Евклидовы кольца

Кольцо $K[[x]]$ *формальных степенных рядов* над полем K состоит из (бесконечных) сумм вида $a_0 + a_1x + a_2x^2 + \ldots$, где $a_i \in K$. Кольцо $K((x))$ *формальных рядов Лорана* над полем K состоит из (бесконечных) сумм вида $a_{-N}x^{-N} + a_{-N+1}x^{-N+1} + a_{-N+2}x^{-N+2} + \ldots$, где $a_i \in K$, а N — произвольное натуральное число. Сложение и умножение в этих кольцах определяются так же, как и для многочленов (т.е., чтобы перемножить два ряда, надо раскрыть скобки, пользуясь соотношением $x^kx^l = x^{k+l}$).

A2.1. а) Выразите явной формулой коэффициенты произведения двух степенных рядов через коэффициенты сомножителей. Убедитесь, что произведение определено корректно, то есть для нахождения каждого из этих коэффициентов необходимо проделать лишь *конечное* число операций сложения и умножения. Верно ли это для рядов Лорана?

б) Является ли кольцо $K[[x]]$ целостным?

в) Найдите все обратимые элементы в $K[[x]]$ и все идеалы в $K[[x]]$.

г) Покажите, что $K((x))$ является полем частных кольца $K[[x]]$.

Кольцо гауссовых чисел $\mathbb{Z}[i]$ состоит из комплексных чисел вида $a + bi$, где $a, b \in \mathbb{Z}$. *Нормой* гауссова числа $z = a + bi$ называется число $n(z) = a^2 + b^2$.

A2.2. а) Докажите, что гауссовы числа действительно образуют кольцо, т.е. замкнуты относительно операций сложения и умножения комплексных чисел. **б)** Найдите поле частных кольца $\mathbb{Z}[i]$ (т.е. опишите это поле как подполе в $\mathbb{C}$). **в)** Докажите, что норма $n\colon \mathbb{Z}[i] \to \mathbb{Z}$ *мультипликативна*, т.е. $n(zw) = n(z)n(w)$ для любых гауссовых чисел $z, w \in \mathbb{Z}[i]$.

A2.3. а) Найдите все обратимые гауссовы числа (т.е. такие $z \in \mathbb{Z}[i]$, для которых $z^{-1} \in \mathbb{Z}[i]$). Чему равняется их норма?

б) Разложите числа 2, 3 и 5 в произведение простых (т.е. не раскладывающихся в произведение необратимых множителей) гауссовых чисел.

A2.4. а) Докажите, что для любых гауссовых чисел $z_1, z_2 \in \mathbb{Z}[i]$ и $z_2 \neq 0$ существуют такие $r, q \in \mathbb{Z}[i]$, что $z_1 = r \cdot z_2 + q$ и $n(q) < n(z_2)$.

б) Докажите, что в кольце гауссовых чисел любой идеал главный.

в) **(Основная теорема арифметики для гауссовых чисел.)** Докажите, что любое гауссово число представляется в виде произведения простых единственным способом (с точностью до обратимых множителей).

A2.5. Докажите, что в кольце $\mathbb{Z}[i\sqrt{5}]$ не выполняется основная теорема арифметики (а, следовательно, существуют неглавные идеалы и нет деления с остатком).

A2.6. а) Докажите, что следующие условия эквивалентны: 1) целое простое число $p \in \mathbb{Z}$ является простым в кольце $\mathbb{Z}[i]$; 2) кольцо $\mathbb{F}_p[x]/(x^2+1)$ является полем; 3) число p имеет вид $4k+3$;

б) Докажите, что следующие условия эквивалентны: 1) целое простое число $p \in \mathbb{Z}$ есть произведение двух различных простых элементов кольца $\mathbb{Z}[i]$, сопряженных друг другу; 2) кольцо $\mathbb{F}_p[x]/(x^2+1)$ изоморфно $\mathbb{F}_p \oplus \mathbb{F}_p$; 3) число p имеет вид $4k+1$;

в) Что происходит при $p = 2$?

A2.7. а) Какие значения может принимать многочлен $x^2 + y^2$ при целых значениях переменных x, y ?

б) Найдите количество целочисленных решений уравнения $x^2 + y^2 = n$ в зависимости от $n \in \mathbb{Z}$, зная разложение числа n на простые множители.

в) Пусть $\tau_1(n)$ – количество натуральных делителей числа n, имеющих вид $4k+1$, а $\tau_3(n)$ – количество натуральных делителей числа n, имеющих вид $4k+3$. Выразите количество целочисленных решений уравнения $x^2 + y^2 = n$ через $\tau_1(n)$ и $\tau_3(n)$.

A2.8*. а) Найдите все неприводимые многочлены степени не выше 3 над $\mathbb{F}_2$ и $\mathbb{F}_3$.

б) Пусть $I_n(q)$ – количество неприводимых многочленов степени n над $\mathbb{F}_q$. Докажите равенство формальных степенных рядов: $(1-qx)^{-1} = \prod\limits_{n=1}^{\infty}(1-x^n)^{-I_n(q)}$.

в) Выразите $I_n(q)$ явной формулой в виде многочлена от q.

Указание. Возьмите логарифм от обеих частей равенства из предыдущего пункта и воспользуйтесь формулой обращения Мебиуса.

A2.9*. а) Решите задачи A2.2–A2.4 для кольца *чисел Эйзенштейна*, состоящего из комплексных числа вида $a + b\rho \in \mathbb{C}$, где $\rho = \frac{i\sqrt{3}-1}{2}$, $a, b \in \mathbb{Z}$.

б) Докажите, что целое простое число $p \in \mathbb{Z}$ является простым в кольце чисел Эйзенштейна $\mathbb{Z}[\rho]$ тогда и только тогда, когда кольцо $\mathbb{F}_p[x]/(x^2+x+1)$ является полем.

в) Докажите, что из натуральных чисел простыми числами Эйзенштейна являются только простые вида $p = 6k-1$ и $p = 2$.

г) Найдите количество целочисленных решений уравнения $x^2 - xy + y^2 = n$ в зависимости от $n \in \mathbb{Z}$.