Кольца и поля

Чтобы подступиться к группам начнём сначала с полей и колец — они наиболее похожи на обычные числа по своей структуре. Дадим сначала определения:

Группой G называется множество G с заданной на нём операцией «умножения» $\cdot : G \times G \to G$, удовлетворяющей следующим аксиомам:

I. Существует нейтральный элемент 1, такой, что

$$1 \cdot g = g \cdot 1 = g, \ \forall g \in G,$$

II. Для любого элемента группы существует обратный, т. е.

$$\forall g \in G \ \exists g^{-1} \in G \ : \ g \cdot g^{-1} = g^{-1} \cdot g = 1,$$

III. Справедлива ассоциатоивность:

$$a(bc) = (ab)c.$$

Множество, удовлетворяющее только пункту **III.** определения группы называется *полугруппой.*

Полугруппа с нейтральным элементом называется *моноидом.*

Кольцом R (коммутативным ассоциативным с единицей) называется множество с двумя операциями «+» и «-», такими, что относительно сложения R — абелева группа, а относительно умножения R — моноид, причём справедлива дистрибутивность: $a \cdot (b + c) = a \cdot b + a \cdot c$, $(b + c) \cdot a = b \cdot a + c \cdot a$.

Телом T называется кольцо, каждый ненулевой элемент которого обратим по умножению.

Поле F — коммутативное тело. Примеры колец: целые числа $\mathbb{Z}$, остатки $\mathbb{Z}_n$, многочлены $\mathbb{R}[x]$.

Примеры полей: рациональные ($\mathbb{Q}$), действительные ($\mathbb{R}$) и комплексные ($\mathbb{C}$) числа, остатки по простому модулю (см. задачу 3), рациональные функции $\mathbb{Q}(x) = \left\{ \frac{P(x)}{Q(x)} | \ P, Q \in \mathbb{Q}[x], \ Q \neq 0 \right\}$.

1. Докажите, что в любом кольце $0 \cdot x = x \cdot 0 = 0$ для любого x.

2. Докажите, что кольцо остатков $\mathbb{Z}_n$ является полем тогда и только тогда, когда n — простое.

3. Какие элементы обратимы в кольцах $\mathbb{Z}_4, \ \mathbb{Z}_6, \ \mathbb{Z}_n$? Найдите делители нуля.

Будем через $R[\sqrt{d}]$, где R кольцо и $d \in R$, обозначать множество формальных выражений $\{a + b\sqrt{d} | \ a, b \in R\}$ с «обычными» сложением и умножением. Можно проверить, что $R[\sqrt{d}]$ — это кольцо. Например, $\mathbb{R}[\sqrt{-1}] = \mathbb{C}$ — поле комплексных чисел.

4. Найдите все обратимые элементы кольца гауссовых чисел $\mathbb{Z}[\sqrt{-1}]$.

5. Докажите, что в поле $\mathbb{Z}_p$ верно «правило двоечника»: $(a + b)^p = a^p + b^p$.

6. Найдите все такие d, что $\mathbb{Q}[\sqrt{d}]$ — поле.

7. Решите в $\mathbb{Z}_p$ уравнение $x^2 = 1$, вычислите произведение всех ненулевых элементов поля $\mathbb{Z}_p$ и докажите теорему Вильсона: если p — простое, то $(p - 1)! + 1$ делится на p.