

Math-Net.Ru

All Russian mathematical portal

A. S. Rapinchuk, Class numbers in the genus of quadratic forms, and algebraic groups, *Izv. Akad. Nauk SSSR Ser. Mat.*, 1981, Volume 45, Issue 4, 775–792

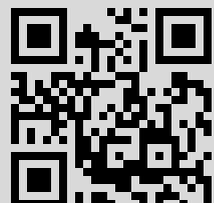
Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use

<http://www.mathnet.ru/eng/agreement>

Download details:

IP: 73.251.173.144

December 11, 2020, 05:55:36



УДК 513.6

РАПИНЧУК А. С.

ЧИСЛА КЛАССОВ В РОДЕ КВАДРАТИЧНЫХ ФОРМ И АЛГЕБРАИЧЕСКИЕ ГРУППЫ

§ 1. Введение и формулировка основных результатов

Пусть f — невырожденная n -мерная квадратичная форма с целыми коэффициентами. Важнейшим арифметическим инвариантом формы f , восходящим к Лагранжу и Гауссу, является число $c(f)$ классов в роде f . С числом $c(f)$ связан ряд классических проблем, представляющих значительный интерес не только для самой теории квадратичных форм, но и для алгебраической теории чисел, теории диофантовых уравнений и т. д.

Большинство гипотез о $c(f)$ естественным образом группируется вокруг основной проблемы определения, т. е. вычисления и характеристики, чисел $c(f)$, которая в самой общей постановке представляется малореальной. Здесь прежде всего следует различать два случая, когда f является соответственно неопределенной и положительно определенной. В первом случае описание значений $c(f)$ было получено Кнезером [14]. Оказалось, что $c(f)$ всегда имеет вид 2^i , причем любая степень двойки на самом деле реализуется как $c(g)$ для подходящей целочисленной формы g , рационально эквивалентной f . Что же касается положительно определенных форм f , то для них получение такого исчерпывающего результата является скорее всего невозможным, ибо число $c(f)$ может принимать весьма разнообразные значения. Поэтому естественно, что в этом случае основную роль играют качественные результаты о числе $c(f)$. В зависимости от метода их получения можно выделить несколько основных направлений.

Первое берет начало от работ Зигеля [17] по аналитической теории квадратичных форм и базируется на классической формуле для веса рода (см. [4], [17], [21]). Второе использует чисто квадратичную технику (описание квадратичных решеток, представимость чисел квадратичными формами и т. д.) и связывается в первую очередь с именами Эйхлера и О'Миры (см. [13], [15], [18], а также классификационные работы [19], [20]). Некоторые важные результаты были получены на стыке этих направлений (см., например, [16]). Наконец, третье основано на понятии группы аделей и интерпретации $c(f)$ как числа классов $cl(G)$ ортогональной группы $G = O_n(f)$, т. е. числа двойных классов $G_{A(\infty)} \times G_{\mathbb{Q}}$ в разложении группы аделей G_A по подгруппам $G_{A(\infty)}$ и $G_{\mathbb{Q}}$ целых и главных аделей соответственно.

Недавно в работах [8], [9] были получены результаты, которые в целом дают вполне законченную картину поведения $\text{cl}(\varphi(G))$ для произвольной полупростой группы G , если рассматривать ее реализации $\varphi: G \rightarrow GL_r$ достаточно большой степени. Результаты и методы этих работ позволили решить ряд классических арифметических задач (см. [9], [10]). Если $G = SO_n(f)$, где f — положительно определенная квадратичная форма, то G принадлежит к выделенному в [9] классу групп компактного типа (т. е. полупростых групп G , обладающих почти простой компонентой G^i с компактной архимедовой частью G_∞^i группы аделей), для которых была доказана следующая теорема: если G — алгебраическая группа степени n , имеющая компактный тип, то для произвольного натурального r существует такая реализация φ_r группы G степени $2n$, что число классов $\text{cl}(\varphi_r(G))$ делится на r . Не умаляя значения этого результата, позволившего, например, впервые показать, что на множестве двойных классов $G_{A(\infty)} \times G_{\mathbf{Q}}$ группы G компактного типа в общем случае заведомо не существует естественной групповой структуры, отметим, что из него непосредственно не удастся получить соответствующий результат для числа классов $c(f)$, так как здесь необходимо исследование числа классов для n -мерных решеток.

Настоящая работа и посвящена n -мерному усилению результата из [9] о числе классов групп компактного типа. При этом мы рассматриваем полупростые алгебраические группы G , определенные над полем алгебраических чисел K , с компактной архимедовой частью G_∞ группы аделей. Это существенно не ограничивает общности, так как для произвольной группы G компактного типа именно компонента G^i с компактной G_∞^i несет основную информацию о $\text{cl}(G)$ (см. [9, § 5]).

Нашим основным результатом является.

ТЕОРЕМА 1. Пусть G — связная линейная алгебраическая группа степени n , определенная над полем алгебраических чисел K , причем архимедова часть G_∞ группы аделей компактна. Тогда для любого натурального r существует такая $\mathcal{O}(K)$ -свободная решетка $L(r) \subset K^n$, что число классов $\text{cl}(G^{L(r)})$ делится на r .

Доказательство теоремы 1 для группы $G = SO_n(f)$, где f — положительно определенная квадратичная форма, без каких либо изменений проходит для группы $G = O_n(f)$, и поскольку $c(f) = \text{cl}(O_n(f)^L)$, L — решетка, натянутая на базис, в котором реализована f (см., например, [12]), то получаем следующий результат.

ТЕОРЕМА 2. Пусть f — положительно определенная квадратичная форма размерности $n \geq 2$ с коэффициентами из кольца целых $\mathcal{O}(K)$ вполне вещественного поля алгебраических чисел K . Тогда для любого натурального r существует такая форма g_r с коэффициентами из $\mathcal{O}(K)$, K -эквивалентная f , что число $c(g_r)$ классов в роде делится на r .

Работа состоит из введения и трех параграфов. § 2 содержит ряд вспомогательных результатов, используемых далее при доказательстве теорем 1, 2. Отметим, в частности, следующий результат, который пока-

зывает, что теорема 2 на самом деле содержит наиболее существенную часть теоремы 1.

Предложение 1. Пусть $G \subset GL_n$ — связная алгебраическая группа, определенная над полем алгебраических чисел K , с компактной группой G_∞ . Тогда существует такая положительно определенная квадратичная форма f с коэффициентами из K от n переменных, что $G \subset SO_n(f)$.

Далее устанавливается ряд утверждений о локальных решетках на квадратичных пространствах (K_v^n, f) над пополнениями K_v . Эти утверждения служат основой для построения локальных компонент искомой решетки $L(r)$ в теореме 1.

Наконец, в § 2 доказывается утверждение, позволяющее строить свободную решетку $L(r)$. Дело в том, что при вычислении $cl(G^L)$ над произвольным полем алгебраических чисел K то или иное значение d реализуется как $cl(G^{L(d)})$ для некоторой, априори не свободной, решетки $L(d) \subset K^n$ (см. [8], [9], [14]). Это, вообще говоря, несколько суживает сферу приложения соответствующего результата, так как, например, несвободным квадратичным решеткам нельзя естественным образом поставить в соответствие квадратичную форму. Все эти трудности, однако, можно обойти, если при вычислении чисел классов иметь в виду

Предложение 4. Пусть K — поле алгебраических чисел с гильбертовым полем классов \bar{K} , L — свободная решетка над кольцом целых $\mathcal{O}(K)$ поля K . Тогда если решетка M обладает свойством: локализации $L_v = M_v$ для всех неархимедовых $v \neq v_0$, а $\bar{K} \subset K_{v_0}$, то M свободна.

Доказательство предложения 4 основано на конструкции некоторого естественного отображения, сопоставляющего решетке элемент группы классов поля K , при этом критерий свободы выглядит следующим образом: решетка L свободна тогда и только тогда, если ей соответствует главный класс идеалов поля K . Отсюда, в частности, вытекает хорошо известный факт о том, что все решетки в основном случае $K = \mathbb{Q}$ являются свободными, так что дополнительные рассуждения типа предложения 4 здесь не нужны.

Используя предложение 4 и его доказательство, можно переформулировать теоремы реализации из [8], [9] для свободных решеток. Мы ограничимся доказательством следующего усиленного варианта теоремы Платонова об одноклассных решетках (см. [8]).

ТЕОРЕМА 3. *Для всякой неопределенной полупростой группы G степени n существует такая свободная решетка $L_0 \subset K^n$, что $cl(G^{L_0}) = 1$.*

(Напомним, что полупростая K -группа G называется неопределенной или группой некомпактного типа, если для любого почти-простого сомножителя G^i группа G_∞^i некомпактна. Это эквивалентно тому, что для односвязной накрывающей \tilde{G} справедлива сильная аппроксимационная теорема (см. [6], [7]).)

В §§ 3, 4 теорема 1 доказывается соответственно для случаев $G = O_n(f)$ или $G = SO_n(f)$ и $G \not\subset SO_n(f)$. При этом рассуждения § 4 су-

щественно опираются на тот структурный факт, что при $n \neq 2, 4$ группа $G = SO_n(f)$ проективно проста, т. е. не имеет нетривиальных связных нормальных делителей.

В работе без пояснений используются следующие обозначения. Для фиксированного поля алгебраических чисел K с кольцом целых $\mathcal{O} = \mathcal{O}(K)$ через V обозначается совокупность всех неэквивалентных нормирований K ; V_∞, V_f — соответственно подмножества архимедовых и неархимедовых нормирований. Если $v \in V$, то K_v — пополнение K относительно v , если к тому же $v \in V_f$, то $\mathcal{O}_v = \mathcal{O}(K_v)$ — кольцо целых в K_v и $U_v = \mathcal{O}_v^*$ — группа v -адических единиц (при $v \in V_\infty$ мы полагаем $\mathcal{O}_v = K_v$). Далее, для любого конечного множества M через $[M]$ обозначается число его элементов; в частности, для группы G и ее подгрупп F, H через $[F \setminus G / H]$ и $[F \setminus G]$ обозначается число двойных и левых смежных классов. Из других часто встречающихся обозначений отметим следующее: если $e = (e_1, \dots, e_n)$ — ортогональный базис относительно невырожденной квадратичной формы f , то $\Gamma(e) = \{\gamma \in O_n(f) \mid \gamma(e_i) = \pm e_i, i=1, 2, \dots, n\}$; ясно, что если базис e определен над полем P , то $\Gamma(e) \subset O_n(f)_P$.

Автор выражает глубокую благодарность В. П. Платонову за постановку задач и постоянное внимание к работе.

§ 2. Предварительные результаты

В этом параграфе будут установлены некоторые вспомогательные факты, используемые далее при доказательстве теоремы 1.

Вначале мы докажем следующее утверждение, которое играет ключевую роль при доказательстве теоремы 1 в общем случае и в то же время представляет самостоятельный интерес.

Предложение 1. Пусть $G \subset GL_n$ — связная алгебраическая группа, определенная над полем алгебраических чисел K , с компактной группой G_∞ . Тогда существует такая положительно определенная квадратичная форма f с коэффициентами из K от n переменных, что $G \subset SO_n(f)$.

Доказательство. Пусть W — пространство всех квадратичных форм от n переменных, которое можно отождествить с пространством симметрических $(n \times n)$ -матриц $A \in M_n(\mathbb{C})$. Обозначим через \tilde{W} подпространство в W , состоящее из матриц, инвариантных относительно группы G_K , т. е. $\tilde{W} = \{A \in W \mid {}^t g A g = A \quad \forall g \in G_K\}$; пространство \tilde{W} K -определено. По условию для любого $v \in V_\infty$ группа $G_{K_v} = G_{\mathbb{R}}$ компактна и поэтому каждое пространство \tilde{W}_{K_v} обязательно содержит положительно определенную матрицу. Действительно, если A — произвольная положительно определенная вещественная матрица, то

$$B = \int_{G_{K_v}} {}^t g A g d g$$

удовлетворяет нашим требованиям (здесь $d g$ — мера Хаара на G_{K_v}). Отсюда следует, что подмножество положительно определенных матриц

в \tilde{W}_{K_v} является непустым и открытым. С другой стороны, будучи K -определенным, пространство \tilde{W} обладает свойством слабой аппроксимации, т. е. естественное вложение

$$\tilde{W}_K \subset \prod_{v \in V_\infty} \tilde{W}_{K_v}$$

имеет плотный образ. Поэтому \tilde{W}_K содержит положительно определенную матрицу F . Пусть f — соответствующая ей квадратичная форма. Тогда $G_K \subset O_n(f)$. Ввиду связности G , множество G_K плотно в G в топологии Зарисского (см., например, [2]), так что $G \subset O_n(f)$, откуда и следует требуемое утверждение. Предложение 1 доказано.

З а м е ч а н и е. Приведенное выше доказательство предложения 1 было предложено И. К. Жуком.

Основой для построения локальных компонент искомых решеток служат

Предложение 2. Пусть $v \in V_f$ и $f = f_1 x_1^2 + \dots + f_n x_n^2$ в базисе $e = (e_1, \dots, e_n)$ пространства K_v^n , $G = O_n(f)$ — соответствующая ортогональная группа. Обозначим через L_v и $L_v^{(d)}$ \mathcal{O}_v -решетки с базисами e_1, e_2, \dots, e_n и $\pi_v^d e_2, \dots, \pi_v^{d(n-1)} e_n$ соответственно, π_v — униформизирующий элемент. Тогда если $f_i \in U_v$ для всех $i = 1, 2, \dots, n$, то стабилизатор

$$G_{\mathcal{O}_v}^{L_v^{(d)}} = \Gamma B_{0v},$$

где

$$\Gamma = \Gamma(e) = \{ \gamma \in G \mid \gamma(e_i) = \pm e_i, i = 1, 2, \dots, n \},$$

$$B_{0v} = \{ x = (x_{ij}) \in G_{\mathcal{O}_v}^{L_v}(\mathfrak{p}_v) \mid x_{ij} \in \pi_v^{d|i-j|} \mathcal{O}_v, i, j = 1, 2, \dots, n \}.$$

(Здесь матричная запись берется относительно базиса e , $G_{\mathcal{O}_v}^{L_v}(\mathfrak{p}_v)$ — конгруэнц-подгруппа уровня $\mathfrak{p}_v = \pi_v \mathcal{O}_v$.)

Доказательство. Пусть $x \in G_{\mathcal{O}_v}^{L_v^{(d)}}$ и $x = (x_{ij})$ в базисе e_1, \dots, e_n . Тогда

$$x(\pi_v^{d(j-1)} e_j) = \sum_{i=1}^n \pi_v^{d(j-i)} x_{ij} (\pi_v^{d(i-1)} e_i)$$

для всех $j = 1, \dots, n$. Поэтому $x_{ij} \in \pi_v^{d(i-j)} \mathcal{O}_v$ при $i \geq j$. С другой стороны, так как $x \in G$, то ${}^t x F x = F$, где $F = \text{diag}(f_1, \dots, f_n)$, ${}^t x$ — транспонированная к x матрица, или $x_{ji} = f_j^{-1} y_{ij}$, где $y = (y_{ij}) = x^{-1}$. Но поскольку $x \in G_{\mathcal{O}_v}^{L_v^{(d)}}$, то и $y \in G_{\mathcal{O}_v}^{L_v^{(d)}}$, так что согласно уже доказанному $y_{ij} \in \pi_v^{d(i-j)} \times \mathcal{O}_v$ при $i \geq j$. Отсюда видно, что $x_{ij} \in \pi_v^{d(j-i)} \mathcal{O}_v$ и при $j \geq i$. Таким образом, во всех случаях $x_{ij} \in \pi_v^{d|i-j|} \mathcal{O}_v$. Далее, из матричного уравнения

${}^t x F x = F$ вытекает, что для любого $j = 1, \dots, n$ $\sum_{i=1}^n f_i x_{ij}^2 = f_j$, откуда

$x_{jj}^2 \equiv 1 \pmod{\pi_v \mathcal{O}_v}$, или $x_{jj} \equiv \pm 1 \pmod{\mathfrak{p}_v}$. Тем самым мы доказали включение $G_{\mathcal{O}_v}^{f,v(d)} \subset \Gamma B_{\mathcal{O}_v}$. Обратное включение следует из выписанной выше формулы действия x на элементы базиса $\pi_v^{d(j-1)} e_j$. Предложение 2 доказано.

Предложение 3. Пусть $f = f_1 x_1^2 + \dots + f_n x_n^2$ в базисе $\mathbf{e} = (e_1, \dots, e_n)$ пространства K^n . Тогда:

(i) если $v(2) = 1$ и $f_1, f_2 \in U_v$, то существует базис $\mathbf{u} = (u_1, \dots, u_n)$ пространства K_v^n , обладающий следующими свойствами: 1) $u_i = e_i$ для $i > 2$; 2) u_1, u_2 — ортогональный базис решетки $\mathcal{O}_v e_1 \perp \mathcal{O}_v e_2$; 3) $u_i^2 = a f_i$, $i = 1, 2$, где $a \in U_v$ — единица, не являющаяся квадратом.

(ii) если дополнительно $f_i \in K_v^{*2}$ для всех $i = 1, \dots, n$, $\Gamma = \Gamma(\mathbf{e})$, $\Gamma_0 = \Gamma(\mathbf{u})$, то для любого $g \in O_n(f)_{K_v}$ $\Gamma \cap g^{-1} \Gamma_0 g = \Gamma \cap g^{-1} \tilde{\Gamma} g$, где $\tilde{\Gamma} = \{\gamma \in \Gamma_0 \mid \det \gamma|_W = 1, W = K_v u_1 \perp K_v u_2\}$.

Доказательство. Пункт (i) легко следует из общих результатов о квадратичных решетках (см. [15]). Докажем (ii). Предположим противное. Тогда найдется $\gamma \in \Gamma_0$ такой, что $\gamma(u_1) = u_1$, $\gamma(u_2) = -u_2$ и $\bar{\gamma} = g^{-1} \gamma g \in \Gamma$. Положим $W^+ = \{\omega \in K_v^n \mid \gamma(\omega) = \omega\}$ и $\bar{W}^+ = \{\omega \in K_v^n \mid \bar{\gamma}(\omega) = \omega\}$. Из равенства $\bar{\gamma} = g^{-1} \gamma g$ вытекает, что $g(\bar{W}^+) = W^+$. В частности, пространства W^+ и \bar{W}^+ изометричны. С другой стороны, в пространстве W^+ может быть выбран базис вида $u_1, u_{i_2}, \dots, u_{i_l}, i_j \neq 2$, так что дискриминант $\text{disc}(W^+) = u_1^2 u_{i_2}^2 \dots u_{i_l}^2 = a f_1 f_{i_2} \dots f_{i_l} \notin K_v^{*2}$. Аналогично, в \bar{W}^+ существует базис вида e_{j_1}, \dots, e_{j_m} , откуда $\text{disc}(\bar{W}^+) = f_{j_1} \dots f_{j_m} \in K_v^{*2}$. Полученное противоречие и доказывает предложение 3.

Займемся теперь вопросом о построении свободных решеток.

Предложение 4. Пусть K — поле алгебраических чисел с гильбертовым полем классов \bar{K} , L — свободная решетка над кольцом целых $\mathcal{O}(K)$ поля K . Тогда если решетка M обладает свойством: локализации $L_v = M_v$ для всех неархимедовых $v \neq v_0$, а $\bar{K} \subset K_{v_0}$, то M свободна.

Доказательство. Напомним вначале, что гильбертовым полем классов для K называется максимальное абелево расширение \bar{K} , неразветвленное во всех точках. При этом \bar{K} соответствует нормальной подгруппе $K^* J_K^\infty \subset J_K$, так что $\text{Gal}(\bar{K}/K)$ изоморфна группе классов $\text{Cl}(K)$ поля K (здесь, как обычно, J_K, J_K^∞ — соответственно группы идеалов и целых идеалов поля K). Кроме того, включение $\bar{K} \subset K_{v_0}$ равносильно тому, что главный класс $K^* J_K^\infty$ содержит все иделы $i^{v_0}(\alpha)$, $\alpha \in K_{v_0}$, с компонентами

$$i_v = \begin{cases} 1, & v \neq v_0, \\ \alpha, & v = v_0, \end{cases}$$

и, таким образом, существует такой униформизирующий элемент $\pi_{v_0} \in \mathcal{O}$, что $\pi_{v_0} \in U_v$ при $v \neq v_0$ (см. [5]).

Пусть $GL_{n,A}$ — группа аделей, соответствующая GL_n . Определим действие $GL_{n,A}$ на решетках $L \subset K^n$. Если $g = (g_v) \in GL_{n,A}$, то $g_v(L_v) = L_v$ для почти всех $v \in V_f$ и поэтому существует такая решетка $M \subset K^n$, $M = g(L)$, что $M_v = g_v(L_v)$ для всех $v \in V_f$ (см. [15]). В случае свободной решетки

L свобода $M=g(L)$ равносильна включению $g \in GL_n(K)GL_{n_A(\infty)}$. Используя сильную аппроксимационную теорему для группы SL_n (см. [6], [7]), нетрудно доказать, что последнее равносильно включению $i(g) = (\det g_v) \in K^*J_{K^\infty}$. Таким образом, отображение δ , сопоставляющее решетке $M=g(L)$ класс $i(g)K^*J_{K^\infty}$ в группе классов, обладает свойством: $\delta^{-1}(e)$ состоит в точности из всех свободных решеток.

Пусть теперь M удовлетворяет условиям предложения. Тогда в качестве аделя g , переводящего L в M , можно взять адель вида $g^{v_0}(a)$, $a \in GL_n(K_v)$, так что $i(g) = (\det g_v) = i^{v_0}(\det a) \in K^*J_{K^\infty}$. Предложение 4 доказано.

Как уже отмечалось во введении, предложение 4 позволяет переформулировать все теоремы реализации из работ [8], [9] для свободных решеток. Наибольший интерес представляет следующий усиленный вариант теоремы Платонова из [8] об одноклассных решетках.

ТЕОРЕМА 3. *Для всякой неопределенной полупростой группы G степени n существует такая свободная решетка $L_0 \subset K^n$, что $cl(G^{L_0}) = 1$.*

Доказательство следует общей схеме рассуждений из [8], поэтому мы укажем лишь на необходимые модификации. Как и в [8], определяющую роль играет доказанное там

Предложение 5. *Пусть G — полупростая K -группа степени n , $\pi: \tilde{G} \rightarrow G$ — универсальное K -определенное накрытие. Тогда для любого $v \in V_f$ существует решетка $N_v \subset K_v^n$, для стабилизатора $B = G_{\mathcal{O}_v}^{N_v}$ которой имеем $G_{K_v} = \text{В}\pi_{K_v}(\tilde{G}_{K_v})$.*

В [9] доказано существование такого конечного подмножества $S_0 \subset V_f$, что при $S \cap S_0 = \emptyset$ группа G обладает свойством слабой аппроксимации относительно S , т. е. диагональное вложение $G_K \hookrightarrow \prod_{v \in S} G_{K_v}$ является плотным. Используя слабую аппроксимацию для поля K , найдем конечное подмножество $S \subset V_f$, $S \cap S_0 = \emptyset$, для которого $J_K = K^*J_{K^S}$, где J_{K^S} — группа S -целых идеалей.

Пусть теперь $L \subset K^n$ — произвольная свободная решетка. Обозначим через D подгруппу в G_A вида

$$D = \prod_{v \in V_\infty} G_{K_v} \times \prod_{v \in V_f \setminus S} G_{\mathcal{O}_v}^{L_v} \times \prod_{v \in S} (G_{\mathcal{O}_v}^{L_v} \cap \pi_{K_v}(G_{K_v}));$$

D открыта в G_A в аделевой топологии. Из свойства слабой аппроксимации относительно S вытекает существование такой конечной системы представителей $\{z_i\}_{i=1}^d$ двойных смежных классов DzG_K и такого конечного подмножества $T \subset V_f$, $T \cap S = \emptyset$, что v -компонента $(z_i)_v = e$ для всех $v \notin T$ и всех $i = 1, \dots, d$. Зафиксируем произвольный набор решеток $M_v \subset K_v^n$ ($v \in S$) и построим решетку $\tilde{L} \subset K^n$ с локальными компонентами

$$\tilde{L}_v = \begin{cases} L_v, & v \notin S \cup T, \\ M_v, & v \in S, \\ N_v, & v \in T, \end{cases} \quad (1)$$

где N_v — решетка из предложения 5. Решетка, удовлетворяющая (1), существует (см. [15]). Рассуждения, приведенные в [8] при доказательстве теоремы об одноклассных решетках, показывают тогда, что $\text{cl}(G^{\sim}) = 1$. С другой стороны, ввиду равенства $J_K = K^* J_K^S$ и произвольности компонент M_v , можно выбрать последние таким образом, чтобы адель $g \in GL_{n_A}$, переводящий L в \tilde{L} , удовлетворял условию:

$$i(g) = (\det g_v) \in K^* J_K^{\infty}.$$

Но это, как мы видели при доказательстве предложения 4, эквивалентно свободе решетки \tilde{L} . Теорема 3 доказана.

Завершает этот параграф

ЛЕММА 1. Пусть G — K -определенная алгебраическая группа и $V_1, V_2 \subset G$ — два замкнутых по Зарисскому K -определенных множества. Тогда если $V_1 \cap V_2 = \emptyset$, то для почти всех $v \in V_f$

$$G_{\mathcal{O}_v}(\mathfrak{p}_v) V_{1\mathcal{O}_v} \cap G_{\mathcal{O}_v}(\mathfrak{p}_v) V_{2\mathcal{O}_v} = \emptyset.$$

Доказательство. Пусть $\mathfrak{a}_i \subset \mathbf{C}[G]$ определяет V_i и $f_1^{(i)}, \dots, f_{s_i}^{(i)} \in K[G]$ порождают \mathfrak{a}_i , $i = 1, 2$. Так как $V_1 \cap V_2 = \emptyset$, то найдутся такие $g_1^{(i)}, \dots, g_{s_i}^{(i)} \in K[G]$, что

$$\sum_{j=1}^{s_1} g_j^{(1)} f_j^{(1)} + \sum_{j=1}^{s_2} g_j^{(2)} f_j^{(2)} = 1.$$

Для почти всех $v \in V_f$ существует гладкая редукция $\mathbf{G}^{(v)}$ группы G по модулю \mathfrak{p}_v (см. [3]) и регулярные функции $f_1^{(1)}, \dots, f_{s_1}^{(1)}, f_1^{(2)}, \dots, f_{s_2}^{(2)}, g_1^{(1)}, \dots, g_{s_1}^{(1)}, g_1^{(2)}, \dots, g_{s_2}^{(2)} \in \mathcal{O}_v[G]$. Для таких v выполняется утверждение леммы. Действительно, пусть $x = g_1 v_1 = g_2 v_2$, где $g_1, g_2 \in G_{\mathcal{O}_v}(\mathfrak{p}_v)$, $v_1 \in V_{1\mathcal{O}_v}$, $v_2 \in V_{2\mathcal{O}_v}$. Тогда

$$\sum_{j=1}^{s_1} g_j^{(1)}(x) f_j^{(1)}(x) + \sum_{j=1}^{s_2} g_j^{(2)}(x) f_j^{(2)}(x) = 1.$$

С другой стороны, переходя к редукции по модулю \mathfrak{p}_v и учитывая, что $\bar{x} = \bar{v}_1 = \bar{v}_2$, получим:

$$\sum_{j=1}^{s_1} \bar{g}_j^{(1)}(\bar{v}_1) \bar{f}_j^{(1)}(\bar{v}_1) + \sum_{j=1}^{s_2} \bar{g}_j^{(2)}(\bar{v}_2) \bar{f}_j^{(2)}(\bar{v}_2) = \bar{0}$$

— противоречие. Лемма 1 доказана.

§ 3. Числа классов в роде положительно определенных квадратичных форм. Доказательство теоремы 2

Пусть G — связная K -определенная группа степени n с компактной архимедовой частью G_{∞} группы аделей. Тогда согласно предложению 1 существует такая положительно определенная квадратичная K -форма f , что $G \subset SO_n(f)$. Поэтому доказательство теоремы 1 естественно распадается

ется на два случая: 1) $G = SO_n(f)$; 2) $G \neq SO_n(f)$. В этом параграфе мы разберем первый случай. При этом рассуждения в равной мере годятся для групп $G = SO_n(f)$ и $G = O_n(f)$. Учитывая, однако, связь $cl(O_n(f))$ с числом классов в роде формы f , мы проведем доказательство в случае $G = O_n(f)$. Таким образом, в этом параграфе утверждение теоремы 1 будет доказано для группы $G = O_n(f)$, что, как отмечалось во введении, автоматически влечет справедливость теоремы 2.

Переходя к доказательству, будем считать, что положительно определенная форма $f = f_1x_1^2 + \dots + f_nx_n^2$ в базисе $e = (e_1, \dots, e_n)$ пространства K^n . Для всякого $v \in V_f$ такого, что $\bar{K} \subset K_v$, выберем простой элемент $\pi_v \in \mathcal{O}$, обладающий свойством $\pi_v \in U_w$ при $w \neq v$, и обозначим через $L^{(v)}$ \mathcal{O} -решетку с базисом $e_1, \pi_v e_2, \dots, \pi_v^{(n-1)} e_n$. Положим также $\Gamma = \Gamma(e) = \{\gamma \in G = O_n(f) \mid \gamma(e_i) = \pm e_i, i = 1, \dots, n\}$.

Предложение 6. Существует $v \in V_f$, для которого $\bar{K} \subset K_v$, и существует разложение

$$G_A = \bigcup_{j=1}^s G_{A(\infty)}^{L^{(v)}} z_j G_K$$

группы аделей G_A по подгруппам целых и главных аделей, обладающее свойством: все группы

$$G_{\mathcal{O}}^{(j)} = z_j^{-1} G_{A(\infty)}^{L^{(v)}} z_j \cap G_K$$

$G_{\bar{K}}$ -сопряжены подгруппе в Γ . При этом для почти всех w w -компонента $(z_j)_w = e, j = 1, 2, \dots, s$.

Доказательство. Пусть $L = \mathcal{O}e_1 \perp \dots \perp \mathcal{O}e_n$ и $G_A = \bigcup_{j=1}^t G_{A(\infty)}^L \bar{z}_j G_K$ — соответствующее разложение. Без ограничения общности можно считать, что для некоторого конечного подмножества $S \subset V_f$ при $w \in V \setminus S$ w -компонента $(\bar{z}_j)_w = e$. Положим $\bar{G}_{\mathcal{O}}^{(j)} = \bar{z}_j^{-1} G_{A(\infty)}^L \bar{z}_j \cap G_K$. Ввиду положительной определенности f , все группы $\bar{G}_{\mathcal{O}}^{(j)}$ конечны. Поэтому из теоремы плотности Чеботарева (см. [5], с. 254) вытекает существование такого $v \in V_f \setminus S$, что 1) $\bar{K} \subset K_v$; 2) $f_1, \dots, f_n \in U_v$; 3) пересечение $\left(\bigcup_{j=1}^t \bar{G}_{\mathcal{O}}^{(j)} \right) \cap G_{\mathcal{O}_v}^{L_v}(v) = \{e\}$.

Покажем, что v — искомое. Так как при $w \neq v$ $L_w^{(v)} = L_w$, то $G_{\mathcal{O}_w}^{L_w^{(v)}} = G_{\mathcal{O}_w}^{L_w}$.

В соответствии с предложением 2 для $w = v$ $G_{\mathcal{O}_v}^{L_v^{(v)}} = \Gamma B_{0v}$; в частности, $G_{\mathcal{O}_v}^{L_v^{(v)}} \subset G_{\mathcal{O}_v}^{L_v}$. Отсюда следует, что представители классов $G_{A(\infty)}^{L^{(v)}} \setminus G_A / G_K$ могут быть выбраны среди аделей $z(a, j)$ с компонентами:

$$z(a, j)_w = \begin{cases} e, & w \notin S \cup \{v\} \\ (\bar{z}_j)_w, & w \in S, \\ a, & w = v \end{cases} \quad a \in G_{\mathcal{O}_v}^{L_v}.$$

Поэтому достаточно показать, что для любого $z(a, j)$ группа

$$G_{\mathcal{O}}^{(a, j)} = z(a, j)^{-1} G_{A(\infty)}^{L(v)} z(a, j) \cap G_K$$

$G_{\bar{K}}$ -сопряжена подгруппе в Γ . Пусть $x \in G_{\mathcal{O}}^{(a, j)}$. Тогда $x \in \bar{G}_{\mathcal{O}}^{(j)}$. Беря проекцию на v -компоненту, получаем $x = a^{-1} \gamma b a$, $\gamma \in \Gamma$, $b \in B_{\mathcal{O}_v}$. Таким образом, $x^2 \in \bar{G}_{\mathcal{O}}^{(j)}$ и $x^2 = a^{-1} (\gamma^{-1} b \gamma b) a \in G_{\mathcal{O}_v}^{L(v)}(\mathfrak{p}_v)$. По построению отсюда следует, что $x^2 = e$. Поэтому требуемое вытекает из следующего утверждения.

ЛЕММА 2. Пусть $\Theta \subset G_{\bar{K}}$ — подгруппа экспоненты 2. Тогда Θ $G_{\bar{K}}$ -сопряжена подгруппе в Γ .

Доказательство. Группа Θ , очевидно, абелева и поэтому существует такой ортогональный базис u_1, \dots, u_n пространства \bar{K}^n , что $\theta(u_i) = \pm u_i$ для всех $i = 1, \dots, n$ и всех $\theta \in \Theta$. Действительно, пусть u_1 — общий собственный вектор для преобразований из Θ и $W_1 = (\bar{K}u_1)^\perp$ — ортогональное дополнение к прямой $\bar{K}u_1$. Тогда W_1 инвариантно относительно Θ и в качестве u_2 можно взять произвольный общий собственный вектор для ограничения $\Theta|_{W_1}$ и т. д. Без ограничения общности можно считать, что $u_i^2 = f_i$. Тогда если преобразование $x \in G_{\bar{K}}$ определяется соответствием $x(e_i) = u_i$, то $x^{-1}\Theta x \subset \Gamma$. Лемма 2 доказана и, таким образом, доказательство предложения 6 завершено.

Согласно предложению 6, можно предполагать, что $f = f_1 x_1^2 + \dots + f_n x_n^2$ в базисе e_1, \dots, e_n пространства K^n , причем для $L = \mathcal{O}e_1 \perp \dots \perp \mathcal{O}e_n$ существует разложение $G_A = \bigcup_{j=1}^s G_{A(\infty)}^L z_j G_K$, для которого все группы $G_{\mathcal{O}}^{(j)} = z_j^{-1} G_{A(\infty)}^L z_j \cap G_K$ $G_{\bar{K}}$ -сопряжены подгруппам в $\Gamma = \Gamma(\mathfrak{e})$, и, кроме того, для почти всех $v \in V_f$ v -компоненты $(z_j)_v = e$, $j = 1, \dots, s$. Зафиксируем элементы $g_j \in G_{\bar{K}}$, для которых $g_j^{-1} G_{\mathcal{O}}^{(j)} g_j \subset \Gamma$. Пусть $S_1 \subset V_f$ — такое конечное подмножество, что при $v \in V_f \setminus S_1$ выполняются следующие условия:

- (i) $r_1 = 2^{2^n} r$, $f_1, \dots, f_n \in U_{\mathcal{O}}$ (r — число из теоремы 1);
- (ii) $(z_j)_v = e$ для всех $j = 1, \dots, s$;
- (iii) g_j в базисе e_1, \dots, e_n целы относительно \mathfrak{w} для всех продолжений \mathfrak{w} нормирования v на \bar{K} , $j = 1, \dots, s$.

Обозначим через P расширение K , порожденное над гильбертовым полем классов \bar{K} примитивным корнем ρ_{r_1} степени r_1 из 1, элементами $\sqrt[r_1]{f_1}, \dots, \sqrt[r_1]{f_n}$ и всеми коэффициентами матриц g_j , $j = 1, \dots, s$.

Далее, пусть $\tilde{\Gamma} = \{\gamma \in \Gamma \mid \det \gamma|_{\mathfrak{w}} = 1, W = Ke_1 \perp Ke_2\}$ и $\Delta(\Gamma)$ — совокупность всех подгрупп группы Γ , которые $G_{\bar{K}}$ -сопряжены подгруппе в $\tilde{\Gamma}$. Для всякой подгруппы $\Gamma' \in \Delta(\Gamma)$ перенумеруем каким-либо образом элементы Γ' , скажем, $\Gamma' = \{\gamma_1', \dots, \gamma_d'\}$ и для $\gamma = (\gamma_1, \dots, \gamma_d) \in \tilde{\Gamma}^d$ положим $V(\Gamma', \gamma) = \{g \in G \mid g^{-1} \gamma_i g = \gamma_i', i = 1, \dots, d\}$. Очевидно, $V(\Gamma', \gamma)$ — замкнутые по Зарисскому K -определенные подмножества в G , причем если $\gamma^1 \neq \gamma^2$, то $V(\Gamma', \gamma^1) \cap V(\Gamma', \gamma^2) = \emptyset$. Поэтому из леммы 1 вытекает существование такого конечного подмножества $S_2 \subset V_f$, что при $v \in V_f \setminus S_2$ выполняется следующее условие:

$$\left. \begin{aligned} &\text{для любой подгруппы } \Gamma' \in \Delta(\Gamma) \text{ порядка } d \text{ и любых} \\ &\gamma^1, \gamma^2 \in \tilde{\Gamma}^d, \gamma^1 \neq \gamma^2, \text{ пересечение } G_{\mathcal{O}_v}(\mathfrak{p}_v) V(\Gamma', \gamma^1)_{\mathcal{O}_v} \cap \\ &\cap G_{\mathcal{O}_v}(\mathfrak{p}_v) V(\Gamma', \gamma^2)_{\mathcal{O}_v} = \emptyset. \end{aligned} \right\} \quad (2)$$

Положим $S = S_1 \cup S_2$. Тогда в соответствии с теоремой плотности Чеботарева (см. [5]) существует $v \in V_f \setminus S$, для которого $P \subset K_v$. Из наших построений вытекает, что удовлетворяются условия предложения 3, и поэтому можно рассматривать базис $u = (u_1, \dots, u_n)$ с описанными там свойствами. Выберем простой элемент $\pi_v \in \mathcal{O}_v$, и обозначим через M_v решетку с \mathcal{O}_v -базисом $u_1, \pi_v u_2, \dots, \pi_v^{(n-1)} u_n$. Искомую решетку $L(r)$ определим через ее локализации следующим образом:

$$L(r)_w = \begin{cases} L_w, & w \neq v, \\ M_v, & w = v. \end{cases} \quad (3)$$

Такая решетка существует (см. [16]). Кроме того, из предложения 4 вытекает, что $L(r)$ свободна. Покажем, что число классов $\text{cl}(G^{L(r)})$ делится на r .

Из (3) вытекает, что стабилизатор $G_{\mathcal{O}_w}^{L(r)_w} = G_{\mathcal{O}_w}^{L_w}$ при $w \neq v$ и $G_{\mathcal{O}_v}^{L(r)_v} = B_v = \Gamma_0 B_{0v}$, где $\Gamma_0 = \Gamma(u) = \{\gamma \in G \mid \gamma(u_i) = \pm u_i, i = 1, \dots, n\}$, $B_{0v} \subset G_{\mathcal{O}_v}^{L_v}$ (см. предложение 2). В частности, $G_{A(\infty)}^{L(r)} \subset G_{A(\infty)}^L$. Обозначим через $c_j(v)$ число двойных смежных классов по подгруппам $G_{A(\infty)}^{L(r)}$ и G_K , на которые распадается класс $G_{A(\infty)}^L z_j G_K$. Имеет место

ЛЕММА 3. $\text{cl}(G^{L(r)}) = \sum_{j=1}^s c_j(v)$, причем $c_j(v) = [B_v \setminus G_{\mathcal{O}_v}^{L_v} / G_{\mathcal{O}}^{(j)}]$.

Доказательство. Первое утверждение леммы очевидно, поэтому докажем второе. Для всякого $a \in G_{\mathcal{O}_v}^{L_v}$ обозначим через $z^v(a)$ адель с компонентами

$$z^v(a)_w = \begin{cases} e, & w \neq v, \\ a, & w = v. \end{cases}$$

Тогда

$$G_{A(\infty)}^L z_j G_K = \bigcup_{a \in G_{\mathcal{O}_v}^{L_v}} G_{A(\infty)}^{L(r)} z^v(a) z_j G_K.$$

Пусть теперь

$$G_{A(\infty)}^{L(r)} z^v(a) z_j G_K = G_{A(\infty)}^{L(r)} z^v(b) z_j G_K. \quad (4)$$

Тогда, так как $(z_j)_v = e$, (4) эквивалентно

$$z_j^{-1} G_{A(\infty)}^{L(r)} z_j z^v(a) G_K = z_j^{-1} G_{A(\infty)}^{L(r)} z_j z^v(b) G_K,$$

т. е. $z^v(a) = x z^v(b) y$, $x \in z_j^{-1} G_{A(\infty)}^{L(r)} z_j$, $y \in G_K$. Поскольку $z^v(b)^{-1} x^{-1} z^v(a) \in z_j^{-1} G_{A(\infty)}^{L(r)} z_j$, то $y \in G_{\mathcal{O}}^{(j)}$, так что, переходя к проекциям на v -компоненту, получим $a \in B_v b G_{\mathcal{O}}^{(j)}$. Обратно, пусть $a = \tilde{x} b \tilde{y}$, где $\tilde{x} \in B_v$, $\tilde{y} \in G_{\mathcal{O}}^{(j)}$. Поло-

жим $x = z^v(a) \tilde{y}^{-1} z^v(b)$. Тогда $z^v(a) = x z^v(b) \tilde{y}$ и достаточно установить, что $x \in z_j^{-1} G_{A(\infty)}^{L(r)} z_j$. Сразу же заметим, что $x \in z_j^{-1} G_{A(\infty)}^L z_j$, и поэтому достаточно показать, что v -компонента $x_v \in B_v$. Но $x_v = a \tilde{y}^{-1} b^{-1} = \tilde{x} \in B_v$. Таким образом, мы показали, что (4) эквивалентно $B_v a G_{\mathbb{O}}^{(j)} = B_v b G_{\mathbb{O}}^{(j)}$, откуда и следует лемма.

Таким образом, для доказательства теоремы достаточно показать, что число двойных классов $[B_v \setminus G_{\mathbb{O}_v}^{L_v} / G_{\mathbb{O}}^{(j)}]$ делится на r для любого $j = 1, \dots, s$. Заметим теперь, что из условия (iii) в (1) вытекает, что $g_j^{-1} G_{\mathbb{O}}^{(j)} g_j \subset \Gamma$, $g_j \in G_{\mathbb{O}_v}^{L_v}$ для всех $j = 1, \dots, s$. Кроме того, так как $\rho_{r_1} \in K_v$ и $v(r_1) = 1$, то если q_v — число элементов поля вычетов для K_v , $q_v - 1$ делится на $r_1 = 2^{2^n} r$. Поэтому требуемое вытекает из следующего утверждения.

Предложение 7. Пусть H — такая конечная подгруппа в $G_{\mathbb{O}_v} = G_{\mathbb{O}_v}^{L_v}$, что $g^{-1} H g \subset \Gamma$ для некоторого $g \in G_{\mathbb{O}_v}$. Тогда число двойных смежных классов $B_v \setminus G_{\mathbb{O}_v} / H$ имеет вид $\frac{a(q_v - 1)}{2^{2^n}}$ для некоторого целого a .

Очевидно, порядок H равен 2^m , $0 \leq m \leq n$. Для всякого $i = 0, 1, \dots, m$ положим

$$D_i = \{g \in G_{\mathbb{O}_v} \mid [H : H \cap (g^{-1} B_v g)] = 2^i\}.$$

ЛЕММА 4. $[B_v \setminus G_{\mathbb{O}_v} / H] = \sum_{i=0}^m 2^{-(n+i)} [B_{0v} \setminus D_i]$ (напомним, что $B_v = \Gamma_0 B_{0v}$, так что $B_{0v} = B_v \cap G_{\mathbb{O}_v}(\mathfrak{p}_v)$).

Доказательство. Имеем $[B_v \setminus G_{\mathbb{O}_v} / H] = \sum_{i=0}^m [B_v \setminus D_i / H]$, поэтому достаточно показать, что $[B_v \setminus D_i / H] = 2^{-(n+i)} [B_{0v} \setminus D_i]$. Установим вначале, что каждый класс $B_v x H$, $x \in D_i$, содержит 2^{n-m+i} классов $B_{0v} y H$. Действительно, $B_v x H = \bigcup_{\gamma \in \Gamma_0} B_{0v} \gamma x H$. Пусть теперь $B_{0v} \gamma_1 x H = B_{0v} \gamma_2 x H$. Тогда $\gamma_2^{-1} \gamma_1 b \in x H x^{-1}$, $b \in B_{0v}$. Таким образом, класс $B_v x H$ распадается в точности на $[\Gamma_0 : \Gamma_0']$ классов $B_{0v} y H$, где $\Gamma_0' = \{\gamma \in \Gamma_0 \mid \gamma B_{0v} \cap (x H x^{-1}) \neq \emptyset\}$. Но если $\gamma b = x h x^{-1}$ ($\gamma \in \Gamma_0$, $b \in B_{0v}$, $h \in H$), то, во-первых, элемент h определен однозначно (т. е. не зависит от b) и лежит в $H \cap (x^{-1} B_v x)$ и, во-вторых, соответствие $\gamma \mapsto h$ определяет биекцию $\Gamma_0' \leftrightarrow H \cap (x^{-1} B_v x)$. Поэтому индекс $[\Gamma_0 : \Gamma_0'] = 2^{n-m} [H : H \cap (x^{-1} B_v x)] = 2^{n-m+i}$. Мы доказали, что $[B_v \setminus D_i / H] = 2^{-(n-m+i)} [B_{0v} \setminus D_i / H]$, и, таким образом, теперь достаточно установить, что $[B_{0v} \setminus D_i / H] = 2^{-m} [B_{0v} \setminus D_i]$. Для этого покажем, что каждый класс $B_{0v} x H$ содержит 2^m классов $B_{0v} y$. Пусть $B_{0v} x h_1 = B_{0v} x h_2$. Тогда $x h_2 h_1^{-1} x^{-1} \in B_{0v} \subset G_{\mathbb{O}_v}(\mathfrak{p}_v)$, так что $h_2 h_1^{-1} \in G_{\mathbb{O}_v}(\mathfrak{p}_v)$, откуда $h_1 = h_2$, что и означает требуемое. Здесь мы воспользовались тем фактом, что $H \cap G_{\mathbb{O}_v}(\mathfrak{p}_v) = (e)$, так как $g^{-1} H g \subset \Gamma$ ($g \in G_{\mathbb{O}_v}$) и $\Gamma \cap G_{\mathbb{O}_v}(\mathfrak{p}_v) = (e)$. Лемма 4 доказана.

Из леммы 4 вытекает, что для доказательства предложения 7 достаточно установить равенство $[B_{0v} \setminus D_i] = a_i(q_v - 1)$ с целым a_i для любого $i = 0, 1, \dots, m$. Пусть H_1, H_2, \dots, H_t — все подгруппы в H индекса 2^i . Положим $D_i^j = \{g \in G_{0v} \mid H \cap (g^{-1}B_v g) = H_j\}$. Тогда, очевидно, $[B_{0v} \setminus D_i] = \sum_{j=1}^t [B_{0v} \setminus D_i^j]$ и поэтому достаточно показать, что каждое $[B_{0v} \setminus D_i^j]$ имеет вид $a_i^j(q_v - 1)$. Другими словами, достаточно доказать следующее: если H' — подгруппа группы H и $D(H') = \{g \in G_{0v} \mid H \cap (g^{-1}B_v g) = H'\}$, то $B_{0v} \setminus D(H')$ делится на $q_v - 1$. Обозначим $\tilde{D}(H') = \{g \in G_{0v} \mid H' \subset \subset g^{-1}B_v g\}$, и пусть $\Psi(H')$ — множество подгрупп группы H , строго содержащих H' . Тогда

$$[B_{0v} \setminus D(H')] = [B_{0v} \setminus \tilde{D}(H')] - [B_{0v} \setminus \bigcup_{H'' \in \Psi(H')} \tilde{D}(H'')].$$

Воспользуемся теперь следующей общеизвестной комбинаторной леммой.

ЛЕММА 5. Пусть A_1, \dots, A_m — конечные множества. Тогда

$$[A_1 \cup \dots \cup A_m] = \sum_{l=1}^m (-1)^{l+1} \sum_{1 \leq i_1 < \dots < i_l \leq m} [A_{i_1} \cap \dots \cap A_{i_l}].$$

Так как $\tilde{D}(H_1'') \cap \tilde{D}(H_2'') = \tilde{D}(H_1'' H_2'')$, то из леммы 5 вытекает существование таких целых $b_{H''}$, что

$$[B_{0v} \setminus \bigcup_{H'' \in \Psi(H')} \tilde{D}(H'')] = \sum_{H'' \in \Psi(H')} b_{H''} [B_{0v} \setminus \tilde{D}(H'')].$$

Поэтому, окончательно, нужно доказать

Предложение 8. Пусть $H' \subset H$. Тогда $[B_{0v} \setminus \tilde{D}(H')]$ делится на $q_v - 1$.

Доказательство. Мы знаем (см. формулировку предложения 7), что для некоторого $g_0 \in G_{0v}$ $g_0^{-1}H'g_0 = \Gamma' = \{\gamma'_1, \dots, \gamma'_d\} \subset \Gamma$.

ЛЕММА 6. $\tilde{D}(H') = \bigcup_{\gamma \in \tilde{\Gamma}^d} B_{0v} V(\Gamma', \gamma)_{0v} g_0^{-1}$.

Доказательство. Пусть $x \in \tilde{D}(H')$, т. е. $H' \subset \subset x^{-1}B_v x$, что эквивалентно $\Gamma'' = xg_0\Gamma'g_0^{-1}x^{-1} \subset B_v$. Так как Γ'' — 2-группа, а Γ_0 — силовская 2-подгруппа проконечной группы B_v , то для некоторого $b \in B_{0v}$ $\Gamma''' = bxg_0\Gamma'g_0^{-1}x^{-1}b^{-1} = b\Gamma''b^{-1} \subset \Gamma_0$ (см. [11]). Пусть $\Gamma''' = \{\gamma_1, \dots, \gamma_d\}$, причем элементы занумерованы таким образом, что $bxg_0\gamma'_i g_0^{-1}x^{-1}b^{-1} = \gamma_i$, $i = 1, \dots, d$. Но тогда $bxg_0 \in V(\Gamma', \gamma)_{0v}$ для $\gamma = (\gamma_1, \dots, \gamma_d)$ и $x \in \in B_{0v} V(\Gamma', \gamma)_{0v} g_0^{-1}$, так что для доказательства леммы осталось установить, что $\Gamma''' \subset \tilde{\Gamma}$, однако это непосредственно вытекает из пункта (ii) предложения 3. Отметим также, что если $\tilde{D}(H') = \emptyset$, то и объединение в правой части пусто. Лемма 6 доказана.

Продолжая доказательство предложения 8, заметим, что из леммы 6 и условия (2) следует, что

$$[B_{0v} \setminus \tilde{D}(H')] = \sum_{\gamma \in \tilde{\Gamma}^d} [B_{0v} \setminus B_{0v} V(\Gamma', \gamma)_{0v}].$$

Далее, если $\gamma = (\gamma_1, \dots, \gamma_d)$, $\bar{\Gamma} = \{\gamma_1, \dots, \gamma_d\}$ и $g_\gamma \in V(\Gamma', \gamma)_{\mathcal{O}_v}$, то $V(\Gamma', \gamma)_{\mathcal{O}_v} = C(\bar{\Gamma})_{\mathcal{O}_v} g_\gamma$, где $C(\bar{\Gamma})$ — централизатор $\bar{\Gamma}$ в G . Поэтому

$$[B_{0v} \setminus \tilde{D}(H')] = \sum_{\gamma \in \Phi_d} [C(\bar{\Gamma})_{\mathcal{O}_v} : C(\bar{\Gamma})_{\mathcal{O}_v} \cap B_{0v}],$$

где $\Phi_d = \{\gamma \in \tilde{\Gamma}^d \mid V(\Gamma', \gamma)_{\mathcal{O}_v} \neq \emptyset\}$; покажем, что $[C(\bar{\Gamma})_{\mathcal{O}_v} : C(\bar{\Gamma})_{\mathcal{O}_v} \cap B_{0v}]$ делится на $q_v - 1$. Действительно, последний индекс делится на $[C(\bar{\Gamma})_{\mathcal{O}_v} : C(\bar{\Gamma})_{\mathcal{O}_v}(\mathfrak{p}_v)]$. Так как $\bar{\Gamma} \subset \tilde{\Gamma}$, то $C(\bar{\Gamma}) \supset T$, где T — одномерный тор $SO_2(W) \perp (e) \perp \dots \perp (e)$, W натянуто на u_1, u_2 (или, что то же самое, на e_1, e_2). Поэтому $[C(\bar{\Gamma})_{\mathcal{O}_v} : C(\bar{\Gamma})_{\mathcal{O}_v}(\mathfrak{p}_v)]$ делится на $[T_{\mathcal{O}_v} : T_{\mathcal{O}_v}(\mathfrak{p}_v)]$. Наконец, T разложим над K_v (так как $f_1, -f_2 \in U_v^2$), откуда $[T_{\mathcal{O}_v} : T_{\mathcal{O}_v}(\mathfrak{p}_v)] = q_v - 1$. Предложения 7, 8 доказаны, а это и завершает доказательство теоремы 1 для $G = O_n(f)$.

§ 4. Доказательство теоремы 1. Общий случай

Пусть G — связная K -определенная алгебраическая группа степени n с компактной группой G_∞ и положительно определенной квадратичная форма f выбрана в соответствии с предложением 1 таким образом, что $G \subset SO_n(f)$. Так как случай $G = SO_n(f)$ был разобран в § 3, то для завершения доказательства теоремы 1 осталось исследовать случай $G \neq SO_n(f)$. Здесь ключевую роль играет

Предложение 9. Пусть G — собственная связная K -определенная подгруппа группы $SO_n(f)$. Тогда существует такой ортогональный относительно f базис $e = (e_1, \dots, e_n)$ пространства K^n , что пересечение $G \cap \Gamma(e)$ лежит в центре $Z(G)$ группы G .

Доказательство. Будем вначале предполагать, что группа $SO_n(f)$ проективно проста, т. е. $n \neq 2, 4$. Пусть $e^0 = (e_1^0, \dots, e_n^0)$ — некоторый ортогональный базис пространства K^n и $\Gamma_0 = \Gamma(e^0)$. Для произвольного $g \in SO_n(f)_K$ обозначим через $g(e^0)$ базис $(g(e_1^0), \dots, g(e_n^0))$. Тогда $\Gamma(g(e^0)) = g\Gamma_0g^{-1}$, так что для доказательства предложения достаточно доказать следующее: существует $g \in SO_n(f)_K$ со свойством $G \cap (g\Gamma_0g^{-1}) \subset Z(G)$. Предположим противное. Тогда для любого $g \in SO_n(f)_K$ найдется нецентральный $x(g) = g\gamma(g)g^{-1} \in G$, $\gamma(g) \in \Gamma_0$. Зафиксируем некоторый максимальный тор $T \subset G$. Ввиду полупростоты $x(g)$ и теоремы сопряженности для максимальных торов (см. [2]), существует такой $h(g) \in G$, что $h(g)x(g)h(g)^{-1} = h(g)g\gamma(g)g^{-1}h(g)^{-1} \in T$. Пусть $\Gamma_0 = \{\gamma_1, \dots, \gamma_{2^n}\}$, t_1, \dots, t_s — все нецентральные элементы второго порядка в T и $I = \{(i, j) \mid \exists g_{ij} \in SO_n(f) \quad g_{ij}\gamma_i g_{ij}^{-1} = t_j\}$. Если в этих обозначениях $\gamma(g) = \gamma_i$, $h(g)x(g)h(g)^{-1} = t_j$, то $t_j = h(g)gg_{ij}^{-1}t_jg_{ij}g^{-1}h(g)^{-1}$, так что $h(g)gg_{ij}^{-1}$ принадлежит централизатору $C(t_j) = C_{SO_n(f)}(t_j)$. Ввиду произвольности g , отсюда следует, что $SO_n(f)_K \subset \bigcup_{(i,j) \in I} GC(t_j)g_{ij}$. Переходя к замыканию в топологии Зарисского, получим $SO_n(f) = \bigcup_{(i,j) \in I} \overline{GC(t_j)} g_{ij}$,

или, учитывая связность $SO_n(f)$, $SO_n(f) = \overline{GC(t_{j_0})} g_{i_0 j_0}$, т. е. $SO_n(f) = \overline{GC(t_{j_0})}$. Из последнего равенства вытекает, что класс сопряженности

$$\{g^{-1}t_{j_0}g\}_{g \in SO_n(f)} \subset \overline{\{g^{-1}t_{j_0}g\}_{g \in G}} \subset G.$$

Поэтому нормальный делитель группы $SO_n(f)$, порожденный t_{j_0} , содержится в G . Но поскольку $G \neq SO_n(f)$, то из проективной простоты $SO_n(f)$ (см., например, [1]) вытекает, что $t_{j_0} \in Z(SO_n(f))$, и тем более $t_{j_0} \in Z(G)$. Полученное противоречие и доказывает требуемое.

Нам осталось разобрать случаи $n=2, 4$. Если $n=2$, то $SO_n(f)$ — одномерный тор, так что $G=(e)$, и доказывать нечего. Пусть теперь $n=4$. Тогда известно (см. [1]), что $H=SO_n(f)=H_1H_2$ — почти прямое произведение двух своих нормальных делителей, изоморфных SL_2 . Рассуждая, как и выше, получим, что если утверждение предложения не выполняется, то G содержит нецентральный нормальный делитель группы H . Поэтому либо H_1 , либо H_2 содержится в G . Пусть для определенности $H_1 \subset G$. Рассмотрим фактор-морфизм $\pi: H \rightarrow H/H_1 = F$; группа F изоморфна PSL_2 . Если допустить, что для всякого $h \in H_K$ найдется $x(h) \in G \cap (h\Gamma_0 h^{-1})$ такой, что $x(h) \notin Z(G)$, то для любого $g \in \pi(H_K)$ существует $y(g) \in \pi(G) \cap (g\pi(\Gamma_0)g^{-1})$, $y(g) \neq e$. Действительно, если $x(h) \in H_1$, то при изоморфизме $H_1 \simeq SL_2$ он перейдет в матрицу $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, так что $x(h) \in Z(H_1)$, а поэтому и $Z(G)$. Таким образом, можно положить $y(g) = x(\pi^{-1}(g))$. Группа $\pi(G)$ связна, так что вышеприведенное рассуждение с использованием плотности $\pi(H_K)$ в F показывает, что $\pi(G) \triangleleft F$. Так как группа F проста, а $\pi(G) \neq (e)$, то $\pi(G) = F$, откуда $G = SO_n(f)$ — противоречие. Предложение 9 полностью доказано.

З а м е ч а н и е. На самом деле в предложении 9 доказывается даже существование такого $g \in SO_n(f)_K$, что $G \cap (g\Gamma_0 g^{-1}) \subset Z(SO_n(f))$.

Зафиксируем ортогональный базис $e = (e_1, \dots, e_n)$ со свойством, указанным в предложении 9, и пусть в этом базисе $f = f_1 x_1^2 + \dots + f_n x_n^2$. Для произвольного нормирования $v \in V_f$ такого, что $\bar{K} \subset K_v$, выберем простой элемент $\pi_v \in \mathcal{O}$ со свойством $\pi_v \in U_w$ для $w \neq v$, и для целого $d > 0$ обозначим через $L^{(v,d)}$ \mathcal{O} -решетку с базисом $e_1, \pi_v^d e_2, \dots, \pi_v^{d(n-1)} e_n$.

Предложение 10. *Существуют такие $v \in V_f, d > 0$, что для некоторого разложения $G_A = \bigcup_{j=1}^s G_{A(\infty)}^{L^{(v,d)}} z_j G_K$ все группы*

$$G_{\mathcal{O}}^{(j)} = z_j^{-1} G_{A(\infty)}^{L^{(v,d)}} z_j \cap G_K$$

содержатся в $Z(G)$. При этом для почти всех v $(z_j)_v = e$.

Доказательство. Положим $L = \mathcal{O}e_1 \perp \dots \perp \mathcal{O}e_n$, и пусть $G_A = \bigcup_{j=1}^t G_{A(\infty)}^L \bar{z}_j G_K$ — такое разложение, что для некоторого конечного подмножества $S \subset V_f$ $(\bar{z}_j)_v = e$ при $v \in V_f \setminus S$. Выберем, исходя из теоремы плот-

ности Чеботарева, такое $v \in V_j \setminus S$, что $\bar{K} \subset K_v$ и $f_1, \dots, f_n \in U_v$. Далее, ввиду компактности G_∞ , все группы $\bar{G}_\theta^{(j)} = \bar{z}_j^{-1} G_{A(\infty)}^L \bar{z}_j \cap G_K$ конечны; положим

$$\Phi = \left(\bigcup_{j=1}^t \bar{G}_\theta^{(j)} \right) \setminus Z(G), \quad D = \{g^{-1} \varphi g \mid g \in G_{\theta_v}^{L_v}, \varphi \in \Phi\}.$$

В силу конечности Φ и компактности $G_{\theta_v}^{L_v}$, множество D компактно. Так как

$$G_{\theta_v}^{L(v,d)} = G \cap O_n(f)_{\theta_v}^{L(v,d)},$$

а из предложения 2 вытекает, что

$$\bigcap_{d=1}^{\infty} O_n(f)_{\theta_v}^{L(v,d)} = \Gamma(\mathfrak{e}),$$

то

$$\bigcap_{d=1}^{\infty} G_{\theta_v}^{L(v,d)} \subset Z(G);$$

в частности,

$$\bigcap_{d=1}^{\infty} (G_{\theta_v}^{L(v,d)} \cap D) = \emptyset.$$

Из компактности D тогда выводим, что для некоторого d_0 пересечение

$$\bigcap_{d=1}^{d_0} (G_{\theta_v}^{L(v,d)} \cap D) = \emptyset,$$

а так как

$$G_{\theta_v}^{L(v,d_1)} \subset G_{\theta_v}^{L(v,d_2)}$$

при $d_1 \geq d_2$, то для $d = d_0$

$$G_{\theta_v}^{L(v,d)} \cap D = \emptyset,$$

т. е. для любого $g \in G_{\theta_v}^{L_v}$

$$(g^{-1} G_{\theta_v}^{L(v,d)} g) \cap \Phi = \emptyset.$$

Покажем, что решетка $L^{(v,d)}$ — искомая.

Как и при доказательстве предложения 6, заключаем, что в качестве представителей классов $G_{A(\infty)}^{L(v,d)} \setminus G_A/G_K$ могут быть выбраны адели $z(a, j)$, $a \in G_{\theta_v}^{L_v}$ с локальными компонентами

$$z(a, j)_w = \begin{cases} e, & w \notin S \cup \{v\}, \\ (\bar{z}_j)_w, & w \in S, \\ a, & w = v. \end{cases}$$

Поэтому достаточно показать, что любая группа

$$G_{\theta_v}^{(a,j)} = z(a, j)^{-1} G_{A(\infty)}^{L(v,d)} z(a, j) \cap G_K$$

содержится в $Z(G)$. Пусть $x \in G_{\mathbb{O}}^{(a,j)}$ и $x \in Z(G)$. Тогда $x \in \overline{G_{\mathbb{O}}^{(j)}}$, так что $x \in \Phi$. С другой стороны, переходя к проекциям на v -компоненту, получим

$$x \in a^{-1}G_{\mathbb{O}_v}^{L(v,d)} a,$$

что противоречит нашим построениям. Предложение 10 доказано.

Теперь уже легко завершить доказательство теоремы 1. Действительно, принимая во внимание предложение 10, можно с самого начала предполагать, что базис e_1, \dots, e_n выбран таким образом, что для некоторого разложения $G_A = \bigcup_{j=1}^s G_{A(\infty)}^L z_j G_K$ все группы $G_{\mathbb{O}}^{(j)} = z_j^{-1} G_{A(\infty)}^L z_j \cap G_K$ содержатся в $Z(G)$, причем для $v \in V_f \setminus S$ $(z_j)_v = e$, где $S \subset V_f$ — конечное подмножество. Зафиксируем некоторый максимальный K -определенный тор $T \subset G$ с полем разложения R и обозначим через P расширение K , порожденное \overline{K} , R и примитивным корнем ρ_{r_1} степени $r_1 = 2^n m r$ из единицы, где $m = \text{H. O. K.} ([G_{\mathbb{O}}^{(1)}], \dots, [G_{\mathbb{O}}^{(s)}])$. Выберем такое нормирование $v \in V_f \setminus S$, что $P \subset K_v$, причем $r_1, f_1, \dots, f_n \in U_v$ и существует гладкая редукция $T^{(v)}$ тора T по модулю v (см. [3]). Пусть $\pi_v \in \mathcal{O}$ — такой простой элемент, что $\pi_v \in U_v$ при $w \neq v$, и $L(r)$ — решетка с базисом $e_1, \pi_v e_2, \dots, \pi_v^{(n-1)} e_n$. Покажем, что число классов $\text{cl}(G^{L(r)})$ делится на r .

Имеем $G_{\mathbb{O}_w}^{L(r)\omega} = G_{\mathbb{O}_w}^{L\omega}$ при $w \neq v$ и $G_{\mathbb{O}_v}^{L(r)v} = B_v = G \cap (\Gamma(e) B_{0v})$ (см. предложение 2), так что $G_{A(\infty)}^{L(r)} \subset G_{A(\infty)}^L$. Обозначим через $c_j(v)$ число классов $G_{A(\infty)}^{L(r)} x G_K$, на которые распадается класс $G_{A(\infty)}^L z_j G_K$. Как и в лемме 3, убеждаемся, что $\text{cl}(G^{L(r)}) = \sum_{j=1}^s c_j(v)$, причем $c_j(v) = [B_v \setminus G_{\mathbb{O}_v}^{L(v)} / G_{\mathbb{O}}^{(j)}]$, а так как $G_{\mathbb{O}}^{(j)} \subset Z(G)$, то $c_j(v) = [G_{\mathbb{O}_v}^{L(v)} : G_{\mathbb{O}}^{(j)} B_v]$. Таким образом, достаточно показать, что все числа $c_j(v)$ делятся на r . Но

$$[G_{\mathbb{O}_v}^{L(v)} : G_{\mathbb{O}}^{(j)} B_v] = \frac{[G_{\mathbb{O}_v}^{L(v)} : G_{\mathbb{O}_v}^{L(v)} \cap B_{0v}]}{[G_{\mathbb{O}}^{(j)} B_v : G_{\mathbb{O}_v}^{L(v)} \cap B_{0v}]};$$

при этом, очевидно, знаменатель делит $2^n m$. Поэтому достаточно показать, что числитель делится на $2^n m r$. С другой стороны, $[G_{\mathbb{O}_v}^{L(v)} : G_{\mathbb{O}_v}^{L(v)} \cap B_{0v}]$ делится на $[G_{\mathbb{O}_v}^{L(v)} : G_{\mathbb{O}_v}^{L(v)}(\mathfrak{p}_v)]$, а значит, и на $[T_{\mathbb{O}_v}^{L(v)} : T_{\mathbb{O}_v}^{L(v)}(\mathfrak{p}_v)]$. Последний индекс, однако, совпадает с числом точек $[T_{k_v}^{(v)}]$ редукции $T^{(v)}$ над полем вычетов k_v , и так как T разложим, то $[T_{k_v}^{(v)}] = (q_v - 1)^{\dim T}$, где $q_v = [k_v]$. Осталось заметить, что $\rho_{r_1} \in K_v$, $v(r_1) = 1$, так что $q_v - 1$ делится на $r_1 = 2^n m r$.

Теорема 1 полностью доказана.

Литература

1. Артин Э. Геометрическая алгебра. М.: Наука, 1969.
2. Борель А. Линейные алгебраические группы. М.: Мир, 1972.
3. Вейль А. Адели и алгебраические группы.— Математика, 1964, т. 8, № 4, с. 3—74.
4. Вейль А. О формуле Зигеля в теории классических групп.— Математика, 1969, т. 13, № 6, с. 18—98.
5. Касселс Дж., Фрелих А. Алгебраическая теория чисел. М.: Мир, 1969.
6. Платонов В. П. Проблема сильной аппроксимации и гипотеза Кнезера — Титса для алгебраических групп.— Изв. АН СССР. Сер. матем., 1969, т. 33, № 6, с. 1211—1219.
7. Платонов В. П. Дополнение к работе «Проблема сильной аппроксимации и гипотеза Кнезера — Титса для алгебраических групп».— Изв. АН СССР. Сер. матем., 1970, т. 34, № 4, с. 775—777.
8. Платонов В. П., Бондаренко А. А., Рапинчук А. С. Числа и группы классов алгебраических групп.— Изв. АН СССР. Сер. матем., 1979, 43, № 3, с. 603—627.
9. Платонов В. П., Бондаренко А. А., Рапинчук А. С. Числа и группы классов алгебраических групп. II.— Изв. АН СССР. Сер. матем., 1980, т. 44, № 2, с. 395—414.
10. Рапинчук А. С. К гипотезе Платонова о роде в арифметических группах.— Докл АН БССР, 1981, т. 25, № 2, с. 101—104.
11. Серр Ж.-П. Когомологии Галуа. М.: Мир, 1968.
12. Borel A. Some finiteness properties of adèle groups over number fields.— Publ. Math. I. H. E. S., 1963, № 16, p. 101—126.
13. Eichler M. Quadratische Formen und orthogonale Gruppen, Berlin — Göttingen — Heidelberg, Springer — Verlag, 1952.
14. Kneser M. Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen.— Arch. Math., 1956, B. 7, № 5, s. 323—332.
15. O'Meara O. T. Introduction to quadratic forms, Berlin — Heidelberg — New York, Springer — Verlag, 1963.
16. Pfeuffer H. Einklassige Geschlechter totalpositiver quadratischer Formen in totalreellen algebraischen Zahlkörpern.— J. Number Theory, 1971, v. 3, s. 371—411.
17. Siegel C. L. Über die analytische Theorie der quadratischen Formen. I, II, III.— Ann. Math., 1935, B. 36, s. 527—606; 1936, B. 37, s. 230—263; 1937, B. 38, s. 212—291.
18. Watson G. L. Integral quadratic forms. Cambridge Univ. Press, 1960.
19. Watson G. L. One-class genera of positive ternary quadratic forms.— Mathematika, 1975, v. 22, № 1, p. 1—11.
20. Watson G. L. One-class genera of positive quadratic forms in at least five variables.— Acta Arithm., 1975, v. 26, № 3, p. 305—327.
21. Weil A. Sur la théorie des formes quadratiques.— Colloq. Théorie des Groupes Algébriques (Bruxelles, 1962), Paris, 1962, p. 9—22.

Поступила в редакцию
1.IV.1981