Говоря вольно, поле — это набор элементов, на которых есть четыре арифметических операции: сложение, вычитание, умножение и деление, обладающие привычными свойствами. Аксиоматизация этих свойств приводит к такому определению:

Определение 1. *Полем* называется любое множество $\Bbbk$, на котором заданы операции *сложения* $(+)$ и *умножения* $(\cdot)$, удовлетворяющие следующим условиям (аксиомам поля):

(A1) Для любых $a, b \in \Bbbk$ выполнено равенство $a + b = b + a$ (*коммутативность сложения*).

(A2) Для любых $a, b, c \in \Bbbk$ выполнено равенство $(a+b)+c = a+(b+c)$ (*ассоциативность сложения*).

(A3) В $\Bbbk$ существует такой элемент 0, что для любого $a \in \Bbbk$ выполнено равенство $a + 0 = a$ (*существование нуля*).

(A4) Для любого $a \in \Bbbk$ существует такой $b \in \Bbbk$, что $a + b = 0$ (*существование противоположного элемента*: такой элемент b называется *противоположным* к a и обозначается $-a$).

(M1) Для любых $a, b \in \Bbbk$ выполнено равенство $a \cdot b = b \cdot a$ (*коммутативность умножения*).

(M2) Для любых $a, b, c \in \Bbbk$ выполнено равенство $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (*ассоциативность умножения*).

(M3) В $\Bbbk$ существует такой элемент 1, не равный нулю, что для любого $a \in \Bbbk$ выполнено равенство $a \cdot 1 = a$ (*существование единицы*).

(M4) Для любого $a \in \Bbbk$, не равного нулю, существует такой $b \in \Bbbk$, что $a \cdot b = 1$ (*существование обратного элемента*: такой элемент b называется *обратным* к a и обозначается $\dfrac{1}{a}$ или a^{-1}).

(AM) Для любых $a, b, c \in \Bbbk$ выполнено равенство $a \cdot (b + c) = a \cdot b + a \cdot c$ (*дистрибутивность умножения относительно сложения*).

Примерами известных вам полей являются $\mathbb{Q}$ — рациональные числа, $\mathbb{R}$ — действительные числа, $\mathbb{C}$ — комплексные числа. Более сложный пример: множество всех алгебраических чисел — корней многочленов с рациональными коэффициентами (основная трудность тут — доказать, что сумма и произведение алгебраических чисел тоже алгебраические числа).

Из множеств вроде целых чисел или многочленов, в которых выполнены все аксиомы, кроме M4 (существование обратного), и нет делителей нуля, можно изготовить *поле частных*: это множество дробей с ненулевым знаменателем (как обычно, дроби a/b и c/d, у которых $ad = bc$, нужно считать равными), которые складываются и умножаются по обычным правилам. Таким образом из целых чисел получаются рациональные числа, а из многочленов — поле рациональных дробей.

Если взять простое число p и рассмотреть множество вычетов по модулю p, то у каждого элемента будет обратный (см. листок 23). Полученное множество $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ будет полем вычетов по модулю простого числа p.

Аналогично если взять неприводимый многочлен P и рассмотреть вычеты (остатки) по модулю многочлена P (точнее, это классы эквивалентности такого отношения: $A \sim B$, если $(A - B) \vdots P$), то тоже окажется, что у каждого вычета есть обратный. Получится поле $\mathbb{R}[x]/P\mathbb{R}[x]$. Если в качестве такого неприводимого многочлена взять $P = x^2 + 1 \in \mathbb{R}[x]$, то вычеты образуют поле $\mathbb{C}$.

Если взять корень α неприводимого многочлена $P \in \mathbb{Q}[x]$ и рассмотреть числа вида $a_0\alpha^m + a_1\alpha^{m-1} + \ldots + a_{m-1}\alpha + a_m$, где $m < \deg P$, $a_i \in \mathbb{Q}$, то они будут перемножаться и складываться в точности, как остатки от деления на многочлен P. Это поле обозначается через $\mathbb{Q}[\alpha]$. Например, $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} = \mathbb{Q}[x]/(x^2 - 2)\mathbb{Q}[x]$.

Аналогичные конструкции можно делать для многочленов с коэффициентами из любого поля.

Задача 1. Пусть $\Bbbk$ — поле. Докажите, что
а) в $\Bbbk$ есть только один ноль; **б)** у каждого элемента только один противоположный;
в) для любого $a \in \Bbbk$ выполнено равенство $-(-a) = a$;
г) для любых $a, b \in \Bbbk$ уравнение $a + x = b$ имеет ровно одно решение в $\Bbbk$ (оно обозначается $b - a$; таким образом, в поле определена операция *вычитания*).

Задача 2. Пусть $\Bbbk$ — поле. Докажите, что
а) в $\Bbbk$ есть только одна единица; **б)** у каждого ненулевого элемента только один обратный;
в) для любого ненулевого $a \in \Bbbk$ выполнено равенство $(a^{-1})^{-1} = a$;
г) для любого $b \in \Bbbk$ и любого ненулевого $a \in \Bbbk$ уравнение $a \cdot x = b$ имеет ровно одно решение в $\Bbbk$ (оно обозначается $\dfrac{b}{a}$; таким образом, в поле определена операция *деления* на ненулевые элементы).

Задача 3. Пусть $\Bbbk$ — поле. Докажите, что
а) для любого $a \in \Bbbk$ выполнено равенство $a \cdot 0 = 0$; **б)** если $a \cdot b = 0$, то $a = 0$ или $b = 0$.
в) Останется ли верным утверждение пункта б), если исключить из аксиом поля аксиому M4?

Задача 4. Пусть $\Bbbk$ — поле. Докажите, что для любого $a \in \Bbbk$ выполнены равенства
а) $a \cdot (-1) = -a$; **б)** $(-a) \cdot (-a) = a \cdot a$; **в)** $(-a)^{-1} = -(a^{-1})$, если $a \neq 0$.

Задача 5. Пусть $\Bbbk$ — поле. Докажите, что для любых $a, c \in \Bbbk$ и любых ненулевых $b, d \in \Bbbk$ выполнено равенство **а)** $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{a \cdot c}{b \cdot d}$; **б)** $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{a \cdot d + b \cdot c}{b \cdot d}$.

Задача 6. **а)** Докажите, что $\mathbb{Q}[\sqrt{2}]$ — поле. **б)** При каких m система вычетов $\mathbb{Z}/m\mathbb{Z}$ — поле?

Задача 7. Образуют ли поле числа вида **а)** $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, где $a, b, c \in \mathbb{Q}$; **б)** $a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}$, где $a, b, c, d \in \mathbb{Q}$, а p, q — фиксированные различные простые; **в)** $\mathbb{Z}[i]/(3+4i)\mathbb{Z}[i]$; **г)** $\mathbb{Z}[i]/(2+i)\mathbb{Z}[i]$?

Задача 8. Избавьтесь от иррациональности в знаменателе: $\frac{1}{5+\sqrt[3]{2}+\sqrt[3]{4}}$.

Задача 9. **а)** Пусть $\mathbb{R}(x) = \left\{ \dfrac{P(x)}{Q(x)} \;\middle|\; P(x), Q(x) \in \mathbb{R}[x], \text{ где } Q(x) - \text{не многочлен } 0 \right\}$. Докажите, что $\mathbb{R}(x)$ — поле (с обычным сложением и умножением). **б)** Всегда ли для множества, удовлетворяющего всем аксиомам, кроме M4, множество классов эквивалентности его дробей будет полем?

Определение 2. *Характеристика поля* $\Bbbk$ (обозначение: $\operatorname{char} \Bbbk$) — такое наименьшее натуральное число m, что $\underbrace{1 + \ldots + 1}_{m} = 0$. Если такого числа нет, характеристика полагается равной 0.

Задача 10. Докажите, что характеристика поля — простое число или 0.

Задача 11. Найдите характеристики полей **а)** $\mathbb{Q}$, $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{C}$; **б)** $\mathbb{Z}[i]/(2+i)\mathbb{Z}[i]$.

Поля характеристики p

Задача 12. Существует ли бесконечное поле характеристики p?

Задача 13. Пусть $\Bbbk$ — поле характеристики p. Докажите, что
а) элементы 1, $1+1$, $1+1+1$, …, $\underbrace{1 + \ldots + 1}_{p}$ образуют поле $\mathbb{F}_p \subset \Bbbk$, «точно такое же, как»[1] $\mathbb{Z}/p\mathbb{Z}$;
б) для произвольных элементов $a, b \in \Bbbk$ выполнено равенство $(a + b)^p = a^p + b^p$.

Задача 14. Пусть $\Bbbk$ — конечное поле из q элементов. **а)** Докажите, что для любого x из $\Bbbk$ верно $x^q = x$. **б)** Для каждого n найдите сумму всех n-х степеней элементов из $\Bbbk$.

Задача 15. Пусть $\Bbbk$ — конечное поле характеристики p. Пусть $x \in \Bbbk \setminus \mathbb{F}_p$. Докажите, что
а) $\Bbbk$ содержит все элементы вида $\alpha x + \beta$, где $\alpha, \beta \in \mathbb{F}_p$; **б)** в $\Bbbk$ как минимум p^2 элементов.
в) в $\Bbbk$ ровно p^n элементов для некоторого n.

1 а	1 б	1 в	1 г	2 а	2 б	2 в	2 г	3 а	3 б	3 в	4 а	4 б	4 в	5 а	5 б	6 а	6 б	7 а	7 б	7 в	7 г	8	9 а	9 б	10	11 а	11 б	12	13 а	13 б	14 а	14 б	15 а	15 б	15 в

[1] Математический термин — *изоморфное*. Поле F с операциями $+$, $\cdot$ и поле G с операциями $\oplus$, $\odot$ называются *изоморфными*, если существует взаимно-однозначное соответствие $\varphi : F \to G$, сохраняющее обе операции, то есть для любых элементов $a, b \in F$ выполнены равенства $\varphi(a + b) = \varphi(a) \oplus \varphi(b); \varphi(a \cdot b) = \varphi(a) \odot \varphi(b)$.