

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}) .

Напомним определение гомоморфизма групп.

Определение 2. Пусть $(G, *)$ и $(H, \circ)$ – две группы. Отображение $\varphi: G \rightarrow H$ называется *гомоморфизмом*, если $\varphi(g_1 * g_2) = \varphi(g_1) \circ \varphi(g_2)$.

Докажем следующие элементарные свойства гомоморфизма.

Лемма 1. Пусть $\varphi: (G, *) \rightarrow (H, \circ)$ – 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, $\varphi(g^{-1}) = \varphi(g)^{-1}$. $\square$

Задача 1. Пусть $(G, *)$ и $(H, \circ)$ – моноиды с единицами e_G и e_H соответственно. И пусть $\psi: G \rightarrow H$ – 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 $\varphi: G \rightarrow H$ называется *изоморфизмом*, а группы G и H при наличии изоморфизма между ними называются *изоморфными*.

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 $\varphi: \mathbb{R} \rightarrow \mathbb{R}_{>0}$, $\varphi(x) = 2^x$. Легко видеть, что φ – изоморфизм.

Пример 2. Группа $\mathbb{Z}_n$ изоморфна группе 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 $GL_n(\mathbb{C})$ 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.

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

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

Образом гомоморфизма φ называется множество

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

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

Лемма 2. Пусть $\varphi: G \rightarrow H$ – гомоморфизм. Тогда

- а) $\text{Ker } \varphi$ – подгруппа в G ,
- б) $\text{Im } \varphi$ – подгруппа в H .

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

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

Теорема 1. (Критерий инъективности гомоморфизма) Гомоморфизм $\varphi: G \rightarrow H$ инъективен тогда и только тогда, когда $\text{Ker } \varphi = \{e\}$.

Доказательство. Пусть $\text{Ker } \varphi \neq \{e\}$. Тогда существует $g \neq e$, $g \in \text{Ker } \varphi$. 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 $g_1 g_2^{-1} \in \text{Ker } \varphi$, но $g_1 g_2^{-1} \neq e$. Значит, $\text{Ker } \varphi \neq \{e\}$. $\square$

Определение 5. Пусть g – элемент группы G , а n – целое число. Определим n -ю степень элемента g следующим образом. Если n положительное, то $g^n = g \cdot \dots \cdot g$ – 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 $\text{ord}(g)$.

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

Доказательство. Пусть $\text{ord } g = n$. 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 $0 \leq r < n$. 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 $\text{ord}(g) = n$.

Рассмотрим отображение $\psi: \mathbb{Z}_n \rightarrow \langle g \rangle$, $\psi(k) = g^k$. 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 $\text{ord } g = \infty$. Рассмотрим отображение $\psi: \mathbb{Z} \rightarrow \langle g \rangle$, $\psi(k) = g^k$. 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 $\text{ord } g = \infty$. Итак, ψ – гомоморфизм и биекция, то есть изоморфизм. $\square$

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: $\langle g \rangle \subset G$.