АЛГЕБРА - 2: КОЛЬЦА И ПОЛЯ

Рассмотрим целые ($\mathbb{Z}$), вещественные ($\mathbb{R}$) или рациональные ($\mathbb{Q}$) числа, полиномы $\mathbb{R}[x]$ или матрицы $\mathrm{Mat}_n(\mathbb{R})$ размером n на n с вещественными коэффициентами. На всех этих множествах заданы:

(1) сложение, которое коммутативно и превращает наше множество в абелеву группу (обозначается знаком "+", взятие обратного элемента относительно сложения обозначается знаком "–");
(2) умножение, которое ассоциативно, но группы не задает, потому что не все элементы обратимы (обозначается знаком $\cdot$, который часто опускают для краткости).

Эти операции и их свойства полезно аксиоматизировать.

Определение 1. Пусть A — множество с двумя операциями: $a + b$ (сложение) и $a \cdot b$ (умножение). Пусть в A заданы элементы 0 (ноль) и 1 (единица). Есливыполнены следующие свойства, то A называется *кольцом*:

(1) $(R, +)$ является абелевой группой, причем 0 играет роль единицы для этой группы;
(2) умножение ассоциативно: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ для всех $a, b, c \in A$;
(3) $1 \cdot a = a \cdot 1 = a$ для всех $a \in A$;
(4) операции сложения и умножения согласованы при помощи закона дистрибутивности:

$$a \cdot (b + c) = a \cdot b + a \cdot b, \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

для всех $a, b, c \in A$.

Если умножение коммутативно, то A называется *коммутативным кольком*. Если к тому же любой ненулевой элемент $a \in A$ обратим, то A называется *полем*. (Эти два условия вместе равносильны тому, что $A^* = A\backslash\{0\}$ является абелевой группой по умножению.)

Все приведенные в самом начале множества кроме множества матириц $\mathrm{Mat}_n(\mathbb{R})$ являются коммутативными кольцами. Множество матриц $\mathrm{Mat}_n(\mathbb{R})$ является примером некоммутативного кольца. Наконец, вещественные и рациональные числа (но не целые!) являются полями.

Задача 1. Являются ли кольцами следующие множества (относительно естественных операций сложения и умножения, если они не указаны явно):

(1) натуральные числа;
(2) четные целые числа;
(3) нечетные целые числа;
(4) иррациональные числа;
(5) пары целых чисел с покоординатными сложением и умножением;
(6) пары целых чисел, сложение покоординатное, а умножение задано формулой $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$;
(7) пары целых чисел, сложение покоординатное, а умножение задано формулой $(a, b) \cdot (c, d) = (ac + 2bd, ad + bc)$;
(8) фигуры на плоскости, сложение — симметрическая разность, умножение — пересечение.

Какие из этих множеств являются полями?

Ненулевой элемент a коммутативного кольца A называется *делителем нуля*, если найдется такой ненулевой элемент $b \in A$, что $ab = 0$.

Задача 2.

(1) Докажите, что в поле не существует делителей нуля.
(2) Приведите пример кольца, у которого нет делителей нуля, но оно тем не менее не является полем.

Задача 3.

(1) Докажите, что множество $\mathbb{Z}_n$ остатков по модулю n является коммутативным кольцом (при любом $n \geq 2$).
(2) Докажите, что Z_n является полем тогда и только тогда, когда n — простое число.

Поля $\mathbb{Z}_p$ для простого p являются примерами полей, состоящих из конечного числа элементов (конечными полями). В общем случае конечное поле из q элементов оброзначается через F_q. Как мы увидим в дальнейшем, такие поля существуют далеко не для всех натуральных чисел q.

Определение 2. Характеристикой поля F называется порядок элемента 1 в аддитивной группе поля F. Если этот порядок бесконечен (то есть $1 + 1 + \cdots + 1 \neq 0$ для любого количества слагаемых), то говорят, что поле F имеет характеристику 0. Характеристика поля F обозначается $\operatorname{char} F$.

Задача 4. Докажите, что если $\operatorname{char} F \neq 0$ отлична от нуля, то $\operatorname{char} F = p$ — простое число.

Задача 5. Пусть F_q — конечное поле из q элементов. Докажите, что в этом случае $\operatorname{char} F_q = p \neq 0$, и p является делителем q. (*Указание: примените теорему Лагранжа.*)

На самом деле, верен более сильный результат, который мы оставляем без доказательства.

Теорема. *Пусть F_q — конечное поле из q элементов, и $p = \operatorname{char} F_q$. Тогда $q = p^k$, причем все поля из q элементов изоморфны друг другу.*

Задача 6. Пусть F_4 — поле из 4 элементов.

(1) Докажите, что $\operatorname{char} F_4 = 2$.
(2) Докажите, что $-1 = 1$, и что $a + a = 0$ для любого элемента $a \in F_4$.
(3) Пусть a — элемент поля F_4, отличный от 0 и 1. Докажите, что $F_4 = \{0, 1, a, a + 1\}$.
(4) Методом исключения докажите, что $a^2 = a + 1$. (*Указание: Используйте тот факт, что поле не содержит делителей нуля.*)
(5) Выпишите таблицы сложения и умножения поля F_4.

Ниже мы приведем общую конструкцию постоения новых полей из уже известных. Для любого поля F обозначим через $F[x]$ множество полиномов с коэффициентами из поля F. Любой полином степени n имеет вид $a_0 + a_1 x + \cdots + a_n x^n$, где $a_i \in F$ и старший коэффициент a_n отличен от нуля. Как и в случае полиномов с вещественными коэффициентами, полиномы $F[x]$ с коэффициентами в поле F образуют коммутативное кольцо.

Так же, как для полиномов с вещественными коэффициентами, мы можем определить деление полиномов в столбик. Другими словами, для любых двух полиномов $p(x), q(x) \in F[x]$ однозначно определены частное $s(x)$ и остаток $r(x)$ при делении $p(x)$ на $q(x)$:

$$p(x) = s(x)q(x) + r(x), \quad \deg r(x) < \deg q(x).$$

Это позволяет использовать алгоритм Эвклида для нахождения наибольшего общего делителя любых двух полиномов с коэффициентами в произвольном поле.

Задача 7.

(1) Пусть $p(x) \in F[x]$. Докажите, что $p(a) = 0$ для некоторого $a \in F$ тогда и только тогда, когда $p(x)$ делится на $x - a$.

(2) Докажите, что полином степени n в $F[x]$ не может иметь более n корней.
(3) Пусть F_q — поле из q элементов. Докажите, что корни полинома $x^q - x$ — это в точности все элементы поля F_q. (*Указание: Докажите, что порядок любого ненулевого элемента в мультипликативной группе F^* является делителем $q-1$.*)

Таким образом, $x^q - x$ является примером ненулевого полинома $p(x) \in F_q[x]$, такого что $p(a) = 0$ для любого элемента $a \in F_q$.

Задача 8. Докажите, что полином $p(x) \in F_q[x]$ обладает свойством $p(a) = 0$ для любого элемента $a \in F_q$, тогда и только тогда, когда он делится на $x^q - x$.

Задача 9. Докажите, что если поле F бесконечно, то полиномов, обладающих таким свойством, не существует.

Полином $p(x) \in F[x]$ называется *неприводимым*, если он не раскладывается в произведение двух полиномов степени ≥ 1. Такие полиномы являются аналогами простых чисел в кольце целых чисел.

Задача 10.
(1) Докажите, что неприводимый полином $p(x) \in F[x]$ не имеет корней в поле F (то есть $p(a) \neq 0$ для любого $a \in F$).
(2) Пусть $F = F_2 = \mathbb{Z}_2$ — поле из двух элементов. Докажите, что $x^2 + x + 1$ — единственный неприводимый полином степени 2 в $F_2[x]$.
(3) Найдите все неприводимые полиномы степени 3 и 4 в $F_2[x]$.
(4) Найдите все неприводимые полиномы степени 2 и 3 в $F_3[x]$.
(5) Опишите все неприводимые полиномы в $\mathbb{R}[x]$.

Пусть $p(x) \in F[x]$ некоторый фиксированный полином степени n. Обозначим через $F[x]/(p)$ все остатки при делении на $p(x)$. Понятно, что $F[x]/(p)$ можно отождествить со всеми полиномами в $F[x]$ степени $\leq n-1$. Как и в случае с целыми числами, множество $F[x]/(p)$ естественным образом наделяется операциями сложения и умножения. (Чтобы умножить два остатка, их нужно сначала умножить как обычные полиномы, а потом найти остаток при делении на $p(x)$). Таким образом, $F[x]/(p)$ является кольцом для любого полинома $p(x)$ степени ≥ 1.

Теорема. *Кольцо $F[x]/(p)$ является полем тогда и только тогда, когда полином $p(x)$ неприводим.*

Доказательство. Если полином $p(x)$ раскладывается на множители $p_1(x)p_2(x)$, то оба множителя $p_1(x)$ и $p_2(x)$ являются делителями

нуля в кольце $F[x]/(p)$. То есть в этом случае $F[x]/(p)$ не может быть полем.

Пусть теперь полином $p(x)$ неприводим, и $q(x) \in F[x]/(p)$ — произвольный ненулевой остаток по модулю $p(x)$.

Задача 11.

(1) Докажите, что полиномы $p(x)$ и $q(x)$ взаимно просты.
(2) Докажите, что найдутся такие полиномы $r(x), s(x) \in F[x]$, что $r(x)p(x) + s(x)q(x) = 1$. (*Указание: воспользуйтесь алгоритмом Эвклида.*)

Но в этом случае $s(x)q(x) = 1$ по модулю $p(x)$. Другими словами, любой ненулевой элемент кольца $F[x]/(p)$ обратим, и оно является полем. □

Задача 12. Пусть поле F конечно и состоит из q элементов. Тогда кольцо $F[x]/(p)$ состоит из q^n элементов.

Задача 13. Докажите, что поле $F_2[x]/(x^2 + x + 1)$ совпадает с построенным выше полем F_4 из 4 элементов.

Задача 14. Проверьте, что поле $\mathbb{R}[x]/(x^2+1)$ совпадает с полем $\mathbb{C}$ комплексных чисел.