Введение в теорию групп

Роман Атангулов

Летняя компьютерная школа
«Берендеевы поляны»
июль 2011 года

Содержание

1 Введение

Предметом нашего курса является *группа* — одна из самых простых алгебраических структур и в то же время основополагающая в алгебре. То есть мы будем заниматься абстрактной алгеброй, а точнее той её частью, которая посвящена теории групп.

Если вообще можно чётко определить предмет алгебры, то это изучение *алгебраических структур* — множеств с определёнными в них операциями. Под *операцией* во множестве M понимается любое отображение

$$M \times M \to M,$$

т.е. правило, по которому из любых двух элементов множества M получается некоторый элемент этого же множества. Элементами множества M могут быть как числа, так и объекты другого рода.

Хорошо известными и важными примерами алгебраических структур являются следующие числовые множества с операциями сложения и умножения:

$\mathbb{N}$ — множество натуральных чисел,
$\mathbb{Z}$ — множество всех целых чисел,
$\mathbb{Z}_+ = \mathbb{N} \cup \{0\}$ — множество неотрицательных целых чисел,
$\mathbb{Q}$ — множество рациональных чисел,
$\mathbb{R}$ — множество всех действительных (вещественных) чисел,
$\mathbb{R}_+$ — множество неотрицательных действительных чисел.

Подчеркнём, что операции сложения и умножения определены далеко не на всяком числовом множестве. Например, во множестве отрицательных чисел не определена операция умножения, так как произведение двух отрицательных чисел является положительным. Во множестве всех нечётных целых чисел определена операция умножения, но не определена операция сложения: сумма двух нечётных чисел — чётное число.

2 Абелевы группы

Сложение действительных чисел обладает следующими свойствами:

(C1) $a + b = b + a$ (коммутативность);
(C2) $(a + b) + c = a + (b + c)$ (ассоциативность);
(C3) $a + 0 = a$;
(C4) $a + (-a) = 0$.

Из этих свойств чисто логическим путём могут быть получены и другие свойства, например, наличие операции вычитания, обратной к сложению. Это означает, что для любых a, b уравнение

$$x + a = b$$

имеет единственное решение. Докажем, что это так. Если c — решение данного уравнения, т.е. $c + a = b$, то

$$(c + a) + (-a) = b + (-a).$$

Пользуясь свойствами (С2)–(С4), получаем

$$(c + a) + (-a) = c + (a + (-a)) = c + 0 = c.$$

Таким образом,

$$c = b + (-a).$$

Это показывает, что если решение существует, то оно единственно и равно $b + (-a)$. С другой стороны, подстановка $x = b + (-a)$ в рассматриваемое уравнение показывает, что $b + (-a)$ действительно является решением:

$$(b + (-a)) + a = b + ((-a) + a) = b + (a + (-a)) = b + 0 = b.$$

Умножение действительных чисел обладает аналогичными свойствами:

(У1) $ab = ba$ (коммутативность);
(У2) $(ab)c = a(bc)$ (ассоциативность);
(У3) $a1 = a$;
(У4) $aa^{-1} = 1$ при $a \neq 0$.

Свойства (У1)–(У4) лишь формой записи отличаются от свойств (С1)–(С4), с единственной оговоркой, что в (У4) мы предполагаем, что $a \neq 0$, в то время как в (4) никаких ограничений на a нет. Поэтому приведённый выше вывод из свойств (С1)–(С4) наличия операции вычитания, будучи переведён на язык умножения даст вывод из свойств (У1)–(У4) наличия операции деления, обратной к умножению. Более точно, таким путём доказывается, что для любого $a \neq 0$ и любого b уравнение $xa = b$ имеет единственное решение, равное ba^{-1}.

Во всех этих рассуждениях нет ничего нового, и сами по себе они не представляют интереса. Они здесь приведены для того, чтобы подчеркнуть

важную для алгебры идею аксиоматического метода. Он состоит в изучении целых классов алгебраических структур, выделяемых теми или иными аксиомами, представляющими собой какие-то свойства операций в этих структурах. При этом совершенно не важно, как в каждом конкретном случае эти операции определяются. Раз выполнены аксиомы, справедлива любая теорема, полученная логическим путём из этих аксиом.

Названия и обозначения операций в алгебраических структурах не имеют принципиального значения, однако чаще всего они называются сложением или умножением и обозначаются соответствующим образом. Это позволяет использовать разработаннцю терминологию и систему обозначений, относящиеся к операциям над действительными числами, а также вызывает полезные ассоциации.

Свойства (С1)–(С4), а также (У1)–(У4) являются по сути дела системой аксиом абелевой группы.

Определение 2.1. *(Аддитивной) абелевой группой* называется множество A с операцией сложения, обладающей следующими свойствами:

1) $a + b = b + a$ для любых $a, b \in A$ *(коммутативность)*;

2) $(a + b) + c = a + (b + c)$ для любых $a, b, c \in A$ *(ассоциативность)*;

3) в A существует такой элемент 0 *(нуль)*, что $a + 0 = a$ для любого $a \in A$;

4) для любого элемента $a \in A$ существует такой элемент $-a \in A$ *(противоположный элемент)*, что $a + (-a) = 0$.

Выведем некоторые простейшие следствия из этих аксиом.

1) Нуль единственен. Пусть 0_1 и 0_2 — два нуля. Тогда

$$0_1 = 0_1 + 0_2 = 0_2.$$

2) Противоположный элемент единственен. Пусть $(-a)_1$ и $(-a)_2$ — два элемента, противоположных a. Тогда

$$(-a)_1 = (-a)_1 + (a + (-a)_2) = ((-a)_1 + a) + (-a)_2 = (-a)_2.$$

3) Для любых a, b уравнение $x + a = b$ имеет единственное решение, равное $b + (-a)$. Доказательство приведено выше. Это решение называется *разностью* элементов b и a и обозначается $b - a$.

Из свойства ассоциативности нетрудно вывести (попробуйте сделать это), что сумма произвольного числа (а не только трёх) элементов не зависит от расстановки скобок. Пользуясь этим, скобки обычно вообще опускают.

По аналогии приведём определение абелевой группы, использующее язык умножения.

Определение 2.2. *(Мультипликативной) абелевой группой* называется множество A с операцией умножения, обладающей следующими свойствами:

1) $ab = ba$ для любых $a, b \in A$ *(коммутативность)*;

2) $(ab)c = a(bc)$ для любых $a, b, c \in A$ *(ассоциативность)*;

3) в A существует такой элемент e *(единица)*, что $ae = a$ для любого $a \in A$;

4) для любого элемента $a \in A$ существует такой элемент $a^{-1} \in A$ *(обратный элемент)*, что $aa^{-1} = e$.

Единица мультипликативной абелевой группы иногда обозначается символом 1.

Простейшие следствия аксиом абелевой группы, полученные выше на аддитивном языке, на мультипликативном языке выглядят следующим образом:

1) Единица единственна.

2) Обратный элемент единственен.

3) Для любых a, b уравнение $xa = b$ имеет единственное решение, равное ba^{-1}. Оно называется *частным* от деления b и a (или *отношением* элементов b и a) и обозначается $\frac{b}{a}$ (или b/a).

Приведём несколько примеров абелевых групп.

Пример 2.1. Числовые множества $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ являются абелевыми группами относительно обычной операции сложения.

Пример 2.2. Множества $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ и $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ являются абелевыми группами относительно обычной операции умножения.

Однако стоит обратить внимание на то, что множество $\mathbb{Z} \setminus \{0\}$ не является абелевой группой относительно обычной операции умножения, так как для чисел, отличных от 1, в этом множестве не существует обратного элемента.

Пример 2.3. Множество векторов (плоскости или пространства) является абелевой группой относительно обычного сложения векторов.

Далее мы познакомимся с общим понятием группы (не обязательно абелевой), которое не включает требования коммутативности операции.

3 Перестановки, подстановки

Такие важные понятия как *перестановка и подстановка* (в некоторых книгах оба эти понятия называются перестановками) пригодятся нам в дальнейшем, поэтому стоит рассмотреть некоторые их свойства. Теория,

касающаяся подстановок весьма велика и может занять объём целой книги, здесь мы рассмотрим лишь самые основные и необходимые нам свойства.

Пусть дано некоторое конечное множество M, состоящее из n элементов. Эти элементы можно занумеровать первыми n натуральными числами. Для нас сейчас природа и индивидуальные свойства объектов, являющихся элементами множества M, не будут иметь значения, поэтому для удобства будем считать, что $M = \{1, 2, \ldots, n\}$.

Понятно, что числа можно записывать в разных порядках ($1, 5, 3, 2, 4$ или $3, 1, 4, 5, 2$ и т.д.).

Определение 3.1. *Перестановкой* из n чисел (или из n символов) называется всякое расположение чисел $1, 2, \ldots, n$ в некотором определённом порядке.

Число различных перестановок из n символов, очевидно, равно $n!$.

Определение 3.2. *Подстановкой n-й степени* называется взаимно однозначное отображение множества $M = \{1, 2, \ldots n\}$ в себя.

Подстановку можно записать в виде таблицы. Например, при $n = 5$ таблица

$$\begin{pmatrix} 3 & 5 & 1 & 4 & 2 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}$$

задаёт подстановку множества $\{1, 2, 3, 4, 5\}$, при которой число 3 переходит в 5, число 5 переходит в 2, число 1 переходит в 3, число 4 *переходит в себя* (или *остаётся на месте*), и, наконец, число 2 переходит в 1.

Часто для удобства таблицу подстановки записывают так, что в верхнем ряду числа упорядочены по возрастанию. В такой записи приведённая выше подстановка будет выглядеть следующим образом:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}.$$

Учитывая этот факт, легко видеть, что количество различных подстановок множества из n элементов равно количеству перестановок этого множества, т.е. $n!$.

Важным примером подстановки n-й степени служит *тождественная подстановка*

$$E = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix},$$

при которой все символы переходят в себя.

Теперь рассмотрим последовательное выполнение двух подстановок n-й степени. Каждая из них по определению является взаимно однозначным отображением множества $M = \{1, 2, \dots n\}$ в себя, поэтому и их последовательное выполнение также будет являться взаимно однозначным отображением множества M в себя, т.е. подстановкой n-й степени. Следовательно, корректно следующее

Определение 3.3. *Композицией (или произведением)* двух подстановок n-й степени φ и ψ называется подстановка n-й степени $\sigma = \psi \circ \varphi$, получающаяся последовательным выполнением этих двух подстановок.

Часто знак композиции опускают и пишут просто $\sigma = \psi\varphi$.

Обратите внимание, выполняется сначала подстановка φ, а после неё подстановка ψ. Мы будем записывать композицию в обратном порядке, как в определении. Это вполне естественно, если вспомнить, как записывается композиция функций, ведь подстановка — ни что иное как функция на множестве M. Например, если подстановка φ переводит символ k в l, а подстановка ψ переводит символ l в m, то композиция $\sigma = \psi\varphi$ переводит символ k в m:

$$\sigma(k) = (\psi\varphi)(k) = \psi(\varphi(k)) = \psi(l) = m.$$

Заметим, что произведение подстановок в общем случае некоммутативно. Так, если даны подстановки четвёртой степени

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \qquad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix},$$

то

$$\psi\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix},$$

в то время как

$$\varphi\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}.$$

Композиция подстановок φ, ψ, χ также будет подстановкой ($\sigma = \chi\psi\varphi$), и вообще, композицией подстановок $\varphi_1, \varphi_2, \dots, \varphi_k$ является подстановка $\sigma = \varphi_k\varphi_{k-1}\dots\varphi_2\varphi_1$.

Заметим, что если поменять строки в таблице подстановки, то получится *обратная подстановка*, т.е. если

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix},$$

то

$$\sigma\sigma^{-1} = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix} = \\ = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix},$$

и в то же время

$$\sigma^{-1}\sigma = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} = \\ = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Пусть φ, ψ, χ — подстановки n-й степени, действующие на множестве M. Тогда для любого $k \in M$ имеем

$$(\varphi(\psi\chi))(k) = \varphi((\psi\chi)(k)) = \varphi(\psi(\chi(k))),$$
$$((\varphi\psi)\chi)(k) = (\varphi\psi)(\chi(k)) = \varphi(\psi(\chi(k))),$$

таким образом, $(\varphi(\psi\chi))(k) = ((\varphi\psi)\chi)(k)$ для всех $k \in M$, следовательно, $\varphi(\psi\chi) = (\varphi\psi)\chi$, т.е. операция композиции ассоциативна. Причем здесь мы никак не использовали свойства, характерные для подстановок, а это значит, что ассоциативной является операция композиции любых отображений, не только подстановок.

Разумеется, перестановку можно перемножать с собой. Пусть дана перестановка σ. Определим её степень σ^k по индукции:

$$\sigma^k = \begin{cases} \sigma(\sigma^{k-1}), & \text{если k} > 0, \\ e, & \text{если k} = 0, \\ \sigma^{-1}((\sigma^{-1})^{-k-1}), & \text{если k} < 0. \end{cases}$$

При таком определении справедливы равенства:

$$\sigma^k\sigma^l = \sigma^{k+l} = \sigma^l\sigma^k, \qquad s, t \in \mathbb{Z}.$$

Другим удобным способом записи подстановок является *разложение в непересекающиеся циклы*. Рассмотрим подстановку

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 7 & 4 & 5 & 8 & 6 & 2 \end{pmatrix}.$$

Символы $1, 4, 5$ остаются на месте, а действительно передвигаются только символы $2, 3, 6, 7, 8$. Причём они *двигаются по циклу*: $2 \to 3 \to 7 \to 6 \to 8 \to 2$. По сути данная подстановка представляет собой именно этот цикл, который принято записывать в виде (2 3 7 6 8), или (3 7 6 8 2), или (6 8 2 3 7) и т.д. В принципе можно записать данную подстановку и в "полном"виде: (1)(4)(5)(2 3 7 6 8). Но так делают редко. Мы только что записали разложение данной перестановки 8-й степени в непересекающиеся циклы. Дадим более общее

Определение 3.4. *Циклом длины* r назовём подстановку, обозначаемую $(i_1\ i_2\ \dots\ i_r)$, переводящую i_k в i_{k+1} для $1 \leqslant k \leqslant r-1$, i_r в i_1, и оставляющую все элементы из $\{1, 2, \dots, n\}$, отличные от $i_1, \dots, i_r$, на месте.

В частности, (k) — цикл длины 1; это означает, что подстановка оставляет символ k на месте.

Определение 3.5. Циклы $(i_1\ i_2\ \dots\ i_r)$ и $(j_1\ j_2\ \dots\ j_s)$ называются *непересекающимися*, если множества $\{i_1, \dots, i_r\}$ и $\{j_1, \dots, j_s\}$ не пересекаются.

Теорема 3.1. *Каждая подстановка* n*-й степени разлагается (и притом единственным образом) в произведение непересекающихся циклов.*

Доказательство здесь приводить не будем, оно несложное и в этом курсе не представляет интереса. Отметим только, что раз циклы τ и σ не пересекаются, то они перестановочны: $\tau\sigma = \sigma\tau$. Это тоже несложно проверить. Это значит, что циклы в разложении подстановки можно записывать в любом порядке.

4 Общее определение группы

Обозначим множество подстановок n-й степени S_n. Из написанного выше следует, что S_n с операцией композиции подстановок обладает следующими свойствами:

0) для любых $\sigma, \tau \in S_n$ $\tau\sigma \in S_n$ (S_n замкнуто относительно операции композиции);

1) если $\varphi, \psi, \chi \in S_n$, то $\varphi(\psi\chi) = (\varphi\psi)\chi$ *(ассоциативность композиции)*;

2) существует тождественная подстановка n-й степени $e \in S_n$ (иногда обозначают id), которая оставляет все символы на месте, причём $\sigma e = e\sigma = \sigma$ для любой $\sigma \in S_n$;

3) для любой $\sigma \in S_n$ существует *обратная подстановка* $\sigma^{-1} \in S_n$, такая что $\sigma\sigma^{-1} = \sigma^{-1}\sigma = e$.

Но вот только *коммутативной* операция композиции не является (пример был приведён выше). Это значит, что множество S_n не является абелевой группой. Но, если так можно сказать, "почти" является. Более строго, множество S_n образует *группу* относительно операции композиции.

Определение 4.1. *Группой* называется множество A с операцией $*$, такой что:

0) для любых $a, b \in A$ $a*b \in A$ *(множество A замкнуто относительно операции $*$)*;

1) $a * (b * c) = (a * b) * c$ для любых $a, b, \in A$ *(ассоциативность)*;

2) существует такой элемент $e \in A$, что $a * e = e * a = a$ для любого $a \in A$ *(нейтральный элемент)*;

3) для любого $a \in A$ существует такой элемент $a^{-1} \in A$, что $a * a^{-1} = a^{-1} * a = e$ *(обратный элемент)*.

Тогда определение абелевой группы можно переписать.

Определение 4.2. Множество A называется *абелевой (или коммутативной) группой* относительно операции $*$, если оно является группой относительно этой операции, и, кроме того, операция коммутативна, т.е. $a * b = b * a$ для любых $a, b \in A$.

Часто группы обозначают парой множество-операция: $(A, *)$.

Как мы только что убедились на примере множества S_n, группы не всегда являются абелевыми.

Пример 4.1. Все те числовые множества, что были приведены в начале являются абелевыми группами, а значит, являются и группами.

Пример 4.2. Множество движений плоскости (т.е. преобразований плоскости, сохраняющих расстояние) является неабелевой группой (две осевые симметрии не всегда коммутируют).

Примеры показывают, что группы бывают как конечными, так и бесконечными. Конечная группа может быть задана своей таблицей умножения. Так, множество $G = \{e, a, b, c\}$ с таблицей умножения

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

является абелевой группой.

5 Подгруппы

Определение 5.1. *Подгруппой* группы G называется всякое подмножество $H \subset G$, удовлетворяющее следующим условиям:

1) если $a, b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$;
3) $e \in H$.

Пример 5.1. Очевидно, что всякая подгруппа сама является группой относительно той же операции.

Пример 5.2. $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ является подгруппой группы $(\mathbb{Z}, +)$. И вообще, $(\mathbb{Z}, +)$ является подгруппой группы $(\mathbb{Q}, +)$, которая в свою очередь является подгруппой группы $(\mathbb{R}, +)$.

Пример 5.3. $(\mathbb{Q}^*, \cdot)$ является подгруппой группы $(\mathbb{R}^*, \cdot)$ (относительно обычного умножения чисел).

Пример 5.4. Во множестве подстановок S_7 есть подгруппы S_2, S_3, S_4 и т.д.

Пример 5.5. В любой группе $\{e\}$ является подгруппой.

Пример 5.6. В группе всех движений плоскости (обозначается $\operatorname{Isom} E^2$) все повороты вокруг центра координат образуют подгруппу.

6 Циклические подгруппы

Так же, как и в группе R^*, в любой группе G могут быть определены *степени* элемента $g \in G$ с целыми показателями:

$$g^k = \begin{cases} \underbrace{gg\dots g}_{k}, & \text{если } k > 0, \\ e, & \text{если } k = 0, \\ \underbrace{g^{-1}g^{-1}\dots g^{-1}}_{-k}, & \text{если } k < 0. \end{cases}$$

Имеет место свойство

$$g^k g^l = g^{k+l}. \tag{1}$$

Это очевидно, если $k, l > 0$. Рассмотрим случай, когда $k > 0, l < 0, k+l > 0$. Тогда

$$g^k g^l = \underbrace{gg\dots g}_{k}\underbrace{g^{-1}g^{-1}\dots g^{-1}}_{-l} = \underbrace{gg\dots g}_{k+l} = g^{k+l}.$$

Аналогично рассматриваются остальные случаи.

Из свойства (1) следует, что

$$(g^k)^{-l} = g^{-k}.$$

Кроме того, $e = g^0$ по определению. Таким образом, степени элемента g образуют подгруппу в группе G.

Определение 6.1. Подгруппа группы G, состоящая из всех целых степеней элемента g называется *циклической подгруппой, порождённой элементом* g, и обозначается через $\langle g \rangle$ (в некоторых книгах можно встретить обозначение (g)).

Возможны два принципиально разных случая: либо все степени элемента g различны, либо нет. В первом случае подгруппа $\langle g \rangle$ бесконечна. Рассмотрим более подробно второй случай.

Пусть $g^k = g^l, k > l$; тогда $g^{k-l} = e$. Наименьшее из натуральных чисел m, для которых $g^m = e$, называется в этом случае порядком элемента g и обозначается через $\operatorname{ord} g$ (или $\operatorname{ord}(g)$).

Утверждение 6.1. *Если* $\operatorname{ord}(g) = n$, *то*

1) $g^m = e \iff n \mid m$;

2) $g^k = g^l \iff k \equiv l \pmod{n}$.

Доказательство. 1) Разделим m на n с остатком:

$$m = qn + r, \qquad 0 \leqslant r < n.$$

Тогда в силу определения порядка

$$g^m = (g^n)^q \cdot g^r = g^r = e \iff r = 0.$$

2) В силу предыдущего

$$g^k = g^l \iff g^{k-l} = e \iff n \mid (k-l) \iff k \equiv l \pmod{n}. \qquad \square$$

Следствие 6.2. *Если* $\operatorname{ord}(g) = n$, *то подгруппа* $\langle g \rangle$ *содержит* n *элементов.*

Доказательство. Действительно,

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\},$$

причём все перечисленные элементы различны. $\square$

В том случае, когда не существует такого натурального m, что $g^m = e$ (т.е. имеет место первый из описанных выше случаев), полагают $\mathrm{ord}(g) = \infty$. Отметим, что $\mathrm{ord}(e) = 1$; порядки всех остальных элементов группы больше 1.

В аддитивной группе говорят не о степенях элемента g, а о его *кратных*, которые обозначают через kg. В соответствии с этим порядок элемента g аддитивной группы G — это наименьшее из натуральных чисел m (если такие существуют), для которых

$$mg \doteqdot \underbrace{g + g + \ldots + g}_{m} = 0.$$

Определение 6.2. Группа G называется *циклической*, если существует такой элемент $g \in G$, что любой элемент группы G является некоторой степенью элемента g с целым показателем. В таком случае g называется *порождающим* элементом группы G.

Пример 6.1. Аддитивная группа $\mathbb{Z}$ целых чисел является циклической, так как порождается элементом 1.

Пример 6.2. Аддитивная группа $\mathbb{Z}_n$ вычетов по модулю n является циклической, так как порождается элементом [1].

Пример 6.3. Мультипликативная группа C_n комплексных корней n-й степени из 1 является циклической. В самом деле, эти корни суть числа

$$\varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} \qquad (k = 0, 1, \ldots, n-1).$$

Ясно, что $\varepsilon_k = \varepsilon_1^k$. Следовательно, группа C_n порождается элементом ε_1.

Для дальшейшего нам необходимы некоторые свойства, которые здесь и рассмотрим (да и вообще их полезно знать).

Утверждение 6.3. *Если* $\mathrm{ord}(g) = n$, *то*

$$\mathrm{ord}(g^k) = \frac{n}{(n,k)}. \tag{2}$$

Доказательство. Пусть

$$(n,k) = d, \quad n = n_1 d, \quad k = k_1 d,$$

так что $(n_1, k_1) = 1$. Имеем

$$(g^k)^m = e \Longleftrightarrow n \mid km \Longleftrightarrow n_1 \mid k_1 m \Longleftrightarrow n_1 \mid m.$$

Следовательно, $\mathrm{ord}(g^k) = n_1$. □

Следствие 6.4. *Элемент g^k циклической группы $G = \langle g \rangle$ порядка n является порождающим тогда и только тогда, когда $(n, k) = 1$.*

Для понимания строения какой-либо группы важную роль играет знание её подгрупп. Все подгруппы циклической группы могут быть легко описаны.

Теорема 6.5. *1) Всякая подгруппа циклической группы является циклической.*

2) В циклической группе порядка n порядок любой подгруппы делит n и для любого делителя q числа n существует ровно одна подгруппа порядка q.

Доказательство. 1) Пусть $G = \langle g \rangle$ — циклическая группа и H — её подгруппа, отличная от $\{e\}$. (Единичная подгруппа, очевидно, является циклической.) Заметим, что если $g^{-m} \in H$ для какого-либо $m \in \mathbb{N}$, то и $g^m \in H$. Пусть m — наименьшее из натуральных чисел, для которых $g^m \in H$. Докажем, что $H = \langle g^m \rangle$. Пусть $g^k \in H$. Разделим k на m с остатком:

$$k = qm + r, \qquad 0 \leqslant r < m.$$

Имеем

$$g^r = g^k (g^m)^{-q} \in H,$$

откуда в силу определения числа m следует, что $r = 0$ и, значит, $g^k = (g^m)^q$.

2) Если $|G| = n$, то предыдущее рассуждение, применённое к $k = n$ (в этом случае $g^k = e \in H$), показывает, что $n = qm$. При этом

$$H = \{e, g^m, g^{2m}, \ldots, g^{(q-1)m}\}, \tag{3}$$

и H является единственной подгруппой порядка q в группе G. Обратно, если q — любой делитель числа n и $n = qm$, то подмножество H, определяемое равенством (3), является подгруппой порядка q. □

Следствие 6.6. *В циклической группе простого порядка любая неединичная подгруппа совпадает со всей группой.*

Пример 6.4. В группе $\mathbb{Z}$ всякая подгруппа имеет вид $m\mathbb{Z}$, где $m \leqslant 0$.

Пример 6.5. В группах $\mathbb{Z}_4$ и $\mathbb{Z}_{12}$ подмножества $\{[0], [2]\}$ и $\{[0], [3], [6], [9]\}$ образуют циклические подгруппы (порождённые элементами $[2]$ и $[3]$ соответственно).

Пример 6.6. В группе C_n корней n-й степени из 1 любая подгруппа есть группа C_q корней q-й степени из 1, где $q \mid n$.

Отметим одно важное свойство подстановок. Пусть есть подстановка σ, которая разлагается в произведение независимых (непересекающихся) циклов длин $p_1, p_2, \ldots, p_s$, то

$$\operatorname{ord}\sigma = \{p_1, p_2, \ldots, p_s\}.$$

7 Разбиение на смежные классы

Определение 7.1. Пусть G — группа и H — её подгруппа. Будем говорить, что элементы $g_1, g_2 \in G$ *сравнимы* по модулю H, и писать

$$g_1 \equiv g_2 \pmod{H},$$

если

$$g_1^{-1} g_2 \in H, \tag{4}$$

т.е. $g_2 = g_1 h$, где $h \in H$.

Это определение обобщает определение сравнимости целых чисел по модулю n, которое получается в случае $G = \mathbb{Z}$, $H = n\mathbb{Z}$.

Утверждение 7.1. *Определённое таким образом отношение сравнимости по модулю H является отношением эквивалентности.*

Доказательство. 1) $g \equiv g \pmod{H}$, так как $g^{-1} g = e \in H$;

2) если $g_1 \equiv g_2 \pmod{H}$, т.е. $g_1^{-1} g_2 \in H$, то $g_2 \equiv g_1 \pmod{H}$, так как

$$g_2^{-1} g_1 = (g_1^{-1} g_2)^{-1} \in H;$$

3) если $g_1 \equiv g_2 \pmod{H}$ и $g_2 \equiv g_3 \pmod{H}$, т.е. $g_1^{-1} g_2, g_2^{-1} g_3 \in H$, то $g_1 \equiv g_3 \pmod{H}$, так как

$$g_1^{-1} g_3 = (g_1^{-1} g_2)(g_2^{-1} g_3) \in H. \qquad \square$$

Классы этой эквивалентности называются *(левыми) смежными классами* группы G по подгруппе H. Ясно, что смежный класс, содержащий элемент g, имеет вид

$$gH = \{gh : h \in H\}.$$

Одним из смежных классов является сама подгруппа H (т.к. $H = eH$).

Поскольку умножение в группе не обязяно быть коммутативным, мы получим, вообще говоря, другое отношение эквивалентности, взяв вместо условия (4) аналогичное ему условие

$$g_2 g_1^{-1} \in H.$$

Классы этой эквивалентности называются *(правыми) смежными классами* группы G по подгруппе H. Они имеют вид

$$Hg = \{hg : h \in H\}.$$

Заметим, что инверсия $g \mapsto g^{-1}$ устанавливает взаимно однозначное соответствие между множествами левых и правых смежных классов. А именно,

$$(gH)^{-1} = Hg^{-1}.$$

Хотя при этом сами по себе множества левых и правых смежных классов могут не совпадать (такие примеры есть).

Пример 7.1. Смежные классы аддитивной группы $\mathbb{C}$ по подгруппе $\mathbb{R}$ изображаются на комплексной плоскости прямыми, параллельными вещественной оси.

Пример 7.2. Смежные классы мультипликативной группы $\mathbb{C}^*$ по подгруппе $\mathbb{R}_+^*$ положительных чисел — это лучи, исходящие из начала координат.

Пример 7.3. Смежные классы группы $\mathbb{C}^*$ по подгруппе $\mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$ — это окружности с центром в начале координат.

Пример 7.4. Множество $\mathbb{Z}/2\mathbb{Z}$ состоит из двух смежных классов — чётных чисел и нечётных.

8 Теорема Лагранжа и её следствия

Определение 8.1. Множество левых смежных классов группы G по подгруппе H обозначается через G/H. Число смежных классов группы G по H (левых или правых, безразлично), если оно конечно, называется *индексом* подгруппы H и обозначается $|G : H|$.

Теорема 8.1 (Лагранжа)**.** *Если G — конечная группа и H — любая её подгруппа, то*

$$|G| = |G : H||H|.$$

Доказательство. Все смежные классы gH содержат одно и то же число элементов, равное $|H|$. Поскольку они образуют разбиение группы G (как классы эквивалентности), порядок группы G равен произведению их числа на $|H|$. □

Следствие 8.2. *Порядок любой подгруппы конечной группы делит порядок группы.*

Мы уже видели это в случае циклических групп.

Следствие 8.3. *Порядок любого элемента конечной группы делит порядок группы.*

Доказательство. Это вытекает из следствия 8.2 и того, что порядок элемента равен порядку порождаемой им циклической подгруппы. □

Следствие 8.4. *Всякая конечная группа простого порядка является циклической.*

Доказательство. В силу следствия 8.2 такая группа должна совпадать с циклической подгруппой, порождённой любым элементом, отличным от нейтрального. □

Следствие 8.5. *Если $|G| = n$, то $g^n = e$ для любого $g \in G$.*

Доказательство. Пусть $\mathrm{ord}(g) = m$. В силу следствия 8.3 имеем $m \mid n$. Значит, $g^n = e$. □

Теперь с помощью этих утверждений докажем *малую теорему Ферма* и *теорему Эйлера*.

Теорема 8.6 (малая теорема Ферма)**.** *Для любого целого числа a, не делящегося на простое p*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Доказательство. Рассмотрим мультипликативную группу $\mathbb{Z}_p^*$. Это абелева группа порядка $p-1$. Следовательно, $g^{p-1} = 1$ для любого элемента $g \in \mathbb{Z}_p^*$, что и является утверждением теоремы, если учесть, что для $g_1, g_2 \in \mathbb{Z}_p^*$ равенство $g_1 = g_2$ по определению означает $a_1 \equiv a_2 \pmod{p}$, где $a_1 \in [g_1], a_2 \in [g_2]$. □

Для любого n порядок мультипликативной группы $\mathbb{Z}_n^*$ обратимых элементов $\mathbb{Z}_n$, равный количеству чисел в последовательности $1, 2, \ldots, n$, взаимно простых с n, обозначается через $\varphi(n)$. Функция φ, определённая таким образом на множестве натуральных чисел, называется *функцией Эйлера*.

Теорема 8.7 (Эйлера)**.** *Для любого целого числа a, взаимно простого с n*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Доказательство. Как видно, это обобщение малой теоремы Ферма. Для доказательства достаточно применить следствие 8.5 теперь уже к группе $\mathbb{Z}_n^*$. □

9 Орбиты, стабилизаторы

Разбиение на смежные классы естественно возникает при изучении групп преобразований.

Определение 9.1. Пусть G — группа преобразований множества X (будем говорить, что группа G *действует на множестве* X). Для любых $g \in G, x \in X$ обозначим за gx точку, являющуюся образом точки x при преобразовании g. Будем говорить, что точки $x, y \in X$ эквивалентны относительно G, и писать $x \underset{G}{\sim} y$, если существует такой элемент $g \in G$, что $y = gx$.

Нетрудно показать, что это отношение эквивалентности.

Определение 9.2. Класс эквивалентности точки $x \in X$ называется её *орбитой*. Иначе говоря, орбита точки x есть множество

$$Orb(x) = \{gx : g \in G\}.$$

Определение 9.3. В группе G подгруппа

$$St(x) = \{g \in G : gx = x\}$$

называется *стабилизатором* точки x.

Пример 9.1. В группе подстановок S_n множества $M = \{1, 2, \ldots, n\}$ орбитой точки k является всё множество M, а стабилизатором — множество всех подстановок, оставляющих k на месте, т.е. имеющих вид

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & k-1 & k & k+1 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(k-1) & k & \sigma(k+1) & \ldots & \sigma(n) \end{pmatrix},$$

т.е. $\sigma(k) = k$. Таких подстановок, очевидно, $(n-1)!$.

Теорема 9.1. *Имеется взаимно однозначное соответствие между орбитой $Orb(x)$ и множеством смежных классов $G/St(x)$, при котором точке $y = gx \in Orb(x)$ соответствует смежный класс $gSt(x)$.*

Доказательство. При $g_1, g_2 \in G$ имеем

$$g_1 \equiv g_2 \pmod{St(x)} \iff g_1^{-1} g_2 \in St(x) \iff g_1^{-1} g_2 x = x \iff g_1 x = g_2 x.$$

Таким образом, элементы одного смежного класса группы G по $St(x)$ характеризуются тем, что они переводят точку x в одну и ту же точку. Более точно, все элементы смежного класса $gSt(x)$, и только они переводят точку x в точку $y = gx$. Тем самым и установлено искомое соответствие. □

Число элементов орбиты $Orb(x)$, если оно конечно, называется её *длиной* и обозначается $|Orb(x)|$.

Следствие 9.2. *Если G — конечная группа, то*

$$|G| = |Orb(x)||St(x)|.$$

Из этой формулы следует, что порядки стабилизаторов всех точек орбиты одинаковы.

Пусть группа G действует на множестве X. Тогда X разбивается на непересекающиеся орбиты. Часто бывает необходимо найти количество орбит. В этом может помочь следующая

Лемма 9.3 (Бернсайда)**.** *Количество орбит в X равно $\frac{1}{|G|}\sum\limits_{g\in G}|Fix(g)|$, где $Fix(g) = \{x \in X : gx = x\}$.*

Доказательство.

$$\frac{1}{|G|}\sum_{g\in G}|Fix(g)| = \frac{1}{|G|}\sum_{g\in G}\sum_{x\in X}\{gx = x\} =$$
$$= \frac{1}{|G|}\sum_{x\in X}\sum_{g\in G}\{gx = x\} = \frac{1}{|G|}\sum_{x\in X}|St(x)| = \sum_{x\in X}\frac{1}{|Orb(x)|},$$

где $\{gx = x\}$ равно 1, если равенство выполняется, 0 в противном случае. Последнее равенство вытекает из следствия 9.2. Вспомним, что множество X распадается на непересекающиеся орбиты. В последней сумме выполним суммирование сначала внутри каждой орбиты, а затем по всем орбитам. В сумме внутри орбиты получаем мощность орбиты, которая сокращается с $\frac{1}{|Orb(x)|}$, и остаётся только сумма $\sum 1$ по всем орбитам, т.е. количество орбит. □

10 Нормальные подгруппы

Определение 10.1. Подгруппа H группы G называется *нормальной*, если

$$gH = Hg \qquad \forall g \in G$$

или, что эквивалентно,

$$gHg^{-1} = H \qquad \forall g \in G.$$

В этом случае пишут $H \lhd G$ (или $G \rhd H$).

Для того, чтобы подгруппа H была нормальной, достаточно (но не необходимо), чтобы каждый элемент группы G был перестановочен с каждым элементом из H. В частности, в абелевой группе любая подгруппа нормальна.

Теорема 10.1. *Отношение сравнимости по модулю подгруппы H согласовано с операцией умножения в группе G тогда и только тогда, когда подгруппа H нормальна.*

Доказательство. Согласованность отношения сравнимости по модулю H с операцией умножения означает следующее:

$$g_1 \equiv g_1' \pmod{H}, \qquad g_2 \equiv g_2' \pmod{H} \implies g_1 g_2 \equiv g_1' g_2' \pmod{H}.$$

Последнее условие, согласно определению, переписывается в виде

$$g_2^{-1} h_1 g_2 \in H.$$

Так как g_2 может быть любым элементом группы G, а h_1 — любым элементом подгруппы H, то это равносильно условию нормальности. □

Если $H \lhd G$, то операция умножения в группе G определяет операцию умножения в множестве G/H по правилу

$$(g_1 H)(g_2 H) = g_1 g_2 H.$$

Эта операция наследует ассоциативность операции в группе G. Для неё имеется единица — смежный класс eH. Каждый смежный класс gH имеет обратный, а именно $g^{-1}H$. Следовательно, G/H — группа.

Определение 10.2. Группа G/H, где $H \lhd G$, называется *факторгруппой* группы G по H.

Очевидно, что если группа абелева, то любая её факторгруппа также абелева.

Пример 10.1. Факторгруппа $\mathbb{Z}/n\mathbb{Z}$ есть группа вычетов $\mathbb{Z}_n$.

Пример 10.2. Смежными классами группы $\mathbb{C}$ по $\mathbb{R}$ являются прямые $L_a = \{z : \operatorname{Im} z = a\}$ $(a \in \mathbb{R})$. Операция сложения в $\mathbb{C}/\mathbb{R}$ задаётся формулой $L_a + L_b = L_{a+b}$, так что факторгруппа $\mathbb{C}/\mathbb{R}$ изоморфна группе $\mathbb{R}$ $(\mathbb{C}/\mathbb{R} \cong \mathbb{R})$.

Пример 10.3. Смежными классами группы $\mathbb{C}^*$ по $\mathbb{T}$ (напомним, что $\mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$) являются окружности $C_r = \{z \in \mathbb{C}^* : |z| = r\}$ $(r > 0)$. Операция умножения в $\mathbb{C}^*/\mathbb{T}$ задаётся формулой $C_r C_s = C_{rs}$, так что $\mathbb{C}^*/\mathbb{T} \cong \mathbb{R}_+^*$.

11 Гомоморфизмы, изоморфизмы

Если внимательно присмотреться, то можно заметить, что многие алгебраические структуры, в частности, группы, имеют значительные сходства в строении. Более того, многие группы имеют одинаковые свойства, разница лишь в обозначениях. К примеру, чем кардинально отличаются аддитивные группы $\mathbb{Z}$ и $2\mathbb{Z}$? $5\mathbb{Z}$ и $2\mathbb{Z}$? Правильный ответ — ничем. Это на самом деле одна и та же группа, только элементы обозначаются по-разному. $\mathbb{Z}_2$ и S_2 тоже на самом деле представляют собой одну и ту же группу.

Сейчас мы увидим, что такие сходства можно формализовать.

Определение 11.1. *Гомоморфизмом* группы $(G, *)$ в группу $(H, \circ)$ называется отображение $f : G \to H$, удовлетворяющее условию

$$f(a * b) = f(a) \circ f(b) \qquad \forall a, b \in G.$$

Имеют место простейшие свойства гомоморфизмов групп.

1) $f(e_G) = e_H$. В самом деле, пусть $f(e_G) = h \in H$; тогда

$$h^2 = f(e_G)^2 = f(e_G^2) = f(e_G) = h,$$

откуда $h = e_H$.

2) $f(a^{-1}) = f(a)^{-1}$, ибо

$$f(a) \circ f(a^{-1}) = f(a * a^{-1}) = f(e_G) = e_H.$$

Определение 11.2. *Изоморфизмом* группы $(G, *)$ в группу $(H, \circ)$ называется биективный гомоморфизм $f : G \to H$ (т.е. взаимно однозначное отображение группы G в группу H, являющееся гомоморфизмом). Соответственно, группы называют изоморфными, если между ними существует изоморфизм, часто пишут $G \cong H$.

Важным примером изоморфизмов групп является следующая

Теорема 11.1. *Всякая бесконечная циклическая группа изоморфна группе $\mathbb{Z}$. Всякая конечная циклическая группа порядка n изоморфна группе $\mathbb{Z}_n$.*

Доказательство. Если $G = \langle g \rangle$ — бесконечная циклическая группа, то в силу формулы (1) отображение $f : \mathbb{Z} \to G, k \mapsto g^k$, есть изоморфизм.

Пусть $G = \langle g \rangle$ — конечная циклическая группа порядка n. Рассмотрим отображение

$$f : \mathbb{Z}_n \to G, \quad [k] \mapsto g^k \quad (k \in \mathbb{Z}).$$

Так как

$$[k] = [l] \quad \Longleftrightarrow \quad k \equiv l \pmod{n} \quad \Longleftrightarrow \quad g^k = g^l,$$

то отображение f корректно определено и биективно. Свойство $f(k+l) = f(k)f(l)$ вытекает из той же формулы (1). Таким образом, f — изоморфизм. □

Таким образом, $\mathbb{Z} \cong n\mathbb{Z} \quad \forall n \in \mathbb{N}$, $\mathbb{Z}_2 \cong S_2$, но $\mathbb{Z}_3 \ncong S_3$.

Элементы групп и операции могут называться по-разному, но если группы изоморфны, то с точки зрения алгебры эти группы одинаковы, так как совпадают *свойства операций*. Вообще, если две алгебраические структуры изоморфны, то любое утверждение, формулируемое только в терминах заданных операций, будет справедливым в одной из этих структур тогда и только тогда, когда оно справедливо в другой.

Поэтому в принципе всё равно, какую из изоморфных друг другу алгебраических структур (в нашем случае — групп) изучать: все они являются различными моделями одного и того же объекта. Однако выбор модели может оказаться небезразличным для фактического решения какой-либо задачи. Определённая модель может предоставить для этого наибольшее удобство. Например, если какая-то модель имеет геометрический характер, то она позволяет применить геометрические методы.

Список литературы

[1] Э. Б. Винберг, *Курс алгебры*. Новое издание, переработанное и дополненное. МЦНМО, Москва, 2011.

[2] А. Г. Курош, *Курс высшей алгебры*. Издание девятое. Издательство «Наука», Москва, 1968.

[3] А. А. Михалёв, А. В. Михалёв, *Начала алгебры, часть I*. Интернет-университет информационных технологий - ИНТУИТ.ру, Москва, 2005.

[4] А. И. Кострикин, *Введение в алгебру. Часть I. Основы алгебры*. Третье издание. ФИЗМАТЛИТ, Москва, 2004.