

ЛЕКЦИЯ 7

Определение 1. Говорят, что группа G задана образующими $g_1, \dots, g_k$ и соотношениями $g_1^{\alpha_1} \dots g_k^{\alpha_k}, \dots, g_1^{\beta_1} \dots g_k^{\beta_k}$, если для гомоморфизма $\varphi: \mathfrak{F}(x_1, \dots, x_k) \rightarrow G$, $x_i \mapsto g_i$ ядро совпадает с $N(x_1^{\alpha_1} \dots x_k^{\alpha_k}, \dots, x_1^{\beta_1} \dots x_k^{\beta_k})$. Тогда

$$G \cong \mathfrak{F}(x_1, \dots, x_k) / N(x_1^{\alpha_1} \dots x_k^{\alpha_k}, \dots, x_1^{\beta_1} \dots x_k^{\beta_k}).$$

В таком случае пишут

$$G = \langle g_1, \dots, g_k \mid g_1^{\alpha_1} \dots g_k^{\alpha_k}, \dots, g_1^{\beta_1} \dots g_k^{\beta_k} \rangle.$$

Пример 1. Докажем, что $D_n = \langle a, b \mid a^2, b^2, (ab)^n \rangle$.

Ясно, что D_n порождается двумя симметриями с минимальным углом между ними. Их композиция – это поворот на $\frac{2\pi}{n}$. Если обозначить эти симметрии a и b , то ясно, что $a^2 = b^2 = (ab)^n = e$. То есть для $\varphi: \langle x_1, x_2 \rangle \rightarrow D_n$, $x_1 \mapsto a, x_2 \mapsto b$ ядро содержит $N(x_1^2, x_2^2, (x_1 x_2)^n)$. Наша цель – доказать, что $\text{Ker } \varphi = N(x_1^2, x_2^2, (x_1 x_2)^n)$. Если это не так, то по следствию из третьей теоремы об изоморфизме имеем:

$$G \cong \langle x_1, x_2 \rangle / \text{Ker } \varphi \cong (\langle x_1, x_2 \rangle / N(x_1^2, x_2^2, (x_1 x_2)^n)) / (\text{Ker } \varphi / N(x_1^2, x_2^2, (x_1 x_2)^n)).$$

Тогда порядок группы G будет строго меньше, чем $H = \langle a, b \mid a^2, b^2, (ab)^n \rangle = \langle x_1, x_2 \rangle / N(x_1^2, x_2^2, (x_1 x_2)^n)$. Докажем, что в H не более $2n$ элементов. Легко видеть, что любой элемент H может быть записан либо в виде конечного слова $abab \dots$, либо в виде $ba ba \dots$. Действительно, $a^{-1} = a, b^{-1} = b$, значит, любое слово от a, b, a^{-1}, b^{-1} – это слово от a и b . При этом если есть сочетание aa или bb , то его можно сократить. Поскольку $(ab)^n = e$, среди слов $abab \dots$ различными являются слова длины $0, 1, 2, \dots, 2n - 1$. С другой стороны $ba = b^{-1}a^{-1} = (ab)^{-1}$. Значит, $(ba)^n = e$ и среди слов $ba ba \dots$ также различными являются слова длины $0, 1, 2, \dots, 2n - 1$. Осталось заметить, что

$$b = (ab)^n b = (ab)^{n-1} a;$$

$$ba = (ab)^n ba = (ab)^{n-1};$$

$$\vdots$$

$$(ba)^{n-1} b = (ab)^n (ba)^{n-1} b = a.$$

Таким образом, все слова вида $ba ba \dots$ представляются словами вида $abab \dots$. Значит, $|H| \leq 2n$. Отсюда следует, что $D_n = H$.

Проблема равенства слов. Пусть S – некоторое множество. И пусть даны два конечных слова от букв $s_i \in S$ и s_i^{-1} . Возникает вопрос: эквивалентны ли эти два слова, то есть дают ли они один и тот же элемент свободной группы $\mathfrak{F}(S)$? Этот вопрос называется проблемой равенства слов.

Один из способов решить проблему равенства слов – это определить некий канонический вид, к которому можно привести каждое слово, причем этот вид должен быть единственным. Если этот подход будет реализован, то для проверки эквивалентности двух слов нужно оба слова привести к каноническому виду и сравнить результаты. Для свободной группы таким каноническим видом является несократимый вид (так как мы доказали, что в каждом классе эквивалентности есть ровно одно несократимое слово.)

Замечание 1. Можно поставить аналогичный вопрос равенства слов не только в свободной группе, но и в группе с соотношениями. В этом случае слова эквивалентны не только, когда они различаются цепочкой сокращений и приписываний, но также можно вставлять в любое место или убирать любые элементы из $N(r_1, \dots, r_k)$, где r_i – соотношения. Оказывается, что проблема равенства слов может стать гораздо сложнее, более того она не всегда разрешима. Более точно, существует конечно порожденная группа с конечным числом соотношений, в которой проблема равенства слов алгоритмически не разрешима.

Напомним, что прямым произведением групп K и H мы называли множество пар $(k, h) \mid k \in K, h \in H$ с покомпонентным умножением. Назовем такое прямое произведение *внешним*.

Определение 2. Пусть K и H – нормальные подгруппы в группе G такие, что $K \cap H = \{e\}$ и G порождается подгруппами K и H . Тогда G называется *внутренним прямым произведением* подгрупп H и K .

Лемма 1. 1) Внешнее прямое произведение групп K и H является внутренним прямым произведением подгрупп $K \times \{e\}$ и $\{e\} \times H$.

2) Пусть K и H – подгруппы в G . И пусть группа G – это внутреннее прямое произведение подгрупп K и H . Тогда G изоморфно внешнему прямому произведению $K \times H$.

Доказательство. 1) Рассмотрим подгруппы $K \times \{e\} = \{(k, e) \mid k \in K\}$ и $\{e\} \times H = \{(e, h) \mid h \in H\}$ во внешнем прямом произведении $K \times H$. (Проверку, что это подгруппы оставляю читателю.) Тогда

$$(a, b)(k, e)(a, b)^{-1} = (a, b)(k, e)(a^{-1}, b^{-1}) = (aka^{-1}, beb^{-1}) = (aka^{-1}, e) \in K \times \{e\}.$$

Значит, подгруппа $K \times \{e\}$ нормальна в $K \times H$. Аналогично, подгруппа $\{e\} \times H$ нормальна в $K \times H$. Пересечение этих подгрупп – это единственный элемент (e, e) , являющийся нейтральным элементом группы. Кроме того, любой элемент (k, h) есть произведение элементов (k, e) и (e, h) , то есть эти подгруппы порождают $K \times H$. Таким образом, группа $K \times H$ является внутренним прямым произведением подгрупп $K \times \{e\}$ и $\{e\} \times H$.

2) Так как группа G порождена подгруппами K и H и подгруппа H нормальна, то по лемме 2 из лекции 5 любой элемент $g \in G$ представляется в виде $g = kh$. Значит отображение

$$\varphi: K \times H \rightarrow G, \quad \varphi(k, h) = kh$$

сюръективно. Докажем, что φ – изоморфизм групп.

Предположим, что $k_1 h_1 = k_2 h_2$. Тогда, умножая слева на k_2^{-1} , а справа – на h_1^{-1} , получаем $k_2^{-1} k_1 = h_2 h_1^{-1} \in K \cap H$. Следовательно, $k_2^{-1} k_1 = h_2 h_1^{-1} = e$, то есть $k_1 = k_2$ и $h_1 = h_2$. Итак, представление $g = kh$ единственно. Это означает инъективность φ .

Осталось проверить, что φ – гомоморфизм. Пусть теперь $k_1, k_2 \in K$ и $h_1, h_2 \in H$. Докажем, что $h_1 k_2 h_1^{-1} k_2^{-1} = e$. В самом деле так как K – нормальная подгруппа, $h_1 k_2 h_1^{-1} = \hat{k} \in K$, с другой стороны, так как H – нормальна подгруппа, $k_2 h_1^{-1} k_2^{-1} = \hat{h} \in H$. Тогда

$$h_1 k_2 h_1^{-1} k_2^{-1} = h_1 \hat{k} = \hat{k} k_2^{-1} \in K \cap H = \{e\}.$$

Итак, $h_1 k_2 h_1^{-1} k_2^{-1} = e$. Значит, $h_1 k_2 = k_2 h_1$. Но тогда

$$\varphi(k_1, h_1) \varphi(k_2, h_2) = k_1 h_1 k_2 h_2 = k_1 k_2 h_1 h_2 = \varphi(k_1 k_2, h_1 h_2).$$

□

В дальнейшем мы не будем различать внутреннее и внешнее прямые произведения и будем использовать единый термин "прямое произведение".

Замечание 2. Так же как в случае абелевой группы мы используем аддитивные обозначения, если группы A и B абелевы, то прямое произведение групп A и B мы будем называть *прямой суммой* и обозначать $A \oplus B$.

Теорема 1 (Китайская теорема об остатках.). Пусть m и n – натуральные числа. Тогда следующие условия эквивалентны:

- 1) $\text{НОД}(m, n) = 1$;
- 2) $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$.

Доказательство. $1 \Rightarrow 2$. Рассмотрим

$$\varphi: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n, \quad \varphi(u) = (u \bmod m, u \bmod n).$$

Докажем, что φ – изоморфизм. Из определения видно, что φ переводит сложение в сложение, то есть является гомоморфизмом.

Пусть $u \in \text{Кер } \varphi$. Тогда u делится и на m , и на n . Значит, так как m и n взаимно просты, u делится на mn . То есть u равен нулю по модулю mn . Следовательно, $\text{Кер } \varphi = \{0\}$, а значит, гомоморфизм φ инъективен. Но поскольку $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \oplus \mathbb{Z}_n|$ из инъективности φ следует его биективность. Итак, φ – изоморфизм.

$2 \Rightarrow 1$. Пусть $\text{НОД}(m, n) = d > 1$. Тогда для любого элемента $(a, b) \in \mathbb{Z}_m \oplus \mathbb{Z}_n$ выполнено

$$\frac{mn}{d}(a, b) = \text{НОК}(m, n)(a, b) = (0, 0).$$

Значит, любой элемент в $\mathbb{Z}_m \oplus \mathbb{Z}_n$ имеет порядок не больше $\frac{mn}{d}$, то есть нет элемента из $\mathbb{Z}_m \oplus \mathbb{Z}_n$, порядок которого равен mn . Значит, группа $\mathbb{Z}_m \oplus \mathbb{Z}_n$ не циклическая и не изоморфна $\mathbb{Z}_{mn}$. □

Далее мы собираемся погрузиться в изучение. Для абелевых групп будем использовать аддитивную терминологию. Операцию будем обозначать "+" и называть сложением. Нейтральный элемент называем нулем. При этом степень g^k элемента g , будет обозначаться kg .

Замечание 3. То, что абелева группа A порождается подмножеством $S \subset A$ означает, что каждый элемент $a \in A$ представляется в виде $a = k_1 s_1 + \dots + k_n s_n$, где $s_i \in S$, $k_i \in \mathbb{Z}$.

Мы почти всегда будем ограничиваться рассмотрением только конечнопорожденных абелевых групп, то есть таких групп A , для которых множество S может быть выбрано конечным.

Определение 3. Система элементов S абелевой группы A называется *линейно независимой* (над $\mathbb{Z}$), если из того, что $k_1 s_1 + \dots + k_n s_n = 0$ для некоторых $k_i \in \mathbb{Z}$, $s_i \in S$, следует что все k_i равны нулю.

Определение 4. *Базис* абелевой группы – это линейно независимая система порождающих этой группы.

Заметим, что не у всякой группы есть базис. Например, у группы $\mathbb{Z}_n$ базиса нет, так как для любой системы $\{s_1, \dots, s_k\}$ выполнено $ns_1 = 0$, что противоречит линейной независимости этой системы.