi(g_2)) = \psi(\varphi(g_1))\psi(\varphi(g_2)) = \psi \circ \varphi(g_1)\psi \circ \varphi(g_2).$$

То есть $\psi \circ \varphi$ – гомоморфизм. С другой стороны, $\psi \circ \varphi$ – биекция. Значит, $\psi \circ \varphi$ – изоморфизм. Транзитивность доказана. □

Из этого предложения следует, что все группы распадаются на непересекающиеся классы изоморфности.

Приведем еще один пример группы.

Пример 3. *Группа комплексных корней из единицы n-ой степени. Пусть μ_n – множество всех комплексных корней степени n из 1. Тогда $(\mu_n, \cdot)$ – абелева группа порядка n. Докажем это. Для того, чтобы доказать, что μ_n – группа мы воспользуемся, тем, что это подмножество в известной нам группе $\mathbb{C}^\times$. Нам надо лишь проверить, что μ_n замкнуто относительно умножения и взятия обратного. Пусть $a, b \in \mu_n$, то есть $a^n = b^n = 1$. Тогда $(ab)^n = a^n b^n = 1$, значит, $ab \in \mu_n$. Мы доказали, что μ_n замкнуто относительно умножения. С другой стороны $(a^{-1})^n = (a^n)^{-1} = 1^{-1} = 1$, следовательно, μ_n замкнуто относительно взятия обратного. То, что группа μ_n абелева следует из того, что она является подгруппой в абелевой группе $\mathbb{C}^\times$.*

Установим следующий изоморфизм групп.

Пример 4. *Группа $\mathbb{Z}_n$ изоморфна группе μ_n. Один из возможных автоморфизмов переводит $k \in \mathbb{Z}_n$ в $\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$. То, что φ – гомоморфизм обеспечивается тем, что при умножении комплексных чисел их аргументы складываются.*

Определим группу, которая называется *группой кватернионов*.

Пример 5. *Группа кватернионов Q_8. Рассмотрим множество из 8 элементов:*

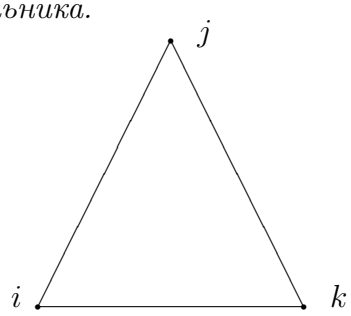
$$\{1, -1, i, -i, j, -j, k, -k\}.$$

Умножение устроено следующим образом: знаки умножаются отдельно,

$$i^2 = j^2 = k^2 = -1,$$

$$ij = k,\ ji = -k,\ ik = -j,\ ki = j,\ jk = i,\ kj = -i.$$

Для того, чтобы запомнить правило умножения элементов i, j и k удобно изобразить их в вершинах треугольника.



Теперь, если мы хотим умножить два элемента, то, если направление движение от первого ко второму по часовой стрелке, получаем третий элемент, а если против часовой стрелки, то минус третий.

Легко видеть, что 1 – нейтральный элемент, и каждый элемент обратим. В самом деле, элементы 1 *и* -1 *являются обратными к самим себе. А для любого другого элемента* x *выполнено* $x^{-1} = -x$*. Для того, чтобы утверждать, что* Q_8 *– группа, необходимо проверить ассоциативность. Перейдем к доказательству этого.*

Предложение 1. Q_8 *– группа*

Доказательство. Рассмотрим следующее множество из 8 комплексных матриц, которое мы обозначим $\overline{Q}_8$.

$$\left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \right\}.$$

Здесь i – это мнимая единица (комплексное число).

Рассмотрим биекцию φ между Q_8 и $\overline{Q}_8$.

$$\pm 1 \mapsto \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; i \mapsto \pm \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \; j \mapsto \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \; k \mapsto \pm \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}.$$

Легко убедиться, что φ переводит умножение в Q_8 в матричное умножение. Следовательно, $(\overline{Q}_8, \cdot)$ – это замкнутое относительно умножения и взятия обратной матрицы подмножество в $\mathrm{GL}_2(\mathbb{C})$. Значит, $\overline{Q}_8$ – подгруппа. Тогда, по теореме 1, Q_8 – группа, изоморфная $\overline{Q}_8$. □

Определение 3. Пусть g – элемент группы G, а n – целое число. Определим n-ю степень элемента g следующим образом. Если n положительное, то $g^n = g \cdot \ldots \cdot g$ – произведение n элементов g. Если n отрицательное, то $g^n = (g^{-1})^n$. Нулевая степень любого элемента равна нейтральному элементу e.

Упражнение 1. Выполнены следующие свойства степеней элемента группы:
1) $g^m g^n = g^{m+n}$,
2) $(g^m)^n = g^{mn}$
Указание. Рассмотреть все случаи знаков m и n.

Определение 4. Пусть g – элемент группы G. Порядок g – это минимальное натуральное число n такое, что $g^n = e$. Если такого числа не существует, то порядок элемента g равен бесконечности. Порядок элемента g обозначается $\mathrm{ord}(g)$.

Определение 5. Группа G называется *циклической*, если найдется элемент $g \in G$ такой, что каждый элемент G имеет вид g^k для некоторого целого числа k.

Элемент g называется *порождающим элементом группы* G, при этом группа G обозначается $\langle g \rangle$.

Замечание 1. В предыдущем определении не требуется, чтобы все степени g были различны.

Пример 6. *а) Группа* $\mathbb{Z}$ *является циклической. В самом деле,* $\mathbb{Z} = \langle 1 \rangle$.
б) Аналогично $\mathbb{Z}_n = \langle 1 \rangle$.

Лемма 2. *Циклическая группа* $\langle g \rangle$ *изоморфна*

- $\mathbb{Z}_n$ *при условии* $\operatorname{ord} g = n$;
- $\mathbb{Z}$ *при условии* $\operatorname{ord} g = \infty$.

Доказательство. Пусть $\operatorname{ord} g = n$. Рассмотрим множество элементов

$$S = \{g^0 = e, g, g^2, \dots g^{n-1}\}.$$

Докажем, что все элементы группы $\langle g \rangle$ лежат в S и что все элементы S различны. В самом деле, пусть g^k – некоторый элемент $\langle g \rangle$. Разделим k на n с остатком: $k = nm + r$, где $0 \leq k < n$. Тогда $g^k = (g^n)^m g^r = g^r \in S$.

С другой стороны. Пусть $0 \leq a < b < n$ и $g^a = g^b$. Умножая последнее равенство на g^{-a}, получаем $e = g^{b-a}$. Поскольку $0 < b - a < n$, это противоречит тому, что $\operatorname{ord}(g) = n$.

Рассмотрим отображение $\psi \colon \mathbb{Z}_n \to \langle g \rangle$, $\psi(k) = g^k$. Элементы $\mathbb{Z}_n$ – это не числа, а классы чисел с одинаковым остатком. Поэтому нам надо доказать, что отображение ψ определено корректно. А именно, пусть $k' = mn + k$ для некоторого $m \in \mathbb{Z}$. Тогда $\psi(k') = g^{k'} = (g^n)^m g^k = g^k = \psi(k)$. Корректность доказана. Теперь проверим, что ψ – гомоморфизм. Действительно, $\psi(k + l) = g^{k+l} = g^k g^l = \psi(k)\psi(l)$. Заметим, что $\mathbb{Z}_n$ состоит из классов чисел $0, 1, \dots, n - 1$. При отображении ψ эти классы переходят в элементы множества S. Причем это отображение очевидно сюръективно и инъективно так как элементы S не совпадают. Итак, ψ – гомоморфизм и биекция, то есть изоморфизм.

Пусть теперь $\operatorname{ord} g = \infty$. Рассмотрим отображение $\psi \colon \mathbb{Z} \to \langle g \rangle$, $\psi(k) = g^k$. Как и в прошлом случае получим, что ψ – гомоморфизм. (В этом случае проверять корректность не нужно, так как элементы $\mathbb{Z}$ – числа, а не классы чисел.) Сюръективность ψ следует из определения циклической группы. Докажем инъективность. Предположим, что $g^a = g^b$, где $a > b$. Домножим это равенство на g^{-b} и получим $g^{a-b} = e$, что противоречит тому, что $\operatorname{ord} g = \infty$. Итак, ψ – гомоморфизм и биекция, то есть изоморфизм. □

Если известно, что порядок g равен n, то группу $\langle g \rangle$ обозначают $\langle g \rangle_n$.

Замечание 2. Для каждого элемента g некоторой группы G можно рассмотреть циклическую подгруппу, порожденную этим элементом: $\langle g \rangle \subset G$.

Лемма 3. *Пусть* g *– элемент группы* G *такой, что* $\operatorname{ord} g = n$, *а* m *– целое число. Тогда*

$$\operatorname{ord} g^m = \frac{n}{НОД(m, n)} = \frac{НОК(m, n)}{m}.$$

Доказательство. Докажем это утверждение только для положительных m, так как $\operatorname{ord}(g^{-m}) = \operatorname{ord}((g^m)^{-1}) = \operatorname{ord}(g^m)$, а также $\operatorname{ord}(g^0) = 1$.

Рассмотрим группу $\langle g \rangle$. По предыдущей лемме она изоморфна $\mathbb{Z}_n$. Более того при построенном изоморфизме этих групп элемент g соответствует $1 \in \mathbb{Z}_n$, и элемент g^m

соответствует $m \in \mathbb{Z}_n$. Таким образом, нам нужно доказать, что порядок $m \in \mathbb{Z}_n$ равен $\frac{n}{\text{НОД}(m,n)} = \frac{\text{НОК}(m,n)}{m}$. Порядок – это такая минимальная натуральная степень k, в которой элемент равен e. В аддитивных обозначениях получаем $\text{ord}(m) = k$, если k – это минимальное натуральное число такое, что $mk = 0$ в $\mathbb{Z}_n$. Для целых чисел условие перепишется как mk делится на n. Получается, что mk – общее кратное m и n. Таким образом, $k \geq \frac{\text{НОК}(m,n)}{m}$.С другой стороны $k = \frac{\text{НОК}(m,n)}{m}$ подходит, так как $mk = \frac{\text{НОК}(m,n)}{m} m = \text{НОК}(m,n)$ делится на n. □

Следующий пример был разобран на семинаре.

Пример 7. *Рассмотрим множество* A_n *чётных перестановок. Докажем, что* A_n *– подгруппа в* S_n*. (И, в частности,* A_n *– группа.) В самом деле,* $\text{id} \in \text{A}_n$*, значит,* $\text{A}_n \neq \varnothing$*. Если* $\sigma, \delta \in \text{A}_n$*, то* $\text{sgn}(\sigma \circ \delta) = \text{sgn}(\sigma)\text{sgn}(\delta) = 1 \cdot 1 = 1$*. То есть* $\sigma \circ \delta \in \text{A}_n$*. Также если* $\sigma \in \text{A}_n$*, то* $\text{sgn}(\sigma^{-1}) = \text{sgn}(\sigma) = 1$*. То есть* A_n *замкнуто относительно композициии и взятия обратного. Итак,* A_n *– подгруппа в* S_n