Квадратичные формы.

Задача 1. Пусть V — конечномерное векторное пространство над полем k, $\operatorname{char} k \neq 2$, $Q\colon V \to k$ — квадратичная форма. Назовем метрическим морфизмом пар (V, Q) и (V', Q') такое линейное отображение $f\colon V \to V'$, что $Q' \circ f = Q$.

a) Пусть $v, w \in V$ — такие два вектора, что $Q(v) = Q(w) \neq 0$. Покажите, что существует метрический автоморфизм V, переводящий v в w.

Подсказка: если $Q(v - w) \neq 0$, то достаточно рассмотреть отражение относительно $v - w$, иначе рассмотрите отражение относительно $v + w$.

b) (Теорема Витта) Пусть V_1 и V_2 подпространства квадратичного пространства (U, Q), $\phi\colon V_1 \to V_2$ — изометрия. Покажите, что ϕ продолжается до метрического автоморфизма (U, Q).

Подсказка: возьмите такие $v \in V_1$ и λ — метрический автоморфизм (U, Q), что $Q(v) \neq 0$ и λ переводит $\phi(v)$ в v. Тогда замена ϕ на $\lambda\phi$ и V_2 на $\lambda(V_2)$ позволяет считать, что $v \in V_1 \cap V_2$. Примените предположение индукции к ортогональному дополнению к v.

c) Переформулируйте и передокажите в инвариантных терминах остальные утверждения о квадратичных формах, доказанные в лекциях.

Подсказка: начните с утверждения о том, что изотропное пространство всегда содержит гиперболическое.

Задача 2°. При каких p следующие формы представляют ноль над $\mathbb{Q}_p$:

a) $5x_1^2 - x_2^2 - 3x_2^2$; b) $x_1^2 + x_2^2 + 7x_3^2 + 5x_4^2$?

Задача 3°. Определите все p, для которых следующие формы эквивалентны над $\mathbb{Q}_p$:

a) $3x_1^2 + 7x_2^2$ и $x_1^2 + 84x_2^2$;

b) $x_1^2 - 3x_2^2 + 15x_3^2$ и $3x_1^2 - 5x_2^2 + 3x_3^2$;

c) $x_1^2 - 5x_2^2 + 3x_3^2 - 7x_4^2$ и $x_1^2 - x_2^2 + x_3^2 - x_4^2$.

Задача 4°. Убедитесь, что символ Гильберта $(a, b)_2$ является невырожденной билинейной формой $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \times \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \to \mathbb{Z}/2\mathbb{Z} = \{\pm 1\}$. Запишите матрицу этой формы в базисе $2, -1, 5$.

Задача 5. a) Пусть $n(x, y, z) = x^2yz + y^2zx + z^2xy + x^2y^2 + y^2z^2 + z^2x^2 - x^4 - y^4 - z^4$. Убедитесь, что $n(x, y, z) \equiv -1 \mod 4$ для всякой примитивной точки $(x, y, z) \in \mathbb{Z}_2^3$.

b) Положим $f(x_1, \ldots, x_9) = n(x_1, x_2, x_3) + n(x_4, x_5, x_6) + n(x_7, x_8, x_9)$ и $F(x_1, \ldots, x_{18}) = f(x_1, \ldots, x_9) + 4f(x_{10}, \ldots, x_{18})$. Покажите, что F не имеет нетривиального нуля в $\mathbb{Q}_2$.

Это даёт контрпример к гипотезе Артина о том, что всякий однородный многочлен степени d над $\mathbb{Q}_p$ от $d^2 + 1$ и более переменных имеет нетривиальный ноль. Эта гипотеза верна для $d = 1, 2, 3$ и для любого d и всех p, больших некоторой границы (зависящей от d).

Задача 6*. a) Определите символ Гильберта для поля степенных рядов $\mathbb{F}_q((t))$. Опишите его основные свойства.

b) Когда квадратичная форма над $\mathbb{F}_q((t))$ представляет ноль? Когда две формы над этим полем эквивалентны? Дайте ответы, аналогичные случаю поля $\mathbb{Q}_p$.

c) Что в этом случае можно сказать про теорему Минковского–Хассе?

Задача 7°. Какие из следующих форм представляют ноль над $\mathbb{Q}$:

a) $x_1^2 + x_2^2 - 15(x_3^2 + x_4^2)$; b) $3x_1^2 + 2x_2^2 - 7x_3^2$; c) $3x_1^2 + 2x_2^2 - 7x_3^2 + 2x_2x_3 + 2x_3x_1 + 2x_1x_2$?

Задача 8°. Какие простые числа рационально представимы следующими формами:

a) $x_1^2 + x_2^2$; b) $x_1^2 + 5x_2^2$; c) $x_1^2 - 5x_2^2$?

Задача 9°. Какие рациональные числа представимы следующими формами

a) $2x_1^2 - 5x_2^2$; b) $2x_1^2 - 6x_2^2 + 15x_3^2$?

Задача 10°. Найдите все рациональные решения уравнения $x^2+y^2-2z^2=0$.

Задача 11°. Какие из следующих форм эквивалентны над $\mathbb{Q}$? Если формы эквиваленты, определите соответствующую замену координат.

a) $x_1^2-15x_2^2$ и $3x_1^2-5x_2^2$;

b) $x_1^2-82x_2^2$ и $2x_1^2-41x_2^2$;

c) $x_1^2+x_2^2+16x_3^2$ и $2x_1^2+2x_2^2+5x_3^2-2x_2x_3-2x_1x_3$.

Подсказка: при поиске замены координат можно воспользоваться тем, что эквивалентные формы представляют одни и те же элементы.

Задача 12. При каких рациональных m формы $(m+1)(x_1^2+x_2^2+x_3^2)+mx_4^2$ и $x_1^2+x_2^2+x_3^2+m(m+1)x_4^2$ эквивалентны над $\mathbb{Q}$?

Задача 13° (Теорема Лежандра). Докажите, что, если a,b,c — попарно взаимно простые целые числа, свободные от квадратов, и a,b,c не все одного знака, то квадратичная форма $ax^2+by^2+cz^2$ представляет ноль над $\mathbb{Q}$ тогда и только тогда, когда разрешимы сравнения $x^2\equiv -bc \mod a$, $x^2\equiv -ca \mod b$ и $x^2\equiv -ab \mod c$.

Задача 14. Пусть f и g регулярные квадратичные формы над $\mathbb{Q}$, эквивалентные над $\mathbb{R}$ и над всеми $\mathbb{Q}_p$, за исключением, возможно, одного $p=p_0$. Покажите, что f и g эквивалентны над $\mathbb{Q}$.

Подсказка: Вам поможет закон взаимности для символа Гильберта.

Задача 15 (немного о целых решениях). a) (лемма Дэвенпорта–Касселса) Пусть $f(x)=\sum\limits_{i,j=1}^{n} a_{ij}x_ix_j$ — положительно определённая квадратичная форма, (a_{ij}) — симметрическая целочисленная матрица. Предположим, что для всякого $x\in\mathbb{Q}^n$ найдется такое $y\in\mathbb{Z}^n$, что $f(x-y)<1$. Тогда, если $n\in\mathbb{Z}$ представимо f над $\mathbb{Q}$, то оно представимо f и над $\mathbb{Z}$.

Подсказка: выберем такое наименьшее целое $t>0$, что $t^2n=f(x)$, $x\in\mathbb{Z}^n$. Пусть $x/t=y+z$, где $f(z)<1$. Покажите, что, если $z\neq 0$, то $t'=at+b$, $x'=ax+by$, $a=f(y)-n$, $b=2(nt-\phi(x,y))$ удовлетворяют условию $t'^2n=f(x')$ и $t'<t$ ($\phi(x,y)$ — билинейная форма, соответствующая f).

b) Пусть далее $n\in\mathbb{N}$. Когда n — сумма двух целых квадратов?

c) (Гаусс) Покажите, что n — сумма трёх целых квадратов тогда и только тогда, когда $n\neq 4^a(8b-1)$, $a,b\in\mathbb{N}$.

d) (Лежандр) Всякое целое положительное число — сумма четырёх квадратов.

Задача 16 (Слабая аппроксимационная теорема). Пусть $|\ |_n$, $n=1,\dots,N$ – неэквивалентные нормирования поля k, k_n — пополнение поля k по норме $|\ |_n$. Покажите, что образ поля k всюду плотен в $\prod\limits_{n=1}^{N} k_n$. Иными словами, для любого набора элементов $\alpha_n\in k_n$ и $\epsilon>0$ найдется такой элемент $\xi\in k$, что $|\xi-\alpha_n|_n<\epsilon$ для $n=1,\dots,N$.

Подсказка: постройте индукцией по N такое $\theta_n\in k$, что $|\theta_n|_n>1$ и $|\theta_n|_m<1$ при $m\neq n$.

Задача 17. a) Пусть $f(x_1,\dots,x_n)$ — регулярная квадратичная форма над $\mathbb{Q}_p, n\geq 3$ и пусть $h(x_1,\dots,x_n)=h_1x_1+\dots+h_nx_n$, где не все h_j равны нулю. Пусть b — решение уравнения $f(b)=0$. Тогда в любой окрестности b найдется такое c, что $f(c)=0$ и $h(c)\neq 0$.

Подсказка: можно считать, что $f(x_1,\dots,x_n)=x_1x_2+g(x_3,\dots,x_n)$, а $b=(1,0,\dots,0)$.

b) Пусть $S\subset V=\{\infty,2,3,5,7,11,\dots\}$ — конечное подмножество. Предположим, что регулярная квадратичная форма f от $n\geq 3$ переменных представляет ноль над $\mathbb{Q}$ и для всех $v\in S$ задано такое $b_v\in\mathbb{Q}_v^n$, что $f(b_v)=0$. Докажите, что для любого $\epsilon>0$ найдется такое $b\in\mathbb{Q}^n$, что $f(b)=0$ и $|b-b_v|_v<\epsilon$ для всех $v\in S$.

Подсказка: из предыдущего пункта можно считать, что $f(c,b_v)\neq 0$ для всех $v\in S$. Воспользуйтесь слабой аппроксимационной теоремой, затем найдите требуемое решение в виде $\lambda c+d$, где d — приближение к b_v.

Задача 18 (Существование рациональных чисел с данными символами Гильберта). Пусть $V = \{\infty, 2, 3, 5, 7, 11, \dots\}$, $\{a_i\}_{i\in I}$ — конечное семейство элементов из $\mathbb{Q}^\times$, а $\{c_{i,v}\}_{i\in I, v\in V}$ — семейство чисел, равных ± 1. Наша цель доказать, что для того, чтобы существовало такое $x \in \mathbb{Q}^\times$, что $(a_i, x)_v = c_{i,v}$ для всех $i \in I, v \in V$ необходимо и достаточно выполнение следующих условий: (1) почти все $c_{i,v}$ равны 1; (2) $\prod\limits_v c_{i,v} = 1$ для всех $i \in I$; (3) для любого $v \in V$ существует такое $x_v \in \mathbb{Q}_v^\times$, что $(a_i, x_v)_v = c_{i,v}$ для всех $i \in I$.

a) Убедитесь, что сформулированные условия являются необходимыми.

b) Пусть $a_i \in \mathbb{Z}$, $S \subset V$ состоит из $\infty, 2$ и простых делителей чисел a_i, а $T = \{v \in V \mid c_{i,v} = -1$ для некоторого $i \in I\}$. Предположим, что $S \cap T = \varnothing$. Положим $a = \prod\limits_{l\in T, l\neq\infty} l$ и $m = 8 \prod\limits_{l\in S, l\neq 2,\infty} l$ и пусть p — простое число, $p \equiv a \mod m$, $p \notin S \cup T$. Убедитесь, что число $x = ap$ удовлетворяет условию задачи.

c) Выведите из пункта b) и слабой аппроксимационной теоремы утверждение задачи в случае произвольных S и T.

Задача 19. Покажите, что квадратичная форма ранга n над $\mathbb{Q}$ с дискриминантом d, инвариантами Хассе $c_v, v \in V$ и сигнатурой (s, r) существует тогда и только тогда, когда (1) $c_v = 1$ для почти всех $v \in V$ и $\prod\limits_{v\in V} c_v = 1$; (2) $c_v = 1$, если $n = 1$ или $n = 2$, а образ d_v дискриминанта d в $\mathbb{Q}_v^*/(\mathbb{Q}_v^*)^2$ равен -1; (3) $r, s \geq 0$ и $r + s = n$ (4) $d_\infty = (-1)^s$; (5) $c_\infty = (-1)^{s(s-1)}$.

Подсказка: разберите отдельно случаи $n = 1, 2, 3$, пользуясь предыдущей задачей и слабой аппроксимационной теоремой. Общее утверждение докажите индукцией по n, рассматривая отдельно формы с сигнатурой $(0, s)$ и $(r, s), r \geq 1$.

Задача 20 (Группа Витта). В этой задаче k — поле, $\operatorname{char} k \neq 2$.

a) Пусть S — абелева полугруппа с сокращением, т.е. на S задана такая коммутативная ассоциативная операция $+$, что $s_1 + s = s_2 + s$ влечёт $s_1 = s_2$. Покажите, что существует единственная группа G и гомоморфизм полугрупп $\alpha\colon S \to G$ со следующим универсальным свойством: для любого морфизма полугрупп $\beta\colon S \to H$ существует единственный гомоморфизм групп $\gamma\colon G \to H$ такой, что $\gamma \circ \alpha = \beta$.

b) Убедитесь, что классы эквивалентности невырожденных квадратичных форм над k образуют абелеву полугруппу с сокращением относительно операции прямой суммы $\oplus$. Группа $G(k)$, получающаяся в результате применения конструкции из a), называется группой Гротендика поля k.

c) Покажите, что фактор $W(k)$ по подгруппе, порождённой классами эквивалентности гиперболических форм $Q(y_1, y_2) = y_1 y_2$ может быть описан так: он состоит из классов эквивалентности невырожденных квадратичных форм над k, при этом две формы f и g представляют один элемент из $W(k)$ тогда и только тогда, когда найдутся такие n и l, что $f \oplus (x_1x_2 + \dots + x_{2n-1}x_{2n}) \sim g \oplus (y_1y_2 + \dots + y_{2l-1}y_{2l})$. Группа $W(k)$ называется группой Витта поля k.

d) Докажите, что $G(k)$ задаётся образующими $\langle a\rangle, a \in k^\times$, которые соответствуют формам ax^2, и соотношениями $\langle a\rangle = \langle ab^2\rangle$, $a, b \in k^\times$ и $\langle a\rangle + \langle b\rangle = \langle a+b\rangle + \langle ab(a+b)\rangle$, $a, b, a+b \in k^\times$.

Подсказка: всякое соотношение имеет вид $\sum\limits_{i=1}^n \langle a_i\rangle = \sum\limits_{j=1}^n \langle b_j\rangle$. Разберите случаи $n = 1, 2$ и воспользуйтесь тем, что любые два ортогональных базиса можно соединить цепочкой ортогональных базисов, в которой на каждом шаге меняется не более двух векторов.

e) Покажите, что $W(k)$ задаётся образующими $\langle a\rangle, a \in k^\times$ и соотношениями $\langle a\rangle = \langle ab^2\rangle$, $a, b \in k^\times$, $\langle a\rangle + \langle b\rangle = \langle a+b\rangle + \langle ab(a+b)\rangle$, $a, b, a+b \in k^\times$ и $\langle 1\rangle + \langle -1\rangle = 0$.

f) Определим тензорное произведение $(V_1 \otimes V_2, Q_1 \otimes Q_2)$ двух квадратичных форм (V_1, Q_1) и

(V_2, Q_2), задав билинейную форму, соответствующую $Q_1 \otimes Q_2$, правилом $\phi(v_1 \otimes v_2, u_1 \otimes u_2) = \phi_1(v_1, u_1)\phi_2(v_2, u_2)$. Убедитесь, что тензорное произведение определяет на $W(k)$ структуру кольца.

g) Вычислите $W(\mathbb{R})$ и $W(\mathbb{C})$.

h) Покажите, что для нечётного q имеется изоморфизм $W(\mathbb{F}_q) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, если $-1 \in (\mathbb{F}_q^\times)^2$ и $W(\mathbb{F}_q) \cong \mathbb{Z}/4\mathbb{Z}$ иначе.

i) Докажите, что при $p \neq 2$ имеет место изоморфизм $W(\mathbb{Q}_p) \cong W(\mathbb{F}_p) \times W(\mathbb{F}_p)$.

j) Покажите, что $W(\mathbb{Q}_2) \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

k) Докажите, что $W(\mathbb{Q}) \cong \bigoplus\limits_p W(\mathbb{F}_p) \oplus \mathbb{Z}/2\mathbb{Z} \oplus W(\mathbb{R})$, где сумма берется по всем нечётным простым p.

l^*) Вычислите $W(\mathbb{F}_p((t)))$ при $p \neq 2$.

Задача 21 (Конечные проективные плоскости). Назовём конечной проективной плоскостью два конечных множества — "множество точек" и "множество прямых" с отношением "точка лежит на прямой", удовлетворяющим четырём свойствам: (1) две различные точки лежат на одной и только одной прямой; (2) две различные прямые пересекаются в одной и только одной точке; (3) на каждой прямой есть не менее трёх точек; (4) найдутся четыре точки, каждые три из которых не лежат на одной прямой. Скажем, что проективная плоскость имеет порядок n, если найдется прямая, содержащая ровно $n+1$ точку. Далее мы рассматриваем проективные плоскости порядка n.

a) Покажите, что найдется точка, через которую проходит ровно $n+1$ прямая.

b) Докажите, что через всякую точку P проходит ровно $n+1$ прямая.

Подсказка: если прямая l с $n+1$ точкой не проходит через P, то поможет рассуждение из предыдущего пункта, иначе постройте прямую, не проходящую через точку P и ещё одну точку вне l, и докажите, что на ней также будет $n+1$ точка.

c) Выведите из предыдущего, что всякая прямая содержит ровно $n+1$ точку. Кроме того, всего имеется $N = n^2+n+1$ прямых и столько же точек.

d) Пусть существует проективная плоскость порядка n. Занумеруем точки и прямые. Каждой прямой на проективной плоскости сопоставим линейную форму $l_k = \sum\limits_j x_j$, где в сумме берётся x_j, если и только если точка с номером j лежит на прямой с номером k. Покажите, что $\sum\limits_{k=1}^N l_k^2 = (n+1)\sum\limits_{i=1}^N x_i^2 + 2\sum\limits_{1\le i<j\le N} x_i x_j$.

e) Выведите из предыдущего, что формы $\sum\limits_{i=1}^N x_i^2$ и $z_1^2 + n\sum\limits_{i=2}^N z_i^2$ эквивалентны.

f) (теорема Брака–Райзера) Пусть n — порядок проективной плоскости и $n \equiv 1 \mod 4$ или $n \equiv 2 \mod 4$. Покажите, что всякое нечётное простое число p, входящее в n в нечётной степени, имеет вид $p = 4n+1$.

Имеется гипотеза о том, что порядок конечной проективной плоскости — степень простого числа (при этом бывает много проективных плоскостей, не совпадающих с $\mathbb{P}^2(\mathbb{F}_n)$). Единственный известный случай несуществования, не покрывающийся теоремой Брака–Райзера, — это $n = 10$. Доказательство — сложный компьютерный перебор.