ЛЕКЦИЯ 6

АВТОМОРФИЗМЫ ГРУПП

ВНУТРЕННИЕ АВТОМОРФИЗМЫ

ТОЧНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ АБЕЛЕВЫХ ГРУПП

АВТОМОРФИЗМЫ ГРУПП

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

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

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 $\mathrm{Aut}\,(G)$.

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

Пример 1 (автоморфизмов групп). 1) Тождественное отображение 1_G является автоморфизмом любой группы G.

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

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

т. е. α — гомоморфизм. Итак, α — автоморфизм.

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

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 $\operatorname{Aut}\big((\mathbb{Z}, +)\big) \cong \mathbb{Z}_2$, $|\operatorname{Aut}(G)| = 2$;*

2) *если $|G| = O(a) = n < \infty$, $G \cong \mathbb{Z}_n$, то $\operatorname{Aut}\big((\mathbb{Z}_n, +)\big) \cong \mathbf{U}(\mathbb{Z}_n)$, $\big|\operatorname{Aut}\big((\mathbb{Z}_m, +)\big)\big| = \varphi(m)$, 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 $f\colon \mathbb{Z} \to \mathbb{Z}$ — 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, $|\operatorname{Aut}(\mathbb{Z})| = 2$, т. е. $\operatorname{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

Случай 2: пусть $G = (a)$, $n = |G| = O(a) < \infty$, $f\colon G \to G$ — 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 $O\big(f(a)\big) = O(a) = n$, т. е. $f(a)$ — образующий циклической группы $G = (a)$, и поэтому $f(a) = a^i$, где $1 \leq i < m$, $(i, m) = 1$.

б) Если же $i \in \mathbb{Z}$, $1 \leq i < n$, $(i, n) = 1$, то отображение $f\colon G \to G$, $f(g) = g^i$ 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

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

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

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

Упражнение 1. Найдите все такие группы G, что $\operatorname{Aut}(G)$ — 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*

$$\tau(g)\colon G \to G, \quad \tau(g)(x) = gxg^{-1} \quad \textit{для} \quad x \in G,$$

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

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

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

т. е. $\tau(g)\colon G \to G$ — гомоморфизм групп.

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

Соберем вместе свойства отображения $\tau\colon G \to \operatorname{Aut}(G)$.

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

1) *отображение $\tau\colon G \to \operatorname{Aut}(G)$, $\tau(g)(x) = gxg^{-1}$, $g \in G$, $x \in G$, является гомоморфизмом групп (называемым гомоморфизмом сопряжения)*;

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

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

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

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

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

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

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

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

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

поэтому

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

следовательно,

$$\operatorname{Inn}(G) \lhd \operatorname{Aut}(G).$$

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

4) В силу теоремы о гомоморфизме для сюръективного гомоморфизма $\tau\colon G \to \operatorname{Inn}(G)$ имеем

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

□

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 $\bigoplus\limits_{i \in I} A_i$ и прямые произведения $\prod\limits_{i \in I} A_i$ 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

$$\ldots \xrightarrow{f_{i-1}} A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} A_{i+2} \to \ldots$$

называется *точной последовательностью*, если

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

и называется *комплексом* абелевых групп, если

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

(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

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

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

2) точность последовательности

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

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

3) точность последовательности

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

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 $f\colon A \to B$ имеем короткую точную последовательность

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

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

1) *Если $f\colon G \to G'$, $h\colon G' \to G$ — 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 $f\colon G \to G'$ — гомоморфизм,*

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

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

3) *Если $h\colon G' \to G$ — гомоморфизм,*

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

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

Доказательство.

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

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

Итак, $\ker h = 0$.

1б) Если $y \in G'$, то

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

Итак, $\operatorname{Im} f = G'$.

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

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

поэтому $x - (hf)(x) \in \ker f$, $h\big(f(x)\big) \in \operatorname{Im} h$. 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

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

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

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

2) Так как для $f|_A\colon A \to G'$ имеем

$$f|_A(A) = f(A \oplus \ker f) = f(G) = G',$$
$$\ker(f|_A) = \ker f \cap A = 0,$$

то $f|_A\colon A \to G'$ — изоморфизм.

Положим

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

Тогда

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

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

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

Тогда для $g' \in G'$ имеем

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

Таким образом, $fh = 1_{G'}$. □

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

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

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

1) *существует гомоморфизм* $j\colon B \to A$*, для которого* $ji = 1_A$ (*расщепляемость последовательности слева*);

2) *существует гомоморфизм* $\rho\colon C \to B$*, 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

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

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 $\pi\colon B \to C$ ($\operatorname{Im} \pi = C$, $\ker j \oplus \ker \pi = B$) лемму о ретракте. Тогда существует гомоморфизм $\rho\colon C \to B$, для которого $\pi\rho = 1_C$. Таким образом, из 1) следует 2).

б) Пусть выполнено условие 2). Применяя к ретракту

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

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

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

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

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

Таким образом, из 2) следует 1). □