Теория чисел. Листок III .

Задачи из этого листка принимаются до 5 декабря 2016 года.

1. (а) Докажите, что $\mathbb{Z}[\sqrt[3]{6}]$ максимальный порядок в $\mathbb{Q}[\sqrt[3]{6}]$.

(б) Найдите все простые числа, над которыми расширение $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{6}]$ разветвлено.

(в) Докажите, что группа классов $\mathbb{Z}[\sqrt[3]{6}]$ тривиальна.

(г)* Докажите, что уравнение

$$3x^3 + 4y^3 + 5z^3 = 0 \tag{0.1}$$

не имеет нетривиальных рациональных решений. Указание: если (x, y, z) - нетривиальное целое решение, то

$$(x + \sqrt[3]{6}y)(x^2 - xy\sqrt[3]{6} + y^2\sqrt[3]{36}) = 10z^3$$

в $\mathbb{Z}[\sqrt[3]{6}]$. Выведите отсюда следующее соотношение между идеалами в $\mathbb{Z}[\sqrt[3]{6}]$

$$(x + \sqrt[3]{6}y) = (\sqrt[3]{6} - 1)(\sqrt[3]{6} - 2)I^3,$$

для некоторого идеала $I \subset \mathbb{Z}[\sqrt[3]{6}]$.

(д) Докажите, что для любого простого p уравнение (0.1) имеет нетривиальное решение в $\mathbb{Q}_p$. (Очевидно, что оно имеет также решение в $\mathbb{R}$.)

2. (а) Пусть $K \supset \mathbb{Q}$ суть конечное расширение, $O_K \subset K$ - максимальный порядок, r_2 - число невещественных вложений $K \hookrightarrow \mathbb{C}$ с точностью до комлексного сопряжения, $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$. Докажите, что

$$Vol(K_{\mathbb{R}}/A) = 2^{-r_2}\sqrt{Disc(K/\mathbb{Q})}.$$

Здесь $Disc(K/\mathbb{Q})$ обозначает дискриминант расширения. (Заметим, что как $\mathbb{R}$-алгебра $K_{\mathbb{R}}$ изоморфна $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ и, что индусированная с $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ форма объема на $K_{\mathbb{R}}$ не зависит от выбора такого изоморфизма. Поэтому выражение $Vol(K_{\mathbb{R}}/A)$ имеет смысл.)

(б) Докажите, что любое нетривиальное расширение $K \supset \mathbb{Q}$ разветвлено хотя бы над одним простым числом.[1] (Воспользуйтесь Леммой Минковского и утверждением из пункта (а).)

3. Пусть $K \supset \mathbb{Q}$ конечное нормальное расширение с группой Галуа G, $O_K \subset K$ - максимальный порядок, $p \in \mathbb{Z}$ - простое число, а

$$(p) = P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m}$$

- разложение на простые идеалы в O_K.

(а) Докажите, что G действует на O_K, т.е. для любого $g \in G$, $g(O_K) \subset O_K$.

(б) Докажите, что G транзитивно действует на множестве простых идеалов $\{P_1, P_2, \cdots P_m\}$. Выведите отсюда, что $e_1 = e_2 = \cdots = e_m =: e$ и что $|G| = emf$, где f определяется из соотношения $p^f = |O_K/P_1|$.

(в) Допустим, что число e пункта (а) равно 1, т.е. расширение неразветвлено над p. Фиксируем $i \in \{1, \cdots, m\}$. Обозначим через G_{P_i} подгруппу в G состоящую из

[1] В алгебраической геометрии это утверждение интерпретируется так: $spec\mathbb{Z}$ - односвязен.

элементов $g \in G$, таких что $g(P_i) = P_i$. Группа G_{P_i} действует на поле $k = O_K/P_i$. Таким образом, получается отображение

$$G_{P_i} \to Gal(k/\mathbb{F}_p).$$

Докажите, что это изоморфизм. В частности, существует единственный элемент $F_{P_i} \in G_{P_i} \subset G$ такой, что $F_{P_i}(a) = a^p \; mod \, P_i$, для любого $a \in O_K$.
(г) Докажите, что элементы F_{P_i} и F_{P_j} сопряжены в G.

Замечание. В обозначениях задачи 3, обозначим через F_p класс сопряженности в G элементов F_{P_i}. F_p называется элементом Фробениуса, отвечающим простому числу p. Пусть T - множество простых чисел над которыми расширение $K \supset \mathbb{Q}$ неразветвлено. Получается отображение

$$T \longrightarrow \text{ классы сопряженности в G}$$

Глубокая и важная теорема Чеботарева утверждает, что это отображение сюрьективно. Более того, прообраз каждого класса сопряженности бесконечен. Как показывает следующая задача, из этого результата следует теорема Дирихле о простых числах в арифметических прогрессиях.

4. Пусть $p > 2$ - простое число, μ_p - примитивный корень из 1 в $\mathbb{C}$.
(а) Докажите, что $\mathbb{Q}(\mu_p) \supset \mathbb{Q}$ нормальное расширение с группой Галуа $(\mathbb{Z}/p)^*$.
(б) Докажите, что максимальный порядок в $\mathbb{Q}(\mu_p)$ равен $\mathbb{Z}[\mu_p]$ и что расширение $\mathbb{Q}(\mu_p) \supset \mathbb{Q}$ разветвлено только над p.
(в) Для простого $l \neq p$ вычислите элемент Фробениуса $F_l \in (\mathbb{Z}/p)^*$.

5. (а) Пусть K - поле характеристики отличной от 2. Докажите, что существует взаимно-однозначное соответствие между классами изоморфизмов центральных простых алгебр размерности 4 над K и классами эквивалентности квадратичных форм ранга 3 с дискриминантом 1 над K.
(б) Докажите, что любая центральная простая алгебра размерности 4 над K изоморфна алгебре обобщенных кватернионов $H_{a,b}(K)$.
(в) Докажите, что над $\mathbb{Q}_p$ существует ровно одна 4-мерная алгебра с делением.
(г) Пусть D - центральная простая алгебра размерности 4 над $\mathbb{Q}$. Для каждого простого числа p определим локальный нвариант $inv_p(D) \in \{1, -1\}$: $inv_p(D) = 1$ если и только если $D \otimes \mathbb{Q}_p$ - матричная алгебра. Аналогично определяется $inv_\infty(D) \in \{1, -1\}$. Докажите, что $\prod inv_v(D) = 1$ (здесь v пробегает все простые и ∞). Более того, D однозначно определяется своими локальными инвариантыми. Наконец, любой набор $(a_v \in \{1, -1\})$, такой что $a_v = 1$ для почти всех v и $\prod a_v = 1$ реализуется подходящей D.

6. Какие рациональные числа представляются формами?
(а) $2x^2 - 5y^2$
(б)$2x^2 - 6y^2 + 15z^2$?