Разложимые формы, решетки, единицы и число классов идеалов.

Задача 1° (Теорема Блихфельда). Пусть $k > 0$ - натуральное число, $X \subset \mathbb{R}^n$, $\mathrm{Vol}(X) > k$. Докажите, что найдется $k+1$ различных точек $s_0, \dots, s_k \in X$ с условием $s_i - s_j \in \mathbb{Z}^n$ при $i, j = 0, \dots, k$.

Задача 2. a) Покажите, что условие $\mathrm{Vol}(X) > 2^n \mathrm{Vol}(\mathbb{R}^n/L)$ в лемме Минковского нельзя заменить более слабым (здесь X — выпуклое центрально-симметричное множество, а L — решетка в $\mathbb{R}^n$).

b) Докажите, что, если X — компактно, то утверждение леммы Минковского остается верными и при $\mathrm{Vol}(X) = 2^n \mathrm{Vol}(\mathbb{R}^n/L)$.

Задача 3°. Пусть $c_1, \dots, c_n$ — вещественные положительные числа, вещественная матрица (a_{ij}) обратима и $c_1 c_2 \dots c_n > |\det(a_{ij})|$. Покажите, что найдутся такие целые числа x_i, не все равные нулю, что $\sum_{i=1}^n a_{ij} x_i < c_i$, $1 \le i \le n$.

Задача 4°. a) Пусть $a_{i,j} \in \mathbb{Z}$, $i, j = 1, \dots, n$, а m_i — целые положительные числа. Покажите, что множество целых точек $(x_1, \dots, x_n) \in \mathbb{R}^n$, удовлетворяющих системе сравнений $\sum_{i=1}^n a_{ij} x_i \equiv 0 \mod m_j$ образует решетку полного ранга в $\mathbb{R}^n$, кообъема не больше $m_1 \dots m_n$.

b) Пусть $m > 0$, r, s — целые числа, для которых $r^2 + s^2 + 1 \equiv 0 \mod m$. Пусть L — множество всех $(x, y, z, w) \in \mathbb{Z}^4$ с условиями $x \equiv rz + sw \mod m$ и $y \equiv sz - rw \mod m$. Покажите, что найдется точка $(a, b, c, d) \neq 0$ из L, для которой $a^2 + b^2 + c^2 + d^2 < 2m$. Выведите отсюда, что $a^2 + b^2 + c^2 + d^2 = m$.

c) Убедитесь, что условия предыдущего пункта выполнены, если m — нечетное или удвоенное нечетное число. Выведите отсюда, что каждое положительное целое число есть сумма квадратов четырех целых чисел.

Задача 5. Пусть $g(x_1, \dots, x_n)$ — квадратичная форма над $\mathbb{Z}$ с определителем D (т. е. её матрица $A \in M_n(\mathbb{Z})$ и $\det A = D$). Пусть $m = \min\limits_{x \in \mathbb{Z}^n} g(x)$. Докажите, что $m \le 4 V_n^{-2/n} |D|^{1/n}$, где V_n — объем единичного шара размерности n.

Подсказка: вам поможет лемма Минковского о выпуклом теле.

Задача 6 (Теорема Минковского–Хассе для трех переменных). Пусть a, b, c — попарно взаимно простые и свободные от квадратов ненулевые целые числа, и пусть $|abc| = 2^\lambda p_1 \dots p_s$, где p_i — различные нечетные простые, а $\lambda = 0$ или 1. Предположим, что форма $ax^2 + by^2 + cz^2$ представляет ноль в $\mathbb{Q}_p$ для всех p.

a) Докажите, что найдутся такие целочисленные линейные формы от трех переменных $L_1, \dots, L_s, L', L''$, что для $u, v, w \in \mathbb{Z}$, удовлетворяющих системе сравнений $L_i(u, v, w) \equiv 0 \mod p_i$ $(1 \le i \le s)$, $L'(u, v, w) \equiv 0 \mod 2^{1+\lambda}$, $L''(u, v, w) \equiv 0 \mod 2$ выполнено $au^2 + bv^2 + cw^2 \equiv 0 \mod 4|abc|$.

b) Пусть M — решетка в $\mathbb{R}^3$, образованная тройками чисел (u, v, w), удовлетворяющими сравнениям из предыдущего пункта. Покажите, что в эллипсоиде $|a|u^2 + |b|v^2 + |c|w^2 < 4|abc|$ найдется точка из M. Выведите, что форма $ax^2 + by^2 + cz^2$ имеет нетривиальный ноль над $\mathbb{Q}$.

Подсказка: проверьте, что объем эллипсоида равен $\frac{32\pi}{3}|abc|$ и воспользуйтесь леммой Минковского.

Задача 7°. a) Найдите группу классов идеалов $\mathbb{Q}(\sqrt{-D})$ для $D = 1, 2, 3, 5, 6, 7, 10, 11, 13, 15$.

Подсказка: используйте границу Минковского. Для получения соотношений в группе классов посчитайте нормы элементов из $\mathbb{Q}(\sqrt{-D})$.

b) Докажите, что в кольце целых поля $\mathbb{Q}(\sqrt{-D})$ имеется однозначное разложение на простые множители для $D = 1, 2, 3, 7, 11, 19, 43, 67, 163$.

Методами теории эллиптических кривых и модулярных форм можно доказать, что этот список исчерпывает все мнимые квадратичные поля с однозначным разложением на простые множители (гипотеза Гаусса).

Задача 8°. Чему равно число классов идеалов поля $\mathbb{Q}(\alpha)$, где α — корень многочлена a) $x^3 - x - 1$; b) $x^3 + x + 1$; c) $x^3 - x + 2$; d) $x^5 - x - 1$.

Задача 9. Пусть $p_1, \dots, p_m$ — различные нечетные простые, $D = p_1 \dots p_m$. Покажите, что группа классов идеалов $\mathbb{Q}(\sqrt{D})$ содержит подгруппу, изоморфную $(\mathbb{Z}/2\mathbb{Z})^{m-1}$.
Подсказка: воспользуйтесь тем, что p_i разветвленные простые.

Задача 10 (Сопряженность матриц и группа классов). Пусть R — кольцо, $M_n(R)$ — множество $n \times n$ матриц с коэффициентами из R. Будем говорить, что A и B из $M_n(R)$ сопряжены над R, если найдется такая обратимая матрица $U \in \mathrm{GL}_n(R)$, что $A = UBU^{-1}$.
a) Пусть $R = F$ — поле. Покажите, что две матрицы из $M_n(F)$ с одинаковым характеристическим многочленом $f(t)$ сопряжены, если $f(t)$ неприводим над F.

b) Покажите, что классы идеалов порядка $\mathbb{Z}[\alpha]$ есть в точности классы изоморфизма $\mathbb{Z}[\alpha]$-модулей, которые изоморфны $\mathbb{Z}^n$ как абелевы группы.

c) Докажите, что классы сопряженности матриц из $M_n(\mathbb{Z})$ с характеристическим многочленом $f(t) \in \mathbb{Z}[t]$ находятся в биективном соответствии с классами идеалов в порядке $\mathbb{Z}[\alpha]$ поля $\mathbb{Q}(\alpha)$, где α — корень $f(t)$.
Подсказка: структура $\mathbb{Z}[\alpha]$-модуля на $\mathbb{Z}^n$ — это то же самое, что линейное отображение $A\colon \mathbb{Z}^n \to \mathbb{Z}^n$, удовлетворяющее условию $f(A) = 0$.

d) Выпишите явно матрицы из $M_2(\mathbb{Z})$, представляющие различные классы сопряженности матриц с характеристическим многочленом $t^2 + 5$.

e) Пусть $d \in \mathbb{Z}$ — не квадрат и $m \geq 2$. Сопряжены ли над $\mathbb{Z}$ матрицы $\begin{pmatrix} 0 & md \\ d & 0 \end{pmatrix}$ и $\begin{pmatrix} 0 & m^2 d \\ 1 & 0 \end{pmatrix}$? Каким классам идеалов они соответствуют?

f^*) Приведите пример такой матрицы $A \in M_2(\mathbb{Z})$, что A и A^T не сопряжены над $\mathbb{Z}$ (над полем эти матрицы всегда сопряжены).

Задача 11 (Орбиты SL_2 и группа классов). a) Пусть K — числовое поле, $SL_2(\mathcal{O}_K)$ — множество обратимых 2×2 матриц с коэффициентами из $\mathcal{O}_K$, имеющих определитель 1. Рассмотрим действие $SL_2(\mathcal{O}_K)$ на $\mathbb{P}^1(K)$ дробно-линейными преобразованиями ($A(x\colon y) = (ax + by\colon cx + dy)$, если $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$). Покажите, что число орбит действия $SL_2(\mathcal{O}_K)$ на $\mathbb{P}^1(K)$ равно числу классов идеалов K.
Подсказка: каждый дробный идеал порождается двумя элементами. Для простоты можете сначала разобрать случай, когда число классов идеалов равно 1.

b) Пусть $\mathcal{O}$ — порядок в мнимом квадратичном поле K с дискриминантом $D = f^2 D_K$. Покажите, что в каждом классе идеалов есть единственный представитель вида $\mathfrak{a} = \mathbb{Z} + \gamma\mathbb{Z}$, где $\gamma = \frac{-b + i\sqrt{D}}{2a}$ и $-a \leq b < a$, $c \geq a$, $b \leq 0$, $c > a$, $b > 0$.
Подсказка: это на самом деле общий результат про подобие решеток в $\mathbb{R}^2 = \mathbb{C}$, вспомните, как устроена фундаментальная область при действии $SL_2(\mathbb{Z})$ на верхнюю полуплоскость.

c^*) Каков аналог предыдущей задачи для вещественных квадратичных полей?

Задача 12 (Квадратичные формы и число классов идеалов). a) Пусть $K/\mathbb{Q}$ — квадратичное расширение с дискриминантом D_K, $\mathfrak{a} \subset K$ — дробный идеал в K, a_1, a_2 — базис $\mathfrak{a}$ как $\mathbb{Z}$-модуля. Покажите, что $Q_{a_1,a_2}(x, y) = (\mathrm{N}\mathfrak{a})^{-1} \cdot \mathrm{N}_{K/\mathbb{Q}}(a_1 x + a_2 y)$ — целочисленная квадратичная форма, имеющая дискриминант D_K.

b) Если $D_K > 0$, определим $\mathrm{Cl}^+(K) = \mathrm{Id}(K)/\mathrm{P}^+(K)$, где $\mathrm{P}^+(K)$ — группа главных идеалов вида (α), где $\sigma(\alpha) > 0$ для любого вложения σ из K в $\mathbb{R}$. Положим $\mathrm{Cl}^+(K) = \mathrm{Cl}(K)$, если $D_K < 0$. Докажите, что класс эквивалентности формы $Q_{a_1,a_2}(x,y)$ зависит только от образа идеала $\mathfrak{a}$ в Cl^+K.

c) Проверьте, что отображение из предыдущего пункта определяет биекцию между классами эквивалентности бинарных квадратичных форм с дискриминантом D_K и группой $\mathrm{Cl}^+(K)$.

В случае расширений большей степени такой биекции между классами идеалов и классами эквивалентности форм уже нет.

d) Как обобщить утверждение предыдущего пункта на случай форм с произвольным дискриминантом?

e) Пусть квадратичная форма $f(x,y)$ соответствует классу идеалов C в порядке $\mathcal{O}$. Покажите, что имеется взаимно однозначное соответствие между неассоциированными решениями уравнения $f(x,y) = m$ и идеалами $\mathcal{O}$, принадлежащими классу C^{-1} и имеющими норму m.

Подсказка: решение, соответствующее идеалу $\mathfrak{a}$ задается таким элементом ξ, что $\mathfrak{a} = \xi\mathfrak{c}^{-1}$, где $\mathfrak{c} \in C^{-1}$.

Задача 13. a) Пусть K — числовое поле, $\mathfrak{a} \subset K$ — дробный идеал в K. Предположим, что $\mathfrak{a}^m = (a)$ — главный идеал. Докажите, что в поле $K(\sqrt[m]{a})$ идеал $\mathfrak{a}$ становится главным.

b) Покажите, что существует такое конечное расширение L/K, что всякий идеал из $\mathcal{O}_K$ становится главным в $\mathcal{O}_L$.

На самом деле каждый идеал из K становится главным в максимальном абелевом неразветвленном расширении L/K (гильбертово поле классов K) и L — наименьшее с таким свойством.

Задача 14. Докажите, что существует конечное число полей алгебраических чисел с заданным дискриминантом.

Подсказка: используя лемму Минковского о выпуклом теле, покажите, что найдется целый примитивный элемент в K, коэффициенты минимального многочлена которого оцениваются в терминах D.

Задача 15°. Пусть S — конечное подмножество множества простых идеалов поля алгебраических чисел K. Определим множество S-целых как $\mathcal{O}_K(S) = \bigcap_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}} = \{\alpha \in K \mid \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0 \text{ для всех } \mathfrak{p} \notin S\}$. Покажите, что группа S-единиц $\mathcal{O}_K(S)^\times = \{\alpha \in K \mid \mathrm{ord}_{\mathfrak{p}}(\alpha) = 0 \text{ для всех } \mathfrak{p} \notin S\}$ является конечно порожденной абелевой группой ранга $r + s + |S| - 1$. Каково её кручение?

Задача 16 (Единицы в вещественных квадратичных полях). Пусть $d > 0$ — свободно от квадратов, $K = \mathbb{Q}(\sqrt{d})$ — вещественное квадратичное поле. Пусть $\mathcal{O}_f = \mathbb{Z}[f\omega] = \mathbb{Z} + \mathbb{Z}f\omega$ — порядок в кольце целых $\mathcal{O}_K$, $\omega = \frac{1+\sqrt{D_K}}{2}$ (D_K — дискриминант K). Пусть ϵ — фундаментальная единица в $\mathcal{O}_f$, однозначно определенная условием $\epsilon > 1$. Предполагаем, что $d \neq 5$ или $f \neq 1$ (в случае $d = 5, f = 1$ все вычисляется явно: $\epsilon = \frac{1+\sqrt{5}}{2}$).

a) Пусть $\eta > 1$ — любая единица из $\mathcal{O}_f^\times$, $\eta = x + yf\omega$. Покажите, что $x, y > 0$.

b) Докажите, что $\left|\frac{x}{y} + f\omega'\right| < \frac{1}{2y^2}$, где $\omega' = \frac{1-\sqrt{D_K}}{2}$.

c) Обоснуйте следующий алгоритм нахождения фундаментальной единицы ϵ. Раскладываем число $-f\omega'$ в цепную дробь $[a_0; a_1, \ldots, a_n, \ldots]$. Считаем подходящие дроби $P_k/Q_k = [a_0; a_1, \ldots, a_k]$ и норму $r_k = \mathrm{N}_{K/\mathbb{Q}}(P_k + \omega f Q_k)$. Если k — первое число такое, что $r_k = \pm 1$, то $\epsilon = P_k + \omega f Q_k$.

Подсказка: классическая теорема из теории цепных дробей утверждает, что, если для $\xi \in \mathbb{R}$ и натуральных взаимно простых x, y имеет место неравенство $\left|\frac{x}{y} - \xi\right| < \frac{1}{2y^2}$, то $\frac{x}{y}$ — одна из подходящих дробей для разложения ξ в цепную дробь.

d^*) Как связано число k из предыдущего пункта с длиной периода цепной дроби для $-f\omega'$?

e°) Найдите основную единицу порядка $\mathbb{Z}[3\sqrt{6}]$ поля $\mathbb{Q}(\sqrt{6})$.

Задача 17°. Найдите фундаментальную единицу и группу классов идеалов поля $\mathbb{Q}(\sqrt{D})$ для $D = 1, 2, 3, 5, 6, 7, 10, 11, 13, 15$.

Задача 18°. Покажите, что в поле $\mathbb{Q}(\sqrt[3]{2})$ всякая единица имеет вид $\pm(1+\sqrt[3]{2})^k, k \in \mathbb{Z}$.

Задача 19°. Пусть a, b — натуральные числа, не являющиеся квадратами. Покажите, что фундаментальная единица порядка $\mathbb{Z}[\sqrt{a}]$ поля $\mathbb{Q}(\sqrt{a})$ является также фундаментальной единицей порядка $\mathbb{Z}[\sqrt{a}, \sqrt{-b}]$ в поле $\mathbb{Q}(\sqrt{a}, \sqrt{-b})$.

Задача 20. a°) Покажите, что ранг группы единиц кубического расширения $K/\mathbb{Q}$ равен 1 тогда и только тогда, когда дискриминант $D_K < 0$.

b) Пусть $K/\mathbb{Q}$ — кубическое расширение с отрицательным дискриминантом, $\epsilon > 1$ — фундаментальная единица K (почему на нее можно наложить такое условие?), $\epsilon = u^2, u \in \mathbb{R}, u > 1$. Пусть элементы сопряженные с ϵ имеют вид $u^{-1}e^{i\theta}$, $u^{-1}e^{-i\theta}$, $0 \le \theta \le \pi$. Положим $D' = D(1, \epsilon, \epsilon^2)$ — дискриминант минимального многочлена для ϵ. Убедитесь, что $D' = 4(\xi - \cos\theta)\sin\theta$, где $2\xi = u^3 + u^{-3}$.

c) Покажите, что $|D'| \le 16(\xi^2 - 2\xi x_0 + x_0^2)(1 - x_0^2)$, где x_0 — корень уравнения $\xi x - 2x^2 + 1 = 0$, $|x_0| \le 1$. Выведите отсюда неравенство $|D'| < 4u^6 + 24$.

d) Получите оценку $|D_K| < 4\epsilon^3 + 24$.

e) Покажите, что α — фундаментальная единица поля $K = \mathbb{Q}(\alpha)$, если α — корень многочлена $x^3 + 10x + 1$.

f) Покажите, что $\mathrm{Cl}(K) \cong \mathbb{Z}/6\mathbb{Z}$ для поля K из предыдущего пункта.

Задача 21. Поле алгебраических чисел K называется вполне вещественным (чисто мнимым), если образ всех вложений K в $\mathbb{C}$ лежит в $\mathbb{R}$ (соответственно не лежит в $\mathbb{R}$). CM-поле L — это чисто мнимое квадратичное расширение вполне вещественного поля L^+. Покажите, что индекс группы $\mu_L \cdot \mathcal{O}_{L^+}^\times$ в $\mathcal{O}_L^\times$ равен 1 или 2. Здесь μ_L — группа корней из 1, содержащихся в L.

Подсказка: реализуйте $\mu_L \cdot \mathcal{O}_{L^+}^\times$ как ядро отображения $\mathcal{O}_L \to \mu_L/\mu_L^2$, переводящего a в $a/\bar{a}$.

Задача 22°. a) Покажите, что в поле $\mathbb{Q}(\sqrt[3]{2})$ кольцом множителей модуля $M = 4\,\mathbb{Z} + \sqrt[3]{2}\,\mathbb{Z} + \sqrt[3]{4}\,\mathbb{Z}$ является порядок $\mathbb{Z} + 2\sqrt[3]{2}\,\mathbb{Z} + 2\sqrt[3]{4}\,\mathbb{Z}$.

b) Найдите кольцо множителей для модуля $M = 2\,\mathbb{Z} + 2\sqrt[3]{2}\,\mathbb{Z} + \sqrt[3]{4}\,\mathbb{Z}$.

Задача 23°. Опишите все решения в целых числах уравнений:

a) $x^2 - 2y^2 = 7$;

b) $3x^2 - 4y^2 = 11$;

c) $17x^2 + 32xy + 14y^2 = 9$;

d) $80x^2 - y^2 = 16$;

e) $13x^2 + 34xy + 22y^2 = 23$.

Задача 24 (Контрпример Сельмера). В этом упражнении наша цель показать, что уравнение $3x^3 + 4y^3 + 5z^3 = 0$ не имеет нетривиального решения в $\mathbb{Q}$. В листке 3 мы видели, что такое уравнение всегда имеет решение в $\mathbb{Q}_p$. Это показывает, что аналог теоремы Минковского–Хассе для форм степени > 3 не выполняется.

a) Пусть $K = \mathbb{Q}(\sqrt[3]{6})$. Покажите, что, если уравнение $3x^3 + 4y^3 + 5z^3 = 0$ имеет нетривиальное рациональное решение, то уравнение $\mathrm{N}_{K/\mathbb{Q}}(a + b\sqrt[3]{6}) = 10c^3$ имеет нетривиальное рациональное решение с попарно взаимно простыми $a, b, c \in \mathbb{Z}$.

b) Убедитесь, что $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{6}]$.

c) Покажите, что $h(K) = 1$.

d) Убедитесь, что группа единиц поля K порождена элементом $\epsilon = 1 - 6\sqrt[3]{6} + 3\sqrt[3]{36}$.

e) Пусть $L/\mathbb{Q}$ — кубическое расширение, $p \in \mathbb{Z}$ — простое и $p\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ — произведение трех различных простых идеалов. Известно, что $\alpha \in \mathcal{O}_L$ делится на $\mathfrak{p}_1\mathfrak{p}_2$ и $\mathrm{Tr}_{L/\mathbb{Q}}(\alpha) = 0$. Докажите, что $\mathfrak{p}_3 \mid \alpha$ и, следовательно, $p \mid \alpha$.

f) Предположим, что уравнение $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = 10c^3$, $\alpha = a + b\sqrt[3]{6} \in \mathcal{O}_K$ имеет решение со взаимно простыми a и b. Докажите, что $\alpha = \alpha_0\xi^3$, где $\xi \in \mathcal{O}_K$, а α_0 — одно из чисел $\lambda\mu, \lambda\mu\epsilon, \lambda\mu\epsilon^2, \lambda\nu, \lambda\nu\epsilon, \lambda\nu\epsilon^2$, где $\lambda = 2 - \sqrt[3]{6}$ ($\mathrm{N}_{K/\mathbb{Q}}(\lambda) = 2$); $\mu = \sqrt[3]{6} - 1$ ($\mathrm{N}_{K/\mathbb{Q}}(\mu) = 5$); $\nu = (\sqrt[3]{36} + \sqrt[3]{6} + 1)^2 = 13 + 8\sqrt[3]{6} + 3\sqrt[3]{36}$ ($\mathrm{N}_{K/\mathbb{Q}}(\nu) = 5 \cdot 5^3$).

Подсказка: примените предыдущий пункт к числу $\alpha \cdot \sqrt[3]{6}$, *используйте также разложение на простые множители в* K *чисел* $2, 3, 5$.

g) В предыдущем пункте положим $\xi = u + v\sqrt[3]{6} + w\sqrt[3]{36}$ и запишем $\alpha = \alpha_0\xi^3 = a_0(u,v,w) + a_1(u,v,w)\sqrt[3]{6} + a_3(u,v,w)\sqrt[3]{36}$. Покажите, что для всех шести возможных значений α_0 уравнение $a_2(u,v,w) = 0$ имеет только тривиальное решение в $\mathbb{Q}_3$ (а значит и в $\mathbb{Q}$).