Группы

Множество G, на котором определена (бинарная[1]) операция $\circ : G \times G \to G$ называется *группой*, если выполнены следующие три условия:

- *(ассоциативность)* для любых $a, b, c \in G$ верно равенство $a \circ (b \circ c) = (a \circ b) \circ c$.
- *(нейтральный элемент)* существует $e \in G$ такой, что $e \circ a = a \circ e = a$ для всех $a \in G$.
- *(обратимость)* для любого $a \in G$ существует $a^{-1} \in G$ такой, что $a^{-1} \circ a = a \circ a^{-1} = e$.

Группа G называется *абелевой (коммутативной)*, если

- *(коммутативность)* для любых $a, b \in G$ верно равенство $a \circ b = b \circ a$.

Примеры

1. Для следующих пар, состоящих из множества и операции, определите, какие из них являются группами, а какие — нет: $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$.

Как показывают следующие примеры, группы не обязательно бесконечны. Для произвольного натурального числа $n > 1$ через $\mathbb{Z}_n$ обозначим набор $\{0, 1, \ldots, n-1\}$, в котором операции сложения и умножения проводятся по модулю n.

2. Докажите, что $\mathbb{Z}_n$ с операцией сложения является группой.
3. Докажите, что $\mathbb{Z}_n \setminus \{0\}$ — группа по умножению, если и только если n простое.

Все рассмотренные нами ранее группы были абелевы. Обозначим через S_3 множество всех симметрий и поворотов, переводящих правильный треугольник в себя.

4. Составьте таблицу умножения в S_3 и проверьте, что эта группа неабелева.
5. Рассмотрим множество всех непостоянных линейных функций с операцией „взятие композиции”. Докажите, что это множество является неабелевой группой.

Следующие простейшие свойства присущи всем группам:

6. Докажите, что в любой группе нейтральный элемент единственен.
7. Докажите, что у любого элемента группы обратный к нему определён однозначно.

Кольца

Для абелевых групп операцию $\circ$ часто обозначают зна́ком $+$, единичный элемент e — через 0, а обратный a^{-1} — через $-a$. Мы будем использовать это обозначение, если требуется подчеркнуть, что рассматриваемая группа абелева. Множество K, на котором определены две бинарные операции: „$+$” и „$\cdot$” называется *кольцом*, если $(K, +)$ — абелева группа, операция „$\cdot$” ассоциативна и выполняется следующий закон:

- *(дистрибутивность)* для любых $a, b, c \in V$ верны равенства: $(a + b) \cdot c = a \cdot c + b \cdot c$ и $a \cdot (b + c) = a \cdot b + a \cdot c$.

Кольцо называется *коммутативным*, если коммутативна операция „$\cdot$”. Если в кольце для операции „$\cdot$” есть нейтральный элемент, его принято обозначать 1 и говорят, что данное кольцо *с единицей*.

Примеры

8. Для следующих троек, состоящих из множества и двух операций операции, определите, какие из них являются кольцами, а какие — нет: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$.

Следующие простейшие свойства присущи всем кольцам:

9. Докажите, что в любом кольце $x \cdot 0 = 0 \cdot x = 0$.
10. Докажите, что в любом кольце $x \cdot (-1) = (-1) \cdot x = -x$.

[1] Операция называется **бинарной**, если она по сопоставляет упорядоченной паре двух элементов множества некоторый элемент множества.

Основная теорема арифметики

Элемент $a \neq 0$ кольца называется *делителем нуля*, если существует $b \neq 0$ такой, что $ab = 0$. Коммутативное кольцо с единицей и без делителей нуля называется **целостным**. В этом и следующем разделах будут рассматриваться только целостные кольца.

Ненулевой элемент a называется *неприводимым*[2], если не существует его представления в виде $a = bc$, где элементы b и c необратимы. Таким образом, все ненулевые элементы разбиваются на три вида: обратимые, неприводимые и приводимые. Кольцо называется *факториальным*, если в нём верна основная теорема арифметики, а именно, любой ненулевой необратимый элемент раскладывается в произведение неприводимых элементов однозначно с точностью до порядка их следования и умножения на обратимый элемент.

Кольцо K называется *евклидовым*, если на нём определена евклидова норма — такая функция $d\colon K \setminus \{0\} \to \mathbb{N}_0$, что для любых ненулевых элементов a и b возможно деление с остатком, т. е. есть равенство $a = bq + r$, где $d(r) < d(b)$ или $r = 0$. Например, в $\mathbb{Z}$ евклидовой нормой является взятие модуля.

При доказательстве основной теоремы алгебры мы пользовались только алгоритмом Евклида, т. е. все доказательства остаются верными для любого евклидового кольца. Таким образом, все евклидовы кольца факториальны.

Нефакториальные кольца

Приведём пример того, что в неевклидовых кольцах разложение на неприводимые множители не всегда однозначно. Рассмотрим множество $\mathbb{Z}[i\sqrt{3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$. Хотя это — формальные записи (мы никак не определяли, что такое $\sqrt{-3}$), введём на этом множестве операции сложения, вычитания и умножения и будем называть их числами. Сложение и вычитание зададим равенствами $(a + b\sqrt{-3}) \pm (c + d\sqrt{-3}) = (a \pm c) + (b \pm d)\sqrt{-3}$, а умножение — $(a + b\sqrt{-3}) \cdot (c + d\sqrt{-3}) = (ac - 3bd) + (ad + bc)\sqrt{-3}$. Нетрудно видеть, что кольцо $\mathbb{Z}[i\sqrt{3}]$ факториально.

11. Найдите все неприводимые в $\mathbb{Z}[i\sqrt{3}]$ элементы.
12. Покажите, что число $\mathbf{3} = 3 + 0 \cdot \sqrt{-3}$ приводимое.
13. Приводимым или неприводимым является число $\mathbf{2} = 2 + 0 \cdot \sqrt{-3}$?
14. Верно ли, что любое число из $\mathbb{Z}[i\sqrt{3}]$ можно представить в виде произведения степеней различных неприводимых чисел?
15. Придумайте пример числа из $\mathbb{Z}[i\sqrt{3}]$, которое имеет два различных представления в виде произведения неприводимых множителей (эти разложения должны отличаться хотя бы одним неприводимым множителем).
16. Наибольшим общим делителем двух чисел $\mathbb{Z}[i\sqrt{3}]$ назовём такой их общий делитель, который делится на любой другой их общий делитель. Можно ли утверждать, что для любых двух чисел определён их НОД (с точностью до обратимого множителя)?

[2] Аналог простого числа в $\mathbb{Z}$.