

## ЛЕКЦИЯ 3

КОММУТАНТ.

НОРМАЛЬНОЕ ЗАМЫКАНИЕ ГРУПП

ГОМОМОРФИЗМЫ ГРУПП

ФАКТОР-ГРУППЫ

ТЕОРЕМЫ О ГОМОМОРФИЗМАХ

## КОММУТАНТ

Пусть  $G$  — группа,  $a, b \in G$ . Коммутатором элементов  $a, b \in G$  называется элемент

$$[a, b] = aba^{-1}b^{-1} \in G.$$

ЛЕММА 1 (СВОЙСТВА КОММУТАТОРОВ). Пусть  $G$  — группа,  $a, b \in G$ . Тогда:

- 1)  $[a, b]ba = ab$ ;
- 2)  $[a, b] = e$  тогда и только тогда, когда  $ab = ba$ ;
- 3)  $[a, b]^{-1} = [b, a]$ ;
- 4)  $g^{-1}[a, b]g = [g^{-1}ag, g^{-1}bg]$  для  $g \in G$ .

*Доказательство.*

- 1)  $[a, b]ba = aba^{-1}b^{-1}ba = ab$ .
- 2)  $[a, b] = aba^{-1}b^{-1} = e$  тогда и только тогда, когда  $ab = ba$ .
- 3)  $[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b, a]$ .
- 4)

$$\begin{aligned} g^{-1}[a, b]g &= g^{-1}aba^{-1}b^{-1}g = \\ &= (g^{-1}ag)(g^{-1}bg)(g^{-1}a^{-1}g)(g^{-1}b^{-1}g) = \\ &= (g^{-1}ag)(g^{-1}bg)(g^{-1}ag)^{-1}(g^{-1}bg)^{-1} = [g^{-1}ag, g^{-1}bg]. \quad \square \end{aligned}$$

Коммутант группы  $G$  определим как подгруппу

$$G' = [G, G] = \langle [a, b] \mid a, b \in G \rangle$$

группы  $G$ , порожденную множеством  $S$  всех коммутаторов  $[a, b]$ ,  $a, b \in G$ .

ТЕОРЕМА 1. 1)  $G' = [G, G] = \{[x_1, y_1][x_2, y_2] \dots [x_k, y_k] \mid x_i, y_i \in G\}$  (т. е. коммутант состоит из всех конечных произведений коммутаторов).

2)  $G' \triangleleft G$  (коммутант группы является нормальной подгруппой группы).

*Доказательство.*

1) Так как  $[a, b]^{-1} = [b, a]$ , то  $G' = \langle S \rangle$ , где  $S$  — множество всех коммутаторов, состоит из произведений конечного числа коммутаторов.

2) Так как для  $g \in G$  имеем

$$g^{-1}(xy)g = (g^{-1}xg)(g^{-1}yg), \quad g^{-1}[a, b]g = [g^{-1}ag, g^{-1}bg],$$

то

$$\begin{aligned} g^{-1}([x_1, y_1] \dots [x_k, y_k])g &= (g^{-1}[x_1, y_1]g) \dots (g^{-1}[x_k, y_k]g) = \\ &= [g^{-1}x_1g, g^{-1}y_1g] \dots [g^{-1}x_kg, g^{-1}y_kg]. \end{aligned}$$

Итак,  $g^{-1}G'g \subseteq G'$  для всех  $g \in G$ , это означает, что  $G' \triangleleft G$ . □

УПРАЖНЕНИЕ 1. 1) Группа  $G$  коммутативна тогда и только тогда, когда  $G' = [G, G] = \{e\}$ .

2) Привести пример группы  $G$ , в которой совокупность коммутаторов не является подгруппой (т. е. произведение двух коммутаторов не является коммутатором).

3) Покажите, что любой элемент группы  $\mathbf{A}_5$  является коммутатором, в частности,  $[\mathbf{A}_5, \mathbf{A}_5] = \mathbf{A}_5$ .

4) Пусть  $G$  — группа,  $\mathbf{Z}(G)$  — ее центр,  $(G : \mathbf{Z}(G)) = n$ . Тогда группа  $G$  имеет не более  $n^2$  различных коммутаторов,  $[G, G]$  — конечная группа,  $|[G, G]| \leq n^{2n^3}$ .

Пусть  $A$  и  $B$  — подгруппы группы  $G$  и

$$[A, B] = \langle \{[a, b] \mid a \in A, b \in B\} \rangle —$$

подгруппа группы  $G$ , порожденная всеми коммутаторами

$$[a, b] = aba^{-1}b^{-1}, \quad \forall a \in A, \quad \forall b \in B$$

(называемая *взаимным коммутантом* подгрупп  $A$  и  $B$ ).

Если  $A \triangleleft G$ , то для  $a \in A, b \in B$

$$[a, b] = a(ba^{-1}b^{-1}) \in A \cdot A = A,$$

и поэтому

$$[A, B] \subseteq A.$$

Аналогично, если  $B \triangleleft G$ , то

$$[a, b] = (a^{-1}b^{-1}a)b \in B \cdot B = B,$$

и поэтому

$$[A, B] \subseteq B.$$

Если же  $A \triangleleft G$ ,  $B \triangleleft G$ , то

$$[A, B] \triangleleft G, \quad [A, B] \subseteq A \cap B.$$

## НОРМАЛЬНОЕ ЗАМЫКАНИЕ ГРУПП

**ЛЕММА 2.** Если  $\{H_i, i \in I\}$  — совокупность нормальных подгрупп группы  $G$ ,  $H_i \triangleleft G$ , то  $H = \bigcap_{i \in I} H_i$  — нормальная подгруппа группы  $G$ .

*Доказательство.* Действительно, мы знаем, что  $H$  — подгруппа. Если  $h \in H$  и  $g \in G$ , то  $h \in H_i$  для всех  $i \in I$ , и так как  $H_i \triangleleft G$ , то  $g^{-1}hg \in H_i$  для всех  $i \in I$ . Поэтому  $g^{-1}hg \in \bigcap_{i \in I} H_i = H$ . Итак,  $H \triangleleft G$ .  $\square$

Пусть  $S$  — непустое подмножество группы  $G$ . Рассмотрим совокупность всех нормальных подгрупп  $H_i \triangleleft G$ ,  $i \in I$ , таких, что  $S \subseteq H_i$  (эта совокупность непуста, поскольку она содержит саму группу  $G$ ). Тогда

$$S \subseteq N(S) = \bigcap_{i \in I} H_i \triangleleft G.$$

Покажем в следующей теореме, что:  $N(S)$  — наименьшая нормальная подгруппа, содержащая  $S$ ; если

$$S^G = \{g^{-1}sg \mid s \in S, g \in G\},$$

то оказывается, что подгруппа  $\langle S^G \rangle$ , порожденная подмножеством  $S^G$ , является наименьшей нормальной подгруппой, содержащей  $S$ , и потому она совпадает с  $N(S)$ .

ТЕОРЕМА 2 (О НОРМАЛЬНОМ ЗАМКЯНИИ ПОДМНОЖЕСТВА ГРУППЫ).  
 Пусть  $S$  — непустое подмножество группы  $G$ ,  $\emptyset \neq S \subseteq G$ . Тогда:

1) пересечение

$$N(S) = \bigcap_{S \subseteq N_i \triangleleft G} N_i$$

всех нормальных подгрупп  $N_i \triangleleft G$  таких, что  $S \subseteq N_i$ , является наименьшей нормальной подгруппой группы  $G$ , содержащей подмножество  $S$  (таким образом, нормальное замыкание  $N$  непустого подмножества  $S$  группы  $G$  существует);

2)  $N(S) = \langle S^G \rangle = \left\{ \prod_{k=1}^t g_k^{-1} s_k^{\pm 1} g_k \mid t \in \mathbb{N}, s_k \in S, g_k \in G \right\}$  (элементы нормального замыкания подмножества  $S$  в группе  $G$  — это в точности конечные произведения элементов вида  $g^{-1} s^{\pm 1} g$ ,  $s \in S$ ,  $g \in G$ ).

*Доказательство.* 1) Так как пересечение нормальных подгрупп — нормальная подгруппа, то  $N = \bigcap N_i \triangleleft G$ . Ясно, что  $S \subseteq N = \bigcap N_i$ , поскольку  $S \subseteq N_i$  для всех  $\{N_i \triangleleft G \mid S \subseteq N_i, i \in I\}$  (это множество содержит  $N_i = G$ , и поэтому не является пустым). Таким образом, нормальная подгруппа  $N$ ,  $S \subseteq N$ , сама принадлежит этому множеству, т. е.  $N = N_i$  для некоторого  $i \in I$ , и следовательно,  $N = \bigcap_{S \subseteq N_i \triangleleft G} N_i$ .

2) В силу 1) из  $S \subseteq N \triangleleft G$  следует, что

$$\langle S^G \rangle = \left\{ \prod_{k=1}^t g_k^{-1} s_k^{\pm 1} g_k \mid t \in \mathbb{N}, s_k \in S, g_k \in G \right\} \subseteq N.$$

Но ясно, что  $\langle S^G \rangle$  — нормальная подгруппа в  $G$ , содержащая  $S$ . Таким образом,  $N \subseteq \langle S^G \rangle$ . Итак,  $\langle S^G \rangle = N$ , и мы имеем общий вид произвольного элемента нормального замыкания  $N(S)$ .  $\square$

Наиболее часто рассматривается нормальное замыкание  $N(H) = \langle H^G \rangle$  подгруппы  $H$  группы  $G$ , т. е. тот случай, когда  $S = H$  — подгруппа в  $G$ .

## ГОМОМОРФИЗМЫ ГРУПП

Пусть  $G$  и  $G'$  — группы. Напомним, что отображение  $f: G \rightarrow G'$ , для которого  $f(ab) = f(a)f(b)$  для всех элементов  $a, b \in G$ , называется *гомоморфизмом*. Биективные гомоморфизмы называются *изоморфизмами*.

ПРИМЕР 1. Пусть  $G = \mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$  с операцией умножения,  $G' = (\mathbb{R}, +)$  с операцией сложения. Так как для отображения  $\ln: \mathbb{R}^+ \rightarrow \mathbb{R}$  имеем  $\ln(ab) = \ln(a) + \ln(b)$  для всех  $a, b \in \mathbb{R}^+$ , то  $\ln$  — гомоморфизм групп. Так как это — биекция, то  $\ln$  — изоморфизм.

ПРИМЕР 2. Если  $G = \mathbf{S}_n$  — группа подстановок и  $G' = \{1, -1\}$  — группа с операцией умножения, то отображение  $\varepsilon: \mathbf{S}_n \rightarrow \{1, -1\}$ , для которого  $\varepsilon(\sigma) = 1$ , если  $\sigma \in \mathbf{A}_n$ , т. е. если  $\sigma$  — четная подстановка, и  $\varepsilon(\sigma) = -1$  для  $\sigma \in \mathbf{S}_n \setminus \mathbf{A}_n$ , т. е. для нечетной подстановки  $\sigma$ , является гомоморфизмом групп, поскольку  $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$  для всех  $\sigma, \tau \in \mathbf{S}_n$ .

ПРИМЕР 3. Пусть  $G = \text{GL}_n(\mathbb{R})$ ,  $G' = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$  с операцией умножения. Так как  $|AB| = |A||B|$  для  $A, B \in \text{GL}_n(\mathbb{R})$ , то отображение  $A \mapsto |A|$  из  $\text{GL}_n(\mathbb{R})$  в  $\mathbb{R}^*$ , ставящее в соответствие матрице  $A$  ее определитель  $|A|$ , является гомоморфизмом групп.

УПРАЖНЕНИЕ 2. Найти все гомоморфизмы  $f: G \rightarrow G'$ , где  $G = \langle a \rangle$ ,  $O(a) = m$ ,  $G' = \langle b \rangle$ ,  $O(b) = n$  (в частности, для  $m = 12$ ,  $n = 15$ ).

Для гомоморфизмов  $f: G \rightarrow G'$  определим:

$$\text{Im } f = \{g' \in G' \mid g' = f(g) \text{ для } g \in G\}$$

(образ гомоморфизма  $f$ );

$$\ker f = \{g \in G \mid f(g) = e'\},$$

где  $e'$  — нейтральный элемент группы  $G'$  (*ядро* гомоморфизма  $f$ ).

УПРАЖНЕНИЕ 3. В рассмотренных выше примерах гомоморфизмов групп найти образ и ядро гомоморфизма.

УПРАЖНЕНИЕ 4. Доказать, что не существует сюръективного гомоморфизма  $(\mathbb{Q}, +) \rightarrow (\mathbb{Z}, +)$ .

ТЕОРЕМА 3 (СВОЙСТВА ГОМОМОРФИЗМА ГРУПП). Пусть  $G$  и  $G'$  — группы,  $e$  и  $e'$  соответственно — их нейтральные элементы,  $f: G \rightarrow G'$  — гомоморфизм групп. Тогда:

- 1)  $f(e) = e'$ ;
- 2)  $f(x^{-1}) = (f(x))^{-1}$  для всех  $x \in G$ ;
- 3)  $H' = \text{Im } f$  — подгруппа группы  $G'$ ;
- 4) если  $G = \langle a \rangle$  — циклическая группа, то  $\text{Im } f = \langle f(a) \rangle$  — также циклическая группа;
- 5) если  $O(a) < \infty$  для  $a \in G$ , то  $O(f(a))$  является делителем числа  $O(a)$  (если  $f$  — инъективный гомоморфизм, то  $O(f(a)) = O(a)$ );
- 6)  $f(g^{-1}hg) = (f(g))^{-1}f(h)f(g)$ ;
- 7)  $f([g, h]) = [f(g), f(h)]$ , и следовательно,  $f([G, G]) = [f(G), f(G)]$ ;
- 8)  $\ker f$  — нормальная подгруппа группы  $G$ ;
- 9) для  $x, y \in G$   $f(x) = f(y)$  тогда и только тогда, когда  $xy^{-1} \in \ker f$ ;
- 10)  $f$  — инъективное отображение тогда и только тогда, когда  $\ker f = \{e\}$ .

*Доказательство.* 1) Так как  $u = f(e) = f(e^2) = f(e)f(e) = u^2$ , то  $u = e'$ , т. е.  $f(e) = e'$ .

2) Так как  $f(x^{-1})f(x) = f(x^{-1}x) = f(e) = e'$  и  $f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e'$ , то  $f(x^{-1}) = (f(x))^{-1}$ .

3) Если  $h'_1 = f(g_1)$  и  $h'_2 = f(g_2)$  — элементы из  $\text{Im } f$ , где  $g_1, g_2 \in G$ , то

$$h'_1 h'_2 = f(g_1) f(g_2) = f(g_1 g_2) \in \text{Im } f.$$

Если  $h' = f(g) \in \text{Im } f$ ,  $g \in G$ , то

$$(h')^{-1} = (f(g))^{-1} = f(g^{-1}) \in \text{Im } f.$$

Итак,  $\text{Im } f$  — подгруппа группы  $G'$ .

4) Если  $G = \langle a \rangle$  и  $h' \in \text{Im } f$ ,  $h' = f(g)$ ,  $g \in G$ , то  $g = a^n$ ,  $n \in \mathbb{Z}$ , и поэтому

$$h' = f(g) = f(a^n) = (f(a))^n.$$

Итак,  $\text{Im } f = \langle f(a) \rangle$  — циклическая группа с образующим  $f(a)$ .

5) Пусть  $n = O(a)$ . Тогда  $a^n = e$ , и поэтому

$$(f(a))^n = f(a^n) = f(e) = e'.$$

Следовательно, число  $O(f(a))$  является делителем числа  $n = O(a)$ .

Если же  $f$  — инъективный гомоморфизм и  $m = O(f(a))$ , то

$$e' = (f(a))^m = f(a^m),$$

поэтому  $a^m = e$ , и следовательно,  $n = O(a)$  является делителем числа  $m$ . Таким образом,  $O(a) = n = m = O(f(a))$ .

6) и 7) следуют из 2).

8) Если  $h_1, h_2 \in H = \ker f$ , то  $f(h_1) = e'$ ,  $f(h_2) = e'$ . Поэтому  $f(h_1 h_2) = f(h_1) f(h_2) = e' \cdot e' = e'$ , т. е.  $h_1 h_2 \in \ker f$ .

Если  $h \in \ker f$ , то  $f(h) = e'$ , и поэтому  $f(h^{-1}) = (f(h))^{-1} = (e')^{-1} = e'$ , т. е.  $h^{-1} \in \ker f$ . Таким образом,  $\ker f$  — подгруппа группы  $G$ .

Если  $h \in H = \ker f$ , то  $f(h) = e'$ . Для любого элемента  $g \in G$  имеем

$$f(g^{-1} h g) = f(g^{-1}) f(h) f(g) = f(g)^{-1} e' f(g) = e'.$$

Таким образом,  $g^{-1}(\ker f)g \subseteq \ker f$  для всех элементов  $g \in G$ , т. е.  $\ker f$  — нормальная подгруппа группы  $G$ .

9)  $f(x) = f(y) \iff e' = f(x) f(y)^{-1} = f(x) f(y^{-1}) = f(x y^{-1}) \iff x y^{-1} \in \ker f$ .

10) а) Если  $\ker f = \{e\}$ , то из  $f(x) = f(y)$  следует, что  $x y^{-1} = e$ , т. е. что  $x = y$ , другими словами,  $f$  — инъективное отображение.

б) Если  $f$  — инъективное отображение, то, так как  $f(e) = e'$ , из  $f(x) = e'$  следует, что  $x = e$ , т. е.  $\ker f = \{e\}$ .  $\square$

**ТЕОРЕМА 4 (ТЕОРЕМА КЭЛИ).** Пусть  $G$  — группа,  $H$  — ее подгруппа,  $L$  — множество всех левых смежных классов группы  $G$  по подгруппе  $H$ ,  $\varphi: G \rightarrow S(L)$ ,  $S(L)$  — группа подстановок на множестве  $L$ ,  $\varphi(g)(xH) = gxH$  для  $x, g \in G$ . Тогда:

1)  $\varphi$  — гомоморфизм групп;

2)  $\ker \varphi = \bigcap_{x \in G} xHx^{-1}$ .



*Доказательство.* 1) Если  $x, g_1, g_2 \in G$ , то

$$\varphi(g_1g_2)(xH) = (g_1g_2)xH = g_1(g_2xH) = \varphi(g_1)(\varphi(g_2)(xH)),$$

поэтому  $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ .

2) Ясно, что:

$$g \in \ker \varphi \iff \{xH = gxH \ \forall xH\} \iff \{g \in xHx^{-1} \ \forall x \in G\}. \quad \square$$

**СЛЕДСТВИЕ 1.** При  $H = \{e\}$ ,  $L = G$ ,  $S(G)$  — группа подстановок на множестве  $G$ :

1)  $\varphi: G \rightarrow S(G)$ ,  $\varphi(g)(x) = gx$  для  $x, g \in G$ , является левым регулярным представлением группы  $G$ , оно осуществляет вложение группы  $G$  в группу  $S(G)$ , поскольку  $\ker \varphi = \bigcap_{x \in G} xex^{-1} = \{e\}$ ;

2) конечная группа  $G$  вкладывается в группу подстановок  $S_m$ , где  $m = |G|$ .

## ФАКТОР-ГРУППЫ, КАНОНИЧЕСКИЙ ГОМОМОРФИЗМ

Пусть  $G$  — группа,  $H$  — ее нормальная подгруппа,  $G/H = \{xH = Hx \mid x \in G\}$  — множество смежных классов по подгруппе  $H$ . Определим на множестве  $G/H$  операцию умножения, полагая  $xH \cdot yH = xyH$ .

Проверим *корректность* этого определения (т. е. что умножение смежных классов не зависит от выбора их представителей).

Действительно, пусть  $xH = x'H$ ,  $yH = y'H$ . Тогда  $x' = xh_1$ ,  $y' = yh_2$ , где  $h_1, h_2 \in H$ . Следовательно,  $x'y' = xh_1yh_2 = xyh'_1h_2$ , где  $h_1y = yh'_1$  (поскольку  $Hу = yH$ ) для  $h'_1 \in H$ . Так как  $h'_1h_2 \in H$ , то  $x'y' = xyh'_1h_2 \in xyH$ , и поэтому  $x'y'H = xyH$ .

Для любых  $x, y, z \in G$  имеем

$$(xHyH)zH = (xy)zH = x(yz)H = xH(yHzH),$$

т. е. операция умножения смежных классов ассоциативна.

Ясно, что для  $H = eH$  имеем

$$eHxH = exH = xH = xeH = xHeH$$

для всех  $xH \in G/H$ , т. е.  $H = eH$  — нейтральный элемент.

Для всякого  $xH \in G/H$  из

$$\begin{aligned}(xH)(x^{-1}H) &= xx^{-1}H = eH = H, \\ (x^{-1}H)(xH) &= x^{-1}xH = eH = H\end{aligned}$$

получаем, что  $(xH)^{-1} = x^{-1}H$ , т. е. у каждого смежного класса  $xH$  имеется обратный элемент  $(xH)^{-1} = x^{-1}H$ .

Таким образом, мы доказали первое утверждение следующей теоремы.

**ТЕОРЕМА 5.** *Если  $H \triangleleft G$ , то:*

1) *множество смежных классов  $G/H = \{xH = Hx \mid x \in G\}$  группы  $G$  по ее нормальной подгруппе  $H \triangleleft G$  с операцией  $xH \cdot yH = xyH$  является группой (называемой фактор-группой группы  $G$  по нормальной подгруппе  $H$ );*

2) *отображение  $\pi = \pi_H: G \rightarrow G/H$ , для которого  $\pi(x) = xH$ ,  $x \in G$ , является сюръективным гомоморфизмом (называемым каноническим гомоморфизмом);*

3)  $\ker \pi_H = H$ ;

4) *если  $|G| < \infty$ , то  $|G/H| = \frac{|G|}{|H|} = (G : H)$ .*

*Доказательство.* Осталось проверить 2), 3) и 4). Действительно, для  $a, b \in G$  имеем

$$\pi(ab) = abH = aH \cdot bH = \pi(a)\pi(b),$$

т. е.  $\pi = \pi_H$  — гомоморфизм.

Если  $g \in G$ , то  $gH = \pi(g)$ , т. е.  $\pi$  — сюръекция.

Если  $a \in G$ , то  $a \in \ker \pi_H$  тогда и только тогда, когда  $\pi(a) = aH = H$ .

Но это равносильно тому, что  $a \in H$ . Итак,  $\ker \pi_H = H$ .

4) следует из теоремы Лагранжа. □

СЛЕДСТВИЕ 2. *Нормальные подгруппы  $H$  группы  $G$  и только они являются ядрами гомоморфизмов  $f: G \rightarrow G'$  из группы  $G$  во все группы  $G'$ .*

## ПРИМЕРЫ ФАКТОР-ГРУПП

1) Пусть  $H = \{e\} \triangleleft G$ . Тогда  $x\{e\} = x$  для всех  $x \in G$ , т. е. все смежные классы по единичной подгруппе — это в точности одноэлементные подмножества, т. е. элементы группы  $G$ , при этом

$$x\{e\} \cdot y\{e\} = xy\{e\} = xy.$$

Таким образом, биекция  $x\{e\} \mapsto x$ ,  $G/\{e\} \rightarrow G$  является изоморфизмом групп.

2) Пусть  $H = G \triangleleft G$ . Тогда имеем один смежный класс  $\bar{e} = eG = G$ . Итак,  $G/G = \{\bar{e}\}$ ,  $|G/G| = 1$ .

3) Группа  $\mathbb{Z}_n$  вычетов по модулю  $n$  как фактор-группа группы  $(\mathbb{Z}, +)$  по подгруппе  $n\mathbb{Z}$ . Пусть  $G = \mathbb{Z}$  — группа целых чисел с операцией сложения,  $n$  — натуральное число и  $H = n\mathbb{Z} = \{nq \mid q \in \mathbb{Z}\}$  — подгруппа целых чисел, делящихся на  $n$ . Для  $k \in \mathbb{Z}$  рассмотрим смежный класс

$$C_k = k + n\mathbb{Z} = \{k + nq \mid q \in \mathbb{Z}\}.$$

Ясно, что  $C_k = C_l$  для  $l \in \mathbb{Z}$  тогда и только тогда, когда  $k - l = nq$ . Так как  $k = nq + r$ , где  $q \in \mathbb{Z}$ ,  $0 \leq r < n$ , то  $C_k = C_r$ . Таким образом, множество всех различных смежных классов  $\mathbb{Z}_n = G/H = \mathbb{Z}/n\mathbb{Z} = \{C_0, C_1, \dots, C_{n-1}\}$  находится в биективном соответствии с остатками  $\{0, 1, 2, \dots, n-1\}$  при делении на число  $n$ . Если  $k, l \in \mathbb{Z}$  и  $k + l = nq + r$ , то

$$C_k + C_l = (k + n\mathbb{Z}) + (l + n\mathbb{Z}) = (k + l) + n\mathbb{Z} = r + n\mathbb{Z} = C_r.$$

Таким образом, операция сложения фактор-группы  $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$  в точности соответствует операции сложения остатков при делении на  $n$  по

модулю числа  $n$  (т. е. сначала надо сложить остатки как целые числа, а затем от суммы взять остаток при ее делении на  $n$ ). Таким образом,  $\mathbb{Z}_n$  — группа.

4) В фактор-группе  $\mathbb{Q}/\mathbb{Z}$  любой элемент имеет конечный порядок; для любого натурального числа  $n$  существует единственная подгруппа группы  $\mathbb{Q}/\mathbb{Z}$  порядка  $n$ .

5) Фактор-группа  $\mathbb{R}/\mathbb{Z}$  имеет естественную интерпретацию как группа  $T = \{z \in \mathbb{C} \mid |z| = 1\}$  единичной окружности (или поворотов плоскости вокруг начала координат против часовой стрелки на угол  $\varphi$ , что равносильно умножению на комплексное число  $\cos \varphi + i \sin \varphi$ ), а именно биекция

$$f: \mathbb{R}/\mathbb{Z} \rightarrow T, \quad f(r + \mathbb{Z}) = \cos 2\pi r + i \sin 2\pi r,$$

осуществляет изоморфизм групп  $\mathbb{R}/\mathbb{Z}$  и  $T$ .

## ТЕОРЕМЫ О ГОМОМОРФИЗМАХ

**ТЕОРЕМА 6 (О ГОМОМОРФИЗМЕ ДЛЯ ГРУПП).** Пусть  $f: G \rightarrow G'$  — сюръективный гомоморфизм (т. е. гомоморфизм из группы  $G$  на группу  $G'$ ). Тогда существует изоморфизм

$$\psi: G/\ker f \rightarrow G'$$

такой, что  $f = \psi\pi$ , где  $\pi: G \rightarrow G/\ker f$  — 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  $\psi: G/\ker f \rightarrow G'$ .* 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  $\psi$  — 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.  $\psi$  — 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.  $\psi$  — сюръекция.

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

$$\begin{aligned} \psi(x \ker f \cdot y \ker f) &= \psi(xy \ker f) = f(xy) = \\ &= f(x)f(y) = \psi(x \ker f)\psi(y \ker f). \end{aligned}$$

Итак, мы показали, что  $\psi: G/\ker f \rightarrow G'$  — изоморфизм.

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

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

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

ПРИМЕР 4. Пусть  $G = (\mathbb{C}^*, \cdot)$ ,  $H = (\mathbb{R}^*, \cdot) \subset G$ .

Рассмотрим сюръективный гомоморфизм

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

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

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

ТЕОРЕМА 7 (ВТОРАЯ ТЕОРЕМА О ГОМОМОРФИЗМЕ). Пусть  $H$  — подгруппа группы  $G$ ,  $K$  — нормальная подгруппа группы  $G$  ( $HK$  — подгруппа группы  $G$ ). Тогда:

- 1)  $H \cap K \triangleleft H$  и  $K \triangleleft HK$ ;
- 2)  $HK/K \cong H/H \cap K$ .

*Доказательство.* Нас интересуют четыре подгруппы:

$$\begin{array}{ccc} & HK & \\ K & \triangleleft & \supseteq \\ & \supseteq & \triangleleft \\ & H \cap K & \end{array} H.$$

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

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

т. е.  $K \triangleleft HK$ .

2) Рассмотрим канонический эпиморфизм

$$\pi_K: G \rightarrow G/K$$

и его ограничение на  $H$

$$\pi_K|_H: H \rightarrow \pi_K(H) \subseteq G/K.$$

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,

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

В силу первой теоремы о гомоморфизмах (ее следствия)

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

**УПРАЖНЕНИЕ 5. 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

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

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

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

( $dl = mn$ ). □

3) Пусть  $G$  — конечная группа,  $H \triangleleft G$ ,  $(|H|, |G/H|) = 1$ . 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,  $K = H$ . □

**ТЕОРЕМА 8 (ТРЕТЬЯ ТЕОРЕМА О ГОМОМОРФИЗМАХ).** Пусть  $G \xrightarrow{f} G'$  — сюръективный гомоморфизм,  $K = \ker f \triangleleft G$  (например, если  $K \triangleleft G$ , то  $f = \pi_K: G \rightarrow G/K$ ),  $H' \subseteq G'$  — 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

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

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

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

*Доказательство.* 1) Ясно, что в нашем случае  $f(f^{-1}(H')) = H'$ . Пусть теперь  $H$  — подгруппа группы  $G$  и  $H \supseteq K$ . Тогда  $f^{-1}(f(H)) \supseteq H$ . 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,  $f^{-1}(f(H)) = H$ .

2) Если  $H \triangleleft G$ ,  $H \supseteq K$ , 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.  $f(H) \triangleleft G'$ .

Если  $H' \triangleleft G'$ ,  $g \in G$ ,  $x \in H = f^{-1}(H')$ , 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.  $f^{-1}(H') \triangleleft G$ .

Рассмотрим теперь сюръективный гомоморфизм

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

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  $\psi$

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

В ситуации  $G \triangleleft H \triangleleft K$  и  $f = \pi_K: G \rightarrow G' = G/K$ ,  $H' = f(H) = H/K \triangleleft G'/K$ , имеем по доказанному  $G/H \cong G'/H' = (G/K)/(H/K)$ .  $\square$