Потеря и спасение факториальности К. Конрад

Дубна, 2017 г. Листок 2

Тексты на диске O: `Zinotes.pdf` и `quadraticideals.pdf`.

1. а) В $\mathbf{Z}[\sqrt{3}]$ покажите явно, что 2 и 3 приводимы, а также докажите, что 5 и 7 неприводимы.

   б) Докажите, что (i) уравнение $11 = x^2 - 3y^2$ не имеет целых решений и (ii) 11 приводимо в $\mathbf{Z}[\sqrt{3}]$, так как $11 = (2\sqrt{3}+1)(2\sqrt{3}-1)$ и множители не обратимы. Почему (i) и (ii) не противоречат друг другу?

2. В $\mathbf{Z}[(1+\sqrt{-3})/2]$ пусть $\theta = (1+\sqrt{-3})/2$. Докажите, что обратимые имеют вид $\{\varepsilon \in \mathbf{Z}[(1+\sqrt{-3})/2] : \mathrm{N}(\varepsilon) = 1\}$ и это множество равно $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$. (Напомним, что $\mathrm{N}(a + b\theta) = a^2 + ab + b^2 = (a + b/2)^2 + 3(b/2)^2$ для целых a и b.)

3. Мы увидели во второй лекции, что если каждое неприводимое π в $\mathbf{Z}[\sqrt{d}]$ удовлетворяет условию

$$\pi \mid \alpha\beta \Rightarrow \pi \mid \alpha \text{ или } \pi \mid \beta \text{ для всех } \alpha \text{ и } \beta \in \mathbf{Z}[\sqrt{d}], \qquad (*)$$

   то разложение на неприводимые в $\mathbf{Z}[\sqrt{d}]$ однозначно (с точностью до порядка членов и умножения множителей на обратимые).

   а) Докажите обратное: если разложение на неприводимые в $\mathbf{Z}[\sqrt{d}]$ однозначно, то каждое неприводимое π в $\mathbf{Z}[\sqrt{d}]$ удовлетворяет условию $(*)$.

   б) Докажите, что всякое *необратимое* $\pi \in \mathbf{Z}[\sqrt{d}]$, которое удовлетворяет условие $(*)$, должно быть неприводимым.

   Поэтому однозначность разложения на неприводимые в $\mathbf{Z}[\sqrt{d}]$ эквивалентна тому, что неприводимые совпадают с необратимыми π, которые удовлетворяют $(*)$.

4. Используйте идеи из доказательства того, что у $\mathbf{Z}[i]$ есть алгоритм деления с остатком относительно нормы для того, чтобы доказать похожие результаты в $\mathbf{Z}[\sqrt{-2}]$, $\mathbf{Z}[\sqrt{2}]$, и $\mathbf{Z}[\sqrt{3}]$ относительно нормы или модуля нормы:

$$\alpha, \beta \in \mathbf{Z}[\sqrt{-2}],\ \ \beta \neq 0 \Rightarrow \text{ сущ. } \gamma, \rho \in \mathbf{Z}[\sqrt{-2}], \text{ т.ч. } \alpha = \beta\gamma + \rho \text{ и } \mathrm{N}(\rho) < \mathrm{N}(\beta),$$

$\alpha, \beta \in \mathbf{Z}[\sqrt{2}],\ \ \beta \neq 0 \Rightarrow$ сущ. $\gamma, \rho \in \mathbf{Z}[\sqrt{2}]$, т.ч. $\alpha = \beta\gamma + \rho$ и $|\,\mathrm{N}(\rho)| < |\,\mathrm{N}(\beta)|$,

$\alpha, \beta \in \mathbf{Z}[\sqrt{3}],\ \ \beta \neq 0 \Rightarrow$ сущ. $\gamma, \rho \in \mathbf{Z}[\sqrt{2}]$, т.ч. $\alpha = \beta\gamma + \rho$ и $|\,\mathrm{N}(\rho)| < |\,\mathrm{N}(\beta)|$.

Используйте геометрический способ для $\mathbf{Z}[\sqrt{-2}]$ как для $\mathbf{Z}[i]$ во второй лекции, а алгебраический подход для $\mathbf{Z}[\sqrt{2}]$ и $\mathbf{Z}[\sqrt{3}]$ как в письменных заметках о $\mathbf{Z}[i]$. (Подсказка: для $\mathbf{Z}[\sqrt{2}]$ и $\mathbf{Z}[\sqrt{3}]$ докажите, что $|x^2 - 2y^2| \leq \max(x^2, 2y^2)$ и $|x^2 - 3y^2| \leq \max(x^2, 3y^2)$ для $x, y \in \mathbf{Z}$.)

5. Используйте метод доказательства для $\mathbf{Z}[\sqrt{2}]$ из предыдущего упражнения, чтобы провести алгоритм Евклида для $9 + 4\sqrt{2}$ и $9 - 4\sqrt{2}$. (После каждого шага алгоритма перепроверьте вычисления, особенно то, что $|\,\mathrm{N}(\rho)| < |\,\mathrm{N}(\beta)|$.)