ЛЕКЦИЯ 5

ТЕОРЕМЫ О ГОМОМОРФИЗМЕ

ПРЯМЫЕ ПРОИЗВЕДЕНИЯ ГРУПП

ТЕОРЕМЫ О ГОМОМОРФИЗМАХ

Теорема 1 (о гомоморфизме для групп). *Пусть* $f\colon G \to G'$ — *сюръективный гомоморфизм* (*т. е. гомоморфизм из группы* G на *группу* G'). *Тогда существует изоморфизм*

$$\psi\colon G/\ker f \to G'$$

такой, что $f = \psi\pi$, *где* $\pi\colon G \to G/\ker f$ — *канонический гомоморфизм из группы* G *на фактор-группу* $G/\ker f$ *по нормальной подгруппе* $\ker f$ (*ядро гомоморфизма* f).

Доказательство. Для смежного класса $x\ker f$, $x \in G$, положим $\psi(x\ker f) = f(x)$.

Корректность отображения $\psi\colon G/\ker f \to G'$. Если для $y \in G$ имеем $x\ker f = y\ker f$, то $x^{-1}y \in \ker f$, поэтому $e' = f(x^{-1}y) = f(x)^{-1}f(y)$, следовательно, $f(x) = f(y)$.

Покажем, что ψ — *биекция.*

а) Если для $x, y \in G$ имеем $f(x) = \psi(x\ker f) = \psi(y\ker f) = f(y)$, то $f(x^{-1}y) = f(x)^{-1}f(y) = e'$, т. е. $x^{-1}y \in \ker f$. Поэтому $x\ker f = y\ker f$, т. е. ψ — инъекция.

б) Если $g' \in G'$, то $g' = f(x)$ для некоторого $x \in G$ (поскольку f — сюръекция). Тогда $g' = f(x) = \psi(x\ker f)$, т. е. ψ — сюръекция.

Проверим, что ψ — *гомоморфизм* групп. Действительно, для $x, y \in G$ имеем

$$\psi(x\ker f \cdot y\ker f) = \psi(xy\ker f) = f(xy) = \\ = f(x)f(y) = \psi(x\ker f)\psi(y\ker f).$$

Итак, мы показали, что $\psi\colon G/\ker f \to G'$ — *изоморфизм.*

Проверим, что $f = \psi\pi$. Действительно, для $x \in G$ имеем

$$(\psi\pi)(x) = \psi\big(\pi(x)\big) = \psi(x\ker f) = f(x). \qquad \square$$

Теорема о гомоморфизме является эффективным средством для вычисления фактор-групп.

Пример 1. Пусть $G = (\mathbb{C}^*, \cdot)$, $H = (\mathbb{R}^*, \cdot) \subset G$.

Рассмотрим сюръективный гомоморфизм

$$f\colon G = \mathbb{C}^* \to T = \{z \in \mathbb{C} \mid |z| = 1\},$$

для которого $f(z) = \frac{z^2}{|z|^2}$ для $z \in \mathbb{C}^*$. Тогда $\ker f = H = \{\mathbb{R}^*, \cdot\}$. В силу теоремы о гомоморфизме

$$T \cong G/\ker f = \mathbb{C}^*/\mathbb{R}^*. \qquad \square$$

Теорема 2 (вторая теорема о гомоморфизме)**.** *Пусть* H *— подгруппа группы* G*,* K *— нормальная подгруппа группы* G *(*HK *— подгруппа группы* G*). Тогда*:

1) $H \cap K \lhd H$ *и* $K \lhd HK$;

2) $HK/K \cong H/H \cap K$.

Доказательство. Нас интересуют четыре подгруппы:

$$\begin{array}{ccccc} & & HK & & \\ & \lhd & & \supseteq & \\ K & & & & H \\ & \supseteq & & \lhd & \\ & & H \cap K & & \end{array}.$$

1) Так как $K \lhd G$, то $H \cap K \lhd H$. Если $h \in H$, $k \in K$, то

$$(hk)^{-1}Khk = k^{-1}(h^{-1}Kh)k = k^{-1}Kk \subseteq K,$$

т. е. $K \lhd HK$.

2) Рассмотрим канонический эпиморфизм

$$\pi_K \colon G \to G/K$$

и его ограничение на H

$$\pi_K|_H \colon H \to \pi_K(H) \subseteq G/K.$$

Ясно, что $\ker \pi_K|_H = H \cap \ker \pi_K = H \cap K$.

Далее, для $h \in H$ и $k \in K$ имеем

$$\pi_K(h) = hK \subseteq HK/K, \quad (hk)K = hK = \pi_K(h)$$

т. е. $HK/K \subseteq \pi_K(H)$. Таким образом,

$$\mathrm{Im}\,(\pi_K|_H) = \pi_K(H) = HK/K.$$

В силу первой теоремы о гомоморфизмах (ее следствия)

$$HK/K = \mathrm{Im}\,(\pi_K|_H) \cong H/\ker(\pi_K|_H) = H/H \cap K. \qquad \square$$

Пример 2. 1) Пусть H — подгруппа группы $\mathbf{S}_n$, $H \not\subseteq \mathbf{A}_n$ (т. е. подгруппа H содержит нечетную подстановку). Тогда

$$H/(H \cap \mathbf{A}_n) \cong \mathbb{Z}_2$$

(другими словами, $H \cap \mathbf{A}_n$ — подгруппа группы H индекса 2).

Доказательство. Если $h \in H$, $h \notin \mathbf{A}_n$, то $h\mathbf{A}_n = \mathbf{S}_n \setminus \mathbf{A}_n$. Следовательно, $H\mathbf{A}_n = \mathbf{S}_n$. Применяя вторую теорему о гомоморфизмах для $K = \mathbf{A}_n$, получаем

$$H/(H \cap \mathbf{A}_n) \cong (H\mathbf{A}_n)/\mathbf{A}_n = \mathbf{S}_n/\mathbf{A}_n \cong \mathbb{Z}_2. \qquad \square$$

2) Пусть $m, n \in \mathbb{Z}$, $d = \text{НОД}(m, n)$, $l = \text{НОК}(m, n)$. Тогда

$$d\mathbb{Z}/n\mathbb{Z} = (m\mathbb{Z} + n\mathbb{Z})/n\mathbb{Z} \cong m\mathbb{Z}/(m\mathbb{Z} \cap n\mathbb{Z}) = m\mathbb{Z}/l\mathbb{Z}$$

$(dl = mn)$. $\square$

3) Пусть G — конечная группа, $H \lhd G$, $(|H|, |G/H|) = 1$. Тогда H — единственная подгруппа группы G порядка $|H|$.

Доказательство. Если $K \subseteq G$, $|K| = |H|$, то $K/K \cap H \cong KH/H \subseteq G/H$ и $|KH/H| = \frac{|KH|}{|H|} = \frac{|K|}{|K \cap H|}$, при этом $|K|/|K \cap H|$ — делитель числа $|G/H|$. Так как $(|H|, |G/H|) = 1$ и $|K| = |H|$, то $|K|/|K \cap H| = 1$, и поэтому $K = K \cap H$, следовательно, $K = H$. $\square$

Теорема 3 (третья теорема о гомоморфизме)**.** *Пусть* $G \xrightarrow{f} G'$ *— сюръективный гомоморфизм,* $K = \ker f \lhd G$ *(например, если* $K \lhd G$*, то* $f = \pi_K \colon G \to G/K$*),* $H' \subseteq G'$ *— подгруппа,* $H = f^{-1}(H') = \{g \in G \mid f(g) \in H'\}$ *— ее полный прообраз при отображении* f *(ясно, что* $H \supseteq K$*, поскольку* $f(K) = e'$*). Тогда:*

1) *естественные соответствия*

$$\begin{gathered} H \mapsto f(H) = H', \\ H = f^{-1}(H') \mapsto H' \end{gathered}$$

устанавливают естественную биекцию между множеством подгрупп H *группы* G*, содержащих нормальную подгруппу* K*, и множеством всех подгрупп* H' *группы* G';

2) *при этом соответствии* $H \lhd G$ *тогда и только тогда, когда* $H' \lhd G'$*, и* $G'/H' \cong G/H$ *(в частности,* $(G/K)/(H/K) \cong G/H$ *для* $G \lhd H \lhd K$*).*

Доказательство. 1) Ясно, что в нашем случае $f\big(f^{-1}(H')\big) = H'$.

Пусть теперь H — подгруппа группы G и $H \supseteq K$.

Тогда $f^{-1}\big(f(H)\big) \supseteq H$. Если $g \in G$ и $f(g) \in f(H)$, т. е. $f(g) = f(h)$ для $h \in H$, то $f(h^{-1}g) = f(h)^{-1}f(g) = e'$, следовательно, $h^{-1}g \in \ker f = K \subseteq H$, т. е. $g \in hH = H$.

Итак, $f^{-1}\big(f(H)\big) = H$.

2) Если $H \lhd G$, $H \supseteq K$, и $g' = f(g) \in G'$, и $a = g(h) \in f(H)$, $h \in H$, то $(g')^{-1}ag' = f(g)^{-1}f(h)f(g) = f(g^{-1}hg) \in f(H)$, т.е. $f(H) \lhd G'$.

Если $H' \lhd G'$, $g \in G$, $x \in H = f^{-1}(H')$, т. е. $f(x) \in H'$, то $f(g^{-1}xg) = f(g)^{-1}f(x)f(g) \in H'$, поэтому $g^{-1}xg \in f^{-1}(H')$, т. е. $f^{-1}(H') \lhd G$.

Рассмотрим теперь сюръективный гомоморфизм

$$\psi = \pi_{H'} \cdot f \colon G \xrightarrow{f} G' \xrightarrow{\pi_{H'}} G'/H'.$$

Если $g \in G$, то $\psi(g) = f(g)H' = H'$ тогда и только тогда, когда $f(g) \in H'$, т.е.

$$\ker\psi = f^{-1}(H') = H.$$

В силу первой теоремы о гомоморфизмах для ψ

$$G/H = G/\ker\psi \cong G'/H'.$$

В ситуации $G \lhd H \lhd K$ и $f = \pi_K \colon G \to G' = G/K$ $H' = f(H) = H/K \lhd G/K$, имеем по доказанному $G/H \cong G'/H' = (G/K)/(H/K)$. $\square$

ПРЯМЫЕ ПРОИЗВЕДЕНИЯ ГРУПП

Сначала рассмотрим *внутреннее прямое произведение нормальных подгрупп*: будем говорить, что группа G является *внутренним произведением своих нормальных подгрупп* H и K, $H \lhd G$, $K \lhd G$, если $G = HK$ и $H \cap K = \{e\}$ (обозначение: $G = H \times K$).

Выведем основные свойства конструкции $G = H \times K$.

Лемма 1. *Если H и K — нормальные подгруппы группы G, $H \lhd G$, $K \lhd G$, и $H \cap K = \{e\}$, то $hk = kh$ для любых $h \in H$, $k \in K$.*

Доказательство. Так как $H \lhd G$ и $K \lhd G$, то

$$[k, h] = (k^{-1}h^{-1}k)h = k^{-1}(h^{-1}kh) \in H \cap K = \{e\},$$

поэтому $hk = kh$. □

Так как $G = HK$, то любой элемент $g \in G$ представи́м в виде $g = hk$, $h \in H$, $k \in K$. Покажем единственность этого представления. Если $g = hk = h'k'$, $h' \in H$, $k' \in K$, то

$$(h')^{-1}h = k'k^{-1} \in H \cap K = \{e\},$$

и поэтому $h' = h$, $k' = k$.

Если $h_1, h_2 \in H$, $k_1, k_2 \in K$, то по лемме 1 $k_1h_2 = h_2k_1$, и поэтому

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_2k_1)k_2 = (h_1h_2)(k_1k_2).$$

Пример 3. Пусть

$$G = \mathbf{V}_4 = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \subseteq \mathbf{S}_4,$$
$$H = \{e, (1\,2)(3\,4)\}, \quad K = \{e, (1\,3)(2\,4)\}, \quad L = \{e, (1\,4)(2\,3)\}.$$

Так как четверная группа Клейна $\mathbf{V}_4$ абелева, то все подгруппы в ней нормальны. Ясно, что

$$H \cap K = K \cap L = H \cap L = \{e\};$$
$$HK = KL = HL = \mathbf{V}_4.$$

Таким образом,

$$\mathbf{V}_4 = H \times K = K \times L = H \times L.$$

Замечание 1. Определение внутреннего прямого произведения можно распространить на любое конечное множество нормальных подгрупп $H_i \lhd G$, $1 \leqslant i \leqslant m$, где

$$G = H_1 H_2 \dots H_m$$

и

$$H_i \cap \left\langle \bigcup_j H_j,\ j = 1, 2, \dots, m,\ j \neq i \right\rangle = \{e\}$$

(обозначение: $G = H_1 \times H_2 \times \ldots \times H_m$).

В этом случае: $h_i h_j = h_j h_i$ для $h_i \in H_i$, $h_j \in H_j$, $i \neq j$; каждый элемент $g \in G$ единственным образом представляется в виде $g = h_1 h_2 \dots h_m$, $h_i \in H_i$; при этом

$$(h_1 h_2 \dots h_m)(h_1' h_2' \dots h_m') = (h_1 h_1')(h_2 h_2') \dots (h_m h_m').$$

Перейдем к рассмотрению конструкции *внешнего прямого произведения*. Пусть нам дано конечное множество групп $G_1, G_2, \ldots, G_m$ (в отличие от внутренней конструкции, они не предполагаются подгруппами одной группы). Рассмотрим множество

$$G = G_1 \times G_2 \times \ldots \times G_m = \{(g_1, g_2, \ldots, g_m) \mid g_i \in G\}$$

с бинарной операцией

$$(g_1, g_2, \ldots, g_m)(g_1', g_2', \ldots, g_m') = (g_1 g_1', g_2 g_2', \ldots, g_m g_m'), \quad g_i, g_i' \in G_i.$$

Ясно, что эта операция ассоциативна, $e = (e_{G_1}, e_{G_2}, \ldots, e_{G_m})$ — нейтральный элемент, $(g_1, g_2, \ldots, g_m)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_m^{-1})$.

Итак, G — группа, называемая *внешним прямым произведением групп* $G_1, G_2, \ldots, G_m$ (обозначение: $G = G_1 \times G_2 \times \ldots \times G_m$).

Группа G_i не является подгруппой внешнего прямого произведения $G = G_1 \times G_2 \times \ldots \times G_m$, но в G имеется подгруппа G_i', изоморфная группе G_i, а именно

$$G_i' = \Big\{(e_{G_1}, e_{G_2}, \ldots, \underset{i}{a}, \ldots, e_{G_m}) \;\Big|\; a \in G_i\Big\}.$$

Так как для $g_i, h_i \in G_i$ имеем

$$(g_1, g_2, \ldots, g_m)^{-1}(h_1, h_2, \ldots, h_m)(g_1, g_2, \ldots, g_m) = \\ = (g_1^{-1} h_1 g_1, g_2^{-1} h_2 g_2, \ldots, g_m^{-1} h_m g_m),$$

то G_i' — нормальная подгруппа в G, $G_i' \lhd G$. Кроме того,

$$G = G_1' G_2' \ldots G_m',$$
$$G_i' \cap \Big\langle \bigcup G_j' \;\Big|\; j = 1, \ldots, m,\ j \neq i \Big\rangle = \{e\}.$$

Итак, внешнее прямое произведение групп $G_1, G_2, \ldots, G_m$ является внутренним прямым произведением своих подгрупп G_i', $G_i' \cong G_i$:

$$G = G_1 \times G_2 \times \ldots \times G_m = G_1' \times G_2' \times \ldots \times G_m'.$$

Кроме того, из анализа строения внутреннего прямого произведения $G = H_1 \times H_2 \times \ldots \times H_m$ нормальных подгрупп $H_i \lhd G$, $1 \leq i \leq m$, мы видим, что группа G изоморфна внешнему прямому произведению групп H_i, $1 \leqslant i \leqslant m$, при соответствии

$$g = h_1 h_2 \ldots h_m \mapsto (h_1, h_2, \ldots, h_m).$$

В дальнейшем мы будем использовать термин “прямое произведение групп” без упоминания прилагательных “внутреннее” и “внешнее”, понимая, что это разные описания одной и той же конструкции.

Замечание 2. 1) Ясно, что прямое произведение групп $G = H_1 \times H_2 \times \ldots \times H_m$ является коммутативной группой тогда и только тогда, когда все группы $H_1, \ldots, H_m$ коммутативны.

2) Пусть A, B, A', B' — группы, $A \cong A'$, $B \cong B'$, $G = A \times B$, $G' = A' \times B'$. Тогда $G \cong G'$.

3) Для прямых разложений возможно, что $G = H_1 \times H_2 = K_1 \times K_2$, но $H_i \ncong K_j$, $i, j \in \{1, 2\}$. *Действительно,*

$$\mathbb{Z}_{30} = \mathbb{Z}_2 \oplus \mathbb{Z}_{15} = \mathbb{Z}_5 \oplus \mathbb{Z}_6.$$

Теорема 4. *Пусть $G_i = (a_i)$, $O(a_i) = n_i$, $i = 1, \ldots, m$, — циклические группы порядка n_i. Тогда прямое произведение $G = G_1 \times G_2 \times \ldots \times G_m$ является циклической группой тогда и только тогда, когда порядки $n_1, n_2, \ldots, n_m$ попарно взаимно просты.*

Доказательство. 1) Пусть числа $n_1, n_2, \ldots, n_m$ попарно взаимно просты и $(a_1, a_2, \ldots, a_m)^k = (e_1, e_2, \ldots, e_m)$, $k > 0$. Тогда $a_i^k = e_i$ для всех $1 \leqslant i \leqslant m$. Поэтому $k = n_i q_i$ и k делится на число $|G| = n = n_1 n_2 \ldots n_m$. Итак, $O\big((a_1, a_2, \ldots, a_m)\big) = n = |G|$, и следовательно, $G = \big((a_1, a_2, \ldots, a_m)\big)$ — циклическая группа с циклическим образующим $(a_1, a_2, \ldots, a_m)$.

2) Если $(n_i, n_j) = d > 1$, то

$$l = \text{НОК}(n_1, n_2, \ldots, n_m) < n = n_1 n_2 \ldots n_m,$$

и поэтому

$$(g_1, g_2, \ldots, g_m)^l = (g_1^l, g_2^l, \ldots, g_m^l) = (e_1, e_2, \ldots, e_m).$$

Таким образом, в группе $G = G_1 \times G_2 \times \ldots \times G_m$ нет элемента порядка $n = |G|$, и следовательно, группа G не является циклической. □

Следствие 1. *Если $n = p_1^{l_1} \ldots p_m^{l_m}$, где $p_1, \ldots, p_m$ — различные простые числа, $l_i > 0$, $1 \leqslant i \leqslant m$, то*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{l_1}} \times \mathbb{Z}_{p_2^{l_2}} \times \ldots \times \mathbb{Z}_{p_m^{l_m}},$$

при этом примарные циклические сомножители $\mathbb{Z}_{p_i^{l_i}}$ далее в прямое произведение неразложимы.