Counting genera of integral quadratic forms

Yao-Rui

2019-02-01

In this note all quadratic forms are assumed to be nondegenerate.

1 Quadratic forms and local-global principles

The local-global problem for quadratic forms is a very classical problem in number theory that motivated a lot of what people currently do in this area of mathematics. The purpose of this talk is to go back to the roots and explore this problem using modern languages and tools.

Let f be an integral quadratic form (that is nondegenerate), so

$$f = \sum_i a_{ii} X_i^2 + \sum_{j \neq k} 2a_{jk} X_j X_k, \qquad a_{ii}, a_{jk} \in \mathbb{Z}.$$

There are two other ways to think about quadratic forms.

- For any f, associate to it the symmetric matrix $A_f = (\alpha_{ij})$ with $\alpha_{ii} = a_{ii}$ and $2\alpha_{jk} = a_{jk}$ for $j \neq k$.
- If f is positive definite, associate to it a lattice of rank n, the number of variables in f, spanned by vectors $v_1, \ldots, v_n$ with $\langle v_i, v_i \rangle = a_{ii}$ and $2\langle v_i, v_j \rangle = a_{jk}$ for $j \neq k$.

Define the *class* $\mathrm{cl}(f)$ of f to be the collection of all integral quadratic forms f' that are equivalent over $\mathbb{Z}$, i.e. such that $g^t f g = f'$ for some $g \in \mathrm{GL}_n(\mathbb{Z})$, and define the *genus* $\mathrm{gen}(f)$ to be the collection of all integral quadratic forms f' that are equivalent over $\mathbb{R}$ and $\mathbb{Z}_p$ for all primes p (but not necessarily over $\mathbb{Z}$; this is the point of the talk!). Clearly

$$\mathrm{gen}(f) = \bigsqcup_{i \in I_f} \mathrm{cl}(f_i),$$

where f_i is a set of representatives in the genus of f. We define the *number of classes* $c(f)$ *of* f to be the cardinality of I_f. Sometimes people refer to $\mathbb{Z}$ as the "global ring of integers", while they refer to $\mathbb{R}$ and $\mathbb{Z}_p$ as the "local ring of integers". The p-adic integers are sometimes called "nonarchimedean" and the real numbers "archimedean" for elementary reasons to do with the triangle inequality.

If one were to work over the field of fractions $\mathbb{Q}$ of $\mathbb{Z}$ and define the analogous definitions by taking the field of fractions of every ring above, then things will be boring: the local-global principle of Hasse and Minkowski tells us that in this case every genus has precisely one class, or in other words, that two integral quadratic forms over $\mathbb{Q}$ are globally equivalent if and only if they are locally equivalent! (See the exercises in [1] for more information.) However, when we work over $\mathbb{Z}$, this is not always the case.

Example 1. Consider the quadratic form $f = 5x^2 + 11y^2$. Then the quadratic form

$$f' = x^2 + 55y^2$$

lies in the same genus and in a different class of f. To see this, consider

$$g_1 = \begin{bmatrix} 1/4 & -11/4 \\ 1/4 & 5/4 \end{bmatrix}, \qquad g_2 = \begin{bmatrix} 1/7 & -22/7 \\ 2/7 & 5/7 \end{bmatrix}.$$

Then $g_1^t f g_1 = f'$ and $g_2^t f g_2 = f'$. Since $g_1 \in \mathrm{GL}_2(\mathbb{Z}_p)$ for all $p \neq 2$ and $g_2 \in \mathrm{GL}_2(\mathbb{Z}_2)$, we see that f and f' are in the same genus. However, a direct computation shows that there does not exist $g \in \mathrm{GL}_2(\mathbb{Z})$ such that $g^t f g = f'$, so they cannot be in the same class.

Let us recall that there is a brute-force way to determine the number of classes of a binary quadratic form f over $\mathbb{Q}$ (algorithms also exists for ternary quadratic forms, and possibly higher order ones). Namely, write down all the classes forms equivalent to f under $\mathrm{SL}_2(\mathbb{Z})$ (which is bounded by the class number of $\mathbb{Q}[\sqrt{\mathrm{disc}(f)}]$), identify those equivalent under $\mathrm{GL}_2(\mathbb{Z})$, and check pairwise if they are equivalent under $\mathbb{Q}$ and $\mathbb{Z}_p$. Using this method, one can show that $c(f) = 2$ for the form $f = 5x^2 + 11y^2$ in the previous paragraph. We can also verify this using Siegel's mass formula (see next part).

In this talk I hope to talk about various results on how to count $c(f)$. Hopefully this first introductory part illustrated the problem well enough. In the second part we provide examples of Siegel's mass formula, which counts the genus of quadratic forms via weighted sums by means of its $\mathbb{Z}$-automorphism group. In the third and last part we will explain how $c(f)$ is the the class number of the adelic orthogonal group.

2 Enumeration of the mass via Siegel's Mass Formula

2.1 Overview of the mass formula

Let f be an integral quadratic form, and preserve the notations $c(f)$ and I_f from before. The mass formula does not compute $c(f)$ but instead a variant of it, weighting each class by the size of its automorphism group. Let us define

$$O_f(\mathbb{Z}) = \{g \in \mathrm{GL}_n(\mathbb{Z}) : g^t A_f g = A_f\}.$$

Definition 2. The *mass* of f is defined to be

$$m(f) = \sum_{i \in I_f} \frac{1}{\#O_{f_i}(\mathbb{Z})}.$$

Theorem 3 ([2, Equation 2])**.** *If f has dimension $n \geq 2$, then*

$$m(f) = 2\pi^{-n(n+1)/4} \prod_{j=1}^{n} \Gamma\left(\frac{j}{2}\right) \prod_p m_p(f),$$

where $m_p(f)$ are the p-masses of f.

A proof of this is somewhere in the literature; for example, see [7] for the case of lattices in general number fields. For $n \geq 1$ there might be an analog of Siegel's mass formula somewhere, but in this case one sees easily that it essentially boils down to computations using Hensel's Lemma and quadratic reciprocity.

In this note we are interested in using this to compute some examples. Let us now define $m_p(f)$, following [2, Section 5]. By the Jordan decomposition theorem one can write

$$f = \sum_q q f_q,$$

where q are powers of p and f_q has discriminant prime to p (see [8, Theorem 1.8.2]). Then

$$m_p(f) = \prod_q M_p(f_q) \prod_{q<q'} \left(\frac{q'}{q}\right)^{n(q)n(q')/2} \qquad (p \neq 2)$$

where q and q' ranges over all powers of p. The number $n(q)$ is the dimension of the form f_q, and

$$M_p(f_q) = \begin{cases} \left[2(1-p^{-2})(1-p^{-4})\cdots(1-p^{1-n})\right]^{-1} & \text{if } n \text{ is odd,} \\ \left[2(1-p^{-2})(1-p^{-4})\cdots(1-p^{2-n})\left(1-\left(\dfrac{(-1)^{n-2}d_q}{p}\right)p^{-n/2}\right)\right]^{-1} & \text{if } n \text{ is even.} \end{cases}$$

Here n is the dimension of f and d_q is the discriminant of f_q. Also, the "fraction" in the second expression is the Jacobi symbol.

For $n = 2$ one has the formula

$$m_2(f) = \prod_q M_2(f_q) \prod_{q<q'} \left(\frac{q'}{q}\right)^{n(q)n(q')/2} 2^{n(I,I)-n(II)}$$

where q and q' are the same as before. The factors $M_2(f_q)$ are difficult to compute and we will not need them here; see [2] for more information. The definitions of $n(I,I)$ and $n(II)$ are as follows. If f_q represents an odd 2-adic integer, then it is of Type I, and of Type II otherwise. Then $n(I,I)$ is the total number of pairs of adjacent constituents (f_q, f_{2q}) that are both of Type I, and $n(II)$ is the sum of the dimensions of all f_q that are of Type II.

For convenience we now define standard mass. Write n as $2s$ or $2s-1$, where n is the dimension of f. Also write $D = (-1)^s d$, where d is the discriminant of f. Then we define

$$\mathrm{std}_p(f) = \left[2(1-p^{-2})(1-p^{-4})\cdots(1-p^{2-2s})(1-\epsilon_p p^{-s})\right]^{-1},$$

where

$$\epsilon_p = \begin{cases} 0 & \text{if } n \text{ is odd,} \\ \left(\dfrac{(-1)^s d}{p}\right) & \text{if } n \text{ is even.} \end{cases}$$

Note that if p is an odd prime not dividing the discriminant of f, then $m_p(f)$ is equal to $\mathrm{std}_p(f)$. If all the p-masses took their standard mass, then $m(f)$ will take the value

$$2\pi^{-n(n+1)/4}\zeta_D(s)\prod_{j=1}^{n}\Gamma\left(\frac{j}{2}\right)\prod_{k=1}^{s-1}\zeta(2k),$$

where the factor $\zeta_D(s)$ is omitted when n is odd, and if n is even

$$\zeta_D(s) = \prod_p \frac{1}{\left(1-\left(\frac{D}{p}\right)p^{-s}\right)}.$$

A list of values of $\zeta_D(s)$ for small D and s can be found in [2, Table 6].

Example 4. Let us compute the mass of the genus corresponding to the quadratic form $f = x^2 + 55y^2$ from the previous part. In this case $n = 2$ and $s = 1$. It is readily seen by definition that

$$m_p(f) = \frac{1}{2\left(1-\left(\frac{-55}{p}\right)p^{-1}\right)} \qquad p \neq 2, 5, 11,$$

since the Jordan decomposition of f in this case is trivial. For $p = 5$ one can write $f = x^2 + 5 \cdot 11y^2$, and

$$m_5(f) = \frac{\sqrt{5}}{2}.$$

Similarly $m_{11}(f) = \sqrt{11}/2$. By the recipe given in [2] one deduces that $m_2(f) = 1/4$, so

$$m(f) = \frac{2}{\pi}\cdot\frac{1}{4}\cdot\frac{\sqrt{5}}{2}\cdot\frac{\sqrt{11}}{2}\cdot\zeta_{-55}(1).$$

From [5, Chapter 6] one has

$$\zeta_{-55}(1) = -\frac{\pi}{55^{3/2}}\sum_{k=1}^{55} k\left(\frac{-55}{k}\right) = \frac{4\pi}{\sqrt{55}},$$

so

$$m(f) = 1/2.$$

A computation tells us that both quadratic forms in Example 1 have automorphism groups of order 4, agreeing with our computation in this example.

Note that the automorphism groups of classes in a genus may have different orders; see [2] for examples such as $7x^2 + y^2 + z^2$ and $7x^2 + 7y^2 + z^2$, having automorphism groups of orders 16 and 8 respectively.

2.2 Unimodular lattices

In this section f will be an *even unimodular* positive definite quadratic form, and we also view f as a lattice Γ_f. Let us now explain what even and unimodular means. The lattice Γ_f is even if all norms are even. To the lattice Γ_f one can define its dual lattice

$$\Gamma_f^* = \{y \in \mathbb{R}^n : x \cdot y \in \mathbb{Z} \text{ for all } x \in \Gamma_f\}.$$

The lattice Γ_f is unimodular if $\Gamma_f^* = \Gamma_f$. One can prove that

$$\operatorname{vol}(\Gamma_f)\operatorname{vol}(\Gamma_f^*) = 1.$$

Thus unimodular lattices have volume 1. See [6] for more information on lattice theory. We now prove the following key proposition.

Proposition 5. *If f is an even unimodular positive definite quadratic form, then $n = \operatorname{rank}\Gamma_f$ must be divisible by 8.*

Proof. Write $q = e^{2\pi i\tau}$. Associate to Γ_f its theta function

$$\theta_{\Gamma_f}(\tau) = \sum_{x\in\Gamma_f} q^{\frac{1}{2}x\cdot x},$$

which is a holomorphic function on the upper half plane. (In fact it is a modular form of weight $n/2$).

We first show that

$$\theta_{\Gamma_f}\left(-\frac{1}{\tau}\right) = \left(\frac{\tau}{i}\right)^{n/2}\theta_{\Gamma_f}(\tau).$$

By the identity theorem from complex analysis, it suffices to show this when $\tau = it$ with $t > 0$. Now, using Poisson's summation formula

$$\sum_{x\in\Gamma_f} f(x) = \frac{1}{\operatorname{vol}(\Gamma_f)}\sum_{y\in\Gamma_f^*}\hat{f}(y) = \sum_{y\in\Gamma_f}\hat{f}(y)$$

and recalling that the Fourier transform of $e^{2\pi i(x\cdot x)/2it} = e^{-\pi(x\cdot x)/t}$ is $(\sqrt{t})^n e^{-\pi t(y\cdot y)}$, one sees that

$$\theta_{\Gamma_f}\left(-\frac{1}{it}\right) = t^{n/2}\sum_{y\in\Gamma_f} e^{-\pi t y\cdot y} = t^{n/2}\theta_{\Gamma_f}(it),$$

as desired.

Recall that there is the standard action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane, and this matrix group is generated by

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad \text{and} \qquad T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

satisfying $(ST)^3\tau = \tau$. Then, since $\theta_{\Gamma_f}(T\tau) = \theta_{\Gamma_f}(\tau+1) = \theta_{\Gamma_f}(\tau)$, the identity shown in the previous section implies

$$\theta_{\Gamma_f}(TS\tau) = \left(\frac{\tau}{i}\right)^{n/2}\theta_{\Gamma_f}(\tau).$$

We now show that $n = \operatorname{rank}\Gamma_f$ must be divisible by 8. Suppose otherwise. Then, by substituting Γ_f with $\Gamma_f \perp \Gamma_f$ or $\Gamma_f \perp \Gamma_f \perp \Gamma_f \perp \Gamma_f$, we can assume $n \equiv 4 \pmod 8$. The above identity then yields

$$\theta_{\Gamma_f}(TS\tau) = (-1)^{n/2}\tau^{n/2}\theta_{\Gamma_f}(\tau) = -\tau^{n/2}\theta_{\Gamma_f}(\tau).$$

A repeated application tells us that

$$\begin{aligned}
\theta_{\Gamma_f}(\tau) &= \theta_{\Gamma_f}\left((TS)^3\tau\right) \\
&= -\left((TS)^2\tau\right)^{n/2}(TS\tau)^{n/2}\tau^{n/2}\theta_{\Gamma_f}(\tau) \\
&= -\left(\frac{-1}{\tau-1}\cdot\frac{\tau-1}{\tau}\cdot\tau\right)^{n/2}\theta_{\Gamma_f}(\tau) \\
&= -\theta_{\Gamma_f}(\tau),
\end{aligned}$$

a contradiction. □

Using this, we are now ready to state Siegel's Mass Formula for even unimodular lattices.

Corollary 6. *Let f be an even unimodular positive definite quadratic form of dimension n. Then*

$$\begin{aligned} m(f) &= \frac{1}{2^{n-1}\pi^{n(n+1)/4}}\Gamma\left(\frac{1}{2}\right)\Gamma\left(\frac{2}{2}\right)\cdots\Gamma\left(\frac{n}{2}\right)\zeta(2)\zeta(4)\cdots\zeta(n-2)\zeta\left(\frac{n}{2}\right) \\ &= \frac{B_{n/2}}{n}\prod_{j=1}^{n/2-1}\frac{B_{2j}}{4j}, \end{aligned}$$

where B_j are the Bernoulli numbers defined by

$$\frac{x}{e^x-1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}.$$

Proof. As the Jordan decomposition is trivial in this case (the determinant of the quadratic form is 1) one sees that $m_p(f) = \mathrm{std}_p(f)$ for $p \neq 2$, and $m_2(f) = 2^{-n}\,\mathrm{std}_2(f)$. (For the situation in hand $n(I,I) = 0$ and $n(II) = n$.) Note that the factor $\zeta_D(n/2)$ equals 1 here, giving us the first equality. The second equality is due to the special values

$$\Gamma\left(k+\frac{1}{2}\right) = \frac{\sqrt{\pi}(2k)!}{4^k k!} \qquad \text{and} \qquad \zeta(2k) = (-1)^{k+1}\frac{B_{2k}(2\pi)^{2k}}{2(2k)!};$$

see [5] for more information. □

The mass formula for even unimodular positive definite quadratic forms is rather interesting in this case because of the following folklore theorem.

Theorem 7. *All the even unimodular lattices of a given rank forms a single genus. Thus we can define*

$$M(n) = \frac{B_{n/2}}{n}\prod_{j=1}^{n/2-1}\frac{B_{2j}}{4j}$$

to be the mass of the non-equivalent classes of even unimodular lattices of rank n.

Proof. See [9, Section 92]. □

We recall that the Bernoulli numbers are all rational, and $B_{2k+1} = 0$ for all positive integers k. Here are a few nonzero Bernoulli numbers:

$$B_0 = 1, \qquad B_1 = -\frac{1}{2}, \qquad B_2 = \frac{1}{6}, \qquad B_4 = -\frac{1}{30}, \qquad B_6 = \frac{1}{42}, \qquad B_{14} = -\frac{7}{6}, \qquad B_{22} = \frac{854513}{138}.$$

The Bernoulli numbers grows rapidly as $n \to \infty$. In fact, by the formula for $\zeta(2k)$ and Stirling's formula

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n,$$

together with the fact that $\zeta(n) \to 1$ as $n \to \infty$, one sees that

$$|B_{2k}| \sim 4\sqrt{\pi k}\left(\frac{k}{\pi e}\right)^{2k}.$$

Hence it should not be surprising that $M(n)$ grows rapidly as n increases.

Example 8. The root lattice of the exceptional lie group E_8 is an even unimodular lattice with automorphism group the Weyl group of E_8. This group has order

$$696729600 = 2^{14}\cdot 3^5\cdot 5^2\cdot 7,$$

which equals $M(8)^{-1}$. Hence there is a unique even unimodular lattice of rank 8 up to equivalence!

Example 9. In dimensions 16 and 24 there are 2 and 24 even unimodular lattices up to equivalence respectively (see [3] for the classification). The classification of even unimodular lattices is near impossible after this point though, since Siegel's mass formula grows rapidly as the dimension increases. For example, $M(32)$ is more than 40 million, so there are more than 80 million such lattices of rank 32!

3 Reinterpretation of the genus via the orthogonal group

In the third part of this note, K will always be a number field.

3.1 The class group

The orthogonal group over $\mathbb{Z}$ parametrizes the automorphisms of a quadratic form. We will see that we can use the class number of the same algebraic group to measure the size of the genus of a quadratic form.

Definition 10. Let G be a linear algebraic group (with a fixed embedding into GL_n for some n). Then its *class group* over K is defined to be

$$Cl(G) := G(\mathbb{A}_K^\infty) \setminus G(\mathbb{A}_K)/G(K),$$

where $\mathbb{A}_K$ is the ring of K-adeles, and $\mathbb{A}_K^\infty = \prod_{v\nmid\infty} \mathcal{O}_v \prod_{v|\infty} K_v$.

The definition above generalizes the classical notion of a class group with $G = \mathrm{GL}_1$; see [10, Chapter 8] for more information and examples. The class group of a linear algebraic group is always finite, but in general the class group of an arbitrary algebraic group is not always finite; see [4, Example 1.5]. We will need the following theorem in what follows.

Theorem 11. SL_n *satisfies absolute strong approximation, i.e.* $\mathrm{SL}_n(K)$ *is dense in* $\mathrm{SL}_n(\mathbb{A}_{K,f})$*, where* $\mathbb{A}_{K,f}$ *is the ring of finite adeles.*

Proof. See [10], where strong approximation is proved in much greater generality. □

The main purpose of this section is to understand the following statement.

Corollary 12. $\#Cl(\mathrm{SL}_n) = 1$.

Proof. In fact, we show that any linear algebraic group G satisfying absolute strong approximation has cardinality 1. Since G satisfies absolute strong approximation, $G(\mathbb{A}_{K,f})G_K$ is dense in $G(\mathbb{A}_K)$. Therefore the open set $G(\mathbb{A}_K^\infty)x$ intersects $G(\mathbb{A}_{K,f})G_K$ nontrivially for any $x \in G(\mathbb{A}_K)$, and consequently

$$G(\mathbb{A}_K) = G(\mathbb{A}_K^\infty)G(\mathbb{A}_{K,f})G_K = G(\mathbb{A}_K^\infty)G_K,$$

where the second equality is because $G(\mathbb{A}_{K,f}) \subset G(\mathbb{A}_K^\infty)$. This implies $G(\mathbb{A}_K)$ has exactly one double coset, so $\#Cl(G) = 1$. □

3.2 An enumeration of the classes

Let $G \subset \mathrm{GL}_n$ be a linear algebraic group acting on an affine m-dimensional variety X. If x and y lie in the same $G(\mathcal{O}_K)$-orbit of $X(\mathcal{O}_K)$, then they clearly lie in the same $G(K)$-orbit of $X(K)$, and $G(\mathcal{O}_v)$-orbit of $G(K_v)$, for all finite place v. A naive local-global problem we can ask if the following: does the converse always hold? As we have stated, one will expect that it usually does not hold, and consequently ask for a measurement of the failure of this local-global problem. Let us now generalize all the definitions in the first part of this note.

Definition 13. Let Let $G \subset \mathrm{GL}_n$ be a linear algebraic group acting on an affine m-dimensional variety X, and let $x \in X(\mathcal{O}_K)$.

- The *genus* $\mathrm{gen}(x)$ of x is the collection of all $y \in X(\mathcal{O}_K)$ such that $y = g_K x$ for some $g_K \in G(K)$, and $y = g_v x$ for some $g_v \in G(\mathcal{O}_v)$ for all finite places v.
- The *class* $\mathrm{cl}(x)$ of x is the $G(\mathcal{O}_K)$-orbit of x.
- If one writes
$$\mathrm{gen}(x) = \bigsqcup_{i\in I_x} \mathrm{cl}(f_x)$$
for some set of representatives f_x in the genus of x, then $f_G(x)$ is defined to be the cardinality of I_x.

Remark. Note that we have left out the infinite places, but this is perfectly kosher: two integral quadratic forms that are equivalent over $\mathbb{Q}$ are also equivalent over $\mathbb{R}$, and the Hasse and Minkowski local-global principle implies that two integral quadratic forms equivalent over $\mathbb{R}$ and $\mathbb{Z}_p$ are also equivalent over $\mathbb{Q}$.

Theorem 14. *Let $G_x = \{g \in G : gx = x\}$. Then $f_G(x)$ is the number of double cosets $G_x(\mathbb{A}_K^\infty)gG_x(K)$ of $G_x(\mathbb{A}_K)$ which are contained in $G(\mathbb{A}_K^\infty)G(K)$. In particular, $f_G(x)$ is finite.*

Proof sketch. Let $\mathfrak{d}$ be the quotient set obtained from $\mathrm{gen}(x)$ by identifying elements belonging to the same class. We will construct the bijection between $\mathfrak{d}$ and the set M of double cosets $G_x(\mathbb{A}_K^\infty)gG_x(K)$ of $G_x(\mathbb{A}_K)$ contained in $G(\mathbb{A}_K^\infty)G(K)$, and leave the verification to the reader (see [10, Theorem 8.2]). Let $\overline{g} = G_x(\mathbb{A}_K^\infty)gG_x(K) \in M$, and write $g = g_\infty g_K$ with $g_\infty \in G(\mathbb{A}_K^\infty)$ and $g_K \in G(K)$. Defining $y_g := g_K x$, the bijection $\theta : M \longrightarrow \mathfrak{d}$ is given by $\theta(\overline{g}) = y_g$. □

Recall that $c(f)$ is the number of classes in the genus of a quadratic form f.

Corollary 15. *If f is a nondegenerate integral quadratic form over $\mathcal{O}_K$, then $c(f) = \#Cl(O_f)$, where recall that*

$$O_f = \{g \in \mathrm{GL}_n : g^t A_f g = A_f\}.$$

Proof. Let $X \subset \mathbb{A}^{n^2}$ be the variety of $n \times n$ symmetric matrices, and consider the action of $G = \mathrm{GL}_n$ by $g(x) = g^t x g$. Clearly $G_f = O_f$. If we can show that $O_f(\mathbb{A}_K) \subset G(\mathbb{A}_K^\infty)G(K)$, then we are done by the theorem above.

For each finite place v, clearly $G(\mathcal{O}_v)$ contains a matrix with determinant -1, so any element $t \in O_f(\mathbb{A}_K)$ has $st \in \mathrm{SL}_n(\mathbb{A}_K)$ for a suitable element $s \in G(\mathbb{A}_K^\infty)$. But we know that $\#Cl(\mathrm{SL}_n(K)) = 1$ as SL_n satisfies absolute strong approximation, so $st = s_\infty s_K$ for some $s_\infty \in \mathrm{SL}_n(\mathbb{A}_K^\infty)$ and $s_K \in \mathrm{SL}_n(K)$. In particular,

$$t = s^{-1} s_\infty s_K \in G(\mathbb{A}_K^\infty)G(K),$$

as desired. □

3.3 A good parametrization of the classes

Until now we have largely avoided using the language of lattices except in dimensions dividing 8. We now briefly describe how to use this language to achieve an honest parametrization of the classes in a genus by means of the adelic special orthogonal group.

Theorem 16. *Let L be a lattice in $V = K^n$. If v is a finite place of K, write $L_v := L \otimes_{\mathcal{O}_K} \mathcal{O}_v$.*

(a) A lattice is uniquely determined by its localizations, i.e $L = \bigcap_{v \nmid \infty}(V \cap L_v)$.

(b) If M is another lattice, then $L_v = M_v$ for almost all finite v.

(c) For every v, let $N_v \subset V \otimes_K K_v$ be local lattices. If $N_v = L_v$ for almost all finite v, then there exists a unique lattice $M \subset V$ such that $M_v = N_v$ for all finite v.

Proof. See [10, Theorem 1.15]. □

Let $\mathcal{L}$ be the set of all lattices in K^n. Then the previous theorem defines an action of $\mathrm{GL}_n(\mathbb{A}_K)$ on $\mathcal{L}$ as follows. If $g = (g_v) \in \mathrm{GL}_n(\mathbb{A}_K)$ and $L \in \mathcal{L}$, then $g_v \in \mathrm{GL}_n(\mathcal{O}_v)$ and $L_v = \mathcal{O}_v^n$ for almost all finite places v, implying $g_v L_v = L_v$. One then defines gL to be the unique lattice M such that $M_v = g_v L_v$ for all finite places v.

Now, view a quadratic form in n variables as a map $\varphi\colon K^n \longrightarrow K$, and let

$$G^\varphi = \{g \in \mathrm{SO}_n : \varphi \circ g = \varphi\}$$

be the group of determinant one invertible linear maps preserving the quadratic form φ. If Λ is a lattice in K^n endowed with the map φ, we can still define its genus and class as in Definition 13 (using the action of the previous paragraph) by letting $G = G^\varphi$.

Proposition 17. *With notations as above, if $D_\Lambda \subset G^\varphi(\mathbb{A}_K)$ is the stabilizer subgroup of Λ under the action of $\mathrm{GL}_n(\mathbb{A}_K)$, then we can parametrize the classes of Λ in its genus by the double quotient*

$$G^\varphi(K) \setminus G^\varphi(\mathbb{A}_K)/D_\Lambda.$$

Proof. The correspondence between $G^\varphi(K) \setminus G^\varphi(\mathbb{A}_K)/D_\Lambda$ and the classes of Λ is given by $g \longmapsto g\Lambda$, and one easily sees that this is a bijection. □

The above proposition is the starting point towards a proof of Siegel's mass formula for lattices via adelic integration on algebraic groups (see [7]).

References

[1] John William Scott Cassels and Albrecht Fröhlich. *Algebraic Number Theory*. Thompson Book Company Inc., 1967.

[2] John H. Conway and Neil J. A. Sloane. Low-Dimensional Lattices IV: The Mass Formula. *Proc. R. Soc. Lond. A* (1988), **419**: 259–286.

[3] John H. Conway and Neil J. A. Sloane. Sphere Packings, Lattices, and Groups. *Springer-Verlag*, 1998.

[4] Brian Conrad. Notes on finiteness of class numbers for algebraic groups.

[5] Harold Davenport. Multiplicative Number Theory. *Springer-Verlag*, 1967.

[6] Wolfgang Ebeling. Lattices and Codes: A Course Partially Based on Lectures by Friedrich Hirzebruch. *Springer Spektrum*, 2012.

[7] Jonathan Hanke. An exact mass formula for quadratic forms over number fields. J. Reine Angew. Math. 584 (2005), 1–27.

[8] Jonathan Hanke. Notes on "Quadratic Forms and Automorphic Forms" from the 2009 Arizona Winter School.

[9] Timothy O'Meara. Introduction to Quadratic Forms. Springer, 1973.

[10] Vladimir Platonov and Andrei Rapinchuk. Algebraic groups and number theory. *Academic Press*, 1993.

Unimportant Remarks. Let us now list some fun comments.

- The Hasse and Minkowski local-global principle for rational quadratic forms can be compared to Liouville's theorem in the following sense. If one asks for an example of Liouville's theorem, the number 7 is sufficient.
- In my opinion, there are a lot of surprising results in the theory of integral quadratic forms. We have talked about Siegel's mass formula and the fact that even unimodular lattices have dimension divisible by 8. Some other ones are the 15-290 Theorems, and higher composition laws via Bhargava's cube.
- The growth of Siegel's mass formula is nothing compared to that of the *Goodstein sequences* $G(n)$. For example, $G(3) = 6$ due to the following computations:

$$\begin{aligned} 3 &= 1 \cdot 2^1 + 1 \cdot 2^0, \\ (1 \cdot 3^1 + 1 \cdot 3^0) - 1 &= 1 \cdot 3^1, \\ (1 \cdot 4^1) - 1 &= 3 \cdot 4^0, \\ (3 \cdot 5^0) - 1 &= 2 \cdot 5^0, \\ (2 \cdot 6^0) - 1 &= 1 \cdot 6^0, \\ (1 \cdot 7^0) - 1 &= 0. \end{aligned}$$

  However $G(4) = 3 \cdot 2^{402653211} - 2$.