Поля

В кольцах операции „+” и „·” называются *сложением* и *умножением* соответственно. Кольцо $\mathcal{F}$ такое, что $\mathcal{F} \setminus \{0\}$ является абелевой группой по умножению, называется *полем*. Вообще говоря, поле обобщает собой понятие множества с двумя операциями, в котором однозначно решается любое (невырожденное) линейное уравнение. В дальнейшем, если речь будет идти о кольце или поле, то знак умножения мы будем для краткости пропускать.

1. Определите, какие из колец $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}_n, +, \cdot)$, $(\mathbb{R}_n, +, \cdot)$,$(\mathbb{Z}_n, +, \cdot)$, являются полями, а какие — нет.
2. Докажите, что $\mathbb{Q}[i\sqrt{3}]$, определённое по аналогии с $\mathbb{Z}[i\sqrt{3}]$, является полем.

Деление многочленов с остатком

Разделить многочлен $p(x)$ на многочлен $q(x)$ с остатком означает следующее: найти многочлены $h(x)$ и $r(x)$ такие, что $p(x) = h(x)q(x) + r(x)$ и многочлен $r(x)$ имеет степень, меньшую степени делителя $q(x)$, либо тождественно равен нулю. Мы будем использовать стандартные обозначения $\deg p$ степени многочлена $p(x)$, а также $\mathcal{K}[x]$ для множества многочленов одной переменной с коэффициентами из кольца $\mathcal{K}[x]$. Ясно, что, деление с остатком зависит от того, откуда выбираются коэффициенты.

3. Разделите с остатком многочлен $2x^5 + 5x^2$ на многочлен $2x^3 + 3x^2$ в $\mathbb{Q}[x]$.
4. Возможно ли такое деление в $\mathbb{Z}[x]$?

Теорема Безу

5. Докажите[1], что остаток от деления многочлена $p(x)$ на многочлен $x - a$ равен $p(a)$.

В частности, если число a является корнем многочлена $p(x)$, если и только если $p(x)$ делится на $x-a$ нацело (остаток равен нулю). Наибольшее число k такое, что $p(x)$ делится на $(x - a)^k$ называется кратностью корня a. Например, многочлен $x^3(x - 1)^2$ имеет два корня: корень 0 кратности три и корень 1 кратности два, в таком случае говорят, что у него пять корней с учётом кратности.

Теорема Безу показывает, что, если найден корень многочлена $p(x)$, то в уравнении $p(x) = 0$ можно понизить степень. Следующая задача показывает, как определить, имеет ли многочлен из $\mathbb{Z}[x]$ рациональные корни.

6. Докажите[2], что, если несократимая дробь $p/q \in \mathbb{Q}$ является корнем многочлена $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, то числитель p делит свободный член a_0, а знаменатель q делит старший коэффициент a_n.
7. Решите уравнение $x^5 - 2x^4 - 4x^3 + 4x^2 - 5x + 6 = 0$.

Основная теорема арифметики для многочленов

Пусть $\mathcal{F}$ — поле, например, $\mathbb{Q}$ или $\mathbb{R}$. Поскольку для многочленов из $\mathcal{F}[x]$ определено деление с остатком, то $\mathcal{F}[x]$ — евклидово кольцо с нормой deg. В частности, $\mathcal{F}[x]$ всегда факториально.

8. Докажите, что многочлен из $\mathcal{F}[x]$ степени n имеет не больше n корней с учётом кратности.
9. Докажите, что многочлен из $\mathbb{Z}[x]$ степени n имеет не больше n корней с учётом кратности, а для кольца $\mathbb{Z}_m[x]$ это в общем случае неверно.
10. Докажите, что, если значения двух многочленов из $\mathcal{F}[x]$ степени не выше n совпадают по крайней мере в $n + 1$ точке, то эти два многочлена равны.

[1] Это утверждение называется **теоремой Безу**.

[2] Это утверждение называется **теоремой о рациональных корнях**.

Факториальность $\mathbb{Z}[x]$

Хотя кольцо $\mathbb{Z}[x]$ и не евклидово, однако оно факториально, как показывает задача 13.

11. Пусть $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ и для некоторого простого числа p все коэффициенты, кроме a_n, делятся на p, а свободный член не делится на p^2. Докажите[3], что многочлен $f(x)$ неприводим над $\mathbb{Z}$.
12. Содержанием многочлена $p \in \mathbb{Z}[x]$ называется наибольший общий делитель его коэффициентов, обозначение: $\mathrm{cont}(p)$. Докажите[4] тождество $\mathrm{cont}(pq) = \mathrm{cont}(p) \cdot \mathrm{cont}(q)$.
13. Докажите, что многочлен $p \in \mathbb{Z}[x]$ приводи́м в $\mathbb{Q}[x]$ тогда и только тогда, когда он приводи́м в $\mathbb{Z}[x]$. В частности, покажите, что кольцо $\mathbb{Z}[x]$ факториально.

Разложение на множители

Для разложения многочленов на множители иногда бывает полезно использовать метод неопределённых коэффициентов, главное при этом понимать, что он не упрощает задачу в общем виде, а позволяет подобрать разложение, используя некоторые допущения.

14. Найдите все линейные функции $p(x)$ и $q(x)$ с вещественными коэффициентами, удовлетворяющие тождеству $p(x)(x^2 - 3x + 2) + q(x)(x^2 + x + 1) = 21$.
15. Разложите на множители многочлен $x^4 + x^3 + x^2 + x + 12$.

Упражнения

16. Найдите остаток от деления $p(x) = x^{2019} + 19x^{20} + 20x^{19} + x$ на **a)** $x - 1$, **b)** $x^2 - 1$.
17. При каких a и b многочлен $p(x) = (a + b)x^5 + abx^2 + 1$ делится на $x^2 - 3x + 2$?
18. Многочлен $p(x)$ даёт остаток 2 при делении на $x - 1$ и остаток 1 при делении на $x - 2$. Какой остаток даёт $p(x)$ при делении на $(x - 1)(x - 2)$?
19. Пусть $p(x) = (2x^2 - 2x + 1)^{20}(3x^2 - 3x + 1)^{19}$. Найдите сумму коэффициентов этого многочлена **a)** при всех, **b)** при чётных и **c)** при нечётных степенях переменной.
20. Докажите, что многочлен с целыми коэффициентами, имеющий больше трёх целых корней, не принимает простых значений в целых точках.
21. Решите уравнение $x^4 + x^3 - x^2 - 2x - 2 = 0$.

Задачи

22. Решите уравнение $n^5 + n^4 = 7^m - 1$ в целых числах n и m.
23. Найдите все многочлены $p(x)$, удовлетворяющие тождеству $p(x + 1) = p(x) + 2x + 1$.
24. При каких n многочлен $1 + x^2 + x^4 + \ldots + x^{2n}$ делится на $1 + x + x^2 + \ldots + x^n$?
25. Найдите все многочлены $p(x)$, удовлетворяющие тождеству $x \cdot p(x - 1) = (x - 26)p(x)$.
26. Найдите все натуральные числа a, для которых найдётся многочлен $p(x)$ с целыми коэффициентами, удовлетворяющий равенствам $p(\sqrt{2} + 1) = 2 - \sqrt{2}$ и $p(\sqrt{2} + 2) = a$.

Немного о полях

Характеристикой поля называется наименьшее $n \in \mathbb{N}$ такое, что $\underbrace{1 + 1 + \ldots + 1}_{n \text{ раз}} = 0$.

Если такого числа не существует, то говорят, что поле имеет характеристику нуль.

27. Докажите, что, если у поля есть характеристика, то она — простое число.

В некотором смысле, поля $\mathbb{Z}_p$ и $\mathbb{Q}$ минимальны. Изоморфизмом полей K и L называется такая биекция $\varphi\colon K \to L$, что $\varphi(ab) = \varphi(a)\varphi(b)$ для любых $a, b \in K$.

28. K — поле характеристики p. Докажите[5], что в K есть подполе, изоморфное $\mathbb{Z}_p$.
29. K — поле характеристики 0. Докажите, что в K есть подполе, изоморфное $\mathbb{Q}$.

---

[3] Это утверждение называется **критерием Эйзенштейна.**

[4] Это утверждение называется **леммой Гаусса.**

[5] В частности, все поля с p элементами изоморфны $\mathbb{Z}_p$, это поле часто обозначают через $\mathbb{F}_p$.