

ЛЕКЦИЯ 4

Определение 1. Подгруппа H группы G называется нормальной, если для любого $g \in G$ выполнено $gH = Hg$. То, что H – нормальная подгруппа G обозначается так: $G \triangleright H$.

Обозначим через gHg^{-1} множество $\{ghg^{-1} \mid h \in H\}$.

Лемма 1. Следующие условия равносильны:

- 1) $G \triangleright H$,
- 2) для каждого $g \in G$ выполнено $gHg^{-1} = H$,
- 3) для каждого $g \in G$ выполнено $gHg^{-1} \subseteq H$,

Доказательство. $1 \implies 2$ В множестве $gH = Hg$ каждый элемент имеет вид $gh_1 = h_2g$. При этом и h_1 и h_2 пробегает всю группу H . Домножим каждый элемент справа на g^{-1} , получим $gh_1g^{-1} = h_2$. То есть $gHg^{-1} = H$.

$2 \implies 3$ Очевидно.

$3 \implies 1$. Для каждого $g \in G$ и $h \in H$ выполнено $ghg^{-1} = \tilde{h} \in H$. Тогда $gh = ghg^{-1}g = \tilde{h}g$. Отсюда $gH \subseteq Hg$. Аналогично $hg = gg^{-1}hg = g\hat{h}$ для $\hat{h} = g^{-1}hg \in H$. Значит, $gH \supseteq Hg$. В итоге $gH = Hg$. $\square$

Пример 1. Любая подгруппа в абелевой группе нормальна, так как $ghg^{-1} = h$.

Пример 2. $SL_n(\mathbb{C})$ – нормальная подгруппа в $GL_n(\mathbb{C})$. Действительно, пусть $A \in GL_n(\mathbb{C})$, $B \in SL_n(\mathbb{C})$. Тогда $\det(ABA^{-1}) = \det A \det B (\det A)^{-1} = 1$. То есть $ABA^{-1} \in SL_n(\mathbb{C})$.

Пример 3. Подгруппа $\langle (1, 2) \rangle = \{id, (1, 2)\} \subseteq S_3$ не является нормальной. В самом деле,

$$(1, 2, 3)(1, 2)(1, 2, 3)^{-1} = (1, 2, 3)(1, 2)(1, 3, 2) = (2, 3) \notin \langle (1, 2) \rangle.$$

Упражнение 1. Найдите явно разбиение группы S_3 на левые и правые смежные классы по подгруппе $\langle (1, 2) \rangle$.

Определение 2. Пусть H – нормальная подгруппа в группе G . Факторгруппа G/H – это множество (левых, они же правые) смежных классов по подгруппе H с операцией

$$(g_1H) \cdot (g_2H) = (g_1g_2)H.$$

Определение умножения в факторгруппе требует проверки корректности, то есть проверки того, что результат умножения не зависит от выбора представителей в смежных классах. Потенциальная проблема содержится в том, что $g_1H = g'_1H$, $g_2H = g'_2H$, но при этом смежный класс g_1g_2H может не совпадать с $g'_1g'_2H$. Тогда умножение называется некорректным.

Предложение 1. Пусть G – группа, H – подгруппа. Тогда умножение на множестве левых смежных классов корректно тогда и только тогда, когда H нормальна.

Доказательство. Пусть H нормальна и $g_1H = g'_1H$, $g_2H = g'_2H$. Получаем, что $g_1'^{-1}g_1 \in H$ и $g_2'^{-1}g_2 \in H$. Обозначим $g_1'^{-1}g_1$ через h . Имеем

$$(g_1'g_2')^{-1}(g_1g_2) = g_2'^{-1}g_1'^{-1}g_1g_2 = g_2'^{-1}hg_2 \in H$$

Это означает, что g_1g_2H совпадает с $g_1'g_2'H$. Значит, умножение корректно.

Пусть теперь H не нормальна. Тогда найдутся $g \in G$ и $h \in H$ такие, что $ghg^{-1} \notin H$. Тогда $gH = (gh)H$. Рассмотрим следующие смежные классы: $gH = (gh)H$ и $g^{-1}H$.

Имеем $gH \cdot g^{-1}H = H$, но $(gh)H \cdot g^{-1}H = (ghg^{-1})H \neq H$. Значит, умножение не корректно. $\square$

Легко видеть, что G/H действительно группа. Ассоциативность произведения следует из ассоциативности произведения в G , единичный элемент – это $eH = H$, обратный к gH элемент – это $g^{-1}H$. Из теоремы Лагранжа следует, что если G – конечная группа, то $|G/H| = \frac{|G|}{|H|}$.

Пример 4. Найдем, чему изоморфна факторгруппа $\mathbb{Z}/n\mathbb{Z}$. Подгруппа $n\mathbb{Z}$ нормальна, так как группа $\mathbb{Z}$ абелева. Смежные классы имеют вид $k+n\mathbb{Z}$. При этом $k+n\mathbb{Z} = l+n\mathbb{Z}$ тогда и только тогда, когда k и l имеют одинаковые остатки при делении на n . Сопоставим смежному классу $k+n\mathbb{Z}$ остаток при делении k на n . Докажем, что это сопоставление – это изоморфизм ψ между $\mathbb{Z}/n\mathbb{Z}$ и $\mathbb{Z}_n$. Действительно, сложению смежных классов соответствует сложение остатков. Кроме того ψ сюръективно, так как любой остаток – это остаток некоторого числа k , а значит, он равен $\psi(k+n\mathbb{Z})$. Для проверки инъективности ψ , воспользуемся критерием инъективности. Ядро ψ – это то, что переходит в остаток ноль, то есть смежный класс $n\mathbb{Z}$, который является нейтральным элементом фактор-группы.

Пусть $\varphi: G \rightarrow \tilde{G}$ – гомоморфизм групп.

Лемма 2. Ядро $\text{Ker } \varphi$ – нормальная подгруппа в группе G .

Доказательство. То, что ядро – подгруппа уже было доказано ранее. Докажем, что подгруппа $\text{Ker } \varphi \subseteq G$ нормальна. Пусть $g \in G$, $h \in \text{Ker } \varphi$. Тогда

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e.$$

Значит, $ghg^{-1} \in \text{Ker } \varphi$, то есть $\text{Ker } \varphi$ – нормальная подгруппа. $\square$

Определение 3. Рассмотрим следующее отображение $\pi_H: G \rightarrow G/H$, $g \mapsto gH$. Из определения операции в факторгруппе следует, что π_H – гомоморфизм. Легко видеть, что он сюръективен. Гомоморфизм π_H называется *каноническим гомоморфизмом*.

Для канонического гомоморфизма ядро – это нормальная подгруппа H , а образ – факторгруппа G/H . Следующая теорема показывает, что ситуация аналогична для любого гомоморфизма.

Теорема 1. (Теорема о гомоморфизме) Пусть $\varphi: G \rightarrow \tilde{G}$ – гомоморфизм групп. Тогда $G/\text{Ker } \varphi \cong \text{Im } \varphi$.

Доказательство. Рассмотрим отображение

$$\Psi: G/\text{Ker } \varphi \rightarrow \text{Im } \varphi, \quad \Psi(g\text{Ker } \varphi) = \varphi(g).$$

Сперва нам надо проверить корректность отображения Ψ , то есть то, что оно не зависит от выбора представителя g из смежного класса. Для этого заметим, что если $g\text{Ker } \varphi = g'\text{Ker } \varphi$, то $g'^{-1}g = h \in \text{Ker } \varphi$. Тогда $g = g'h$. Получаем $\varphi(g) = \varphi(g'h) = \varphi(g')\varphi(h) = \varphi(g')e = \varphi(g')$. Таким образом, отображение Ψ определено корректно.

Докажем, что Ψ – изоморфизм. То, что Ψ – гомоморфизм следует из равенства:

$$\Psi((g\text{Ker } \varphi)(f\text{Ker } \varphi)) = \Psi(gf\text{Ker } \varphi) = \varphi(gf) = \varphi(g)\varphi(f) = \Psi(g\text{Ker } \varphi)\Psi(f\text{Ker } \varphi).$$

Инъективность Ψ проверим по критерию инъективности. Если $g\text{Ker } \varphi \in \text{Ker } \Psi$, то $\Psi(g\text{Ker } \varphi) = \varphi(g) = e$. Значит, $g \in \text{Ker } \varphi$. То есть $g\text{Ker } \varphi = \text{Ker } \varphi$ – единица фактор-группы. Сюръективность Ψ очевидна, так как для любого элемента $\varphi(g)$ в $\text{Im } \varphi$ в него отображается смежный класс $g\text{Ker } \varphi$. $\square$

Следствие 1. Если $|G| < \infty$ и $\varphi: G \rightarrow \tilde{G}$ – гомоморфизм, то

$$|\text{Ker } \varphi| \cdot |\text{Im } \varphi| = |G|.$$

Пример 5. Найдем, чему изоморфна факторгруппа $\mathbb{Z}/n\mathbb{Z}$ по теореме о гомоморфизме. Для того, чтобы применить теорему о гомоморфизме, нам нужно построить гомоморфизм $\varphi: \mathbb{Z} \rightarrow G'$ для некоторой группы G' такой, что $\text{Ker } \varphi = n\mathbb{Z}$. Легко видеть, что подходит следующий гомоморфизм

$$\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_n, \quad k \mapsto k \pmod{n}$$

Действительно, φ – гомоморфизм, $\text{Ker } \varphi = n\mathbb{Z}$ и φ – сюръекция, то есть $\text{Im } \varphi = \mathbb{Z}_n$. По теореме о гомоморфизме $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Определение 4. Центр группы G – это множество $Z(G)$ элементов, коммутирующих со всеми элементами группы. $Z(G) = \{z \in G \mid \forall g \in G : gz = zg\}$.

Лемма 3. Центр – это нормальная подгруппа G .

Доказательство. Пусть $z_1, z_2 \in Z(G)$. Тогда для любого $g \in G$ выполнено

$$z_1 z_2 g = z_1 g z_2 = g z_1 z_2.$$

Значит, $Z(G)$ – замкнутое относительно операции подмножество. Для доказательства замкнутости относительно взятия обратного заметим, что если $z \in Z(G)$, то для любого $g \in G$ выполнено $zg^{-1} = g^{-1}z$. Тогда

$$z^{-1}g = (g^{-1}z)^{-1} = (zg^{-1})^{-1} = gz^{-1}.$$

Кроме того $Z(G) \neq \emptyset$, так как $e \in Z(G)$.

То, что подгруппа $Z(G)$ нормальна следует из равенства $gzg^{-1} = z \in Z(G)$. $\square$

Предложение 2. Факторгруппа группы G по центру изоморфна группе внутренних автоморфизмов $\text{Inn}(G)$.

Доказательство. Докажем, что отображение $\Psi: G \rightarrow \text{Inn}(G)$, $g \mapsto \varphi_g$ является гомоморфизмом. В самом деле

$$\begin{aligned} \Psi(g_1 g_2)(h) &= \varphi_{g_1 g_2}(h) = (g_1 g_2)h(g_1 g_2)^{-1} = g_1 g_2 h g_2^{-1} g_1^{-1} = \\ &= g_1 (g_2 h g_2^{-1}) g_1^{-1} = \varphi_{g_1} \circ \varphi_{g_2}(h) = \Psi(g_1) \circ \Psi(g_2)(h). \end{aligned}$$

Таким образом $\Psi(g_1 g_2) = \Psi(g_1) \circ \Psi(g_2)$. По определению внутренних автоморфизмов гомоморфизм Ψ сюръективен. Ядро Ψ состоит из тех элементов $g \in G$, для которых $\varphi_g = \text{id}$, то есть $\forall h \in G$ выполнено $ghg^{-1} = h$. Это означает $g \in Z(G)$. Итак, $\text{Ker } \varphi = Z(G)$, $\text{Im } \varphi = \text{Inn}(G)$. По теореме о гомоморфизме $G/Z(G) \cong \text{Inn}(G)$. $\square$

Предложение 3. 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, $G/Z(G) \cong \{e\}$.) $\square$

Предложение 4. Подгруппа внутренних автоморфизмов $\text{Inn}(G)$ нормальна в группе $\text{Aut}(G)$.

Доказательство. Пусть $\psi \in \text{Aut}(G)$ и $g \in G$. Получаем

$$\begin{aligned}\psi \circ \varphi_g \circ \psi^{-1}(h) &= \psi(\varphi_g(\psi^{-1}(h))) = \psi(g\psi^{-1}(h)g^{-1}) = \\ &= \psi(g)\psi(\psi^{-1}(h))\psi(g^{-1}) = \psi(g)h\psi(g)^{-1} = \varphi_{\psi(g)}(h).\end{aligned}$$

Значит, $\psi \circ \varphi_g \circ \psi^{-1}(h) = \varphi_{\psi(g)}(h) \in \text{Inn}(G)$. $\square$

Замечание 1. Не существует хорошей интерпретации, чему изоморфна группа $\text{Aut}(G)/\text{Inn}(G)$, поэтому доказать нормальность $\text{Inn}(G)$, реализовав эту подгруппу как ядро гомоморфизма не получается.

Определение 5. 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 (образующих) группы G .

Лемма 4. Пусть S – подмножество в группе G . Тогда подгруппа $\langle S \rangle$, порождаемая S , совпадает с множеством конечных произведений элементов из S и обратных к ним, то есть

$$\langle S \rangle = \{s_1^{\varepsilon_1} \dots s_n^{\varepsilon_n} \mid s_i \in S, \varepsilon_i = \pm 1, n \in \mathbb{N}\}.$$

Доказательство. Обозначим $P = \{s_1^{\varepsilon_1} \dots s_n^{\varepsilon_n} \mid s_i \in S, \varepsilon_i = \pm 1, n \in \mathbb{N}\}$. Нам надо доказать, что $P = \langle S \rangle$. Сперва скажем, что $P \subseteq \langle S \rangle$. В самом деле так как $s_i \in S \subseteq \langle S \rangle$ и $\langle S \rangle$ – подгруппа, выходит, что $s_1^{\varepsilon_1} \dots s_n^{\varepsilon_n} \in \langle S \rangle$.

Обратно. Легко видеть, что множество P замкнуто относительно произведения и взятия обратного. Кроме того в нем лежит $ss^{-1} = e$. Значит, это подгруппа, содержащая S , и следовательно, она содержит $\langle S \rangle$. $\square$

Упражнение 2. 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) $A_n = \langle (1, 2, 3), (1, 2, 4), \dots, (1, 2, n) \rangle$.