

# ЛЕКЦИЯ 6

## АВТОМОРФИЗМЫ ГРУПП

## ТОЧНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ

## ПЕРИОДИЧЕСКАЯ ЧАСТЬ

## АВТОМОРФИЗМЫ ГРУПП

Напомним, что *автоморфизмом* группы  $G$  называется биекция  $f: G \rightarrow G$ , являющаяся гомоморфизмом. Через  $\text{Aut}(G)$  обозначим множество всех автоморфизмов группы  $G$ .

**Лемма 1.** *Если  $G$  — группа, то  $\text{Aut}(G)$  — группа, являющаяся подгруппой группы подстановок  $\mathbf{S}(G)$ ,  $\text{Aut}(G) \subseteq \mathbf{S}(G)$ .*

*Доказательство.* Так как произведение автоморфизмов — автоморфизм (из свойств гомоморфизмов и изоморфизмов), то операция произведения в группе подстановок  $\mathbf{S}(G)$  на множестве  $G$  не выводит нас из  $\text{Aut}(G)$ .

Ассоциативность этой операции на  $\text{Aut}(G)$  является следствием ассоциативности операции умножения в  $\mathbf{S}(G)$ . Ясно, что тождественное отображение  $1_G$  является автоморфизмом и нейтральным элементом в  $\text{Aut}(G)$ . Если  $f \in \text{Aut}(G)$ , то  $f^{-1}$  также автоморфизм (из свойств гомоморфизмов и изоморфизмов). Итак,  $\text{Aut}(G)$  — группа, являющаяся подгруппой группы подстановок  $\mathbf{S}(G)$  на множестве  $G$ .  $\square$

**ПРИМЕР 1 (АВТОМОРФИЗМОВ ГРУПП).** 1) Тождественное отображение  $1_G$  является автоморфизмом любой группы  $G$ .

2) Если  $(A, +)$  — абелева группа, то отображение  $\alpha: A \rightarrow A$ , где  $\alpha(a) = -a$  для  $a \in A$ , является автоморфизмом. Действительно,  $\alpha$  — биекция, при этом

$$\alpha(x + y) = -(x + y) = -x - y = \alpha(x) + \alpha(y),$$

т. е.  $\alpha$  — гомоморфизм. Итак,  $\alpha$  — автоморфизм.

**Лемма 2.**  $\alpha \in \text{Aut}(G) \implies O(\alpha(g)) = O(g) \forall g \in G$ .

**Теорема 1.** Пусть  $G = G(a)$  — циклическая группа с образующим элементом  $a$ . Тогда:

1) если  $|G| = O(a) = \infty$  (т. е. если  $G$  — бесконечная циклическая группа,  $G \cong (\mathbb{Z}, +)$ ), то  $\text{Aut}((\mathbb{Z}, +)) \cong \mathbb{Z}_2$ ,  $|\text{Aut}(G)| = 2$ ;

2) если  $|G| = O(a) = n < \infty$ ,  $G \cong \mathbb{Z}_n$ , то  $\text{Aut}((\mathbb{Z}_n, +)) \cong \mathbf{U}(\mathbb{Z}_n)$ ,  $|\text{Aut}((\mathbb{Z}_m, +))| = \varphi(m)$ , где  $\varphi(m)$  — функция Эйлера.

*Доказательство.* Пусть  $G = (a)$  — циклическая группа.

Случай 1:  $G = (a)$ ,  $O(a) = \infty$ ,  $G \cong (\mathbb{Z}, +)$ , — бесконечная циклическая группа. Если  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  — автоморфизм группы  $(\mathbb{Z}, +)$ , то  $f$  полностью определяется целым числом  $n = f(1) \in \mathbb{Z}$ , поскольку

$$f(m) = f(m \cdot 1) = mf(1) = mn$$

для всех  $m \in \mathbb{Z}$ . Так как  $f$  — сюръекция, то  $1 = f(t)$  для некоторого  $t \in \mathbb{Z}$ , поэтому

$$1 = f(t) = f(t \cdot 1) = tf(1) = tn.$$

Таким образом,  $n = \pm 1$ . Итак, либо  $f = 1_{\mathbb{Z}}$  ( $f(1) = 1$ ), либо  $f(m) = -m$  для всех  $m \in \mathbb{Z}$  ( $f(1) = -1$ ). Следовательно,  $|\text{Aut}(\mathbb{Z})| = 2$ , т. е.  $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$ .

Случай 2: пусть  $G = (a)$ ,  $n = |G| = O(a) < \infty$ ,  $f: G \rightarrow G$  — автоморфизм.

а) Ясно, что  $f$  полностью определяется элементом  $f(a) \in G$ , поскольку  $f(a^k) = f(a)^k$  для всех  $k \in \mathbb{Z}$ . Так как  $f$  — изоморфизм, то  $O(f(a)) = O(a) = n$ , т. е.  $f(a)$  — образующий циклической группы  $G = (a)$ , и поэтому  $f(a) = a^i$ , где  $1 \leq i < n$ ,  $(i, n) = 1$ .

б) Если же  $i \in \mathbb{Z}$ ,  $1 \leq i < n$ ,  $(i, n) = 1$ , то отображение  $f: G \rightarrow G$ ,  $f(g) = g^i$  для всех  $g \in G$ , является гомоморфизмом, поскольку  $G = (a)$  — абелева группа:

$$f(g_1 g_2) = (g_1 g_2)^i = g_1^i g_2^i = f(g_1) f(g_2)$$

для всех  $g_1, g_2 \in G$ .

Так как  $f(a) = a^i$  и  $(i, n) = 1$ , то

$$O(f(a)) = O(a^i) = \frac{n}{(i, n)} = n,$$

поэтому  $f(a)$  является образующим группы  $G = (a)$ , и следовательно,  $\text{Im } f = G$ , т. е.  $f: G \rightarrow G$  — сюръективное отображение. Но  $G$  — конечное множество, поэтому  $f$  — биекция, т. е.  $f \in \text{Aut}(G)$ .

в) Итак, мы описали строение всех автоморфизмов  $f \in \text{Aut}(G)$ , где  $G = (a)$ ,  $|G| = O(a) = n < \infty$ ,  $G \cong \mathbb{Z}_n$ , доказав, что  $\text{Aut}(\mathbb{Z}_n) \cong \mathbf{U}(\mathbb{Z}_n, \cdot)$ . Из этого описания следует, что  $|\text{Aut}(G)| = \varphi(n)$  для  $G = (a)$ ,  $|G| = O(a) = n < \infty$ , где  $\varphi(n)$  — функция Эйлера.  $\square$

УПРАЖНЕНИЕ 1. Найдите все такие группы  $G$ , что  $\text{Aut}(G)$  — тривиальная группа.

## ВНУТРЕННИЕ АВТОМОРФИЗМЫ

ОПРЕДЕЛЕНИЕ 1. Пусть  $G$  — группа,  $g, x \in G$ . Элемент  $gxg^{-1} \in G$  называется элементом, сопряженным с элементом  $x$  с помощью элемента  $g$  (иногда используется обозначение  $gxg^{-1} = x^g$ ).

**Лемма 3.** Пусть  $G$  — группа. Для каждого элемента  $g \in G$  отображение

$$\tau(g): G \rightarrow G, \quad \tau(g)(x) = gxg^{-1} \quad \text{для } x \in G,$$

является автоморфизмом группы  $G$  (называемым внутренним автоморфизмом группы  $G$ , индуцированным элементом  $g \in G$ ).

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

$$\tau(g)(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = (\tau(g)x)(\tau(g)y),$$

т. е.  $\tau(g): G \rightarrow G$  — гомоморфизм групп.

2) Так как  $\tau(g^{-1}) = \tau(g)^{-1}$ , то  $\tau(g)$  — биекция, и поэтому  $\tau(g)$  — автоморфизм группы  $G$ .  $\square$

Соберем вместе свойства отображения  $\tau: G \rightarrow \text{Aut}(G)$ .

**Теорема 2** (свойства внутренних автоморфизмов). Пусть  $G$  — группа. Тогда:

1) отображение  $\tau: G \rightarrow \text{Aut}(G)$ ,  $\tau(g)(x) = gxg^{-1}$ ,  $g \in G$ ,  $x \in G$ , является гомоморфизмом групп (называемым гомоморфизмом сопряжения);

2) образ гомоморфизма  $\tau: G \rightarrow \text{Aut}(G)$ , т. е. совокупность  $\text{Inn}(G) = \{\tau(g) \in \text{Aut}(G) \mid g \in G\} = \text{Im } \tau$  всех внутренних автоморфизмов  $\tau(g)$ ,  $g \in G$ , является нормальной подгруппой группы автоморфизмов  $\text{Aut}(G)$  (группа  $\text{Inn}(G)$  называется группой внутренних автоморфизмов группы  $G$ );

3)  $\ker(\tau) = \mathbf{Z}(G)$ , т. е. ядро  $\ker(\tau)$  гомоморфизма  $\tau$  совпадает с центром  $\mathbf{Z}(G)$  группы  $G$ ;

4)  $\text{Inn}(G) \cong G/\mathbf{Z}(G)$ , группа  $\text{Inn}(G)$  внутренних автоморфизмов изоморфна фактор-группе группы  $G$  по ее центру  $\mathbf{Z}(G)$ .

*Доказательство.* 1) Если  $g, h \in G$ , то

$$\tau(gh)(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = \tau(g)(\tau(h)(x))$$

для всех  $x \in G$ . Итак,  $\tau(gh) = \tau(g)\tau(h)$  для всех  $g, h \in G$ , т. е.  $\tau: G \rightarrow \text{Aut}(G)$  — гомоморфизм групп.

2) Совокупность  $\text{Inn}(G) = \{\tau(g) \in \text{Aut}(G) \mid g \in G\}$  всех внутренних автоморфизмов  $\tau(g)$ ,  $g \in G$ , в группе  $\text{Aut}(G)$  как образ гомоморфизма  $\tau$  является подгруппой группы  $\text{Aut}(G)$ .

Если  $\alpha \in \text{Aut}(G)$  и  $g \in G$ ,  $x \in G$ , то

$$\begin{aligned} \tau(\alpha(g))(x) &= \alpha(g)x\alpha(g)^{-1} = \alpha(g)x\alpha(g^{-1}) = \\ &= \alpha(g\alpha^{-1}(x)g^{-1}) = \alpha(\tau(g)(\alpha^{-1}(x))) = (\alpha\tau(g)\alpha^{-1})(x), \end{aligned}$$

поэтому

$$\alpha\tau(g)\alpha^{-1} = \tau(\alpha(g)) \in \text{Inn}(G),$$

следовательно,

$$\text{Inn}(G) \triangleleft \text{Aut}(G).$$

3) Элемент  $g \in G$  принадлежит ядру  $\ker \tau$  гомоморфизма  $\tau$  тогда и только тогда, когда  $\tau(g)(x) = x$  для всех  $x \in G$ , т. е.  $g x g^{-1} = x$ , или  $g x = x g$ , но это означает, что  $g \in \mathbf{Z}(G)$ . Итак,  $\ker \tau = \mathbf{Z}(G)$ .

4) В силу теоремы о гомоморфизме для сюръективного гомоморфизма  $\tau: G \rightarrow \text{Inn}(G)$  имеем

$$\text{Inn}(G) = \text{Im } \tau \cong G / \ker \tau = G / \mathbf{Z}(G).$$

□

## ПРИМЕРЫ АБЕЛЕВЫХ ГРУПП

1) *Циклические группы*  $G = \langle a \rangle$ , поскольку  $a^m a^n = a^{m+n} = a^n a^m$  для всех  $m, n \in \mathbb{Z}$ .

2) Прямые суммы  $\bigoplus_{i \in I} A_i$  и прямые произведения  $\prod_{i \in I} A_i$  абелевых групп  $A_i, i \in I$ , являются абелевыми группами.

3) *Аддитивная группа рациональных чисел*  $\mathbb{Q} = (\mathbb{Q}, +)$  (эта группа без кручения, она является делимой (для любого  $a \in \mathbb{Q}$  и любого  $n \in \mathbb{Z}$  уравнение  $nx = a$  разрешимо в  $\mathbb{Z}$ ) и по этой причине не является прямой суммой циклических групп).

4) *Квазициклическая группа*  $\mathbb{Z}(p^\infty)$  — группа по умножению всех корней степени  $p^n$ , где  $p$  — фиксированное простое число,  $n \in \mathbb{N} \cup \{0\}$ .

## ТОЧНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ

Последовательность абелевых групп и гомоморфизмов

$$\dots \xrightarrow{f_{i-1}} A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} A_{i+2} \rightarrow \dots$$

называется *точной последовательностью*, если

$$\operatorname{Im} f_i = \ker f_{i+1} \quad \forall i \in \mathbb{N},$$

и называется *комплексом* абелевых групп, если

$$f_{i+1}f_i = 0 \quad \forall i \in \mathbb{N}$$

(это равносильно тому, что  $\operatorname{Im} f_i \subseteq \ker f_{i+1}$ , и поэтому в этом случае можно рассмотреть фактор-группу  $D_{i+1} = \ker f_{i+1} / \operatorname{Im} f_i$ , называемую  $(i + 1)$ -й группой гомологий комплекса).

Следующие примеры точных последовательностей наиболее употребительны в нашем курсе:

1) точность последовательности

$$0 \rightarrow A \xrightarrow{i} B$$

означает, что  $\ker i = 0$ , т. е.  $i$  — инъективный гомоморфизм (моморфизм);

2) точность последовательности

$$B \xrightarrow{\pi} C \rightarrow 0$$

означает, что  $\operatorname{Im} \pi = C$ , т. е.  $\pi$  — сюръективный гомоморфизм;

3) точность последовательности

$$0 \rightarrow A \xrightarrow{i} B \xrightarrow{\pi} C \rightarrow 0$$

означает, что  $\ker i = 0$ ,  $\operatorname{Im} i = \ker \pi$ ,  $\operatorname{Im} \pi = C$ , т. е. что  $A \cong \operatorname{Im} i$ ,  $B/\operatorname{Im} i = B/\ker \pi \cong C$  (в частности, для сюръективного гомоморфизма  $f: A \rightarrow B$  имеем короткую точную последовательность

$$0 \rightarrow \ker f \subseteq A \xrightarrow{f} \operatorname{Im} f = B \rightarrow 0).$$

**Лемма 4** (о ретракте абелевых групп). Пусть  $G$  и  $G'$  — абелевы группы.

1) Если  $f: G \rightarrow G'$ ,  $h: G' \rightarrow G$  — гомоморфизмы и  $fh = 1_{G'}$  (пара  $f, h$  — ретракт), то:

- а)  $\ker h = 0$ ;
- б)  $\operatorname{Im} f = G'$ ;
- в)  $\operatorname{Im} h \oplus \ker f = G$ .

2) Если  $f: G \rightarrow G'$  — гомоморфизм,

$$\operatorname{Im} f = G' \text{ и } A \oplus \ker f = G$$

для некоторой подгруппы  $A \subseteq G$ , то существует гомоморфизм  $h: G' \rightarrow G$ , для которого  $fh = 1_{G'}$ .

3) Если  $h: G' \rightarrow G$  — гомоморфизм,

$$\ker h = 0 \text{ и } \operatorname{Im} h \oplus B = G$$

для некоторой подгруппы  $B \subseteq G$ , то существует гомоморфизм  $f: G \rightarrow G'$ , для которого  $fh = 1_{G'}$ .

*Доказательство.*

1а) Если  $y \in \ker h \subseteq G'$ , то  $h(y) = 0$ , и поэтому

$$y = 1_{G'}(y) = (fh)(y) = f(h(y)) = f(0) = 0.$$

Итак,  $\ker h = 0$ .

1б) Если  $y \in G'$ , то

$$y = 1_{G'}(y) = (fh)(y) = f(h(y)) \in \operatorname{Im} f.$$

Итак,  $\operatorname{Im} f = G'$ .

1в) Если  $x \in G$ , то  $x = h(f(x)) + (x - (hf)(x))$ , при этом, поскольку  $fh = 1_{G'}$ ,

$$f(x - (hf)(x)) = f(x) - (fhf)(x) = f(x) - f(x) = 0,$$

поэтому  $x - (hf)(x) \in \ker f$ ,  $h(f(x)) \in \operatorname{Im} h$ . Таким образом,  $G = \operatorname{Im} h + \ker f$ .

Если  $z \in \operatorname{Im} h \cap \ker f$ , то  $z = h(y)$  для  $y \in G'$  и  $f(z) = 0$ , поэтому

$$y = 1_{G'}(y) = (fh)(y) = f(h(y)) = f(z) = 0.$$

Таким образом,  $\operatorname{Im} h \cap \ker f = 0$ .

Итак,  $G = \operatorname{Im} h \oplus \ker f$ .

2) Так как для  $f|_A: A \rightarrow G'$  имеем

$$\begin{aligned} f|_A(A) &= f(A \oplus \ker f) = f(G) = G', \\ \ker(f|_A) &= \ker f \cap A = 0, \end{aligned}$$

то  $f|_A: A \rightarrow G'$  — изоморфизм.

Положим

$$h = (f|_A)^{-1}: G' \rightarrow A \subseteq G.$$

Тогда

$$fh = f(f|_A)^{-1} = 1_{G'}.$$

3) Гомоморфизм  $h: G' \rightarrow \text{Im } h$  является изоморфизмом, поскольку  $\ker h = 0$ . Рассмотрим изоморфизм  $h^{-1}: \text{Im } h \rightarrow G'$ . Пусть  $\pi: G = \text{Im } h \oplus B \rightarrow \text{Im } h$  — проекция на первое прямое слагаемое. Рассмотрим гомоморфизм

$$f = h^{-1}\pi: G = \text{Im } h \oplus B \xrightarrow{\pi} \text{Im } h \xrightarrow{h} G'.$$

Тогда для  $g' \in G'$  имеем

$$(fh)(g') = f(h(g')) = h^{-1}(\pi(h(g'))) = h^{-1}(h(g')) = g'.$$

Таким образом,  $fh = 1_{G'}$ . □

**Теорема 3** (условия расщепления короткой точной последовательности абелевых групп). Пусть

$$0 \rightarrow A \xrightarrow{i} B \xrightarrow{\pi} C \rightarrow 0$$

— короткая точная последовательность абелевых групп ( $\ker i = 0$ ,  $\operatorname{Im} i = \ker \pi$ ,  $\operatorname{Im} \pi = C$ ). Тогда эквивалентны следующие условия:

- 1) существует гомоморфизм  $j: B \rightarrow A$ , для которого  $ji = 1_A$  (расщепляемость последовательности слева);
- 2) существует гомоморфизм  $\rho: C \rightarrow B$ , для которого  $\pi\rho = 1_C$  (расщепляемость последовательности справа).

*Доказательство.* а) Пусть выполнено условие 1). Тогда в силу леммы о ретракте (п. 1с) для ретракта

$$i: A \rightarrow B, \quad j: B \rightarrow A, \quad ji = 1_A,$$

имеем:

$$\operatorname{Im} i \oplus \ker j = B.$$

Так как  $\operatorname{Im} i = \ker \pi$ , то

$$\ker \pi \oplus \ker j = B.$$

Это позволяет применить к гомоморфизму  $\pi: B \rightarrow C$  ( $\operatorname{Im} \pi = C$ ,  $\ker j \oplus \ker \pi = B$ ) лемму о ретракте. Тогда существует гомоморфизм  $\rho: C \rightarrow B$ , для которого  $\pi\rho = 1_C$ . Таким образом, из 1) следует 2).

б) Пусть выполнено условие 2). Применяя к ретракту

$$\pi : B \rightarrow C, \quad \rho : C \rightarrow B, \quad \pi\rho = 1_C,$$

лемму о ретракте (п. 1с), имеем  $\text{Im } \rho \oplus \ker \pi = B$ .

Так как  $\text{Im } i = \ker \pi$ , то  $\text{Im } i \oplus \text{Im } \rho = B$ .

Это позволяет применить к гомоморфизму  $i: A \rightarrow B$  ( $\ker i = 0$ ,  $\text{Im } i \oplus \text{Im } \rho = B$ ) лемму о ретракте (п. 3).

Тогда существует гомоморфизм  $j: B \rightarrow A$ , для которого  $ji = 1_A$ .

Таким образом, из 2) следует 1). □

## ПЕРИОДИЧЕСКАЯ ЧАСТЬ АБЕЛЕВОЙ ГРУППЫ

Как мы видели, совокупность

$$\mathbf{T}(G) = \{g \in G \mid O(g) < \infty\}$$

элементов некоммутативной группы может не быть подгруппой (например,  $\mathbf{T}(\mathrm{GL}_2(\mathbb{Z}))$ ). Для абелевых групп  $A$  элементы конечного порядка образуют подгруппу, называемую *периодической частью* группы  $A$ . Периодическая часть  $\mathbf{T}(A)$  абелевой группы — важный инвариант группы  $A$ .

Если  $\mathbf{T}(A) = 0$  (в группе  $A$  все ненулевые элементы имеют бесконечный порядок), то будем говорить, что группа  $A$  — без кручения.

**Теорема 4.** Пусть  $A$  — абелева группа,

$$\mathbf{T}(A) = \{a \in A \mid O(a) < \infty\} —$$

ее периодическая часть. Тогда:

- 1)  $\mathbf{T}(A)$  — периодическая подгруппа группы  $A$ ;
- 2)  $\mathbf{T}(A/\mathbf{T}(A)) = 0$  (другими словами,  $A/\mathbf{T}(A)$  — группа без кручения).

*Доказательство.* 1) Если  $a, b \in \mathbf{T}(A)$ ,  $ra = 0 = sb$ ,  $r > 0$ ,  $s > 0$ ,  $r, s \in \mathbb{N}$ , то

$$rs(a + b) = s(ra) + r(sb) = 0 + 0 = 0, \quad r, s > 0,$$

$$r(-a) = -ra = 0, \quad r > 0,$$

и поэтому  $a + b \in \mathbf{T}(A)$ ,  $-a \in \mathbf{T}(A)$ . Таким образом,  $\mathbf{T}(A)$  — подгруппа группы  $A$ . Конечно,  $\mathbf{T}(A)$  — периодическая группа.

2) Если  $a + \mathbf{T}(A) \in \mathbf{T}(A/\mathbf{T}(A))$ , то

$$s(a + \mathbf{T}(A)) = sa + \mathbf{T}(A) = \bar{0} = \mathbf{T}(A), \quad s > 0,$$

поэтому  $sa \in \mathbf{T}(A)$ . Следовательно,

$$r(sa) = (rs)a = 0, \quad r > 0.$$

Так как  $rs > 0$ , то  $a \in \mathbf{T}(A)$ , и поэтому  $a + \mathbf{T}(A) = \mathbf{T}(A) = \bar{0}$ . Итак,  $\mathbf{T}(A/\mathbf{T}(A)) = \bar{0}$ .  $\square$

**ЗАМЕЧАНИЕ 1.** Эта теорема объясняет, почему структурная теория абелевых групп разбивается на три части:

*1-я часть* посвящена изучению периодических абелевых групп (когда  $\mathbf{T}(A) = A$ );

*2-я часть* заключается в изучении абелевых групп  $A$  без кручения (когда  $\mathbf{T}(A) = 0$ );

*3-я часть* анализирует в общем случае расширение

$$0 \rightarrow \mathbf{T}(A) \rightarrow A \rightarrow A/\mathbf{T}(A) \rightarrow 0$$

периодической группы  $A$  с помощью группы  $A/\mathbf{T}(A)$  без кручения.