Группы

Множество G, на котором определена операция $\circ : G \times G \to G$ называется *группой*, если выполнены следующие три условия:

• **ассоциативность:** $a \circ (b \circ c) = (a \circ b) \circ c$ для любых $a, b, c \in G$;

• существует $e \in G$ такой, что $e \circ a = a \circ e = a$ для всех $a \in G$;

• для любого $a \in G$ существует $a^{-1} \in G$ такой, что $a^{-1} \circ a = a \circ a^{-1} = e$.

Элемент e называется *нейтральным*, а a^{-1} – *обратным к* a.

Группа G называется *абелевой (коммутативной)*, если ещё и

• для любых $a, b \in G$ верно равенство $a \circ b = b \circ a$.

Вообще говоря, группа обобщает понятие „множество G, наделённое бинарной операцией $\circ$ такой, что для любых $a, b \in G$ уравнения $a \circ x = b$ и $x \circ a = b$ всегда имели ровно по одному решению каждое". В абелевой группе решения этих двух уравнений совпадают.

1. Для следующих пар, состоящих из множества и операции, определите, какие из них являются группами, а какие — нет: $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_n \setminus \{0\}, \cdot)$.
2. Докажите, что множество всех непостоянных линейных функций с операцией „взятие композиции" является неабелевой группой.
3. Обозначим через S_3 множество всех симметрий и поворотов, переводящих правильный треугольник в себя. Составьте таблицу умножения в S_3 и проверьте, что эта группа неабелева.
4. Докажите, что в группе нейтральный элемент единственен.
5. Докажите, что в группе обратный элемент определён однозначно.

Кольца

Для абелевых групп операцию $\circ$ обозначают зна́ком $+$, единичный элемент e – через 0, а обратный a^{-1} – через $-a$. Множество R, на котором определены две бинарные операции: „$+$" и „ $\cdot$ " называется *кольцом*, если $(R, +)$ – абелева группа, а операция „ $\cdot$ " ассоциативна и выполнена

• **дистрибутивность:** $(a + b) \cdot c = a \cdot c + b \cdot c$ и $a \cdot (b + c) = a \cdot b + a \cdot c$ для любых $a, b, c \in R$.

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

6. Для следующих троек, состоящих из множества и двух операций операции, определите, какие из них являются кольцами, а какие – нет: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$, $(\mathbb{Z}[x], +, \cdot)$.
7. Пусть M – произвольное множество, а V – множество всех его подмножеств. Докажите, что $(V, \triangle, \cap)$ – кольцо.
8. Докажите, что в кольце $x \cdot 0 = 0 \cdot x = 0$ и $x \cdot (-1) = (-1) \cdot x = -x$.

Обобщаем понятие простых чисел

Элемент $a \neq 0$ кольца R называется *делителем нуля*, если существует $b \neq 0$ такой, что $ab = 0$. Коммутативное кольцо с единицей и без делителей нуля называется *целостным.*

Ненулевой элемент ε целостного кольца R называется *единицей*, если $\varepsilon^{-1} \in R$. Элементы $a, b \in R$ называются *ассоциированными*, если $a = \varepsilon b$ для некоторой единицы ε. Ненулевой элемент называется *неразложимым*, если каждый его делитель либо ассоциирован с ним, либо является единицей. Наконец, ненулевой и неединичный элемент $a \in R$ называется *простым*, если из $a \mid bc$, $b, c \in R$, следует, что $a \mid b$ или $a \mid c$.

9. Что собой представляют единичные, неразложимые и простые элементы кольца $(\mathbb{Z}[x], +, \ \cdot\ )$?

Факториальные кольца

Кольцо R называется *евклидовым*, если на нём определена евклидова норма – функция $d\colon R\backslash\{0\} \to \mathbb{N}_0$ такая, что для любых $a, b \neq 0$ возможно деление с остатком: есть равенство $a = bq + r$, где $d(r) < d(b)$ или $r = 0$.

Целостное кольцо называется *факториальным*, если в нём верна основная теорема арифметики: каждый необратимый ненулевой элемент представляется в виде произведения неприводимых элементов однозначно с точностью до порядка следования множителей и единиц.

При доказательстве основной теоремы арифметики в $\mathbb{Z}$ используется только существование евклидовой нормы $|\cdot|$ в $\mathbb{Z}$ (алгоритмом Евклида), аналогичные доказательства подходят для любого евклидового кольца. В частности, факториальны $\mathbb{Q}[x]$ и $\mathbb{R}[x]$.

Нефакториальные кольца

Рассмотрим множество $\mathbb{Z}[i\sqrt{3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$. Сложение и вычитание определим как $(a+b\sqrt{-3}) \pm (c+d\sqrt{-3}) = (a \pm c) + (b \pm d)\sqrt{-3}$, а умножение – $(a + b\sqrt{-3}) \cdot (c + d\sqrt{-3}) = (ac - 3bd) + (ad + bc)\sqrt{-3}$.

10. Найдите все обратимые в $\mathbb{Z}[i\sqrt{3}]$ элементы.
11. Являются ли приводимыми числа $\mathbf{3} = 3 + 0 \cdot \sqrt{-3}$ и $\mathbf{2} = 2 + 0 \cdot \sqrt{-3}$?
12. Верно ли, что любое число из $\mathbb{Z}[i\sqrt{3}]$ можно представить в виде произведения степеней различных неприводимых чисел?
13. Можно ли утверждать, что это разложение всегда единственно?
14. Наибольшим общим делителем двух чисел – это такой их общий делитель, который делится на любой другой их общий делитель. Можно ли утверждать, что для любых двух чисел из $\mathbb{Z}[i\sqrt{3}]$ определён НОД?
15. Верно ли, что: 1) каждое простое число является неразложимым; 2) каждое неразложимое число является простым.