Теория полей классов

Задача 1°. В этом упражнении и дальше $\mathrm{Cl}(K)$ — группа классов идеалов числового поля K, $h_K = |\mathrm{Cl}(K)|$ — число классов идеалов, $H(K)$ — гильбертово поле классов. a) Пусть E — конечное расширение поля K. Докажите, что $H(K) \subset H(E)$ и что h_K делит $h_E \cdot [E : K]$.
b) Пусть E, F — два конечных расширения $\mathbb{Q}$ внутри $\bar{\mathbb{Q}}$. Докажите, что если $h_E = h_F = 1$, то $h_{E \cap F} = 1$.

Задача 2. a) Пусть E — конечное расширение K, обозначим через L максимальное абелево *вполне неразветвлённое расширение K внутри E (т.е. все простые из K, включая бесконечные, неразветвлены в E). Покажите, что коядро отображения нормы* $N_{E/K}\colon \mathrm{Cl}_E \to \mathrm{Cl}_K$ *изоморфно* $\mathrm{Gal}(L/K)$.
b) Пусть n — положительное целое число, ζ_n — примитивный корень степени n из единицы. Докажите, что число классов $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ делит число классов $\mathbb{Q}(\zeta_n)$.

Задача 3. Гильбертова башня полей классов поля K — это последовательность полей

$$H^{(0)}(K) = K \subset H^{(1)}(K) = H(K) \subset H^{(2)}(K) = H(H(K)) \subset \ldots \subset H^{(i)}(K) \subset \ldots,$$

где каждое $H^{(i)}(K)$ — гильбертово поле классов для $H^{(i-1)}(K)$. Говорят, что она конечная, если $H^{(i+1)}(K) = H^{(i)}(K)$ для какого-то i. Докажите, что гильбертова башня полей классов K конечна тогда и только тогда, когда существует конечное расширение E над K с $h_E = 1$. Голод и Шафаревич доказали в 1964, что существуют числовые поля K, для которых гильбертова башня полей классов бесконечна.

Задача 4°. Покажите, что Гильбертово поле классов $\mathbb{Q}(\sqrt{-5})$ совпадает с $\mathbb{Q}(\sqrt{-5}, \sqrt{5})$.

Задача 5°. Пусть α — корень многочлена $X^3 - X - 1$ в алгебраическом замыкании $\mathbb{Q}$, и пусть $K = \mathbb{Q}(\sqrt{-23})$, $L = K(\alpha)$.
a) Докажите, что L — замыкание Галуа $\mathbb{Q}(\alpha)$ над $\mathbb{Q}$ и что $K \subset L$ — абелево расширение степени 3.
b) Докажите, что в точности два простых в $\mathbb{Q}(\alpha)$ разветвлены над $\mathbb{Q}$ и что они лежат над 23 и ∞. Докажите, что в обоих случаях индекс ветвления равен 2.
c) Докажите, что $K \subset L$ полностью неразветвлено.
d) Докажите, что L — Гильбертово поле классов K.

Задача 6°. Для какого-то простого числа p положим m_p — число различных нулей $X^3 - X - 1$ в $\mathbb{F}_p$. Докажите следующие утверждения:
a) $m_p = 0$ тогда и только тогда, когда $\left(\frac{p}{23}\right) = 1$ и p не может быть записано в виде $p = a^2 + 23b^2$ с $a, b \in \mathbb{Z}$.
b) $m_p = 1$ тогда и только тогда, когда $\left(\frac{p}{23}\right) = -1$.
c) $m_p = 2$ тогда и только тогда, когда $p = 23$.
d) $m_p = 3$ тогда и только тогда, когда p может быть записано в виде $p = a^2 + 23b^2$ с $a, b \in \mathbb{Z}$ и $a \neq 0$.

Задача 7. a) Докажите, что поле $\mathbb{Q}(\sqrt{5})$ имеет число классов 1 и что группа единиц его кольца целых порождена -1 и $(1 + \sqrt{5})/2$.
b) Пусть p — простое число. Докажите, что существует такое поле K, что

$$[K : \mathbb{Q}] = 4, \quad \sqrt{5} \in K, \quad \left|\Delta_{K/\mathbb{Q}}\right| = 25p$$

тогда и только тогда, когда $p \neq 2, 3 \mod 5$. Докажите также, что если такое поле существует, то оно единственным образом с точностью до изоморфизма определяется p. Мы будем обозначать это поле через $K_{(p)}$.

c) Докажите, что среди всех полей $K_{(p)}$ единственным расширением Галуа $\mathbb{Q}$ является поле $K_{(5)}$. Можно ли вложить $K_{(5)}$ в круговое расширение поля $\mathbb{Q}$?

Задача 8. Числовое поле называется вполне вещественным, если оно не имеет комплексных простых; вполне комплексным, если не имеет вещественных простых; и смешанным, если оно не является ни вполне вещественным, ни вполне комплексным. Пусть p — простое число и $p \equiv 1$ или $4 \mod 5$, $K_{(p)}$ — как в предыдущей задаче, а F_n — последовательность чисел Фибоначчи.

a) Докажите, что $K_{(p)}$ смешанное тогда и только тогда, когда $p \equiv 3 \mod 4$.

b) Предположим, что $p \equiv 1 \mod 8$. Докажите, что $K_{(p)}$ вполне вещественное, если p делит $F_{(p-1)/4}$, и вполне комплексное иначе.

c) Предположим, что $p \equiv 5 \mod 8$. Докажите, что $K_{(p)}$ вполне комплексное, если p делит $F_{(p-1)/4}$, и вполне вещественное иначе.

Задача 9. Пусть p — простое число и $p \equiv 11$ или $19 \mod 20$, и пусть $K_{(p)}$ — как и выше. Докажите, что $K_{(p)}$ имеет в точности одно простое, лежащее над 5, если $p \equiv 11 \mod 20$, и в точности два простых, лежащих над 5, если $p \equiv 19 \mod 20$.

Задача 10. $K \subset L$ — конечное абелево расширение числовых полей, $F(L/K)$ — кондуктор L над K, т. е. наибольший общий делитель всех модулей $\mathfrak{m}$ в K, для которых L содержится в полей классов лучей по модулю $\mathfrak{m}$. Пусть $\mathfrak{p}$ — конечное простое из K, лежащее над $p \in \mathbb{Q}$, положим $e = e(\mathfrak{p}/p)$ — индекс ветвления $\mathfrak{p}$ над p. Обозначим через $m = \mathfrak{m}_\mathfrak{p}$ показатель, с которым простое $\mathfrak{p}$ из K входит в $F(L/K)$. Для натурального $i > 0$ обозначим через U_i открытую подгруппу $1 + \mathfrak{p}^i$ в $K_\mathfrak{p}^\times$. Докажите следующие утверждения:

a) Если i, j — положительные целые с $j \not\equiv 0 \mod p$, тогда отображение $U_i \longrightarrow U_i$, отправляющее каждый x в x^j, является изоморфизмом.

b) Если $i > e/(p-1)$, то существует изоморфизм $U_i \longrightarrow U_{i+e}$, отправляющий каждый x в x^p.

c) Если j — положительное целое число, то $(K_\mathfrak{p}^\times)^j$ — открытая подгруппа в $K_\mathfrak{p}^\times$, содержащая $U_{e'+ke}$, где e' — наименьшее целое $> e/(p-1)$ и k — максимальная степень p, на которую делится j.

d) Если $K_\mathfrak{p} \subset E$ — конечное расширение, то $N_{E/K_\mathfrak{p}}(E^\times)$ — открытая подгруппа в $K_\mathfrak{p}^\times$, содержащая $U_{e'+ke}$, где e' такое же, как предыдущем пункте, а k — максимальная степень p, на которую делится $[E : K_\mathfrak{p}]$.

e) Докажите, что $m \leq e' + ke$, где e' — наименьшее целое $> e/(p-1)$ и k — максимальная степень p, на которую делится $[L : K]$.

f) Более точно, докажите, что $m \leq e' + ke$, где e' такое, как раньше, а k — максимальная степень p, делящая показатель группы инерции $I_\mathfrak{p}$ в $\mathrm{Gal}(L/K)$.