

Группы 1

Определения и примеры

— А у меня, — говорит Большой Боб, — хорошие новости.
А куда все подевались?
— Это и есть хорошие новости, — говорит Большой Боб.
— Группа расформирована. Я пришёл сюда на всякий случай,
чтобы сообщить это тем, кто ещё не знает.
Я падаю, закрыв глаза, на одну из кушеток из магазина для
бедных.
— Хорошие новости, — уточняет Большой Боб, — это то,
что вместо неё создана другая группа, первое правило кото-
рой — никому о ней не говорить.

"Бойцовский клуб", Чак Паланик.

Определение 1. Пара $(G, \circ)$, где G — множество, а $\circ$ — бинарная операция на этом множестве (то есть функция от двух аргументов из множества G , принимающая значение в этом же множестве: $\circ : G \times G \rightarrow G$), называется *группой*, если выполнены следующие три условия:

1. $\forall a, b, c \in G \quad (a \circ b) \circ c = a \circ (b \circ c)$ — ассоциативность;
2. $\exists e \in G \quad \forall a \in G \quad a \circ e = e \circ a = a$ — существование единицы;
3. $\forall a \in G \quad \exists b \in G \quad a \circ b = b \circ a = e$ — обратимость.

Элемент e часто называют *единицей*, а элемент b из свойства 3 — *обратным* к элементу a и обозначают a^{-1} . Для краткости речи обычно само множество G (наряду с парой $(G, \circ)$) называют группой, если из контекста понятно, о какой операции идёт речь (например, если на множестве G задана одна-единственная операция).

Определение 2. Группа $(G, \circ)$ называется *абелевой* или *коммутативной*, если в ней, кроме прочих, выполнено ещё одно условие

4. $\forall a, b \in G \quad a \circ b = b \circ a$ — коммутативность.

Замечание. Понятно, что групповая операция не всегда обозначается кружочком (равно как и групповое множество не обязательно обозначается буквой G). Согласно традиции для некоммутативных групп часто используется *мультипликативная запись*, то есть операция обозначается как обычное умножение, единица обозначается e или даже 1, обратный элемент обозначается g^{-1} . Для коммутативных же групп обычно используется *аддитивная запись*, то есть операция обозначается плюсом, единица называется *нулём* и обозначается 0, а обратный элемент обозначается $-g$. Существуют и другие виды записи.

В дальнейшем, если не оговорено противное, мы будем использовать мультипликативную запись.

Задача 1. Докажите, что в любой группе для любых двух элементов a и b выполнено $(ab)^{-1} = b^{-1}a^{-1}$.

Задача 2. Докажите, что в группе не может быть двух единиц, то есть двух различных элементов, удовлетворяющих пункту 2 определения группы.

Задача 3. Докажите, что у любого элемента группы не может быть двух обратных, то есть двух различных элементов, удовлетворяющих пункту 3 определения группы.

Пример 1. Простейшим примером группы является $(\mathbb{R}, +)$, где $+$ обозначает обычное сложение.

Задача 4. Какие из следующих пар являются группами (везде $+$ обозначает обычное сложение):

а). $(\mathbb{N}, +)$, б). $(\mathbb{Z}, +)$, в). $(2\mathbb{Z}, +)$, где $2\mathbb{Z} = \{2z \mid z \in \mathbb{Z}\}$, д). $(\{-1, 0, 1\}, +)$, е). $(\mathbb{Q}, +)$, ф). $(\mathbb{R}^*, +)$, где $\mathbb{R}^* = \{x \in \mathbb{R} : x \neq 0\}$, г). $(\mathbb{R}^+, +)$, где $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$, h). $(\mathbb{R}_+, +)$, где $\mathbb{R}_+ = \{x \in \mathbb{R} : x \geq 0\}$?

Пример 2. Другим важным примером группы является множество векторов на плоскости с операцией сложения: $(\mathbb{R}^2, +)$.

Задача 5. Является ли $(\mathbb{R}^3, +)$ группой, где $\mathbb{R}^3$ — множество векторов в пространстве?

Пример 3. Вы также знакомы с группами относительно умножения, например, с $(\mathbb{R}^*, \cdot)$.

Задача 6. Какие из следующих пар являются группами (везде $\cdot$ обозначает обычное умножение; смысл индексов у букв $\mathbb{Z}$ и $\mathbb{Q}$ такой же, как и у $\mathbb{R}$ в задаче 4) а). $(\mathbb{N}, \cdot)$, б). $(\mathbb{Z}, \cdot)$, в). $(2\mathbb{Z}, \cdot)$, д). $(\mathbb{Z}^*, \cdot)$, е). $(\{-1, 0, 1\}, \cdot)$, ф). $(\{-1, 1\}, \cdot)$, г). $(\{\frac{1}{2}, 1, 2\}, \cdot)$, h). $(\mathbb{Q}, \cdot)$, i). $(\mathbb{Q}^*, \cdot)$, j). $(\mathbb{Q}^+, \cdot)$, k). $(\mathbb{Q}_+, \cdot)$?

Задача 7. Является ли пара $(\mathbb{R}^2, \cdot)$, где $\cdot$ обозначает скалярное произведение векторов, группой?

Пример 4. Группа $(\{e\}, \cdot)$ из одного элемента — единицы — называется *тривиальной*.

Упражнение. Поймите, как устроено умножение в тривиальной группе.

Задача 8. Существуют ли группы с пустым групповым множеством?

ПРИМЕР 5. Задавать группы можно по-разному. Один из способов — в явном виде перечислить все элементы группового множества и в явном виде выписать для них полную таблицу умножения. Введём по такому методу *четверную группу Клейна* $(V_4, \cdot)$ следующим образом: $V_4 = \{e, a, b, c\}$, а таблица умножения имеет следующий вид:

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

Задача 9. Докажите, что четверная группа Клейна действительно является группой. Является ли это группа абелевой?

Задача 10. Докажите, что для любой группы таблица умножения без заголовочных строки и столбца будет обладать следующим свойством: в каждой строке и в каждом столбце каждый элемент группы встречается ровно один раз.

ПРИМЕР 6. Другой способ описания группы состоит в следующем. Вводят несколько элементов группы, называемых *образующими* и некие равенства, связывающие их и, возможно, единицу, — *образующие соотношения*. Чтобы получить по этим данным все остальные элементы группы надо делать следующие операции: перемножать в различных комбинациях и брать обратные от уже полученных элементов, начиная с образующих, производя везде, где возможно, сокращения согласно образующим соотношениям. Этот процесс необходимо продолжать до тех пор, пока все элементы группы не будут получены. Рассмотрим пример: пусть дан только один образующий элемент z и одно образующее соотношение $z^5 = e$. Начав с элемента z проделывать описанные выше операции, мы можем получить любой элемент вида z^n , $n \in \mathbb{Z}$ и больше ничего. Однако, согласно теореме о делении с остатком, любое $n \in \mathbb{Z}$ можно представить в виде $n = 5q + r$, где $q, r \in \mathbb{Z}$, $0 \leq r < 5$. Поэтому, произведя k раз сокращения в соответствии с образующим соотношением, получим, что $z^n = z^r$, где $0 \leq r < 5$, причём это верно для любого n . Отсюда следует, что всё групповое множество нашей группы состоит из пяти элементов и имеет вид: $\{z^0 = e, z^1 = z, z^2, z^3, z^4\}$. Такая группа называется *циклической группой* порядка 5 и обозначается Z_5 (или, более формально, $(Z_5, \cdot)$); однако мы будем всё реже использовать эту формально более правильную, но слишком громоздкую форму записи; тем не менее о ней следует помнить). Нетрудно догадаться, что, если заменить образующее соотношение на $z^n = e$ для любого натурального числа n , то получится группа Z_n , состоящая из n элементов и называемая *циклической группой* порядка n . Если же образующих соотношений нет, то группа с одним образующим имеет бесконечное число элементов: $\{\dots, z^{-2}, z^{-1}, e, z, z^2, \dots\}$ и называется *циклической группой* бесконечного порядка.

Задача 11. Любая группа с одним образующим элементом является циклической.

ПРИМЕР 7. Введём теперь с помощью образующих соотношений *симметрическую* группу степени 3, обозначаемую S_3 . У нас будет два образующих элемента — a и b — и три образующих соотношения: $a^2 = e$, $b^2 = e$, $(ab)^3 = e$.

Задача 12. Выпишите все элементы группы S_3 . Сколько их?

ПРИМЕР 8. Ещё один способ описания группы мы так и назовём — описательным. Например, пусть на плоскости дан квадрат. Рассмотрим его симметрии. Их восемь: тождественное преобразование (то есть преобразование, оставляющее все точки на месте; его также можно рассматривать как поворот относительно центра квадрата на 0°), ещё три поворота относительно центра квадрата — на 90° , 180° и 270° , две симметрии относительно диагоналей и ещё две симметрии относительно прямых, проходящих через середины противоположных сторон квадрата. Эти преобразования составляют группу D_4 называемую *группой диэдра-4*.

Задача 13. Пусть z и d — элементы группы D_4 , z — поворот на 90° , а d — симметрия относительно одной из диагоналей. Запишите остальные элементы группы D_4 в виде произведений элементов z и d и, возможно, обратных к ним.

Задача 14. Запишите три образующих соотношения на элементы z и d : одно только на z , второе только на d , а третье на оба сразу.

Задача 15. Достаточно ли двух образующих z и d и трёх образующих соотношений, которые вы придумали в прошлой задаче, чтобы задать группу D_4 по методу образующих соотношений? Если нет, то измените (дополните) список образующих соотношений, чтобы это было выполнено.

ПРИМЕР 9. В общем случае, *группа диэдра- n* , при $n \geq 3$, обозначаемая D_n , — это группа симметрий правильного n -угольника на плоскости.

Задача 16. Подсчитайте количество элементов в группе D_n , $n \geq 3$.

Задача 17. Дайте разумное определение группы D_2 .