Поля

В кольцах операции „+” и „$\cdot$ ” называются *сложением* и *умножением* соответственно. Кольцо $\mathcal{F}$ такое, что $\mathcal{F}\setminus\{0\}$ – абелева группа по умножению, называется *полем.* В дальнейшем, если речь будет идти о кольце или поле, знак умножения будем для краткости опускать.

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 $\mathbb{Z}[i\sqrt{3}]$, – поле.

Факториальность колец 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. Хотя кольцо $\mathbb{Z}[x]$ и не евклидово, однако оно факториально, как показывает задача 4.

3. **Лемма Гаусса.** *Содержанием* многочлена $p\in\mathbb{Z}[x]$ называется наибольший общий делитель его коэффициентов, обозначение: $\operatorname{cont}(p)$. Докажите тождество $\operatorname{cont}(pq)=\operatorname{cont}(p)\cdot\operatorname{cont}(q)$.
4. Докажите, что многочлен $p\in\mathbb{Z}[x]$ приводи́м в $\mathbb{Q}[x]$ тогда и только тогда, когда он приводи́м в $\mathbb{Z}[x]$.

Поле отношений целостного кольца $\mathcal{K}$ строится так же, как $\mathbb{Q}$ строилось из $\mathbb{Z}$. А именно, рассмотрим множество дробей $\frac{a}{b}$, где $a,b\in\mathcal{K}$, $b\neq 0$. При этом, дроби $\frac{a}{b}$ и $\frac{c}{d}$ отождествим, если $ad=bc$, а действия с дробями определим привычным образом.

5. Докажите, что поле отношений, действительно, является полем.

Пусть $\mathcal{K}$ ещё и факториально. Одновременно с $\mathcal{K}[x]$ полезно рассматривать $\mathcal{L}[x]$, где $\mathcal{L}$ – поле отношений кольца K.

6. Объясните, почему кольца $\mathcal{L}[x]$ и $\mathcal{K}[x]$ факториальны.
7. Докажите, что кольцо $\mathcal{K}[x_1,x_2,\dots,x_n]$ факториально.

Из результата последней задачи в частности следует факториальность кольца $\mathcal{F}[x_1,x_2,\dots,x_n]$, для произвольного поля $\mathcal{F}$.

Теорема Виета

Многочлен, не изменяющийся при любых перестановках своих переменных называется симметрическим. Зафиксируем натуральное число n и для каждого k от 1 до n построим многочлен σ_k от n переменных: x_1, x_2, $\dots$, x_n, равный сумме всех произведений по k переменных.

8. **Теорема Виета.** Многочлен $a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ имеет n корней с учётом кратности: x_1, x_2, $\dots$, x_n. Докажите равенства $\sigma_1=-a_{n-1}/a_n$, $\sigma_2=a_{n-2}/a_n$, $\dots$, $\sigma_n=(-1)^na_0/a_n$.

Рассмотрим *лексикографический* порядок на множестве многочленов: одночлен $ax_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$ старше одночлена $bx_1^{\beta_1}x_2^{\beta_2}\dots x_n^{\beta_n}$, $a,b\neq 0$, если для некоторого номера k, $0 \leqslant k \leqslant n$, выполнено неравенство $\alpha_k > \beta_k$, а также $\alpha_s = \beta_s$ при всех $s < k$.

9. Можно ли выписать бесконечную последовательность одночленов от n переменных, в которой каждый следующий младше предыдущего?
10. Докажите, что любой симметрический многочлен представи́м в виде многочлена от элементарных симметрических многочленов.

Ещё 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.

11. Докажите, что ненулевая характеристика поля – простое число.

В некотором смысле, поля $\mathbb{F}_p$ и $\mathbb{Q}$ минимальны. *Изоморфизмом* полей K и L называется такая биекция $\varphi\colon K \to L$, что для любых $a, b \in K$ верны равенства $\varphi(a +_K b) = \varphi(a) +_L \varphi(b)$ и $\varphi(a \cdot_K b) = \varphi(a) \cdot_L \varphi(b)$.

12. K – поле характеристики p. Докажите, что в K есть подполе, изоморфное $\mathbb{Z}_p$.
13. K – поле характеристики 0. Докажите, что в K есть подполе, изоморфное $\mathbb{Q}$.

Результат задачи 12 оправдывает единое обозначение $\mathbb{F}_p$ для всех полей простой характеристики p.

Упражнения

14. **Критерий Эйзенштейна.** Пусть $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$ и для некоторого простого числа p все коэффициенты, кроме a_n, делятся на p, а свободный член не делится на p^2. Докажите, что многочлен $f(x)$ неприводим над $\mathbb{Z}$.
15. Пусть p – простое число. Докажите, что многочлен деления круга $x^{p-1} + x^{p-1} + \ldots + x + 1$ неприводим.
16. Найдите все числа $a \in \mathbb{N}$, для которых найдётся многочлен $p \in \mathbb{Z}[x]$, удовлетворяющий равенствам $p(\sqrt{2}+1) = 2 - \sqrt{2}$ и $p(\sqrt{2}+2) = a$.
17. **Тождества Ньютона.** Пусть $x_1, \ldots, x_n$ – вещественные числа. Для каждого натурального m обозначим $S_m = x_1^m + \ldots + x_n^m$. При всех $m > n$ положим $\sigma_m = 0$. Для каждого $m > 1$ докажите равенство $S_m = \sigma_1 S_{m-1} - \sigma_2 S_{m-2} + \ldots + (-1)^m \sigma_{m-1} S_1 + (-1)^{m+1} m \sigma_m$.
18. Многочлен $ax^n - ax^{n-1} + c_2 x^{n-2} + \ldots + c_{n-2} x^2 - n^2 bx + b$ имеет ровно n положительных корней. Докажите, что все корни равны между собой.
19. Найдите наибольшее число C, при котором для любой тройки вещественных чисел (x, y, z) такой, что $x + y + z = -1$, верно неравенство $C \cdot |x^3 + y^3 + z^3 + 1| \leqslant |x^5 + y^5 + z^5 + 1|$.