Лекция 5

Следствие 1. *(Из теоремы о гомоморфизме) Если* $|G| < \infty$ *и* $\varphi\colon G \to \widetilde{G}$ *– гомоморфизм, то*
$$|\operatorname{Ker}\varphi| \cdot |\operatorname{Im}\varphi| = |G|.$$

Предложение 1. *Если группа* G *не коммутативна, то группа* $G/Z(G)$ *не является циклической.*

Доказательство. Предположим, что $G/Z(G) = \langle aZ(G)\rangle$, $a \in G$. Тогда для любого $g \in G$ выполнено $g \in a^k Z(G)$, то есть $g = a^k z$, где $z \in Z(G)$. Возьмем $g_1, g_2 \in G$, тогда $g_1 = a^k z_1$, $g_2 = a^m z_2$. Имеем
$$g_1 g_2 = a^k z_1 a^m z_2 = a^{k+m} z_1 z_2 = a^{k+m} z_2 z_1 = a^m z_2 a^k z_1 = g_2 g_1.$$
Таким образом, G коммутативна. (И следовательно, $G/Z(G) \cong \{e\}$.) □

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 группа G содержит подмножество S. *Подгруппой, порожденной подмножеством* S, называется минимальная подгруппа, содержащая S. Обозначается эта подгруппа $\langle S\rangle$. Если $G = \langle S\rangle$, то S называется *множеством порождающих группы* G.

Лемма 1. *Пусть* $G = \langle S\rangle$, *тогда* G *совпадает с множеством конечных произведений элементов из* S *и обратных к ним, то есть*
$$\{s_1^{\pm 1} \dots s_n^{\pm 1} \mid s_i \in S, n \in \mathbb{N}\}.$$

Доказательство. Легко видеть, что множество конечных произведений элементов из S и обратных к ним замкнуто относительно произведения и взятия обратного. Кроме того в нем лежит $ss^{-1} = e$. Значит, это подгруппа, содержащая S, и следовательно, совпадает с G. □

Упражнение 1. Докажите, что
а) $\mathbb{Z} = \langle 1\rangle$,
б) $S_n = \langle (1,2), (2,3) \dots, (n-1, n)\rangle = \langle (1,2), (1,2,\dots,n)\rangle$,
в) $A_n = \langle (1,2,3), (1,2,4), \dots, (1,2,n)\rangle$.

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 3. 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 2. *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 $K \times \{e\} = \{(k,e)|k \in K\}$ и $\{e\} \times H = \{(e,h)|h \in H\}$ 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, то любой элемент в G имеет вид

$$h_1^{\varepsilon_1} k_1^{\varepsilon'_1} \dots h_m^{\varepsilon_m} k_m^{\varepsilon'_m},$$

где $h_i \in H$, $k_i \in K$ и $\varepsilon_j, \varepsilon'_j = \pm 1$. Так как обратный к элементу подгруппы также лежит в этой подгруппе, можно считать, что все элементы G имеют вид

$$h_1 k_1 \dots h_m k_m.$$

Рассмотрим элемент $\alpha = hkh^{-1}k^{-1}$. Так как H нормальна, $\alpha = h(kh^{-1}k^{-1})$ содержится в H. Так как подгруппа K нормальна, элемент $\alpha = (hkh^{-1})k^{-1}$ лежит в K. Следовательно, $\alpha \in H \cap K = \{e\}$. Итак, $hkh^{-1}k^{-1} = e$.мУмножая это равенство на kh справа, получаем $hk = kh$. Итак, элементы из K и H можно переставлять между собой.

Получаем, что любой элемент $g \in G$ представляется в виде $g = kh$. Значит отображение

$$\varphi\colon K \times H \to G, \qquad \varphi(k,h) = kh$$

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, $h_1 k_2 h_1^{-1} = \widehat{k} \in K$, с другой стороны, так как H – нормальна подгруппа, $k_2 h_1^{-1} k_2^{-1} = \widehat{h} \in H$. Тогда

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

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 внутренннее и внешнее прямые произведения и будем использовать единый термин "прямое произведение".

Теорема 1 (Теорема о факторизации прямого произведения)**.** *Пусть $G_1, \ldots, G_k$ – группы. В каждой группе G_i фиксируем нормальную подгруппу H_i. Тогда $H_1 \times \ldots \times H_k$ является нормальной подгруппой $G_1 \times \ldots \times G_k$ и*

$$(G_1 \times \ldots \times G_k)/(H_1 \times \ldots \times H_k) \cong G_1/H_1 \times \ldots \times G_k/H_k.$$

Доказательство. Рассмотрим отображение

$$\varphi\colon G_1 \times \ldots \times G_k \to G_1/H_1 \times \ldots \times G_k/H_k,$$
$$\varphi\colon (g_1, \ldots, g_k) \mapsto (g_1H_1, \ldots, g_kH_k).$$

Легко видеть, что φ – это сюръективный гомоморфизм, ядро которого совпадает с $H_1 \times \ldots \times H_k$. Это доказывает оба утверждения. □

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 2 (Китайская теорема об остатках.)**.** *Пусть m и n – натуральные числа. Тогда следующие условия эквивалентны:*
1) НОД$(m, n) = 1$;
2) $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$.

Доказательство. $1 \Rightarrow 2$. Рассмотрим

$$\varphi\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \oplus \mathbb{Z}_n, \qquad \varphi(u) = (u \bmod m, u \bmod n).$$

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

Пусть $u \in \operatorname{Ker}\varphi$. 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, $\operatorname{Ker}\varphi = \{0\}$, 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 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 $\mathbb{Z}_{mn}$. □

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 обозначатся kg.

Замечание 3. То, что абелева группа A порождается подмножеством $S \subset A$ означает, что каждый элемент $a \in A$ представляется в виде $a = k_1s_1 + \ldots + k_ns_n$, где $s_i \in S$, $k_i \in \mathbb{Z}$.

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