ЛЕКЦИЯ 13

ИЗОМОРФИЗМЫ ГРУПП

ИЗОМОРФИЗМ ЦИКЛИЧЕСКИХ ГРУПП ОДНОГО ПОРЯДКА

ИЗОМОРФИЗМЫ

Рассмотрим сначала два примера.

Пример 1. Рассмотрим равносторонний треугольник ABC и рассмотрим все движения, которые переводят его самого в себя.

Понятно, что их шесть:

(1) Тождественное движение

(2) Поворот по часовой стрелке на 120°

(3) Поворот против часовой стрелки на 120°

(4)–(6) Отражения треугольника относительно медиан, проходящих через вершины A, B и C соответственно.

Понятно, что на этих движениях можно ввести операцию композиции, которая, конечно же, будет ассоциативна (как любая композиция). При этом существует тождественное движение, превращающее множество движений треугольника в моноид. Кроме того, для каждого движения существует обратное: надо просто перевести все точки в обратном направлении.

В нашем случае движения (1) и (4)–(6) будут обратны сами себе, а повороты — взаимно обратны.

Таким образом, множество движений треугольника ABC оказывается группой из шести элементов.

Теперь пронумеруем вершины треугольника (то есть теперь это будет не треугольник ABC, а треугольник 123) и заметим, что при каждом движении вершины обязательно переходят вершины. Кроме того, если известно, как отобразились в вершины, то движение полностью определено. Значит, можно отобразить каждое движение в перестановку трех вершин.

Введенная группа становится очень похожа на группу S_3.

Пример 2. Теперь рассмотрим две уже рассмотренных группы. Одна из них — $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.

Другая — введенная выше циклическая группа, порожденная элементом a порядка n, которая состоит из элементов $e, a, a^2, \ldots, a^{n-1}$.

Обозначим вторую группу через G.

Попробуем временно заменить элементы вида a^k на числа k (просто как бы заменим обозначения).

Заметим, что если мы перемножим два исходных элемента a^k и a^l, то получим элемент a^{k+l}, то есть при замене элементов их показателями эти самые показатели будут складываться, причем по модулю n.

Благодаря этому группа G отождествляется с группой $\mathbb{Z}_n$.

Два последних примера показывают, что иногда группы внешне выглядят и вводятся по-разному, но при этом по сути очень похожи, получаются друг из друга какими-то переобозначениями.

Эти примеры обобщает понятие изоморфизма.

Определение 1. Две группы G и G' с операциями $*$ и $\circ$ называются *изоморфными*, если существует отображение $f : G \to G'$ такое, что:

(1) $f(a * b) = f(a) \circ f(b)$ для всех $a, b \in G$;

(2) f биективно.

Данное отображение называется *изоморфизмом.*

Факт изоморфизма групп часто обозначается символом $G \cong G'$.

Отметим простейшие свойства изоморфизма.

(1) *Единица переходит в единицу.*

Действительно, если e — единица группы G, то

$$e * a = a * e = a,$$

и, значит,

$$f(e) \circ f(a) = f(a) \circ f(e) = f(a),$$

откуда следует, что

$$f(e) = e'$$

— единица группы G'.

В этом рассуждении использованы, хотя частично, об свойства изоморфизма.

Для первого свойства это очевидно, а свойство (2) обеспечивает сюръективность f, так что элементами $f(g)$ исчерпывается все группа G'.

(2) *Обратный элемент переходит в обратный элемент.*
Пусть $a \in G$, $f : G \to G'$ — изоморфизм групп.
Покажем, что $f(a^{-1}) = (f(a))^{-1}$.
Действительно,

$$a * a^{-1} = e \Longrightarrow f(a) \circ f(a^{-1}) = f(e) = e',$$

откуда получаем, что элементы $f(a)$ и $f(a^{-1})$ взаимно обратны.

(3) Обратное отображение $f^{-1} : G' \to G$ (существующее в силу биективности f) тоже является изоморфизмом.

Мы уже знаем, что обратное к биекции отображение тоже биективно.

Поэтому остается только проверить свойство (1).

Пусть $a', b' \in G'$. Тогда ввиду биективности f имеем

$$a' = f(a), \quad b' = f(b)$$

для каких-то $a, b \in G$.

Поскольку f — изоморфизм,

$$a' \circ b' = f(a) \circ f(b) = f(a * b).$$

Отсюда имеем

$$a * b = f^{-1}(a' \circ b'),$$

а так как в свою очередь

$$a = f^{-1}(a'), \quad b = f^{-1}(b'),$$

то

$$f^{-1}(a' \circ b') = f^{-1}(a') * f^{-1}(b').$$

(4) *Композиция изоморфизмов — изоморфизм.*

Действительно, если $f : G \to G'$ и $h : G' \to G''$ — изоморфизмы, то их композиция $hf : G \to G''$ является биекцией и для всех $a, b \in G$ выполнено

$$hf(a * b) = h(f(a * b)) = h(f(a) \circ f(b)) = \\ = h(f(a)) \cdot h(f(b)) = hf(a) \cdot hf(b),$$

что и требовалось.

Теорема 1. *Все циклические группы одного и того же порядка (в том числе и бесконечного) изоморфны.*

Доказательство. В самом деле, если $\langle g\rangle$ — бесконечная циклическая группа, то все степени g^k образующего g различны и мы получим изоморфизм

$$f : \langle g\rangle \to (\mathbb{Z}, +),$$

полагая

$$g^k \mapsto f(g^k) = k.$$

Биективность f очевидна, а свойство

$$f(g^m g^n) = f(g^n) + f(g^m)$$

вытекает из свойств степени.

Пусть теперь

$$G = \{e, g, \ldots, g^{q-1}\} \text{ и } G' = \{e', g', \ldots, (g')^{q-1}\}$$

— две циклические группы порядка q (для удобства не будем различать операции в G и G').

Определим биективное отображение

$$f : g^k \mapsto (g')^k, \quad k = 0, 1, \ldots, q-1.$$

Полагая $n+m = lq+r$, $0 \leqslant r < q$, для любых $n, m = 0, 1, \ldots, q-1$, будем иметь

$$f(g^{n+m}) = f(g^r) = (g')^r = (g')^{n+m} = (g')^n (g')^m = f(g^n) f(g^m).$$

□

Фраза “с точностью до изоморфизма” отражает сущность не только теории групп, стремящейся объединить в один класс все изоморфные группы, но и математики в целом, которая без таких обобщений была бы лишена смысла.

Положив $G = G'$ в определении изоморфизма, мы получим изоморфное отображение $\varphi : G \to G$ группы G на себя. Оно называется *автоморфизмом* группы G.

Например, единичное отображение $e_G = 1 : g \mapsto g$ всегда является автоморфизмом. Чаще всего группа G обладает и нетривиальными автоморфизмами.

Пример 3. Например, группа $\mathbb{Z}_2$, состоящая только из 0 и 1, не имеет нетривиальных автоморфизмов, так как 0 обязательно должен отображаться сам в себя как нейтральный элемент группы, поэтому для единицы нет больше никаких возможностей — только отобразиться в саму себя.

Если же мы рассмотрим группу $\mathbb{Z}_3$, то в ней уже возникает нетривиальный автоморфизм

$$a \mapsto -a,$$

при котором 0 останется на месте, а 1 и -1 поменяются местами.

Лемма 1. *При изоморфизме (автоморфизме) $\varphi : G \to G'$ любой элемент $x \in G$ порядка n (или бесконечного порядка) переходит в элемент того же порядка.*

Доказательство. Действительно, если $x^n = e$, то $\varphi(x)^n = \varphi(e) = e'$, то есть порядок элемента $\varphi(x)$ является делителем числа n.

С другой стороны, изоморфизм (или автоморфизм) — это обратимое отображение, можно применить те же рассуждению к изоморфизму φ^{-1}, поэтому окажется, что и число n делит порядок элемента $\varphi(x)$. Значит, эти два числа совпадают. □

Пример 4. Рассмотрим симметрическую группу S_3. Заметим, что транспозиции должны переходить в транспозиции, так как они являются элементами порядка два. При этом, понятно, они должны переставляться. Кроме того, если мы знаем образы транспозиций, то полностью знаем автоморфизм, так как транспозициями порождается вся группа S_3.

Значит, можно считать, что группа автоморфизмов $\operatorname{Aut} S_3$ содержится в S_3.

В реальности можно насчитать шесть разных автоморфизмов, которые задаются отображениями

$$\varphi_\sigma : \tau \mapsto \sigma\tau\sigma^{-1}, \text{ где } \sigma, \tau \in S_3.$$

Значит, $\operatorname{Aut} S_3 \cong S_3$.

Заметим, что композиция автоморфизмов — автоморфизм, обратный к автоморфизму — автоморфизм, то есть все автоморфизмы данной группы образуют группу $\operatorname{Aut}(G)$.