Вспоминаем определения

Пусть $\mathcal{F} \supset \mathbb{Q}$ – расширение полей. Элемент $a \in \mathcal{F}$ называется *алгебраическим*, если он является корнем многочлена с целыми коэффициентами, а такой многочлен наименьшей степени называется *минимальным многочленом* числа[1] a. Алгебраическое число называется *алгебраическим целым*, если его минимальный многочлен приведённый.

Обозначим через $\mathcal{R}$ множество целых алгебраических чисел. Элемент $\varepsilon \neq 0$ называется *единицей*, если $\varepsilon^{-1} \in \mathcal{R}$. Элементы $a, b \in \mathcal{R}$ называются *ассоциированными*, если $a = \varepsilon b$ для некоторой единицы ε. Ненулевой элемент множества $\mathcal{R}$ называется *неразложимым*, если каждый его делитель является либо ассоциирован с ним, либо является единицей. Наконец, ненулевой и неединичный элемент $a \in \mathcal{R}$ называется *простым*, если из $a \mid bc$, $b, c \in \mathcal{R}$, следует, что $a \mid b$ или $a \mid c$.

Квадратичные расширения

Пусть $d \neq 1$ – целое число, свободное от квадратов. *Квадратичным расширением* $\mathbb{Q}$ называется поле $\mathbb{Q}[\sqrt{d}]$, все алгебраические операции, а также понятия „сопряжение" и „норма" считаем известными. Нас будет интересовать теория делимости в кольце целых алгебраических чисел этого расширения.

1. Опишите все целые алгебраические числа в поле $\mathbb{Q}[\sqrt{d}]$.
2. Опишите все единицы в поле $\mathbb{Q}[\sqrt{d}]$, $d < -4$.
3. Опишите все единицы в поле[2] $\mathbb{Q}[\sqrt{-1}]$.
4. Опишите все единицы в поле[3] $\mathbb{Q}[\sqrt{-3}]$.
5. Из теоремы о рациональных приближениях докажите, что при $d > 1$ существует бесконечно много целых алгебраических чисел с нормой, не превышающей $3\sqrt{d}$, и выведите отсюда ещё раз, что любое уравнение Пелля имеет нетривиально решение.
6. Опишите все единицы вещественного поля $\mathbb{Q}[\sqrt{d}]$, $d > 1$.
7. Докажите или опровергните следующие два утверждения: 1) каждое простое число является неразложимым; и 2) каждое неразложимое число является простым.

Квадратичное поле $\mathbb{Q}[\sqrt{d}]$ называется *факториальным* или *евклидовым*, если таковым является его кольцо целых алгебраических чисел.

8. В терминах задачи 7 сформулируйте и докажите критерий факториальности $\mathbb{Q}[\sqrt{d}]$.
9. Докажите, что $\mathbb{Q}[\sqrt{d}]$ евклидово при $d = -2$, -1, 2 и 3.
10. Докажите, что $\mathbb{Q}[\sqrt{d}]$ евклидово при $d = -11$, -7, -3, 5 и 13.
11. Докажите, что $\mathbb{Q}[\sqrt{d}]$ не евклидово при всех отрицательных d, кроме перечисленных в предыдущих двух пунктах.

Все евклидовы поля получаются при $d = -11$, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57 и 73.

Известны все мнимые квадратичные поля, у которых кольцо алгебраических целых чисел факториально, они получаются при $d = -1$, -2, -3, -7, -11, -19, -43, -67, -163. Насколько я знаю, все такие вещественные поля не описаны.

---

[1] Элементы расширения $\mathcal{F}$ для удобства будем называть числами.

[2] Целые алгебраические числа этого расширения называются *гауссовыми числами*.

[3] Целые алгебраические числа этого расширения называются *целыми числами Эйзенштейна*.

Упражнения

12. Опишите все гауссовы простые числа.
13. Найдите все единицы в $\mathbb{Q}[\sqrt{2}]$ и $\mathbb{Q}[\sqrt{3}]$.
14. Объясните, почему равенство $2 \cdot 11 = (5+\sqrt{3})(5-\sqrt{3})$ не противоречит факториальности поля $\mathbb{Q}[\sqrt{3}]$, а равенство $2 \cdot 3 = (\sqrt{-6}) \cdot (-\sqrt{-6})$ доказывает нефакториальность поля $\mathbb{Q}[\sqrt{-6}]$.
15. Решите в целых числах уравнение $x^2 + 2 = y^3$.
16. Решите в целых числах уравнение $x^3 - 4 = y^2$.
17. Пусть p – простое число. Вычислите $\prod_{k=1}^{p-1}(k^2+1) \pmod{p}$.
18. Докажите, что у решения $x^3 + y^3 + z^3 = 0$ нет нетривиальных решений в $\mathbb{Z}^3$.
19. Докажите аналог малой теоремы Ферма для гауссовых чисел: если π – гауссово простое число и a – гауссово число, взаимно простое с π, то $a^{N(\pi)} - a$ кратно π.
20. Докажите, что в любом квадратичном поле есть бесконечно много неразложимых чисел.

Off topic

21. Пусть p – простое число вида $4k+1$, а $d^2 \equiv -1 \pmod{p}$. На координатной плоскости рассмотрим решётку с базисными векторами $(1,0)$, $(\frac{d}{p},1)$ и эллипс в ней, заданный уравнением $px^2 + \frac{y^2}{p} = 1$. При помощи теоремы Минсковского ещё раз докажите, что число p представимо в виде суммы двух квадратов натуральных чисел.
22. Докажите, что каждое натурально число представимо в виде суммы четырёх квадратов целых чисел.