Серия 4. Поля

Множество $\mathbb{F}$ с заданными на нём операциями $+\colon \mathbb{F}\times\mathbb{F}\to\mathbb{F}$ и $\cdot\colon \mathbb{F}\times\mathbb{F}\to\mathbb{F}$ называется *полем*, если выполнены следующие *аксиомы поля*:
(1) $\forall a,b\in\mathbb{F}\colon\ a+b=b+a$ (коммутативность сложения)
(2) $\forall a,b,c\in\mathbb{F}\colon\ a+(b+c)=(a+b)+c$ (ассоциативность сложения)
(3) В $\mathbb{F}$ существует такой элемент 0, что $\forall a\in\mathbb{F}\colon\ a+0=0$ (существование нейтрального элемента по сложению)
(4) $\forall a\in\mathbb{F}\ \ \exists b\in\mathbb{F}\colon\ a+b=0$ (существование противоположного элемента)
(5) $\forall a,b\in\mathbb{F}\colon\ a\cdot b=b\cdot a$ (коммутативность умножения)
(6) $\forall a,b,c\in\mathbb{F}\colon\ a\cdot(b\cdot c)=(a\cdot b)\cdot c$ (ассоциативность умножения)
(7) В $\mathbb{F}$ существует такой отличный от 0 элемент 1, что $\forall a\in\mathbb{F}\colon\ a\cdot 1=a$ (существование нейтрального элемента по умножению)
(8) $\forall a\in\mathbb{F}\backslash\{0\}\ \ \exists b\in\mathbb{F}\colon\ a\cdot b=1$ (существование обратного элемента)
(9) $\forall a,b,c\in\mathbb{F}\colon\ a\cdot(b+c)=a\cdot b+a\cdot c$ (дистрибутивность умножения относительно сложения)

Нейтральный элемент по сложению принято называть *нулём*, нейтральный элемент по умножению – *единицей*. Противоположный к a элемент обозначатся как $-a$, обратный к a – как $1/a$ или a^{-1}. Точку, обозначающую умножение, мы часто будем опускать.

1. Определите, какие из следующих множеств являются полями (относительно естественных операций сложения и умножения): $\mathbb{Z}$; $\mathbb{Q}$; $\mathbb{R}$; $\mathbb{R}_{\geqslant 0}$ (неотриц. действительные числа); $\mathbb{C}$; $\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}\subset\mathbb{C}$. При каких натуральных m множество $\mathbb{Z}/m\mathbb{Z}$ остатков по модулю m является полем?

2. Выведите из аксиом поля, что для любого поля выполнены следующие свойства (все буквы – произвольные элементы поля):
(a) В любом поле ноль единственен, единица единственна.
Для любого a противоположный к a единственен, для любого $a\neq 0$ обратный элемент единственен.
(b) $-(a+b)=(-a)+(-b)$; $(ab)^{-1}=a^{-1}b^{-1}$; $a\cdot 0=0$
Если $ab=0$, то либо $a=0$, либо $b=0$.
Если $ac=ab$ и $a\neq 0$, то $b=c$.

3. Докажите, что для любых $a,b\in\mathbb{F}$ существует единственное решение уравнения $b+x=a$. Это решение обозначается как $a-b$ и называется *разностью* элементов a и b. Таким образом, в поле определена операция *вычитания*.
Докажите, что для любых $a\in\mathbb{F}$, $b\in\mathbb{F}\backslash\{0\}$ существует единственное решение уравнения $bx=a$. Это решение обозначается как a/b и называется *частным* элементов a и b. Таким образом, в поле определена операция *деления* на ненулевые элементы.

4. Пусть $a, b, c, d \in \mathbb{F}$. Докажите равенства:
(a) $-a = -1 \cdot a$; $a(-b) = -(ab)$; $(-a) \cdot (-a) = a^2$.
(b) $(a+b)(c+d) = ac + bc + ad + bd$; $a - (b+c) = a - b - c$.
(c) Теперь ещё известно, что b, d не равны 0. Докажите равенства:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd};\ \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd};\ (-c)^{-1} = -c^{-1}.$$

Подмножество $\mathbb{L}$ поля $\mathbb{K}$, называется *подполем* поля K, если L содержит 0 и 1 и замкнуто относительно операций сложения, умножения и взятия обратного элемента по сложению и умножению. Ясно, что подполе само является полем.

5. Докажите, что любое поле $\mathbb{F}$ содержит в качестве подполя либо $\mathbb{Q}$, либо $\mathbb{Z}/p\mathbb{Z}$ для некоторого простого p.

Подполя поля комплексных чисел называются *числовыми полями*. Пусть $\mathbb{K}$ — числовое поле, $x_1, x_2, \ldots, x_k \in \mathbb{C}$. Символом $\mathbb{K}(x_1, x_2, \ldots, x_k)$ будем обозначать минимальное по включению числовое поле, включающее $\mathbb{K}$ и содержащее все x_i.

6. Докажите, что любое числовое поле содержит все рациональные числа. Докажите, что поле $\mathbb{K}(x_1, x_2, \ldots, x_k)$, определённое выше, в самом деле существует и единственно.

Пусть $x_0 \in \mathbb{C}$, $\mathbb{K}$ — числовое поле. Элемент x_0 называется *алгебраическим* над полем $\mathbb{K}$, если существует многочлен $P(x)$ с коэффициентами из $\mathbb{K}$ такой, что $P(x_0) = 0$; в противном случае x_0 называется *трансцендентным* над $\mathbb{K}$. Для алгебраического x_0 многочлен $P(x)$ с коэффициентами из $\mathbb{K}$ наименьшей степени, удовлетворяющий $P(x_0) = 0$, называется *минимальным многочленом* x_0 над $\mathbb{K}$. Алгебраические (трансцендентные) над $\mathbb{Q}$ числа называют просто *алгебраическими (трансцендентными)*.

7. Из задачи 1 мы знаем, что $\mathbb{Q}(\sqrt{2})$ есть множество чисел вида $a + b\sqrt{2}$, где $a, b \in \mathbb{Q}$. Найдите аналогичное представление для $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

8. Докажите, что $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Найдите минимальный многочлен над $\mathbb{Q}$ числа $\sqrt{2} + \sqrt{3}$.

9. **(a)** Пусть $\mathbb{K}$ — числовое поле. Пусть $p, q \in \mathbb{Q}$ таковы, что многочлены $x^2 - q$ и $x^2 - q/p$ не имеют корней в поле $\mathbb{K}$. Докажите, что многочлен $x^2 - q$ не имеет корней в поле $\mathbb{K}(\sqrt{p})$.
(b) Пусть $p_1, \ldots, p_k$ – различные простые числа. Доказать: $\sqrt{p_1} + \ldots + \sqrt{p_k} \notin \mathbb{Q}$.

10. Пусть $\mathbb{K}$ — числовое поле, а $x_0 \in \mathbb{C}$ — алгебраический элемент над $\mathbb{K}$.
(a) Докажите, что минимальный многочлен $P(x)$ элемента x_0 над $\mathbb{K}$ неприводим над $\mathbb{K}$.
(b) Докажите, что любой многочлен $Q(x)$ с коэффициентами из $\mathbb{K}$, удовлетворяющий $Q(x_0) = 0$, делится на $P(x)$. В частности, минимальный многочлен единственен с точностью до умножения на ненулевую константу из $\mathbb{K}$.
(c) Доказать: $\mathbb{K}(x_0) = \{a_0 + a_1 x_0 + a_2 x_0^2 + \ldots + a_{n-1} x_0^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{K}\}$, где $n = \deg P(x)$.