Лекция 2

Кроме базовых примеров групп есть еще конструкции, которые позволяют конструировать одни группы из других. Примером такой конструкции служит конструкция прямого произведения.

Определение 1. Пусть G и H – две группы. *Прямым произведением* $G \times H$ называется множество пар (g, h), где $g \in G$, $h \in H$, с операцией $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

Замечание 1. Прямое произведение групп является группой. Действительно, ассоциативность умножения следует из ассоциативности умножения в каждой из групп G и H, нейтральным элементом является элемент (e_G, e_H), обратным к элементу (g, h) является элемент (g^{-1}, h^{-1}).

Определение 2. 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. 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, $\varphi(g^{-1}) = \varphi(g)^{-1}$. □

.

Задача 1. Пусть $(G, *)$ и $(H, \circ)$ – моноиды с единицами e_G и e_H соответственно. И пусть $\psi\colon G \to H$ – отображение такое, что $\psi(g_1 * g_2) = \psi(g_1) \circ \psi(g_2)$. Может ли так быть, что $\psi(e_G) \neq \psi(e_H)$?

Определение 3. 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.

Теорема 1. *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.

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* $\mathbb{Z}_n$ *изоморфна группе* $\mathcal{C}_n$. *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.*

Пример 3. *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 2. *Пусть* G *– группа, а* H *– группоид (то есть множество с операцией). 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

$$h_1(h_2h_3) = \varphi(g_1)(\varphi(g_2)\varphi(g_3)) = \varphi(g_1)\varphi(g_2g_3) = \\ = \varphi(g_1(g_2g_3)) = \varphi((g_1g_2)g_3) = \varphi(g_1g_2)\varphi(g_3) = (\varphi(g_1)\varphi(g_2))\varphi(g_3) = (h_1h_2)h_3.$$

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. □

Теперь мы готовы доказать, что Q_8 – группа.

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 2, Q_8 – группа, изоморфная $\overline{Q}_8$. □

Определение 4. Пусть $\varphi\colon G \to H$ – гомоморфизм групп. Ядром гомоморфизма φ называется множество

$$\operatorname{Ker}\varphi = \{g \in G \mid \varphi(g) = e\} \subseteq G.$$

Образом гомоморфизма φ называется множество

$$\operatorname{Im}\varphi = \{\varphi(g) \mid g \in G\} \subseteq H.$$

Поскольку $\varphi(e) = e$, нейтральный элемент всегда лежит в ядре.

Лемма 2. *Пусть $\varphi\colon G \to H$ – гомоморфизм. Тогда*
а) $\operatorname{Ker}\varphi$ *– подгруппа в* G,
б) $\operatorname{Im}\varphi$ *– подгруппа в* H.

Доказательство. а) Пусть $g_1, g_2 \in \operatorname{Ker}\varphi$. Тогда $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = ee = e$. Значит, $g_1 g_2 \in \operatorname{Ker}\varphi$. То есть ядро замкнуто относительно операции. Кроме того $\varphi(g_1^{-1}) = \varphi(g_1^{-1})\varphi(g_1) = \varphi(g_1^{-1} g_1) = \varphi(e) = e$. Значит, $g_1^{-1} \in \operatorname{Ker}\varphi$. Таким образом, ядро замкнуто относительно взятия обратного. Осталось заметить, что $e \in \operatorname{Ker}\varphi$. Следовательно, $\operatorname{Ker}\varphi$ – подгруппа в G.

б) Пусть $h_1, h_2 \in \operatorname{Im}\varphi$. Тогда найдутся $g_1, g_2 \in G$ такие, что $h_1 = \varphi(g_1)$, $h_2 = \varphi(g_2)$. Тогда $h_1 h_2 = \varphi(g_1 g_2) \in \operatorname{Im}\varphi$ и $h_1^{-1} = \varphi(g_1^{-1}) \in \operatorname{Im}\varphi$. Кроме того $e = \varphi(e) \in \operatorname{Im}\varphi$. То есть образ замкнут относительно операции, взятия обратного и содержит единицу. Следовательно, $\operatorname{Im}\varphi$ – подгруппа в H. □

Теорема 3. *(Критерий инъективности гомоморфизма) Гомоморфизм $\varphi\colon G \to H$ инъективен тогда и только тогда, когда* $\operatorname{Ker}\varphi = \{e\}$.

Доказательство. Пусть $\operatorname{Ker}\varphi \neq \{e\}$. Тогда существует $g \neq e$, $g \in \operatorname{Ker}\varphi$. То есть $\varphi(g) = e = \varphi(e)$. Следовательно, гомоморфизм φ не инъективен.

Допустим, гомоморфизм φ не инъективен. Тогда $\varphi(g_1) = \varphi(g_2)$ для некоторых $g_1 \neq g_2 \in G$. Значит, $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e$. То есть $g_1 g_2^{-1} \in \operatorname{Ker}\varphi$, но $g_1 g_2^{-1} \neq e$. Значит, $\operatorname{Ker}\varphi \neq \{e\}$. □

Определение 5. 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 6. 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 $\operatorname{ord}(g)$.

Определение 7. 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 2. В предыдущем определении не требуется, чтобы все степени g были различны.

Пример 4. *а) Группа $\mathbb{Z}$ является циклической. В самом деле, $\mathbb{Z} = \langle 1 \rangle$.*
б) Аналогично $\mathbb{Z}_n = \langle 1 \rangle$.

Лемма 3. *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 $0 \le r < n$. Тогда $g^k = (g^n)^m g^r = g^r \in S$.

С другой стороны. Пусть $0 \le a < b < n$ 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 3. Для каждого элемента g некоторой группы G можно рассмотреть циклическую подгруппу, порожденную этим элементом: $\langle g \rangle \subset G$.