ЛЕКЦИЯ 5

ОБРАЗУЮЩИЕ И ОПРЕДЕЛЯЮЩИЕ СООТНОШЕНИЯ

АВТОМОРФИЗМЫ ГРУПП

ВНУТРЕННИЕ АВТОМОРФИЗМЫ

ОБРАЗУЮЩИЕ И ОПРЕДЕЛЯЮЩИЕ СООТНОШЕНИЯ

Как можно было заметить из первых лекций, для групп с понятным устройством (например, для циклических) нет необходимости составлять таблицы умножения (таблицы Кэли). Условная запись

$$\mathbb{Z}_n = \langle c \mid c^n = e \rangle$$

дает всю необходимую информацию об абстрактной циклической группе $\mathbb{Z}_n$ порядка n; подразумевается, что $\mathbb{Z}_n = \{e, c, c^2, \ldots, c^{n-1}\}$, причем $c^s c^t = c^{s+t}$ при $s+t < n$ и $c^s c^t = c^{s+t-n}$ при $s+t \geqslant n$. С другой стороны, любая циклическая группа является с точностью до изоморфизма гомоморфным образом одной-единственной группы $(\mathbb{Z}, +)$.

Рассмотрим множество S, состоящее из объединения множеств

$$\{x_1, x_2, \ldots, x_n\} \cup \{x_1^{-1}, \ldots, x_n^{-1}\}.$$

Теперь рассмотрим множество всех слов в алфавите S (включая пустое слово e) с операцией конкатенации и будем считать, что два слова

$$x_{i_1}^{\varepsilon_1} \ldots x_{i_t}^{\varepsilon_t} \text{ и } x_{j_1}^{\mu_1} \ldots x_{j_s}^{\mu_s}, \text{ где } \varepsilon_1, \ldots, \varepsilon_t, \mu_1, \ldots, \mu_s = \pm 1,$$

эквивалентны, если из одного можно получить другое за конечное число преобразований из следующего списка:

(1) из слова можно вычеркнуть любое подслово вида $x_i x_i^{-1}$ или $x_i^{-1} x_i$, $i = 1, \ldots, n$;

(2) в слово в любом месте можно вставить подслово вида $x_i x_i^{-1}$ или $x_i^{-1} x_i$, $i = 1, \ldots, n$.

Множество всех слов с точностью до данной эквивалентности обозначим через F_n.

Покажем, что получилась группа.

1. Замкнутость F_n относительно операции конкатенации очевидна. Ассоциативность тоже очевидна.

2. Единичным элементом является пустое слово e, что также очевидно.

3. Обратным к слову $x_{i_1}^{\varepsilon 1} \dots x_{i_t}^{\varepsilon t}$ является слово $x_{i_t}^{-\varepsilon t} \dots x_{i_1}^{-\varepsilon t}$.

Построенную группу мы будем называть *свободной группой* (порожденной образующими $x_1, \dots, x_n$).

Заметим, что если имеется слово вида

$$x_{i_1}^{l_1} \dots x_{i_t}^{l_t},$$

где $l_1, \dots, l_t \in \mathbb{Z} \setminus \{0\}$ и $i_m \neq i_{m+1}$ при $m = 1, \dots, t-1$, то очевидно, что оно не может быть эквивалентно пустому слову при $t = 1$, а при $t > 1$ имеет по крайней мере две разных буквы внутри слова. Для того, чтобы сойтись к пустому слову, надо уменьшить количество разных букв в слове, но это невозможно, так как никакая из операций (1) или (2) этого не сделает.

Таким образом, любой элемент (то есть класс эквивалентных элементов) в F_n имеет единственного представителя, либо являющегося пустым словом, либо имеющего вид

$$x_{i_1}^{l_1} x_{i_2}^{l_2} \dots x_{i_t}^{l_t}, \quad l_1, \dots, l_t \in \mathbb{Z} \setminus \{0\},\ i_m \neq i_{m+1} \text{ при } m = 1, \dots, t-1.$$

Очевидно, что при данном n две свободных группы F_n и G_n изоморфны, достаточно построить взаимно-однозначное соответствие между образующими.

Предложение 1 (универсальное свойство свободной группы)**.** *Если F_n — свободная группа ранга n, а G — некоторая группа,*

порожденная n элементами $g_1, \ldots, g_n$, то существует и единственен сюръективный гомоморфизм $\Phi : F_n \to G$, для которого $\Phi(x_i) = g_i$ для всех $i = 1, \ldots, n$.

Доказательство. Рассмотрим образующие $x_1, \ldots, x_n$ группы F_n и построим гомоморфизм $\Phi : F_n \to G$, для которого произвольный элемент $x = x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \ldots x_{i_k}^{\varepsilon_k} \in F_n$ отображается в элемент

$$\Phi(x) = g_{i_1}^{\varepsilon_1} g_{i_2}^{\varepsilon_2} \ldots g_{i_k}^{\varepsilon_k} \in G.$$

Надо проверить, что такое отображение корректно, то есть если два слова в F_n лежат в одном классе эквивалентности, то их образы совпадут.

Действительно, пусть два слова x и x' лежат в одном классе эквивалентности, то есть от одного до другого можно дойти за конечное число преобразований вида (1) или (2). Ясно, что тогда без ограничения общности можно полагать, что из x получается x' за одно преобразование вида (1) или (2).

Пусть, например,

$$x = x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \ldots x_{i_k}^{\varepsilon_k},$$

а

$$x' = x_{i_1}^{\varepsilon_1} \ldots x_{i_j}^{\varepsilon_j} x_{i_0}^{\varepsilon_0} x_{i_0}^{-\varepsilon_0} x_{i_{j+1}}^{\varepsilon_{j+1}} \ldots x_{i_k}^{\varepsilon_k}.$$

Тогда

$$\Phi(x') = g_{i_1}^{\varepsilon_1} \ldots g_{i_j}^{\varepsilon_j} g_{i_0}^{\varepsilon_0} g_{i_0}^{-\varepsilon_0} g_{i_{j+1}}^{\varepsilon_{j+1}} \ldots g_{i_k}^{\varepsilon_k} = \\ = g_{i_1}^{\varepsilon_1} \ldots g_{i_j}^{\varepsilon_j} g_{i_{j+1}}^{\varepsilon_{j+1}} \ldots g_{i_k}^{\varepsilon_k} = \Phi(x),$$

что и требовалось.

Мы доказали, что отображение Φ корректно.

Также очевидно, что отображение Φ сюръективно (так как прообразом произвольного элемента $g = g_{i_1}^{s_1} g_{i_2}^{s_2} \ldots g_{i_k}^{s_k}$ является

элемент $x_{i_1}^{s_1} x_{i_2}^{s_2} \dots x_{i_k}^{s_k}$). Наконец, отображение Φ является гомоморфизмом просто по построению. $\square$

Таким образом, любая группа с n порождающими является гомоморфным образом свободной группы F_n, то есть

$$G \cong F_n / \ker \Phi.$$

Определение 1. Пусть F_n — свободная группа с n свободными образующими $x_1, \dots, x_n$, $S = \{w_i, i \in I\}$ — некоторое подмножество элементов $w_i(x_1, \dots, x_n) \in F_n$ и $K = \langle S^{F_n} \rangle$ — наименьшая нормальная подгруппа в F_n, содержащая S (пересечение всех нормальных подгрупп, содержащих S). Говорят, что группа G задана n образующими $a_1, \dots, a_n$ и соотношениями $w_i(a_1, \dots, a_n) = e$, $i \in I$, если существует эпиморфизм $\pi : F_n \to G$ с ядром K такой, что $\pi(x_k) = a_k$, $1 \leqslant k \leqslant n$.

При этом пишут

$$G = \langle a_1, \dots, a_n \mid w_i(a_1, \dots, a_n) = e,\ i \in I \rangle$$

и называют G *конечно определенной группой*, если $|I| < \infty$.

Сама группа F_n свободна от соотношений, чем и объясняется ее название. Одна и та же группа допускает много разных заданий образующими и соотношениями, хотя для конкретной группы G иногда не так легко указать хотя бы одно задание. Проблема еще в том, что не существует общего алгоритма, который бы для любой конечно определенной группы давал бы ответ о конечности группы, о равенстве двух ее слов и т. д.

Перейдем теперь к примерам как свободных групп, так и задания различных известным нам групп образующими и соотношениями.

Пример 1 (свободная группа ранга 1). Это очень просто: $F_1 \cong (\mathbb{Z}, +)$ — свободная абелева группа ранга 1, или, что то же самое, бесконечная циклическая группа.

Пример 2 (свободная группа ранга 2). Пусть $\mathbb{Z}[t]$ — кольцо многочленов от t с целыми коэффициентами. В специальной линейной группе $\mathrm{SL}_2(\mathbb{Z}[t])$ рассмотрим подгруппу F, порожденную матрицами

$$A = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \text{ и } B = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}.$$

Докажем, что F — свободная группа.

Индукция по k показывает, что элемент

$$W_k = A^{\alpha_1} B^{\beta_1} \dots A^{\alpha_k} B^{\beta_k}, \qquad \alpha_i, \beta_i \neq 0, \quad 1 \leqslant i \leqslant k,$$

имеет вид

$$W_k = \begin{pmatrix} 1 + \dots + \sigma_k t^{2k} & t(\dots + \sigma_{k-1}\alpha_k t^{2(k-1)}) \\ t(\dots + \alpha_1^{-1}\sigma_k t^{2(k-1)}) & 1 + \dots + \alpha_1^{-1}\sigma_{k-1}\alpha_k t^{2(k-1)} \end{pmatrix},$$

где $\sigma_k = \alpha_1\beta_1 \dots \alpha_k\beta_k$, а точками обозначены одночлены меньшей степени относительно t. Ясно, что $W_k \neq E$. Произвольный элемент группы F или записывается в виде $B^\beta A^\alpha \neq E$, либо в виде $W = B^\beta W_k A^\alpha$. Если $W = E$, то $W_k = B^{-\beta} A^{-\alpha}$, что, однако невозможно.

Пример 3 (группа диэдра). Рассмотрим группу

$$G = \langle a, b \mid a^n = b^2 = abab = e \rangle$$

с двумя образующими и тремя соотношениями.

Такая группа имеет порядок $|G| \leqslant 2n$, поскольку $ba = a^{-1}b^{-1} = (a^n)^{-1}a^{n-1}b(b^2)^{-1} = a^{n-1}b$, откуда G исчерпывается элементами $e, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b$.

Произведение любых двух таких элементов однозначно определено из соотношений.

Покажем, что такая группа изоморфна уже известной нам группе диэдра (движения правильного n-угольника) $\mathbf{D}_n$.

Действительно, сопоставим поворот на угол $2\pi/n$ многоугольника через a, а отражение многоугольника, которое оставляет на месте вершину 1 и меняет местами вершины 2 и $n-1$, — через b. Тогда все соотношения выполнены, в группе ровно $2n$ элементов, откуда следует, что нашими соотношениями задана ровно группу диэдра.

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 4 (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 2. 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

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

□