Лекция 8

Лемма 1. *Подгруппа* $\mathrm{Inn}(G)$ *внутренних автоморфизмов нормальна в группе* $\mathrm{Aut}(G)$.

Доказательство. Рассмотрим $\varphi_g \in \mathrm{Inn}(G)$ и $\psi \in \mathrm{Aut}(G)$. Имеем

$$\psi \circ \varphi_g \circ \psi^{-1}(h) = \psi(\varphi_g(\psi^{-1}(h))) = \psi(g\psi^{-1}(h)g^{-1}) = \psi(g)\psi(\psi^{-1}(h))\psi(g^{-1}) = \\ = \psi(g)h\psi(g)^{-1} = \varphi_{\psi(g)}(h).$$

Так как это верно для всех h, получаем $\psi\circ\varphi_g\circ\psi^{-1} = \varphi_{\psi(g)}$, это доказывает утверждение. □

Определение 1. Пусть G – группа и g – элемент в ней. Классом сопряжчнности элемента g в группе G называется множество

$$C(g) = \{hgh^{-1} \mid h \in G\}$$

всех элементов, сопряженных с g.

Замечание 1. Класс сопряженности зависит не только от элемента, но и от группы, в которой этот элемент лежит. Например, если H подгруппа в G, то класс сопряженности элемента $h \in H$ в H может отличаться от класса сопряженности h в G.

Лемма 2. *Быть сопряженными – это отношение эквивалентности. (И, соответственно, классы сопряженности – это классы эквивалентности.)*

Доказательство. Так как $ege^{-1} = g$, данное отношение рефлексивно.

Если $g' = hgh^{-1}$, то $g = h^{-1}g'h = h^{-1}g'(h^{-1})^{-1}$. Это доказывает симметричность рассматриваемого отношения.

Если $b = gag^{-1}$ и $c = hbh^{-1}$, то $c = hgag^{-1}h^{-1} = hga(hg)^{-1}$. Это показывает транзитивность отношения сопряженности. □

Пример 1. *В любой группе есть класс сопряженности* $C(e) = \{e\}$.

Пример 2. *Центр группы – это в точности те элементы, классы сопряженности которых состоят из одного элемента. В частности, все классы сопряженности одноэлементны тогда и только тогда, когда группа абелева.*

Пример 3. *Классы сопряженности в* $\mathrm{GL}_n(\mathbb{C})$ *– это множества матриц с одинаковой ЖНФ.*

Давайте разберемся, как выглядят классы сопряженности в S_n.

Определение 2. *Цикловой структурой* элемента S_n называется набор (с кратностями) длин независимых циклов.

Пример 4. *У перестановки* $(1, 2, 3)(4, 5, 6)(7, 8)(9)(10)$ *два цикла длины 3, один цикл длины 2 и два цикла длины 1. Это и есть цикловая структура данной перестановки.*

Предложение 1. *Пусть* $\sigma \in \mathrm{S}_n$. *Тогда класс сопряженности* $C(\sigma)$ *состоит из всех перестановок с такой же, как у* σ *цикловой структурой.*

Доказательство. Пусть $\pi \in \mathrm{S}_n$ и

$$\sigma = (a_1, \ldots, a_k)(b_1, \ldots, b_m) \ldots (c_1, \ldots, c_l).$$

Тогда

$$\pi(a_1,\dots,a_k)(b_1,\dots,b_m)\dots(c_1,\dots,c_l)\pi^{-1} = \\ = (\pi(a_1),\dots,\pi(a_k))(\pi(b_1),\dots,\pi(b_m))\dots(\pi(c_1),\dots,\pi(c_l)).$$

Таким образом, цикловая структура $\pi\circ\sigma\circ\pi^{-1}$ такая же как у σ.

С другой стороны, если

$$\sigma' = (a'_1,\dots,a'_k)(b'_1,\dots,b'_m)\dots(c'_1,\dots,c'_l) \ -$$

перестановка с такой же цикловой структурой, что и у σ, то для

$$\pi = \begin{pmatrix} a_1 & a_2 & \dots & a_k & \dots & c_1 & \dots & c_l \\ a'_1 & a'_2 & \dots & a'_k & \dots & c'_1 & \dots & c'_l \end{pmatrix}$$

выполнено $\pi\circ\sigma\circ\pi^{-1} = \sigma'$. □

Для абелевых групп будем использовать аддитивную терминологию. Операцию будем обозначать "+"и называть сложением. Нейтральный элемент называем нулем. При этом степень g^k элемента g, будет обозначатся kg.

Замечание 2. То, что абелева группа A порождается подмножеством $S \subset A$ означает, что каждый элемент $a \in A$ представляется в виде $a = k_1s_1 + \ldots + k_ns_n$, где $s_i \in S$, $k_i \in \mathbb{Z}$.

Мы почти всегда будем ограничиваться рассмотрением только конечно порожденных абелевых групп, то есть таких групп A, для которых множество S может быть выбрано конечным.

Определение 3. Система элементов S абелевой группы A называется *линейно независимой* (над $\mathbb{Z}$), если из того, что $k_1s_1 + \ldots + k_ns_n = 0$ для некоторых $k_i \in \mathbb{Z}$, $s_i \in S$, следует что все k_i равны нулю.

Определение 4. *Базис* абелевой группы – это линейно независимая система порождающих этой группы.

Заметим, что не у всякой группы есть базис. Например, у группы $\mathbb{Z}_n$ базиса нет, так как для любой системы $\{s_1,\dots,s_k\}$ выполнено $ns_1 = 0$, что противоречит линейной независимости этой системы.

Определение 5. Пусть в абелевой группе A есть базис $\{e_1,\dots,e_n,\dots\}$. Тогда группа A называется *свободной абелевой группой*. Будем обозначать эту группу

$$\mathcal{A}(e_1,\dots,e_n,\dots).$$

Если базис конечен и имеет мощность n, то будем говорить, что A – свободная абелева группа ранга n и обозначать $\operatorname{rk} A = n$.

Задача 1. Докажите, что

$$\mathcal{A}(e_1,\dots,e_n) = \langle e_1,\dots,e_n \mid e_ie_je_i^{-1}e_j^{-1}, 1\le i<j\le n\rangle.$$

Лемма 3. *Пусть в абелевой группе A есть базис $\{e_1,\dots,e_n\}$. Тогда любой другой базис этой группы также состоит из n элементов. (То есть ранг свободной абелевой группы определен однозначно.)*

Доказательство. Пусть в группе A есть другой базис $\{e'_1, \ldots, e'_m, \ldots\}$ и количество элементов в нем не равно n. Без ограничения общности мы можем считать, что в нем больше, чем n элементов. Рассмотрим $e'_1, \ldots, e'_{n+1}$ Так как $\{e_1, \ldots, e_n\}$ – базис, каждый элемент e'_j выражается через $\{e_1, \ldots, e_n\}$ с целыми коэффициентами: $e'_j = c_{1j}e_1 + \ldots + c_{nj}e_n$. Можно собрать все коэффициенты c_{ij} в целочисленную матрицу C размера $n \times n+1$ такую, что

$$(e'_1, \ldots, e'_{n+1}) = (e_1, \ldots, e_n)C.$$

Интерпретируем столбцы $C^{(1)}, \ldots, C^{(n+1)}$ матрицы C как векторы из пространства $\mathbb{Q}^n$ строк с рациональными коэффициентами длины n. Тогда столбцы – это $n+1$ векторов в n-мерном векторном пространстве. По основной лемме о линейной зависимости столбцы C линейно зависимы, то есть есть рациональные числа $\frac{p_1}{q_1}, \ldots, \frac{p_{n+1}}{q_{n+1}}$ не все равные нулю такие, что

$$\frac{p_1}{q_1}C^{(1)} \ldots + \frac{p_{n+1}}{q_{n+1}}C^{(n+1)} = 0.$$

Домножим это равенство на произведение знаменателей и получим

$$k_1C^{(1)} \ldots + k_{n+1}C^{(n+1)} = 0$$

для некоторых $k_i \in \mathbb{Z}$ не всех равных нулю. Но тогда $k_1e'_1 + \ldots + k_{n+1}e'_{n+1} = 0$, что противоречит линейной независимости $\{e'_1, \ldots, e'_{n+1}, \ldots\}$. □

Замечание 3. Пусть $F = \mathcal{A}(e_1, \ldots, e_n)$. Тогда $F = \langle e_1 \rangle \oplus \ldots \oplus \langle e_n \rangle \cong \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$. В самом деле, сопоставим элементу $k_1e_1 + \ldots k_ne_n \in \mathcal{A}(e_1, \ldots, e_n)$ элемент $(k_1e_1, \ldots, k_ne_n) \in \langle e_1 \rangle \oplus \ldots \oplus \langle e_n \rangle$. Легко проверить, что это изоморфизм.

Предложение 2. *Подгруппа L свободной абелевой группы F ранга n – это свободная абелева группа ранга $m \leq n$.*

Доказательство. Докажем это утверждение индукцией по n.

База индукции $n = 1$. $F \cong \mathbb{Z}$. По теореме **??**(2) подгруппа в $\mathbb{Z}$ имеет вид $k\mathbb{Z}$. При $k \neq 0$ это свободная абелева группа ранга 1. Если же $k = 0$ получаем свободную абелеву группу ранга ноль.

Шаг индукции. Пусть для $n < k$ утверждение доказано. Рассмотрим

$$P = \mathcal{A}(e_1, \ldots, e_{n-1}) \subset F.$$

Обозначим $B = P \cap L$. Так как P – свободная группа ранга $n-1$, по предположению индукции $B \subset P$ – свободная абелева группа ранга не более $n-1$. Если $L \subset P$, то $L = B$ – свободная абелева группа ранга не более $n-1$. Пусть $L \neq B$. Рассмотрим гомоморфизм $\pi\colon F \to \mathbb{Z}$, $\pi(k_1e_1 + \ldots + k_ne_n) = k_n$. Тогда образ π – циклическая группа и найдется $l \in L$ такой, что $\operatorname{Im}\pi = \langle \pi(l) \rangle$. Пусть $s = t_1e_1 + \ldots t_ne_n \in L$. Тогда $\pi(s) \in \langle \pi(s) \rangle$. То есть $\pi(s) = q\pi(s)$ для некоторого целого q. Получаем $\pi(s - ql) = 0$, то есть $s - ql \in B$. Значит, $s \in B \oplus \langle l \rangle$ (данные две подгруппы пересекаются только по нулю, так как $\pi(l) \neq 0$). Получаем $L = B \oplus \langle l \rangle$ – свободная абелева группа ранга $\operatorname{rk} B + 1 \leq n$. □

Теорема 1 (Универсальное свойство свободной абелевой группы)**.** *Пусть A – абелева группа с образующими $a_1, \ldots, a_n$. Тогда существует сюрьективный гомоморфизм*

$$\varphi\colon \mathcal{A}(x_1, \ldots, x_n) \to A,$$

причем $\varphi(x_i) = a_i$.

Доказательство. Подходит гомоморфизм определенный по правилу

$$\varphi(k_1x_1 + \ldots + k_nx_n) = k_1a_1 + \ldots + k_na_n.$$

$\square$

Применяя теорему о гомоморфизме, получаем следствие.

Следствие 1. *Каждая конечно порожденная абелева группа изоморфна факторгруппе свободной абелевой группы по некоторой подгруппе (ядру гомоморфизму φ).*