Глобальные поля: кольца целых, разложение на простые, адели.

Задача 1 (Евклидовы кольца). Кольцо $\mathcal{O}_K$ называется евклидовым относительно функции $f\colon \mathcal{O}_K \to \mathbb{N}$, если $f(x) = 0$ тогда и только тогда, когда $x = 0$, и для всех $\alpha, \beta \in \mathcal{O}_K \setminus \{0\}$ существует такое $\gamma \in \mathcal{O}_K$, что $f(\alpha - \gamma\beta) < f(\beta)$.

a°) Покажите, что, если $\mathcal{O}_K$ — евклидово, то оно является кольцом главных идеалов.

На самом деле „почти известно“, что „почти“ верно обратное: в предположении обобщённой гипотезы Римана кольцо $\mathcal{O}_K$ для K, не являющегося мнимым квадратичным, евклидово тогда и только тогда, когда оно является кольцом главных идеалов.

b) Покажите, что для евклидова кольца функцию f можно выбрать удовлетворяющей неравенству $f(a) \le f(ab)$ для всех ненулевых a и b.

Подсказка: замените произвольную функцию f на $g(x) = \min\limits_{a \in \mathcal{O}_K \setminus \{0\}} f(ax)$.

c) Назовем $\mathcal{O}_K$ почти евклидовым относительно функции $f : \mathcal{O}_K \to \mathbb{N}$, если $f(x) = 0$ тогда и только тогда, когда $x = 0$, и для всех $\alpha, \beta \in \mathcal{O}_K$, $\beta \nmid \alpha$ существуют такие $\gamma, \delta \in \mathcal{O}_K$, что $0 < f(\alpha\gamma - \beta\delta) < f(\beta)$. Докажите, что $\mathcal{O}_K$ почти евклидово тогда и только тогда, когда оно является кольцом главных идеалов.

Подсказка: в кольце главных идеалов качестве f можно взять $f(x) = 2^{n_1 + \dots + n_m}$, где $x = \epsilon p_1^{n_1} \dots p_m^{n_m}$ — разложение на простые, $\epsilon \in \mathcal{O}_K^\times$.

d) Пусть d — целое отрицательное число, свободное от квадратов, $K = \mathbb{Q}(\sqrt{d})$. Докажите, что кольцо $\mathcal{O}_K$ является евклидовым относительно $f(x) = N_{K/\mathbb{Q}}(x) = x \cdot \bar{x}$ тогда и только тогда, когда сдвиги единичного круга на вектора решётки $\mathcal{O}_K$ покрывают все $\mathbb{C}$.

e) Убедитесь, что условие предыдущего пункта выполнено в том и только в том случае, когда $d \in \{-1, -2, -3, -7, -11\}$.

f^*) Покажите для значений d, не принадлежащих этому списку, $\mathcal{O}_K$ не является евклидовым ни для какой функции $f(x)$.

Подсказка: выберите среди всех необратимых элементов γ с наименьшим значением функции f. Тогда всякое $\alpha \in \mathcal{O}_K$ будет сравнимо с $0, \pm 1$ по модулю γ.

g) Является ли кольцо целых поля $\mathbb{Q}(\sqrt{2})$ евклидовым относительно $N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(x)$?

h^*) Покажите, что кольцо целых поля $\mathbb{Q}(\sqrt{47})$ является кольцом главных идеалов, но не является евклидовым относительно $N_{\mathbb{Q}(\sqrt{47})/\mathbb{Q}}(x)$.

Для квадратичных полей известен полный список колец $\mathcal{O}_K$, являющихся евклидовыми относительно нормы. В случае произвольных расширений $\mathbb{Q}$ такое описание неизвестно.

Задача 2°. Пусть ω — примитивный корень степени три из единицы.

a) Опишите разложение простых из $\mathbb{Z}$ в $\mathbb{Q}(\omega)$.

b) Покажите, что $\mathbb{Q}(\omega)$ является кольцом главных идеалов.

c) Докажите, что простое $p \in \mathbb{Z}$ имеет вид $p = x^2 + xy + y^2$, $x, y \in \mathbb{Z}$ тогда и только тогда, когда $p \equiv 1 \mod 3$ или $p = 3$.

Задача 3. Сколько решений в зависимости от n имеют уравнения:

a) $x^2 + y^2 = n$; b) $x^2 + 2y^2 = n$; c) $x^2 + xy + y^2 = n$; d) $x^2 + xy + 2y^2 = n$; e) $x^2 + xy + 3y^2 = n$.

Задача 4. Покажите, что уравнение $x^4 + 2y^4 = 17z^4$ имеет только тривиальное решение в $\mathbb{Q}$.

Подсказка: используйте однозначность разложения на простые в $\mathbb{Z}[\sqrt{-2}]$.

Задача 5°. Как устроено разложение на простые идеалы простых элементов из $\mathbb{Z}$ для следующих полей:

a) $x^3 - 2$; b) $x^3 - 10$; c) $x^3 - 12x + 2$; d) $x^4 + 2x^2 + 3x + 1$; e) $x^5 - x - 1$.

Задача 6°. Пусть $f_1(x) = x^3 - x^2 - 20x - 1$, $f_2(x) = x^3 - x^2 - 34x - 24$, $f_3(x) = x^3 - x^2 - 52x + 159$, $f_4(x) = x^3 - 41x - 95$ и пусть $K_i/\mathbb{Q}$ — соответствующие расширения.

a) Покажите, что $\mathrm{Disc}_{K_i} = 32009$ для любого i.

b) Убедитесь, что K_i попарно не изоморфны.

Подсказка: Посмотрите на разложение простых в $\mathcal{O}_{K_i}$.

Задача 7. a) Пусть $K = \mathbb{Q}(\alpha)$ — конечное расширение, $\alpha \in \mathcal{O}_K$. Покажите, что, если минимальный многочлен α является многочленом Эйзенштейна как многочлен над $\mathbb{Q}_p$, то $p \nmid [\mathcal{O}_K \colon \mathbb{Z}[\alpha]]$.

b) Найдите кольца целых расширений $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(\sqrt[5]{2})$.

Задача 8 (круговые поля). a) Покажите, что расширение $\mathbb{Q}(\zeta_{p^k})$, полученное присоединением примитивного корня степени p^k из единицы, неразветвлено вне p.

Подсказка: посмотрите на производную $x^{p^k} - 1 \mod p$.

b) Убедитесь, что расширение $\mathbb{Q}(\zeta_{p^k})$ вполне разветвлено в p.

Подсказка: элементы $\frac{\zeta^i - 1}{\zeta^j - 1}$ обратимы в $\mathcal{O}_K$ (здесь $\zeta = \zeta_{p^k}$), так как $\frac{1-\zeta^i}{1-\zeta} = 1 + \zeta + \dots + \zeta^{i-1}$. При этом

$$f(X) = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = \prod_{0 < i < p^k, (i,p)=1} (X - \zeta^i),$$

и $f(1) = p$.

c) Используя предыдущие пункты, покажите, что $\mathcal{O}_{\mathbb{Q}(\zeta_{p^k})} = \mathbb{Z}[\zeta_{p^k}]$.

d) Пусть $K \subset L \subset M$ — расширения числовых полей. Покажите, что

$$\mathrm{Disc}_{M/K} = \mathrm{Disc}_{L/K}^{[M \colon L]} \cdot N_{L/K}(\mathrm{Disc}_{M/L}).$$

e) Найдите кольцо целых циклотомического (т.е. кругового) поля $\mathbb{Q}(\zeta_m)$ для произвольного m.

f) Посчитайте дискриминант кругового поля.

Подсказка: Для $K = \mathbb{Q}(p^k)$ дискриминант равен $\pm p^{p^{k-1}(pk-k-1)}$, где знак минус берется при $p^k = 4$ и $p \equiv 3 \mod 4$, и знак плюс иначе.

g) Как устроено разложение на простые в $\mathbb{Q}(\zeta_m)$?

Циклотомическое расширение $\mathbb{Q}(\zeta_m)$ является важнейшим примером в алгебраической теории чисел, многие общие результаты (теорема Дирихле о единицах, разложение на простые, теория полей классов) доказывались для случая этого поля, а затем переносились (если получалось) на более сложные поля. С теоремы Кронекера–Вебера о том, что всякое абелево расширение $\mathbb{Q}$ вкладывается в $\mathbb{Q}(\zeta_m)$ начинается теория полей классов.

Задача 9. a) Пусть $K/\mathbb{Q}$ — конечное расширение. Определите кольцо целых расширения $K(\sqrt{\alpha})$, где $\alpha \in \mathcal{O}_K$ свободно от квадратов.

b) Пусть k — поле, $K = k(t)$ — поле рациональных функций от t, $L = K(\sqrt{f(t)})$, где $f(t) \in k[t]$ — приведённый неприводимый многочлен. Найдите целое замыкание $k[t]$ в L.

Задача 10 (расширения Куммера). Пусть $K/\mathbb{Q}$ — конечное расширение, содержащее примитивный корень степени n из единицы, $E = K(\sqrt[n]{a})$, где $a \neq b^m$, $b \in K$ для $m \mid n$.

a) Покажите, что дискриминант $D_{E/K} \mid n^n a^{n-1}$.

b) Предположим, что простой идеал $\mathfrak{p} \subset O_K$ неразветвлён в $\mathcal{O}_E$ (т. е. $\mathfrak{p} \nmid na$). Покажите, что степень поля классов вычетов $\mathfrak{p}$ равна f, где f — такое наименьшее натуральное число, что сравнение $x^n \equiv a^f \mod \mathfrak{p}$ разрешимо.

c) Покажите, что, если $\mathfrak{p}^r \mid a$, $\mathfrak{p}^{r+1} \nmid a$, $\mathfrak{p} \nmid n$, где $2 \leq r \leq n-1$, то индекс ветвления идеала $\mathfrak{p}$ равен $n/(r,n)$.

d) Найдите кольцо целых расширения $\mathbb{Q}(\alpha)/\mathbb{Q}, \alpha^n = a$, где a свободно от квадратов.

e^*) Как изменится ответ в предыдущем упражнении, если a не свободно от квадратов?

Задача 11. Опишите кольцо целых $\mathcal{O}_K$ поля разложения многочлена $x^3 - a$ при $a = 2,\ 3,\ 5,\ 6$. Как разлагаются простые из $\mathbb{Z}$ в $\mathcal{O}_K$?

Задача 12. a) Пусть $K/\mathbb{Q}$ — конечное расширение и идеал (p) имеет больше p простых сомножителей с нормой p в разложении в произведение простых идеалов в $\mathcal{O}_K$. Покажите, что $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ для любого $\alpha \in K$.

b) Пусть $K = \mathbb{Q}(\gamma)$, $\gamma^3 - 2\gamma^2 - 9\gamma + 2 = 0$. Найдите базис $\mathcal{O}_K$ и вычислите Disc_K.

c) Покажите, что $2\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, где $\mathfrak{p}_i \subset \mathcal{O}_K$ — простые идеалы. Таким образом $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ для любого $\alpha \in K$. Как устроено разложение остальных простых из $\mathbb{Z}$ в $\mathcal{O}_K$?

d^*) Докажите, что для любого n найдется конечное расширение $\mathbb{Q}$, кольцо целых которого не порождается n элементами (как кольцо над $\mathbb{Z}$).

Задача 13 (вычисление групп Галуа). Пусть K — числовое поле, $f(x) \in \mathcal{O}_K[x]$ — приведённый многочлен без кратных корней, $\deg f = n$, G — группа Галуа поля разложения $f(x)$.

a°) Предположим, что G имеет в точности s орбит как группа перестановок n-элементного множества корней $f(x)$, а порядки орбит равны $n_1, \ldots, n_s$. Тогда имеется разложение $f(x) = f_1(x) \ldots f_s(x)$, где $f_i(x) \in K[x]$ — неприводимые многочлены степени n_i.

b°) Пусть $\mathfrak{p}$ — простой идеал $\mathcal{O}_K$ и $f(x) \equiv f_1(x) \ldots f_s(x) \mod \mathfrak{p}$, где $f_i(x)$ — различные неприводимые многочлены степени n_i с коэффициентами из $k = \mathcal{O}_K/\mathfrak{p}$. Тогда в G найдется перестановка σ, являющаяся произведением непересекающихся циклов длин n_i.

c°) Каков аналог утверждения предыдущего пункта для вещественных нормирований?

d°) Вычислите группу Галуа многочлена $x^5 - x - 1$.

e°) Пусть $K/\mathbb{Q}$ — расширение Галуа, в котором простой идеал $(p) \subset \mathbb{Z}$ остаётся простым. Покажите, что группа $\mathrm{Gal}(K/\mathbb{Q})$ является циклической.

f) Пусть H — подгруппа S_n, действующая транзитивно на множестве корней и содержащая $(n-1)$-цикл и транспозицию. Тогда $H = S_n$.

g) Используя предыдущую задачу, найдите для всех n многочлен степени n над $\mathbb{Q}$, имеющий группу Галуа S_n.

h) Пусть $K/\mathbb{Q}$ — поле алгебраических чисел степени n с дискриминантом, свободным от квадратов. Покажите, что нормальное замыкание K имеет степень $n!$ над $\mathbb{Q}$ и группу Галуа S_n.

Этот метод вычисления групп Галуа применим к произвольным многочленам и является самым эффективным на практике. Дополнительными ингредиентами, которые обеспечивают работу метода, являются теорема плотности Чеботарёва, гарантирующая существование простого, элемент Фробениуса которого имеет любой заданный циклический тип из G, а также характеризацию подгрупп S_n (при небольших n) в терминах классов сопряжённости.

Задача 14. a) Для поля дискретного нормирования K с кольцом нормирования $\mathcal{O}$ и максимальным идеалом $\mathfrak{m}$ покажите, что замыкание $\mathcal{O}$ в пополнении поля $\hat{K}$ изоморфно $\varprojlim \mathcal{O}/\mathfrak{m}^n\mathcal{O}$, где $n \in \mathbb{N}$.

b) Пусть K — поле алгебраических чисел, $\hat{\mathcal{O}}_K = \varprojlim \mathcal{O}_K/n\mathcal{O}_K$, где n пробегает все натуральные числа. Покажите, что $\hat{\mathcal{O}}_K^\times \cong \prod\limits_{v<\infty} \hat{\mathcal{O}}_{K,v}^\times$ в смысле изоморфизма топологических групп.

Задача 15 (характеры $\mathbb{Q}$). Цель этой задачи — описать характеры аддитивной группы $\mathbb{Q}$, то есть $\mathrm{Hom}(\mathbb{Q}, S^1)$, где $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$.

a) Покажите, что все *непрерывные* характеры $\mathbb{R}$ есть отображения вида $x \mapsto \psi_\infty(xy) = \exp(-2\pi i y x)$, $y \in \mathbb{R}$.

b) Для $x \in \mathbb{Q}_p$ обозначим через $\{x\}_p \in \mathbb{Q}$ p-адическую дробную часть x, т. е. вклад членов с отрицательными степенями p в p-адическом разложении x. Покажите, что все непрерывные (т. е. локально-постоянные) характеры $\mathbb{Q}_p$ имеют вид $x \mapsto \psi_p(xy) = e^{2\pi i\{xy\}_p}$, $y \in \mathbb{Q}_p$.
c) Для $a = (a_\infty, a_2, a_3, \dots) \in \mathbb{A}_\mathbb{Q}$ определим характер $\mathbb{Q}$ формулой

$$r \mapsto \psi_a(r) = \psi_\infty(a_\infty r) \prod_p \psi_p(a_p r).$$

Докажите, что $\psi_a = \psi_{a'}$ тогда и только тогда, когда $a - a' \in \mathbb{Q}$.
Подсказка: всякий элемент из $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$ имеет единственный представитель из множества $[0,1) \times \prod_p \mathbb{Z}_p$.
d) Докажите, что группа характеров $\mathbb{Q}$ изоморфна группе классов аделей $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$.
Подсказка: разбейте характер χ группы $\mathbb{Q}$ в произведение локальных характеров χ_∞, χ_p, где $\chi_\infty(1) = \chi(1)$, *а χ_p принимают значения в группе корней степени p^k из единицы,* $k = 1, 2, \dots$.
e) Обобщите предыдущий результат на произвольное поле алгебраических чисел $K/\mathbb{Q}$.

Задача 16 (фундаментальные области). Пусть K — поле алгебраических чисел, V_∞ — множество его архимедовых нормирований.
a) Пусть $w_1, \dots, w_n$ — базис $\mathcal{O}_K/\mathbb{Z}$, $F_\infty = \{t_1 w_1 + \dots + t_n w_n \mid 0 \le t_i < 1\} \subset \prod_{v \in V_\infty} K_v$. Покажите, что $F_\infty \times \prod_{v \notin V_\infty} \hat{\mathcal{O}}_{K,v}$ — фундаментальная область для группы классов аделей $\mathbb{A}_K/K$.
b) Фиксируем $v_0 \in V_\infty$, $V'_\infty = V_\infty \setminus \{v_0\}$. Пусть $l\colon I_K^1 \to I_{K,V_\infty}^1 \to H^{r-1} \subset \mathbb{R}^r$ — логарифмическое отображение из группы иделей с содержанием 1 в гиперплоскость $H^{r-1}\colon x_1 + \dots + x_r = 0$, $r = r_1 + r_2$. Обозначим через ϵ_i базис свободной части группы единиц K, а через ω число корней из 1 в K. Пусть P множество точек вида $\sum_{i=1}^{r-1} z_i l(\epsilon_i)$ с $0 \le z_i < 1$. Рассмотрим $E = \{b \in l^{-1}(P) \mid 0 \le \arg b_{v_0} \le \frac{2\pi}{\omega}\}$ и элементы $b_1, \dots, b_h \in I_K^1$, представляющие все классы идеалов K. Докажите, что множество $Eb_1 \cup Eb_2 \cup \dots \cup Eb_h$ является фундаментальной областью группы классов иделей с содержанием один $I_K^1/K^\times$.
c) Вычислите объем $\mathbb{A}_K/K$ и $I_K^1/K^\times$ относительно меры Хаара.

Задача 17. a) Пусть K — глобальное поле, $\mathfrak{a}$ — собственный идеал в $\mathcal{O}_K$. Покажите, что естественное отображение $SL_n(\mathcal{O}_K) \longrightarrow SL_n(\mathcal{O}_K/\mathfrak{a})$ является сюръекцией.
Подсказка: теорема об аппроксимации Вам поможет.
b) Проделайте то же самое для группы GL_n.