Поля

▷ **Определение 1.** Набор $(\mathcal{F}, +, \cdot, 0, 1)$, где $\mathcal{F}$ — множество, "+" и "$\cdot$" — отображения $\mathcal{F} \times \mathcal{F} \to \mathcal{F}$, а 0 и 1 — различные элементы множества $\mathcal{F}$, называется *полем*, если выполнены следующие условия ("аксиомы"):

A_1) $\forall a, b, c \in \mathcal{F}\ (a + b) + c = a + (b + c)$ *("ассоциативность сложения")*;
A_2) $\forall a \in \mathcal{F}\ a + 0 = a = 0 + a$;
A_3) $\forall a, b \in \mathcal{F}\ a + b = b + a$ *("коммутативность сложения")*;
A_4) $\forall a \in \mathcal{F}\, \exists a' \in \mathcal{F} : a + a' = 0 = a' + a$ *("существование противоположного")*;
D) $\forall k, x, y \in \mathcal{F}\ k(x + y) = kx + ky, (x + y)k = xk + yk$ *("билинейность умножения")*;
M_1) $\forall a, b, c \in \mathcal{F}\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$ *("ассоциативность умножения")*;
M_2) $\forall a \in \mathcal{F}\ a \cdot 1 = a = 1 \cdot a$;
M_3) $\forall a, b \in \mathcal{F}\ a \cdot b = b \cdot a$ *("коммутативность умножения")*;
M_4) $\forall a \in \mathcal{F} \setminus \{0\}\, \exists a' \in \mathcal{F} : a \cdot a' = 1 = a' \cdot a$ *("существование обратного")*;

Если отбросить последнее условие — получится определение *(коммутативного) кольца.*

Задача 1. а) Для любого элемента $a \in \mathcal{F}$ элемент a' из аксиомы A_4 единственен (обозначение: $-a$).
б) $-(a + b) = (-a) + (-b)$.

Задача 2. а) Для любого элемента $a \in \mathcal{F} \setminus \{0\}$ элемент a' из аксиомы M_4 единственен (обозначение: a^{-1}).
б) Сколько решений может иметь в поле линейное уравнение $(ax = b)$?

Задача 3. а) $a \cdot 0 = 0$; б) $(-1) \cdot a = -a$; в) $(-a)^2 = a^2$.

Задача 4. а) В поле "нет делителей нуля": если $a \cdot b = 0$, то либо $a = 0$, либо $b = 0$.
б*) Если множество $\mathcal{F}$ конечно, то аксиому M_4 в определении поля можно заменить на отсутствие делителей нуля. (Существенна ли конечность множества $\mathcal{F}$?)

Задача 5. а) Сколько решений в поле может иметь квадратное уравнение?
б*) Сколько решений в поле может иметь уравнение степени n?

Задача 6. а) Выпишите таблицы сложения и умножения в $\mathbb{Z}/n\mathbb{Z}$ для $n = 2, 3, 4, 5$.
б) $\mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, \times, [0], [1])$ — поле. (Существенна ли простота p?)

Задача 7*. Пусть A — множество, $P(A)$ — множество его подмножеств. Является ли $(P(A), \cup, \cap, \varnothing, A)$ полем? А, наоборот, $(P(A), \cap, \cup, A, \varnothing)$?

Задача 8. В любом поле $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{ac}{bd}$; $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{ad + bc}{bd}$.

Задача 9. Рассмотрим множество F формальных записей вида $\dfrac{a}{b}$, где a и b — целые числа, $b \neq 0$.
а) Введем на F операции сложения и умножения как в предыдущей задаче. Будет ли результат (при подходящем выборе нуля и единицы) полем?
б) Рассмотрим на F отношение $\dfrac{a}{b} \sim \dfrac{a'}{b'} \iff \exists k, l \in \mathbb{Z} \setminus \{0\} : ka = la', kb = lb'$. Докажите, что это отношение эквивалентности, а операции из предыдущего пункта спускаются на фактормножество.
в) Результат является полем (это поле называется *полем рациональных чисел* и обозначается $\mathbb{Q}$).

▷ **Определение 2.** *Изоморфизом* полей $(K, +_K, \cdot_K, 0_K, 1_K)$, $(L, +_L, \cdot_L, 0_L, 1_L)$ называется биекция $f\colon K \to L$ такая, что
$f(0_K) = 0_L$, $f(a +_K b) = f(a) +_L f(b)$ (согласованность со сложением);
$f(1_K) = 1_L$, $f(a \cdot_K b) = f(a) \cdot_L f(b)$ (согласованность с умножением).
Изоморфизм поля с собой называется *автоморфизмом*.

Задача 10*. Любое поле содержит либо подполе, изоморфное $\mathbb{F}_p$ (в этом случае говорят, что поле имеет *характеристику* p), либо подполе, изоморфное $\mathbb{Q}$ (в этом случае говорят, что поле имеет нулевую характеристику).

Задача 11*. Существует ли поле из а) 4; б) 6; в) 8; г) 9 элементов?

▷ **Определение 3.** Пусть $\mathcal{F}$ — поле, d — его элемент. Через $\mathcal{F}(\sqrt{d})$ будем обозначать множество формальных записей вида $a + b\sqrt{d}$ $(a, b \in \mathcal{F})$ с естественными операциями (а именно, $(a + b\sqrt{d}) + (a' + b'\sqrt{d}) = (a + a') + (b + b')\sqrt{d}$; $(a + b\sqrt{d}) \cdot (a' + b'\sqrt{d}) = (aa' + dbb') + (ab' + a'b)\sqrt{d}$).

Задача 12*. а) При каких d будет полем $\mathbb{Q}(\sqrt{d})$?
б) При каких p будем полем $\mathbb{F}_p(\sqrt{-1})$?

Задача 13*. Найдите все автоморфизмы полей а) $\mathbb{F}_p$, $\mathbb{Q}$; б) $\mathbb{F}_p(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-d})$.