Quadratic Forms

October 13, 2025

These notes are based on a course of the same title given by Professor Jack Thorne at Cambridge during Lent Term 2025. They have been written up by Alexander Shashkov. I have added details to certain proofs which we did not cover in full, and made a few off-hand remarks. As a result, there are likely plenty of errors, which are my own.

Contents

1 Introduction

Let k be a field of characteristic not equal to 2. We can develop the theory of quadratic forms in quadratic 2, but it is a bit more tricky.

Definition 1.1. A *quadratic form* is a polynomial $f(\mathbf{x}) = f(x_1, \ldots, x_n) = \sum_{1 \leq i,j \leq n} A_{ij} x_i x_j$, where $A_f = (A_{ij}) \in M_{n \times n}(k)$ is a symmetric matrix.

Example 1.2. If $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$, then the associated quadratic form f is $ax_1^2 + 2bx_1x_2 + cx_2^2$. From this we can see why characteristic 2 might be a bit weird, as in characteristic 2 we have that $2b = 0$.

Definition 1.3. A quadratic form f is *regular* is $\det(A_f) \neq 0$.

1.1 Classical motivation

The classical motivation for studying quadratic forms is that they give the first examples of interesting nonlinear Diophantine equations.

Example 1.4. If $A = I_n$, then $f = x_1^2 + \cdots + x_n^2$.

A classical question is to characterize $f(\mathbb{Z}^n)$. If $n \geq 4$, then the image is all of $\mathbb{Z}$, otherwise there are some interesting things going on.

Another motivation is that from geometry, as quadratic forms define projective varieties.

Example 1.5. Let f be a regular quadratic form with associated matrix $A_f \in M_{n \times n}(k)$. Define $X_f \subseteq \mathbb{P}^{n-1}$ to be the vanishing locus of f. As $\det(A_f) \neq 0$ and the characteristic is not 2, X_f is a nonsingular variety.

An important question is to decide whether $X_f(k) \neq \emptyset$. This is especially interesting when k is an arithmetically interesting field, for example $k = \mathbb{Q}$ or k is a number field. The Hasse-Minkowski theorem gives an answer to this question.

Definition 1.6. Let k be a number field, and let M_k to be the set of places of k, equivalence classes of non-trivial valuations on k.

Theorem 1.7 (Hasse-Minkowski)**.** *$X_f(k) \neq \emptyset$ if and only if $X_f(k_v) \neq 0$ for all $v \in M_k$.*

This is useful because working over a local field is very nice, as we can do analysis (e.g Hensel's lemma). Suppose our form has at least 3 variables (in 1 or two variables the question is easy). Then $X_f(k_v) \neq 0$ for all but finitely many places. For the places for which this does not hold trivially, we can use Hensel's lemma to reduce the question to working over a finite ring.

Corollary 1.8. *There's an easy algorithm to decide if $X_f(k) \neq \emptyset$.*

This is a very nice property of quadratic forms.

1.2 Modern motivation

We want to study the symmetries of quadratic forms.

Definition 1.9. A *quadratic space* over k is a pair (V, ψ) where V is a finite-dimensional vector space over k and $\psi : V \times V \to k$ is a symmetric bilinear form on V.

If we fix a basis $b = \{e_1, \ldots, e_n\}$ on V, then ψ has Gram matrix $[\psi]_B = (\psi(e_i, e_j))_{ij} \in M_{n\times n}(k)$ symmetric. We define $f(\mathbf{x}) = \psi(\sum x_i e_i, \sum x_i e_i)$ to be the quadratic form with $A_f = [\psi]_B$. We sometimes write $\psi(v, v) = \psi(v)$.

A quadratic space is *regular* if $\det[\psi]_B \neq 0$. Equivalently, ψ defines an isomorphism $V \cong V^*$.

Definition 1.10. Let (V, ψ) be a regular quadratic space over K. Then we define

$$\mathrm{O}(V) = \{g \in \mathrm{GL}(V) | \psi(gv, gw) = \psi(v, w) \forall v, w \in V\} \tag{1.1}$$

$$\mathrm{SO}(V) = \{g \in \mathrm{O}(V) | \det g = 1\} \tag{1.2}$$

These are abstract groups, but they are also k-points of linear algebraic groups over k. Recall that a linear algebraic group over k is an affine group variety defined over k, or equivalently, a closed subgroup scheme of GL_V, where V is a finite dimensional k-vector space. Thus we can write

$$\mathrm{O}_V = \{g \in \mathrm{GL}_V \mid \forall v, w \in V,\ \psi(gv, gw) = \psi(v, w)\}. \tag{1.3}$$

Even more abstractly we can say that O_V is the group scheme over k representing the functor

$$\begin{aligned} &k-\mathsf{alg} \to \mathsf{grp} \\ &\quad R \mapsto \mathrm{O}_V(R) = \{g \in \mathrm{Aut}_R(V \otimes_k R) \mid \forall v, w \in V \otimes_k R,\ \psi(gv, gw) = \psi(v, w)\} \end{aligned} \tag{1.4}$$

We won't need this definition or any complicated algebraic geometry, but it is very nice as it allows us to define $\mathrm{O}_V(R)$ for arbitrary k-algebras.

We can similarly define SO_V.

If k is a local field and V is anisotropic, then $\mathrm{O}(V)$ is compact.

1.3 What can we do?

Group action. One thing we can do is study the action of SO_V on $X_V \subseteq \mathbb{P}(V)$. This is a homogeneous space, which is a space with a transitive group action in the sense of algebraic groups. For our cases, what this means is that the group action is transitive over $\overline{k}$ algebraically closed.

This puts us in the typical setting of arithmetic geometry, where we first pass to the algebraic closure, which allows us to forget all the arithmetic of the field and just do geometry, and then descend back to our base field.

In order to prove the Hasse-Minkowski theorem, we use class field theory and this transitive group action.

Representation theory. Another thing we can do is study the representation theory of the group $\mathrm{O}(V)$ and see if that tells us anything about the quadratic space. Let $f(x) = x^{2g+1} + c_1 x^{2g} + \cdots + c_{2g+1} \in k[x]$ be a monic separable polynomial, and let $C_f^0 : y^2 = f(x)$ be the associated smooth curve over k, and let C_f be the unique smooth projective completion. This is a hyperelliptic curve of genus g.

From the point of view of algebraic geometry, hyperelliptic curves are in some sense the "simplest" curves of genus g. The arithmetic of hyperelliptic curves is of interest, and they are connected to quadratic forms.

Let $J_f = \operatorname{Pic}^0 C_f$ be the Jacobian variety, which is an abelian of dimension g equipped with a natural embedding $C_f \hookrightarrow J_f$. Then there's an embedding

$$J_f(k)/2J_f(k) \hookrightarrow (V \otimes_k V)/\operatorname{SO}(V) \tag{1.5}$$

Here V is the "simplest possible quadratic space of dimension $2g+1$ and $d(V) \equiv (-1)^g$". This is given by the matrix with 1s on the anti-diagonal and zeros elsewhere. The tricky piece is that $J_f(k)/2J_f(k)$ naturally embeds into $(W \otimes_k W)/\operatorname{SO}(W)$, where $W = H^0(X, \mathcal{O}_X(D))$ is the global sections of some line bundle, and we need to show that V is naturally isomorphic to W. We also need to shows that we can upgrade the embedding (1.5) into an embedding into $V_{\mathbb{Z}} \otimes V_{\mathbb{Z}}/\operatorname{SO}(V_{\mathbb{Z}})$.

The group $J_f(k)/2J_f(k)$ is very nice and appears in other instances, for instance the proof of the weak Mordell-Weil theorem (cf. elliptic curves). We won't discuss how this embedding comes up, but here are some nice applications.

1. Bhargava-Gross used this embedding to calculate the average size of the 2-Selmer group.
2. Poonen-Stoll showed that when $k = \mathbb{Q}$, then 0% of the hyperelliptic curves as defined above have $C_f^0(\mathbb{Q}) \neq \emptyset$ as $g \to \infty$.
3. Bhargava-Shankar-Wang computed the density of polynomials $f(x) \in \mathbb{Z}[x]$ monic of degree $2g+1$ such that $\operatorname{disc}(f)$ is squarefree. This result was very surprising as it had previously only been done by assuming that abc-conjecture.

Automorphic forms. Groups like SO_V carry interesting automorphic forms, which are roughly speaking functions on $\operatorname{SO}_V(\mathbb{A}_k)/\operatorname{SO}_V(k)$. Recall (we will define all this in more detail later) that

$$\mathbb{A}_k \prod_{v \in M_k}{}' k_v \tag{1.6}$$

$\operatorname{SO}_V(\mathbb{A}_k)$ is a huge locally compact group, and k embeds diagonally in $\mathbb{A}_k$ so $\operatorname{SO}_V(k)$ maps into $\operatorname{SO}_V(\mathbb{A}_k)$ by functoriality, and in fact this map is an embedding. Thus we can define the quotient space.

Automorphic forms are very interesting for a lot of reasons. For instance, they participate in the θ-correspondence, which relates automorphic forms on different groups. This is a generalization of the classical theory of modular forms and their connection with quadratic forms.

One application is the Smith-Minkowski-Siegel mass formula, which uses the θ-correspondence.

Shimura varieties. For certain quadratic spaces $V/\mathbb{Q}$, the group SO_V can be used to construct a Shimura variety (or even a family of Shimura varieties). These are algebraic varieties over number fields with lots of symmetries which play a very important role in the Langlands correspondence.

A major area of research is developing an "arithmetic" θ-correspondence and "arithmetic" Siegel-Weil formula. Shimura varieties are essential in this.

These Shimura varieties (for appropriate choices of V) can be interpreted as moduli spaces of polarized K3 surfaces. This has been used to complete the proof of the Tate conjecture over finite fields for K3 surfaces. The Tate conjecture is one of the most important conjectures about the cohomology of algebraic varieties. It is as important, and as difficult as the Hodge conjecture, so its solution is a very big deal.

1.4 Goals for this course

We won't get into any of the above applications. We'll instead study the fundamentals of quadratic forms and their classification over number fields. Having a firm grasp on these basic topics will allow one to define Shimura varieties, automorphic forms, and understand the embedding (1.5).

We will also study aspects of the integral theory, over $\mathbb{Z}$ or O_K the ring of integers of a number field. This includes things like genus, Spin groups, spinor genus, and strong approximation.

2 Quadratic forms over a field

Let k be a field of characteristic not equal to 2.

2.1 Basics

Definition 2.1. Two quadratic forms f, g are *equivalent* if there exists $P \in \mathrm{GL}_n(k)$ such that $A_g = P^t A_f P$. This is the same as f and g being related by a linear change of variables given by P. We write $f \sim g$ or $f \sim_k g$ if we want to emphasize the isomorphism is defined over k.

If $a \in k$, we say that f *represents* a if there exists $v \in k^n \setminus \{0\}$ such that $f(v) = a$.

If f represents 0, we say that f is *isotropic*. Otherwise we say that f is anisotropic.

Definition 2.2. A *morphism* of quadratic spaces $\alpha : (V, \psi) \to (V', \psi')$ is a linear map $\alpha : V \to V'$ such that for all $v, w \in V$, $\psi'(\alpha(v), \alpha(w)) = \psi(v, w)$.

We say that V, V' are *equivalent* and write $V \sim V'$ if they are isomorphic.

If $a \in k$, we say that V *represents* a if there exists $v \in V \setminus \{0\}$ such that $\psi(v, v) = a$. V is *isotropic* if it represents 0. Otherwise we say that V is anisotropic.

We can pass between quadratic spaces and quadratic forms.

Recall that if we fix a basis $B = \{e_1, \dots, e_n\}$ for V, so an isomorphism $V \cong k^n$, then $f(\mathbf{x}) = \psi(\sum x_i e_i, \sum x_i e_i)$ is a quadratic form with matrix $A_f = [\psi]_B$. To go the other way, we have the polarisation identity

$$\begin{aligned} \psi(v, w) &= \frac{1}{2}(\psi(v + w, v + w) - \psi(v, v) - \psi(w, w)) \\ &= \frac{1}{2}(f(\mathbf{x} + \mathbf{y}) - f(\mathbf{x}) - f(\mathbf{y})) \end{aligned} \tag{2.1}$$

From this it is clear that characteristic 2 might cause us some problems, as we can pass from quadratic spaces to quadratic forms, but we cannot go the other way as we cannot divide by 2.

Now, recall that a quadratic form f is regular if $\det A_f \neq 0$, and a quadratic space (V, ψ) is regular if $\det[\psi]_B \neq 0$. We define the determinant

$$d(V) = \det[\psi]_B \mod (k^\times)^2 \in k^\times/(k^\times)^2. \tag{2.2}$$

So V is regular if and only if $d(V) \neq 0$. If $V \sim V'$, then $d(V) \equiv d(V')$ (we sometimes write $\equiv$ instead of $=$ to emphasize that the equivalence is over $k \times /(k^\times)^2$.

Next we will discuss subspaces. The fact that subspaces of quadratic spaces are very nice is one of the reasons the coordinate-free point of view is so useful.

Definition 2.3. Let (V, ψ) be a quadratic space, and $W \subseteq V$ a k-linear subspace. Then $(W, \psi|_{W \times W}$

1. We say that $W \subseteq V$ is regular if it is regular as a quadratic space.

2. The orthogonal complement of W is

$$W^\perp = \{v \in V \mid \forall w \in W,\ \psi(v,w) = 0\} \tag{2.3}$$

3. If $W' \subseteq V$ is another subsapce, we say that W, W' are orthogonal if $W \subseteq (W')^\perp$, if and only if $W' \subseteq W^\perp$, if and only if $\psi(W, W') = 0$.

Definition 2.4. If $(V,\psi),\ (V',\psi')$ are quadratic spaces, then $V \oplus V' = (V \oplus V', \psi \oplus \psi')$ denotes the orthogonal direct sum. $\psi \oplus \psi'$ is the unique quadratic form which makes the natural projection maps $V \oplus V' \to V$ and $V \oplus V' \to V'$ morphisms of quadratic spaces.

Lemma 2.5. *Let V be a regular quadratic space, and $W \subseteq V$ a regular subspace. Then $V = W \oplus W^\perp$.*

Proof. First, we can use that fact that W is regular to check that $W \cap W^\perp = 0$.

Next we can check that $V = W + W^\perp$. If $v \in V$, then $\psi(v,\cdot)|_W \in W^*$. Thus as W is regular, there exists $w \in W$ such that $\psi(v,w') = \psi(w,w')$ for all $w' \in W$. Then $v - w \in W^\perp$. □

Definition 2.6. If $A \in M_{n\times n}(k)$ is symmetric, then $\langle A\rangle = (k^n, v^t A w)$ is the quadratic space associated with A (so $\psi(v,w) = v^t A w$).

In particular, if $n = 1$, then $A = a \in k$, and $\langle a\rangle = (k, vaw)$.

Corollary 2.7. *If V is regular quadratic space, then there exists $a_1, \dots, a_n \in k^\times$ such that $V \sim \langle a_1\rangle \oplus \cdots \oplus \langle a_n\rangle$.*

What this corollary says is that there is a basis for V such that the associated Gram matrix is diagonal. The associated quadratic form is then $f(\mathbf{x}) = a_1x_1^2 + \cdots + a_nx_n^2$.

Proof. Induction on n. The base case $n = 1$ is done as the matrix is already diagonal.

Now for the inductive step. Since V is regular, there exists $v \in V$ such that $\psi(v,v) \neq 0$. Then $kv \subseteq V$ is a one-dimensional regular subspace, so $V = (kv) \oplus (kv)^\perp$. Then $(kv)^\perp$ is $(n-1)$-dimensional, so we are done by the induction hypothesis. □

We are going to define some invariants associated with quadratic forms which are quite simple. But it's going to be the case that these invariants these invariants completely determine quadratic forms of rank at most 3. However, if k is a field of low cohomological dimension such as a number field or a local field, then these invariants characterize quadratic forms of all rank, which allows us to prove the Hasse-Minkowski theorem.

The following lemma is the first example of the above behavior.

Lemma 2.8. *Let V be a regular quadratic space of dimension 2. The following are equivalent:*

(i) $d(V) \equiv -1$.

(ii) *V is isotropic.*

(iii) $V \sim \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$.

Proof. (iii) $\to$ (ii): If $V = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$, then $\psi(e_1, e_1) = 0$, so we are done.

(ii) $\to$ (iii): Let $v \in V \setminus \{0\}$ be such that $\psi(v, v) = 0$. Then V is regular, so there exists $v \in V$ such that $\psi(v, w) \neq 0$, and we can rescale so that $\psi(v, w) = 1$. Then $\{v, w\}$ is a basis. Also, $\psi(v, w + \lambda v) = 1$ and $\psi(w + \lambda v, w + \lambda v) = \psi(w, w) + 2\lambda$ so we can replace w by $w + \lambda v$ without changing the property that $\psi(v, w) = 1$. So after replacing w by $w - \frac{1}{2}\psi(w, w)v$, we can assume that $\psi(w, w) = 0$, so $[\psi]_{\{v,w\}} = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$

(iii) $\to$ (i): $\det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -1$.

(i) $\to$ (ii): $V \sim \langle a_1 \rangle \oplus \langle a_2 \rangle$ for some $a_1, a_2 \in k$. Then $d(V) = a_1 a_2 \equiv -1$ by assumption, so $a_2 \equiv -a_1 \mod (k^\times)^2$. Taking change of variables matrix $P = \begin{pmatrix} 1 & 0 \\ 0 & a_1 \end{pmatrix}$ gives that $\langle a_1 \rangle \oplus \langle a_2 \rangle \sim \langle a_1 \rangle \oplus \langle -a_1 \rangle$. But the associated quadratic form is then $a_1 x_1^2 - a_1 x_2^2$, so $(1, 1) \in \langle a_1 \rangle \oplus \langle -a_1 \rangle$ is an isotropic vector, so V is isotropic. □

Definition 2.9. Let $H = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$ be the two-dimensional quadratic space define above. H is the *hyperbolic plane*. The previous lemma shows that H is the unique regular isotropic quadratic space of rank 2, and the unique regular quadratic space with $d(V) \equiv -1$. The quadratic form associated with H is $f(\mathbf{x}) = 2x_1 x_2$, so H represents every element of k.

The next lemma is very useful, as it shows that any isotropic quadratic space contains a copy of H.

Lemma 2.10. *Let V be a regular quadratic space. The following are equivalent:*

(i) V is isotropic.

(ii) There's an isomorphism $V = H \oplus V'$ for some subspace $V' \subseteq V$.

Proof. (ii) $\to$ (i) is immediate as H is isotropic.

(i) $\to$ (ii): We can find $v \in V \setminus \{0\}$ such that $\psi(v, v) = 0$. As before, we can find $w \in V$ such that $\psi(v, w) = 1$ and $\psi(w, w) = 0$. Then v, w are linearly independent and $\langle v, w \rangle \subseteq V$ is a regular quadratic space congruent to H. Then $V \sim H \oplus H^\perp$. □

Corollary 2.11. *Let (V, ψ) be a regular quadratic space and $a \in k^\times$. The following are equivalent:*

(i) V represents a.

(ii) $V \oplus \langle -a \rangle$ is isotropic.

Proof. (i) $\to$ (ii): If $\psi(v, v) = a$, then $(v, 1) \in V \oplus \langle -a \rangle$ is isotropic.

(ii) $\to$ (i): As $V \oplus \langle -a \rangle$ is isotropic, we can find $v \in V$, $\lambda \in k^\times$ not both zero such that $\psi(v, v) - \lambda^2 a = 0$ (recall the definition of a quadratic form on the direct sum).

If $\lambda \neq 0$, then $\psi(\lambda^{-1} v, \lambda^{-1} v) = a$, so ψ represents a

If $\lambda = 0$, then there exists $v \in V \setminus \{0\}$ such that $\psi(v, v) = 0$, so V is isotropic. Thus $V = H \oplus V'$ by Lemma 2.10. H represents every element of k (see Definition 2.9), so we are done. □

Let (V, ψ) be a regular quadratic space with matrix A_ψ. Recall the definition of the groups $\mathrm{O}(V)$ and $\mathrm{SO}(V)$. If $g \in \mathrm{O}(V)$, then $g^t A_\psi g = A_\psi$, so $\det(g)^2 = 1$, so $\det(g) = \pm 1$.

Now, if $\psi(v, v)$ $ne0$, then $V = (kv) \oplus (kv)^\perp$. There exists a unique $\tau_V : V \to V$ preserving this decomposition, such that $\tau_v(v) = -v$, and $\tau_v|_{(kv)^\perp} = \mathrm{id}_V|_{(kv)^\perp}$. This preserves ψ as $\psi(\tau_v(v), \tau_v(v)) = \psi(-v, -v) = \psi(v, v)$ and τ_v is the identity on $(kv)^\perp$. Also, $\det \tau_v = -1$, so $\tau_v \in \mathrm{O}(V) \setminus \{\mathrm{SO}\}(V)$. We call τ_v a *simple reflection.*

Lemma 2.12. *Suppose $v, w \in V$, $\psi(v) = \psi(w) \neq 0$, and $\psi(v - w) \neq 0$. Then $\tau_{v-w}(v) = w$.*

Proof. In general, we have that if $x \in V$ and $\psi(x) \neq 0$, then we have the reflection formula

$$\tau_x(y) = y - \frac{2\psi(x, y)}{\psi(x, x)} \cdot x. \tag{2.4}$$

We have that $\psi(v - w) = \psi(v) - 2\psi(v, w) + \psi(w) = 2\psi(v) - 2\psi(v, w) = 2\psi(v, v - w)$, so putting $x = v - w$ and $y = v$ in the above formula gives $\tau_{v-w}(v) = w$ as desired. □

Proposition 2.13. *Let V be a regular quadratic space of dimension $n \geq 1$.*

1. *Suppose $n \geq 2$. If $v, w \in V$ and $\psi(v) = \psi(w) \neq 0$, then there exist simple reflections $\tau, \tau' \in \mathrm{O}(V)$ such that $\tau\tau'(v) = w$. In particular, if $a \in k^\times$, then $\mathrm{SO}(V)$ acts transitively on $\{v \in V \mid \psi(v) = a\}$.*

2. *$\mathrm{O}(V)$ is generated by simple reflections.*

Proof.

1. We have that $\psi(v + w) + \psi(v - w) = 2\psi(v) + 2\psi(w) \neq 0$ so either $\psi(v + w)$ or $\psi(v - w)$ is nonzero.

First suppose $\psi(v - w) \neq 0$. Then $\tau_{v-w}(v) = w$. We have that $V = kw \oplus (kw)^\perp$, and we can choose $u \in (kw)^\perp$ such that $\psi(u) \neq 0$. Then $\tau_u(w) = w$ so $\tau_u \tau_{v-w}(v) = w$.

Next suppose that $\psi(v + w) \neq 0>$ Then $\tau_{v+w}(v) = -w$, $\tau_w(w) = -w$, so $\tau_w \tau_{v+w}(v) = w$ so we are done.

2. If $n = 1$, then $\mathrm{O}(V) = \{\pm 1\}$ so we are done. If $n > 1$, we argue by induction. Choose $g \in \mathrm{O}(V)$ and $v \in V$ such that $\psi(v) \neq 0$. Then $\psi(v) = \psi(gv)$, so by part 1 there exists $\tau, \tau' \in \mathrm{O}(V)$ such that $\tau\tau' v = gv$, so $\tau'\tau g v = v$. Then $\tau'\tau g \in \mathrm{O}(V)$. We have the direct sum decomposition $V = (kv) \oplus (kv)^\perp$. Since $\tau'\tau g \in \mathrm{O}(V)$ and $\tau'\tau g v = v$, we have that $\tau'\tau g$ preserves the direct sum decomposition. Thus $(\tau'\tau g)|_{(kv)^\perp} \in \mathrm{O}((kv)^\perp)$.

By induction, there exists $w_1, \ldots, w_r \in (kv)^\perp$ such that $(\tau'\tau g)|_{(kv)^\perp} = \tau_{w_1} \cdots \tau_{w_r}$. Then we can consider τ_{w_i} as an element of $\mathrm{O}(V)$ which preserves the decomposition $V = (kv) \oplus (kv)^\perp$ and fixes v. So $\tau'\tau g = \tau_{w_1} \cdots \tau_{w_r}$ as elements of $\mathrm{O}(V)$, so g is the product of simple reflections.

□

Theorem 2.14 (Witt's lemma)**.** *Let V be a regular quadratic space. Let $W_1, W_2 \subseteq V$ be regular subspaces. Let $\alpha : W_1 \to W_2$ be an isomorphism of quadratic spaces. Then there exists $g \in \mathrm{O}(V)$ such that $g|_{W_1} = \alpha$.*

The above theorem tells us that the orthogonal group acts transitively on isomorphic subspaces. The first part of the previous proposition told us that the orthogonal group acts transitively on vectors of the same nonzero length (one-dimensional regular subspaces), this is a generalization of that.

Proof. We argue by induction on $n = \dim W_1$. If $n = 1$, then $w_1 = kv$, $\psi(v) \neq 0$, and $W_2 = k\alpha(v)$, and $\psi(v) = \psi(\alpha(v))$ as α is an isomorphism of quadratic spaces. By the proposition, there exists $g \in \mathrm{SO}(V)$ such that $g(v) = \alpha(v)$, so we are done.

If $n > 1$, choose a decomposition $W_1 = U \oplus U'$, where $\dim U, \dim U' \geq 1$. Consider $\alpha|_U : U \to \alpha(U)$. By induction, we can find $\beta \in \mathrm{O}(V)$ such that $\beta|_U = \alpha|_U$.

We now consider $\beta^{-1} \circ \alpha : W_1 \to V$. We have that $(\beta^{-1} \circ \alpha)|_U = \mathrm{id}\,|_U$. Therefore $\beta^{-1} \circ \alpha$ sends $U' = (U^\perp \cap W_1) \to U^\perp \subseteq V$ as $\beta^{-1} \circ \alpha$ preserves ψ.

By the induction hypothesis applied to $U' \subseteq U^\perp$, and $(\beta^{-1} \circ \alpha)|_{U'}$, we can find $\beta' \in \mathrm{O}(U^\perp)$ such that $\beta' = \beta^{-1} \circ \alpha|_{U'}$. We extend β' to an element of $\mathrm{O}(V)$ in the unique way such that β' preserves the decomposition $V = U \oplus U^\perp$ and $\beta'|_U = \mathrm{id}_U$ (in matrix form this looks like a block diagonal with β' in the first block and the identity in the second block).

Thus we have that $\beta^{-1} \circ \alpha|_U = \mathrm{id}_U$ and $\beta^{-1} \circ \alpha|_{U^\perp} = \beta'|_{U^\perp}$. Then $\beta \circ \beta' \in \mathrm{O}(V)$, and $\beta\beta'|_U = \alpha|_U$. Also, as $\beta' = (\beta^{-1} \circ \alpha)|_{U'}$ and $U' = U^\perp \cap W_1$, we have that

$$\beta\beta'|_{U'} = \beta\beta^{-1}\alpha|_{U'}\alpha|_{U'}. \tag{2.5}$$

As $W_1 = U \oplus U_1$, we have that $\beta\beta'|_{W_1} = \alpha|_{W_1}$ as desired. □

Corollary 2.15 (Witt's cancellation theorem)**.** *If V, V', V'' are regular quadratic spaces and $V \oplus V'' \sim V' \oplus V''$, then $V \sim V'$.*

Proof. Let $V \oplus V'' \sim V' \oplus V'' \sim W$. Let W_1, W_2 denote the images of the two copies of V'' in W for $V \oplus V''$ and $V' \oplus V''$, respectively. Then there is an isomorphism $\alpha : W_1 \to W_2$, so by Witt's lemma there is $g \in \mathrm{O}(V)$ such that $g|_{W_1} = \alpha$. Then $g|_V : V \to W$ has image V', so $V \sim V'$.

This is confusing but the point is you have an isomorphism between the two copies of V'', which extends to an isomorphism of the entire quadratic space by Witt's lemma, and this isomorphism restricts to an isomorphism from $V \to V'$. □

Recall the definition of the hyperbolic plane Definition 2.9.

Corollary 2.16. *If V is a regular quadratic space, then there exists an anisotropic quadratic space V' and an $r \geq 0$ such that $V \sim V' \oplus H^r$. Moreover, the isomorphism class of V' and the integer r are determined uniquely by V.*

Proof. Such a decomposition exists because if V is isotropic then $V \sim V' \oplus H$, and we can keep splitting off copies of H until we get something anisotropic.

If $V' \oplus H^r \sim V'' \oplus H^s$ are two different decompositions, then WLOG $r \geq s$. Then $V' \oplus H^{r-s} \sim V''$ by Corollary 2.15, so $r = s$ because V'' is anisotropic, so $V' \sim V''$. □

Definition 2.17. The *Witt group* of k, denoted $W(k)$, is the we set of equivalence classes $[V]$ of regular quadratic spaces over k, where $[V] = [V']$ if and only if there exists $r, s \geq 0$ such that $V \oplus H^r \sim V' \oplus H^s$.

The group operation is defined by $[V] + [V'] = [V \oplus V']$. We have that $-[V] = [\langle -1 \rangle \otimes_k V]$. To see this, let $e_1, \ldots, e_n$ be a basis for V, and $1 \otimes e_1, \ldots, 1 \otimes e_n$ be a basis for $\langle -1 \rangle \otimes_k V$. Then the span of $e_i, 1 \otimes e_i$ is two dimensional and isotropic, hence isomorphic to H, so $[V] - [V] = [H^n] = [0]$.

- The Witt group is functorial in k : if K/k is a field extension then there is a morphism

$$\begin{aligned} W(k) &\to W(K) \\ [V] &\mapsto [V \otimes_k K] \end{aligned} \tag{2.6}$$

- We can additionally endow the Witt group with a ring structure using the tensor product.
- By Corollary 2.16, there is a unique anisotropic representative of each equivalence class $[V] \in W(k)$. Thus describing the elements of the Witt group is the same as classifying the quadratic forms over k, and this is a decent approach.

However, the Witt group is not well-suited to proving the Hasse-Minkowski theorem, as it is hard to apply class field theory. Instead, we use the Clifford invariant, defined in the next section.

2.2 Clifford Algebra

We first make precise the notion of a k-algebra.

Definition 2.18. A k-algebra A is a k-vector space $(A, +, 0_A)$ together with a k-bilinear form $x : A \times A \to A$ and $1_A \in A$ such that for all $a \in A$ $1_A \times a = a \times 1_A = a$ and for all $a, b, c \in A$, $a \times (b \times c) = (a \times b) \times c$.

We do not assume that algebras are commutative!

Example 2.19. $M_n(k)$ is a k-algebra for any $n \geq 1$. It is a finite k-algebra, as $\dim_k A < \infty$.

Example 2.20. If $X_1, \ldots, X_n$ are symbols, the free k-algebra $k\{X_1, \ldots, X_n\}$ has k-basis the set of all monomials $\{X_{i_1} \cdots X_{i_m}\}$. Since we do not assume commutativity we have that $X_i X_j \neq X_j X_i$ for $i \neq j$. This k-algebra is not finite.

We can also define the free k-algebra without using coordinates, using the tensor algebra

Definition 2.21. Let V be a k-vector space. The *tensor algebra* is

$$T(V) = \bigoplus_{m \geq 0} V^{\otimes m} \tag{2.7}$$

with multiplication given by concatenation of tensors. If $x_1, \ldots, x_n$ is a k-basis of V, then $T(V) \cong k\{x_1, \ldots, x_n\}$.

$T(V)$ has the following universal property: if A is a k-alg, then there is a canonical isomorphism

$$\mathrm{Hom}_{k-\mathsf{alg}}(T(V), A) \cong \mathrm{Hom}(V, A) \tag{2.8}$$

Remark 2.22 (Ignore)**.** $T(V)$ is a representation (?) of the adjunct of the forgetful functor from k-algebras to k-vector spaces.

Definition 2.23. A *2-sided ideal* $I \subseteq A$ is a k-linear subspace such that for all $a \in A$, $aI \subset I$ and $Ia \subset I$.

If $I \subseteq A$ is two sided, then A/I can be given the structure of a k-algebra.

Definition 2.24. If A has no proper 2-sided ideals, then A is simple.

Example 2.25. $M_n(k)$ is a simple k-algebra

Definition 2.26. Let $a, b \in k^\times$. Then a *quaternion algebra* over k is a k-algebra of the form

$$(a, b)_k = k\{i, j\}/\langle i^2 - a, j^2 - b, ij + ji \rangle. \tag{2.9}$$

Lemma 2.27.

1. *$(a,b)_k$ is a simple k-algebra with basis $\{1,i,j,k=ij\}$.*
2. *$(a^2,-a^2)_k \cong M_2(k)$.*

Remark 2.28.

1. It is unfortunate that we use the symbol k for a standard basis element of quaternion algebras and for our base field.
2. $(-1,-1)_{\mathbb{R}} = \mathbb{H}$ is the algebra of Hamiltonian quaternions.
3. Class field theory gives a classification of quaternion algebras over K a number field.

Proof. $1,i,j,ij$ span $(a,b)_k$ as a k-vector space, so $(a,b)_k$ has dimension at most 4.

2. Let $A = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}$ and $B = \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix}$. Then $A^2 = a^2 I$, $B^2 = -a^2 I$, $AB = \begin{pmatrix} 0 & a^2 \\ a^2 & 0 \end{pmatrix}$ and $BA = -AB$. Thus $i \mapsto A$ and $j \mapsto B$ gives a map $\langle i,j\rangle \to M_2(k)$. By the universal property of tensor algebras, this extends to a map $\tilde{\varphi} k\{i,j\} \to M_2(k)$ which is in fact surjective (as A^2, A, B, AB form a basis for $M_2(k)$). Now, as $A^2 = a^2 I$ and $B^2 = -a^2 I$ and $AB = -BA$, $\ker \tilde{\varphi}$ contains $\langle i^2 - a^2, j^2 + a^2, ij + ji$. Thus $\tilde{\varphi}$ descends to a surjection $\varphi : (a^2,-a^2)_k \twoheadrightarrow M_2(k)$. But as $(a^2,-a^2)_k$ has dimension at most 4 and $M_2(k)$ has dimension 4, φ is an isomorphism.

1. Let $\overline{k}/k$ be an algebraic closure. Then $a, -b$ are squares in $\overline{k}$. If $a = c^2$ and $-b = d^2$ in $\overline{k}$. As $(a,b)_{\overline{k}}$ is spanned by $\{i,j\}$, replacing j by dj/c we get that $(a,b)_{\overline{k}} \cong (a,-a)_{\overline{k}}$. But $(a,-a)_{\overline{k}} \cong (c^2,-c^2) \cong M_2(\overline{k})$ by part 1. So $(a,b)_k \otimes_k \overline{k} \cong (a,b)_{\overline{k}} \cong (a,-a)_{\overline{k}} \cong M_2(\overline{k})$. Then $\dim_k (a,b)_k = 4$.

If $I \subsetneq (a,b)_k$ is a 2-sided ideal, then $I \otimes_k \overline{k} \subseteq (a,b)_{\overline{k}} \cong M_2(\overline{k})$ is a 2-sided ideal, so $I \otimes_k \overline{k} = 0$ or $I \otimes_k \overline{k} = (a,b)_{\overline{k}}$, so $I = 0$ or $I = (a,b)_k$, so $(a,b)_k$ is simple. □

Definition 2.29. Let V be a quadratic space. The *Clifford algebra* $C(V)$ is

$$C(V) = T(V)/\langle v^2 - \psi(v,v) \mid v \in V\rangle. \tag{2.10}$$

The Clifford algebra has the following universal property: if A is a k-algebra, then

$$\mathrm{Hom}_{k-\mathsf{alg}}(C(V),A) = \{\alpha \in \mathrm{Hom}(V,A) \mid \forall v \in V, \alpha(v)^2 = \psi(v,v)\} \tag{2.11}$$

$C(V)$ has a $\mathbb{Z}/2\mathbb{Z}$-grading, inherited from the $\mathbb{Z}$-grading of $T(V)$: we have that $C(V) = C_0(V) \oplus C_1(V)$, where $C_0(V) = \mathrm{Span}_k(v_1 \cdots v_{2m} \mid v_j \in V, m \geq 0)$ and $C_1(V) = \mathrm{Span}_k(v_1 \cdots v_{2m+1} \mid v_j \in V, m \geq 0)$. We have $C_0 \cdot C_0 \subseteq C_0$, $C_0 \cdot C_1 \subseteq C_1$, and $C_1 \cdot C_1 \subseteq C_0$.

We have a natural embedding $V \hookrightarrow C(V)$ induced by the natural embedding $V \hookrightarrow T(V)$, so any $v \in V$ can be considered as an element of $C(V)$.

Lemma 2.30.

1. *For all $v, w \in V$, $vw + wv = 2\psi(v,w)$.*

2. If $v_1, \dots, v_n$ is a k-basis of V, then

$$\{v_{i_1} \cdots v_{i_n} \mid i_1 < \cdots < i_m,\ m \geq 0\} \tag{2.12}$$

spans $C(V)$, so $\dim C(V) \leq 2^n$.

Proof.

1. For all $v, w \in V$, in $C(V)$ we have that $(v+w)^2 = \psi(v+w, v+w) = \psi(v) + \psi(w) + 2\psi(v,w)$, and $(v+w)^2 = v^2 + vw + wv + w^2 = \psi(v) + \psi(w) + vw + wv$, so $2\psi(v,w) = vw + wv$.

2. Let $W = \mathrm{Span}_k\{v_{i_1} \cdots v_{i_n} \mid i_1 < \cdots < i_m\} \subseteq C(V)$.

We claim that for any monomial we have that $v_{i_1} \cdots v_{i_r} \in W$. We show the claim by induction on $r \geq 0$. If $r = 0$ we are done.

In general, take $v_{i_1} \cdots v_{i_r} \in C(V)$ to be any monomial. Then $v_{i_j} \cdot v_{i_{j+1}} = -v_{i_{j+1}} \cdot v_{i_j} = 2\psi(v_{i_j}, v_{i_{j+1}})$. So

$$v_{i_1} \cdots v_{i_r} = v_{i_1} \cdots v_{i_{j+1}} v_{i_j} \cdots v_{i_r} \mod W \tag{2.13}$$

by induction, so we can assume that $i_1 \leq \cdots \leq i_r$. But if $i_j = i_{j+1}$, $v_{i_j}^2 = \psi(v_{i_j})$, so $v_{i_1} \cdots v_{i_r} = \psi(v_{i_j}) v_{i_1} \cdots v_{i_{j-1}} v_{i_{j+2}} \cdots v_{i_r}$. Then we are done by the induction hypothesis. □

Definition 2.31. Let A, B be $\mathbb{Z}/2\mathbb{Z}$-graded k-algebras. Then the graded tensor product $A \hat{\otimes}_k B$ is the $\mathbb{Z}/2\mathbb{Z}$-graded k-algebra with underlying vector space $A \otimes_k B$ and rth graded part

$$(A \hat{\otimes}_k B)_r = \bigoplus_{i+j=r} A_i \otimes_k B_j. \tag{2.14}$$

Multiplication is given by the unique k-bilinear operation satisfying

$$(x \otimes b_j)(a_i \otimes y) = (-1)^{ij}(xa_i) \otimes (b_j y) \tag{2.15}$$

for $x \in A$, $y \in B$, $a_i \in A_i$, $b_j \in B_j$. We can check that this gives a graded k-algebra.

The graded tensor product has the following universal property: Let C be a $\mathbb{Z}/2\mathbb{Z}$-graded k-algebra and $f_A : A \to C$ and $f_B : B \to C$ be graded homomorphisms such that for all $a_i \in A_i$, $b_j \in B_j$ we have that $f_A(a_i) f_B(b_j) = (-1)^{ij} f_B(b_j) f_A(a_i)$. Then there exists a unique graded homomorphism $f : A \hat{\otimes}_k B \to C$ such that for all $a \in A$, $f(a \otimes 1) = f_A(a)$ and for all $b \in B$, $f(1 \otimes b) = f_B(b)$.

Example 2.32. Let $a, b \in k^\times$. If we consider $k[x]/(x^2 - a)$ and $k[y]/(y^2 - b)$ as k-algebras with the standard grading $\deg x = 1$ and $\deg y = 1$, then we have that

$$(a, b)_k = k[x]/(x^2 - a) \hat{\otimes}_k k[y]/(y^2 - b). \tag{2.16}$$

Note that if we instead take the ordinary tensor product $k[x]/(x^2 - a) \otimes_k k[y]/(y^2 - b)$, we get a commutative ring (which will be a field if a and b are in distinct classes of $k^\times/(k^\times)^2$).

The Clifford algebra has the following nice decomposition property.

Proposition 2.33. *If $V = U \oplus W$, the $C(V) \cong C(U) \hat{\otimes}_k C(W)$ as $\mathbb{Z}/2\mathbb{Z}$-graded algebras.*

Proof. We first want to construct a map $C(V) \to C(U)\hat{\otimes}_k C(W)$. By the universal property of Clifford algebras it suffices t construct a map $V \to C(U)\hat{\otimes}_k C(W)$ such that $\alpha(v)^2 = \psi(v)$. Let $v = (u, w) \in V = U \oplus W$. Then sending $(u, w) \mapsto u \otimes 1 + 1 \otimes w$, we have that

$$\begin{aligned}(u \otimes 1 + 1 \otimes w)^2 &= u^2 \otimes 1 + u \otimes w - u \otimes w + 1 \otimes w^2 \\ &= u^2 \otimes 1 + 1 \otimes w^2 \\ &= (\psi(u) + \psi(w))(1 \otimes 1) \\ &= \psi(u) + \psi(w) \\ &= \psi(v) \end{aligned} \tag{2.17}$$

so we are all good ($1 \otimes 1$ is the unit in $C(U)\hat{\otimes}_k C(W)$ so we can drop it by abuse of notation).

Thus by the universal property of Clifford algebras we get a map

$$g : C(V) \to C(U)\hat{\otimes}_k C(W). \tag{2.18}$$

Next we want to construct the inverse map $C(U)\hat{\otimes}_k C(W) \to C(V)$. By the universal property of the graded tensor product it suffices to give $f_U : C(U) \to C(V)$ and $f_W : C(W) \to C(V)$ such that for all $u \in C_i(U)$, $w \in C_j(w)$,

$$f_U(u) f_W(w) = (-1)^{ij} f_W(w) f_U(u). \tag{2.19}$$

The maps f_U and f_W are the obvious ones induces by the inclusions $U \to V \to C(V)$ and $W \to V \to C(V)$. Consider $u = u_1 \cdots u_i \in C_i(U)$ and $w = w_1 \cdots w_j \in C_j(W)$ where $u_k \in U$, $w_\ell \in W$. By Lemma 2.30 we have that

$$u_k w_\ell + w_\ell u_k = 2\psi(u_k, w_\ell) = 0 \tag{2.20}$$

as $V = U \oplus W$ so u_k and w_ℓ are orthogonal. Thus $u_k w_\ell = -w_\ell u_k$, so

$$\begin{aligned} f_U(u) f_W(w) &= u_1 \cdots u_i w_1 \cdots w_j \\ &= (-1)^{ij} w_1 \cdots w_j u_1 \cdots u_i \\ &= (-1)^{ij} f_W(w) f_U(u) \end{aligned} \tag{2.21}$$

as desired. Thus by the universal property of the graded tensor product we get a map

$$f : C(U)\hat{\otimes}_k C(W) \to C(V). \tag{2.22}$$

We can check that these maps are inverses of each other. First, if $v_1 \cdots v_n \in C(V)$, we have that

$$\begin{aligned} f \circ g(v_1 \cdots v_n) &= f((u_1 \otimes 1 + 1 \otimes w_1) \cdots (u_n \otimes 1 + 1 \otimes w_n)) \\ &= (u_1 + w_1) \cdots (u_n + w_n) \\ &= v_1 \cdots v_n. \end{aligned} \tag{2.23}$$

Next, if $u_1 \cdots u_n \otimes w_1 \cdots w_m \in C(U)\hat{\otimes}_k C(W)$, we have that

$$\begin{aligned} &g \circ f(u_1 \cdots u_n \otimes w_1 \cdots w_m) \\ &\qquad = g \circ f((u_1 \otimes 1) \cdots (u_n \otimes 1)(1 \otimes w_1) \cdots (1 \otimes w_m)) \\ &\qquad = g(u_1 \cdots u_n \cdots w_1 \cdots w_m) \\ &\qquad = u_1 \cdots u_n \otimes w_1 \cdots w_m. \end{aligned} \tag{2.24}$$

□

Corollary 2.34. $\dim_k C(V) = 2^{\dim_k(V)}$. *If $v_1, \ldots, v_n$ is a k-basis for V, then $\{v_{i_1} \cdots v_{i_r} \mid 1 \leq i_1 < \cdots < i_r \leq n\}$ is a k-basis for $C(V)$.*

Proof. We have $V \cong \langle a_1 \rangle \oplus \cdots \oplus \langle a_n \rangle$, $a_i \in k$. Then $C(V) \cong C(\langle a_1 \rangle) \hat{\otimes}_k \cdots \hat{\otimes}_k C(\langle a_n \rangle)$. Also, we have that $C(\langle a \rangle) = T(k)/(v^2 - \psi(v)) = k[x]/(x^2 - a)$ is 2-dimensional. The result follows from Lemma 2.30. □

Example 2.35. Let $V = \langle a \rangle \oplus \langle b \rangle = \langle a, b \rangle$ with $a, b \in k^\times$. We have that $\langle a \rangle$ is spanned by x with $\psi(x) = a$, and $\langle b \rangle$ is spanned by y with $\psi(y) = b$. So in $C(V)$ we have that $x^2 = a$, $y^2 = b$, $xy + yx = 2\psi(x, y) = 0$, so $xy = -yx$. Thus $C(V)$ has basis $1, x, y, xy$, and $C(V) \cong (a, b)_k$ as k-algebras.

Example 2.36. Let $V = \langle a, b, c \rangle$, spanned by x, y, z. We have that $C(V) = C_0(V) \oplus C_1(V)$. $C_0(V)$ is spanned by $1, xy, yz, xz$. We have that $(xy)^2 = xyxy = -x^2y^2 = -ab$. Similar computations show that $C_0(V) = (-ab, -bc)_k$.

For C_1, we have that $(xyz)^2 = -abc$, and $x(xyz) = (xyz)x$ and so on. It follows that xyz is in the center of $C(V)$, so the center is nontrivial (so $C(V)$ is not central). So we get a map

$$\begin{aligned} C_0(V) \hat{\otimes}_k k[\alpha]/(\alpha^2 + abc) &\to C(V) \\ \alpha &\mapsto xyz \end{aligned} \tag{2.25}$$

This map is an isomorphism for dimension reasons.

2.3 The Brauer group and the Clifford invariant

We have constructed the Clifford algebra and shown that it has some nice properties. Similar to how regular quadratic spaces live inside the Witt group, we want our Clifford algebra to live inside some nice group. This is the *Brauer group*, although we need to do some work to make this precise. First we introduce the notion of a central simple algebra.

Definition 2.37. Let A be a k-algebra. Then A is a central simple k-algebra (CSA) if it is simple and the center $Z_A = k$ is trivial.

If $A \otimes_k K \cong M_n(K)$ for some field extension K/k, then we say that A is *split* over K.

Proposition 2.38. *Let A be a finite k-algebra. The following are equivalent:*

(i) A is a CSA.

(ii) For some $n \geq 1$, there is an isomorphism $A \otimes_k \overline{k} \cong M_n(\overline{k})$ as k-algebras.

Proof. Omitted. □

Example 2.39. $M_n(k)$ is a CSA split over k

The quaternion algebras $(a, b)_k$ are CSAs (see the proof of Lemma 2.27), but not necessarily split over k.

Definition 2.40. Let A be a k-algebra. The opposite algebra A^{op} is equivalent to A as a vector space, with multiplication given by $a \times_{\text{op}} b = b \times a$.

Proposition 2.41.

1. *If A, B are CSAs over k, then $A \otimes_k B$ is a CSA.*

2. *If A is a CSA, then $A \otimes_k A^{\mathrm{op}}$ is split.*

Proof.

1. We can pass to the algebraic closure and assume that $A \cong M_n(k)$, $B \cong M_m(k)$. We want to show that $M_n(k) \otimes_k M_m(k) \cong M_{mn}(k)$.

We use the map

$$\begin{aligned} M_n(k) \otimes_k M_m(k) &\to \mathrm{End}_k(M_{n\times m}(k)) \cong M_{mn}(k) \\ a \otimes b &\mapsto (x \mapsto ax(b^t)). \end{aligned} \tag{2.26}$$

2. We use the map

$$\begin{aligned} A \otimes_k A^{\mathrm{op}} &\to \mathrm{End}_k(A) \\ a \otimes b &\mapsto (x \mapsto axb) \end{aligned} \tag{2.27}$$

□

Definition 2.42. The *Brauer group* $\mathrm{Br}(k)$ is the group of equivalence classes $[A]$ of CSAs A over k, where $[A] = [B]$ if any of the equivalent conditions are satisfied:

(i) There exists $r, s \geq 1$ such that $M_r(A) \cong M_s(B)$ as k-algebras. We have that $M_r(A) = M_r(k) \otimes_k A$.

(ii) $A \otimes_k B^{\mathrm{op}}$ is split.

(iii) There exists a division CSA D over k (an algebra D is a division algebra if for every $d \in D\backslash\{0\}$, there exists $e \in D$ such that $de = ed = 1_D$) and $r, s \geq 1$ such that $A \cong M_r(D)$, $B \cong M_s(D)$, so that $[A] = [B] = [D]$. The division algebra D is a canonical representative for the class.

The group operation in the Brauer group is $[A] + [B] = [A \otimes_k B]$. From this it is clear that the identity element is $[k]$, and by Proposition 2.41 we have that $-[A] = [A^{\mathrm{op}}]$.

We would like the Clifford algebra to lie in the Brauer group, but Example 2.36 shows that this is not always true. However, Example 2.36 does show that if V is a 3-dimensional quadratic space, then $C_0(V)$ is a CSA. The following proposition generalizes this example.

Proposition 2.43. *Let V be a regular quadratic space. Then*

1. *If $\dim_k V$ is even, then $C(V)$ is a CSA, isomorphic to the tensor product of quaternion algebras.*

2. *If $\dim_k V$ is odd, then $C_0(V)$ is a CSA, isomorphic to the product of quaternion algebras.*

Proof. $\dim_k V = 1$ is trivial as $C_0(V) \cong k$, and we've done dimensions 2 and 3 in Examples 2.35 and 2.36, respectively.

In the general case, we argue by induction. Let $\dim_k V > 3$, and choose a decomposition $V = U \oplus W$, where $\dim U = 3$. Then $C(V) = C(U)\hat{\otimes}_k C(W)$, and $C(U) = A_U \hat{\otimes}_k k[x]/(x^2 + d(U))$

(see Example 2.36) where $A_U = C_0(U)$ with the trivial grading (everything has degree 0). In particular, A_U is a quaternion algebra. So

$$\begin{aligned} C(V) &= A_U \hat{\otimes}_k C(\langle -d(U)\rangle) \hat{\otimes}_k C(W) \\ &= A_U \hat{\otimes}_k C(W \oplus \langle -d(U)\rangle). \end{aligned} \tag{2.28}$$

and $W \oplus \langle -d(U)\rangle$ is a quadratic space of dimension $\dim V - 2$.

If $\dim V$ is even, then $C(V) \cong A_U \otimes_k C(W \oplus \langle -d(U)\rangle)$ as k-algebras. This is because we can forget about the grading, as the trivial grading of A_U means that the graded tensor product is the same as the ordinary tensor product. A_U is a CSA as it is a quaternion algebra, and by induction $C(W \oplus \langle -d(U)\rangle)$ is a CSA, so $C(V)$ is a CSA by Proposition 2.41.

If $\dim V$ is odd, then we similarly have that $C_0(V) \cong A_U \otimes_k C_0(W \oplus \langle -d(U)\rangle)$ as k-algebras, so $C_0(V)$ is a CSA by induction and Proposition 2.41. □

Thus to any regular quadratic space V we can associate a CSA, which we define below as the Clifford invariant.

Definition 2.44. Let V be a regular quadratic space. The *Clifford invariant* $c(V) \in \mathrm{Br}(k)$ is

$$c(V) = \begin{cases} [C(V)] & \dim V \text{ is even} \\ [C_0(V)] & \dim V \text{ is odd} \end{cases} \tag{2.29}$$

The Clifford invariant is very useful when proving the Hasse-Minkowski theorem, as the Brauer group plays very nicely with class field theory. This is not true of the Witt invariant (the class of V in the Witt group), which is why we have put in the extra effort to define the slightly more confusing Clifford invariant.

Lemma 2.45. *$c(V) = c(V \oplus H)$, where H is the hyperbolic plane (cf. Definition 2.9).*

Proof. This proof was left as an exercise so I'm not sure it is entirely correct.

We have that $C(V \oplus H) = C(V)\hat{\otimes}_k C(H)$ by Proposition 2.33. We also have $H \cong \langle 1\rangle \oplus \langle -1\rangle$ by Lemma 2.8, and so $C(H) \cong (1,-1)_k$ by Example 2.35.

Let A be any finite $\mathbb{Z}/2\mathbb{Z}$-graded k-algebra. We claim that $A\hat{\otimes}_k(1,-1)_k \cong A \otimes_k (1,-1)_k$ as graded k-algebras. We have a morphism $f_B : (1,-1)_k \to A \otimes_k (1,-1)_k$ given by $v \mapsto 1 \otimes v$, and a morphism $f_A : A \to A \otimes_k (1,-1)_k$ given by $a_0 \mapsto a_0 \otimes 1$ and $a_1 \mapsto a_1 \otimes xy$ for $a_0 \in A_0$ and $a_1 \in A_1$. We can verify that f_A and f_B satisfy the conditions for the universal property of the graded tensor product (cf. Definition 2.31), so we obtain a morphism $f : A\hat{\otimes}_k(1,-1)_k \to A \otimes_k (1,-1)_k$. We can verify that f is surjective, and since $A\hat{\otimes}_k(1,-1)_k$ and $A \otimes_k (1,-1)_k$ are finite dimensional vector spaces of the same dimension, f is an isomorphism. This proves the claim.

Thus we have that $C(V \oplus H) \cong C(V) \otimes_k C(H)$ as graded k-algebras.

If $\dim V$ is even, then $c(V) = [C(V)]$ and $c(V \oplus H) = [C(V \oplus H)] = [C(V) \otimes_k C(H)] = [C(V)] + [C(H)]$. But $C(H) \cong (1,-1)_k \cong M_2(k)$, so $[C(H)] = [k] = 0$, so $c(V) = c(V \oplus H)$.

Now suppose $\dim V = 1$, so that $V = \langle a\rangle$. We have that $c(V) = [k] = 0$. We have that $H \cong \langle a\rangle \oplus \langle -a\rangle$, so $V \oplus H \cong \langle a\rangle \oplus \langle a\rangle \oplus \langle -a\rangle$, so $c(V \oplus H) = [C_0(V \oplus H)] = [(a^2, -a^2)_k] = [M_2(k)] = 0$ by Example 2.36 and Lemma 2.27.

Now suppose that $\dim V \geq 3$ is odd. As in the proof of Proposition 2.43, we write $V = U \oplus W$ where $\dim U = 3$. Then $C_0(V) \cong A_U \otimes_k C_0(W \oplus \langle -d(U)\rangle)$, and $C_1(V) \cong A_U \otimes_k C_1(W \oplus \langle -d(U)\rangle)$

where $A_U = C_0(U)$ with the trivial grading. As $C(V \oplus H) \cong C(V) \otimes_k C(H)$, we have that $C_0(V \oplus H) = (C_0(V) \otimes_k C_0(H)) \oplus (C_1(V) \otimes_k C_1(H))$. Thus we have that

$$\begin{aligned} C_0(V \oplus H) &= (C_0(V) \otimes_k C_0(H)) \oplus (C_1(V) \otimes_k C_1(H)) \\ &= (A_U \otimes_k C_0(W \oplus \langle -d(U) \rangle \otimes_k C_0(H)) \oplus (A_U \otimes_k C_1(W \oplus \langle -d(U) \rangle \otimes_k C_1(H)) \\ &= A_U \otimes_k \big((C_0(W \oplus \langle -d(U) \rangle \otimes_k C_0(H)) \oplus (C_1(W \oplus \langle -d(U) \rangle \otimes_k C_1(H)) \big) \\ &= A_U \otimes_k C_0(W \oplus \langle -d(U) \rangle \oplus H) \end{aligned} \tag{2.30}$$

so $c(V \oplus H) = [A_U] + c(W \oplus \langle -d(U) \rangle \oplus H)$. As $W \oplus \langle -d(U) \rangle$ is a quadratic space of dimension $\dim V - 2$, by induction we have that $c(W \oplus \langle -d(U) \rangle \oplus H) = c(W \oplus \langle -d(U) \rangle)$. We then have that

$$\begin{aligned} c(V \oplus H) &= [A_U] + c(W \oplus \langle -d(U) \rangle) \\ &= [A_U] + [C_0(W \oplus \langle -d(U) \rangle)] \\ &= [A_U \otimes_k C_0(W \oplus \langle -d(U) \rangle)] \\ &= [C_0(V)] \\ &= c(V) \end{aligned} \tag{2.31}$$

as desired. □

The previous lemma shows that c factors through a map $W(k) \to \mathrm{Br}(k)$, but this is not a group homomorphism in general (c is a map from the set of regular quadratic spaces to $\mathrm{Br}(k)$).

2.4 Quaternion arithmetic

In order to complete the classification of quadratic forms of rank at most 3 in the next section, we will exploit the fact that low rank quadratic forms are connected to quaternion algebras. This requires a couple lemmas.

Lemma 2.46. *Let $a, b \in k^\times$, and let $A = (a, b)_k$. Then $A = k \oplus P$, where*

$$P = \{0\} \cup \{\alpha \in A \setminus k \mid \alpha^2 \in k\} \tag{2.32}$$

Proof. Let $(a, b)_k$ be spanned by $1, x, y, xy$ with $x^2 = a$ and $y^2 = b$. We need to check that P is the k-span of x, y, xy. Let $\alpha = \kappa + \lambda x + \mu y + \nu xy$. We have that

$$\begin{aligned} (\kappa + \lambda x + \mu y + \nu xy)^2 &= \kappa^2 + \lambda^2 a + \mu^2 b - \nu^2 ab + \lambda\nu xy - \lambda\nu xy + \lambda\nu x^2 y - \lambda\nu x^2 y + \mu\nu yxy - \mu\nu yxy \\ &\quad + 2\kappa(\lambda x + \mu y + \nu xy) \\ &= \kappa^2 + \lambda^2 a + \mu^2 b - \nu^2 ab + 2\kappa(\lambda x + \mu y + \nu xy). \end{aligned} \tag{2.33}$$

Thus $\alpha^2 \in k$ if and only if $\alpha \in k$ or $\alpha \in P$. Thus $P = \mathrm{Span}_k(x, y, xy)$. □

P is the "subspace of **P**ure quaternions"

Corollary 2.47. *If V is a regular quadratic space, then $c(V) \in \mathrm{Br}(k)[2]$.*

Proof. We showed that the $c(V)$ is the tensor product of quaternion algebras in Proposition 2.43. So if we want to show that $c(V) \in \mathrm{Br}(k)[2]$, it suffices to show that if $A = (a, b)_k$, then $[A] \in \mathrm{Br}(k)[2]$. We have that $A = k \oplus P$. Define $f : A \to A$ by $f(\lambda, \mu) = (\lambda, -\mu)$. This is a k-linear isomorphism, but not a k-algebra isomorphism as we have that $f(xy) = -xy = yx = f(y)f(x)$. In fact, it is a k-algebra isomorphism $f : A \to A^{\mathrm{op}}$. Thus $[A] = [A^{\mathrm{op}}] = -[A]$, so $[A] \in \mathrm{Br}(k)[2]$. □

Lemma 2.48. *Let $a, b, c, d \in k^\times$. The following are equivalent:*

(i) $(a, b)_k \cong (c, d)_k$ *as k-algebras.*

(ii) $\langle a, b, -ab\rangle \cong \langle c, d, -cd\rangle$ *as quadratic spaces.*

(iii) $\langle 1, -a, -b, ab\rangle \cong \langle 1, -c, -d, cd\rangle$ *as quadratic spaces.*

Proof. (ii) $\iff$ (iii): We have that $\langle a, b, -ab\rangle \cong \langle c, d-cd\rangle$ if and only if $\langle -a, -b, ab\rangle \cong \langle -c, -d, cd\rangle$ if and only if $\langle 1, -a, -b, ab\rangle \cong \langle 1, -c, -d, cd\rangle$ by Witt's cancellation theorem Corollary 2.15.

(i) $\to$ (ii): We have that $(a, b)_k = k \oplus P$ and $(c, d)_k = k \oplus P'$. As $(a, b)_k \cong (c, d)_k$ we have that $P \cong P'$. Now, P and P' have a quadratic form defined by $f : \alpha \mapsto \alpha^2$. As $P \cong P'$ as k-algebras, we also have that $P \sim P'$ as quadratic spaces.

The quadratic form f induces the symmetric bilinear form

$$\begin{aligned}\psi(\alpha, \beta) &= \frac{1}{2}(f(\alpha + \beta) - f(\alpha) - f(\beta)) \\ &= \frac{1}{2}(\alpha\beta + \beta\alpha). \end{aligned} \tag{2.34}$$

If $P = \mathrm{Span}_k(x, y, xy)$ with $x^2 = a$ and $y^2 = b$, then we have that x, y, xy are mutually orthogonal under ψ, so $\langle a, b, -ab\rangle \sim P \sim P' \sim \langle c, d, -cd\rangle$.

(ii) $\to$ (i): We are given an isomorphism $g : P \to P'$ of quadratic spaces where P, P' are equipped with the quadratic form ψ define above. Set $X = g(x)$, $Y = g(y)$. Then $X^2 = x^2 = a$, $Y^2 = y^2 = b$, and as $XY + YX = 2\psi(X, Y) = 2\psi(x, y) = 0$. Thus X, Y satisfy the quaternion relations for $(a, b)_k$, so we obtain an induced k-algebra homomorphism $\tilde{g} : (a, b)_k \to (c, d)_k$. As g is an isomorphism (injective, surjective), $\tilde{g}$ must be as well. □

Corollary 2.49. *Let $a, b \in k^\times$. The following are equivalent:*

(i) $(a, b)_k \cong (-1, 1)_k \cong M_2(k)$.

(ii) $\langle a, b, -ab\rangle$ *is isotropic.*

(iii) $b \in \mathrm{im}(N : k(\sqrt{a})^\times \to k^\times)$.

Proof. (i) $\to$ (ii): If $(a, b)_k \cong (1, -1)_k$, then $\langle a, b, -ab\rangle \cong \langle 1, -1, 1\rangle$ by Lemma 2.48, which is isotropic.

(ii) $\to$ (i): If $P = \langle a, b, -ab\rangle$ is isotropic, then $H \subseteq P$ by Lemma 2.10, so $P \sim \langle 1, -1, -d(V)\rangle \sim \langle 1, -1, 1\rangle$, so $(a, b)_k \cong (1, -1)_k$ by Lemma 2.48.

(ii) $\iff$ (iii): We have that $\langle a, b, -ab\rangle$ is isotropic if and only if $\langle (ab)a, (ab)b, (ab)(-ab)\rangle \sim \langle a, b, -1\rangle$ is isotropic. Now, $\langle a, b, -1\rangle$ is isotropic if and only if $ax^2 + by^2 - z^2 = 0$ has a nontrivial solution, if and only if $by^2 = z^2 - ax^2$ has a nontrivial solution. Let (x, y, z) be such a solution. If $y = 0$, then $a \in (k^\times)^2$. If $y \neq 0$, then we can divide to get a solution to $b = z^2 - ax^2$. Thus $by^2 = z^2 - ax^2$ has a nontrivial solution if and only if $a \in (k^\times)^2$ or $b = z^2 - ax^2$ has a nontrivial solution.

If $a \in (k^\times)^2$, then $k(\sqrt{a}) = k$, so $N : k^\times \to k^\times$ is just the identity, so $b \in \mathrm{im}\, N$. If $a \notin (k^\times)^2$ and $b = z^2 - ax^2$ has a nontrivial solution, then $k(\sqrt{a})$ is a quadratic extension and $N(z + x\sqrt{a}) = (z + x\sqrt{a})(z - x\sqrt{a}) = z^2 - ax^2$.

Likewise, if $b \in \mathrm{im}\, N$, then either $a \in (k^\times)^2$ or $b = N(z + x\sqrt{a})$.

□

2.5 Low rank quadratic forms

We are now ready to complete the classification of quadratic forms or rank at most 3 using the determinant and Clifford invariant. We also classify isotropic quadratic forms of rank at most 4.

Theorem 2.50. *Let V, V' be regular quadratic spaces of dimension n with $1 \leq n \leq 3$. The following are equivalent:*

(i) $V \sim V'$.

(ii) $d(V) \equiv d(V')$ *and* $c(V) = c(V')$.

Proof. (i) $\to$ (ii): done.

(ii) $\to$(i): If $n = 1$, then $V = \langle d(V) \rangle$, so we are done.

If $n = 2$, then $V = \langle a, b \rangle$ and $V' = \langle c, d \rangle$. We have that $c(V) = [(a, b)_k] = c(V') = [(c, d)_k]$. Now, as $(a, b)_k$ is either a division algebra or split, we have that $[(a, b)_k] = [(c, d)_k]$ implies that $(a, b)_k \cong (c, d)_k$ (see Definition 2.42). Thus $\langle a, b, -ab \rangle \sim \langle c, d, -cd \rangle$ by Lemma 2.48. As $d(V) \equiv ab \equiv cd \equiv d(V')$, we have that $\langle a, b, -ab \rangle \sim \langle c, d, -ab \rangle$, so $\langle a, b \rangle \sim \langle c, d \rangle$ by Witt's cancellation theorem (Corollary 2.15).

If $n = 3$, then $V = \langle a, b, c \rangle$ and $V' = \langle d, e, f \rangle$. Then $c(V) = [(-ab, -bc)_k]$ and $c(V') = [(-de, -ef)_k]$ by Example 2.36. Then arguing as in the $n = 2$ case we have that $\langle -ab, -bc, -ac \rangle \sim \langle -de, -ef, -df \rangle$. We also have $-d(V) \equiv -abc \equiv -def \equiv -d(V')$. Thus we have that

$$\begin{aligned} V &\sim \langle c, a, b \rangle \\ &\sim \langle (-abc)(-ab), (-abc)(-bc), (-abc)(-ac) \rangle \\ &\sim \langle (-def)(-de), (-def)(-ef), (-def)(-df) \rangle \\ &\sim \langle f, d, e \rangle \\ &\sim V' \end{aligned} \tag{2.35}$$

as desired. □

Remark 2.51.

1. The previous result holds for $n > 3$ if k is a local field, which we prove in Theorem 4.5.
2. The regular quadratic spaces of rank n are classified by $H^1(k, \mathrm{O}_n)$ where O_n is the orthogonal group associated with a quadratic space of rank n.
3. The central simple algebras of rank n^2 are classified by $H^1(k, \mathrm{PGL}_n)$.
4. The reason the above argument works is that there is an exceptional isomorphism $\mathrm{SO}_3 \cong \mathrm{PGL}_2$, which is why the Clifford invariant is related to quadratic spaces in low dimension.

We now classify isotropic quadratic spaces of rank at most 4. This can be seen as a low rank version of the Hasse-Minkowski theorem.

Theorem 2.52. *Let V be a regular quadratic space of rank n. Then*

1. *If $n = 2$, then V is isotropic if and only if $d(V) \equiv -1$.*
2. *If $n = 3$, then V is isotropic if and only if $c(V) = [k] = 0$.*

3. *If $n = 4$, then V is isotropic if and only if $c(V_K) = [K] = 0$ in $\mathrm{Br}(K)$, where $K = k(\sqrt{d(V)})$ and $V_K = V \otimes_k K$.*

Proof.

1. This is Lemma 2.8.

2. Assume $n = 3$ and suppose that V is isotropic. Then $V = \langle 1, -1, -d(V)\rangle$ because $H \subseteq V$ by Lemma 2.10. We have that $c(V) = [(1, -d(V))_k]$ by Example 2.36, and $(1, -d(V))_k \cong M_2(k)$ by Corollary 2.49, so $c(V) = [M_2(k)] = [k]$.

Now suppose that $V = \langle a, b, c\rangle$ and $c(V) = [(-ab, -bc)_k] = [k]$, so that $(-ab, -bc)_k$ is split. Then $(-ab, -bc)_k \cong (-1, 1)_k$, so comparing pure quaternions gives $\langle -ab, -bc, -ac\rangle \sim 1, -1, 1\rangle$. Multiplying through by $-abc$ gives $\langle a, b, c\rangle \sim \langle -abc, abc, -abc\rangle$, which is isotropic.

3. First assume that $d(V) \equiv 1 \mod (k^\times)^2$, so $K = k(\sqrt{d(V)}) = k$.

Suppose V is isotropic, then $H \subseteq V$ so $V \sim \langle 1, -1, a, -a\rangle$ for some $a \in k^\times$, so $V \sim H \oplus H$, and $c(V) = [k]$ by Lemma 2.45.

Now suppose $V = \langle a, b, c, d\rangle$ and $c(V) = [k]$ is trivial. We can calculate that (using something like (4.5))

$$C(V) \cong (-ab, -bc)_k \otimes_k (d, -abc)_k. \tag{2.36}$$

We have that $d \equiv abc \mod (k^\times)^2$, so $(d, -abc)_k \cong (abc, -abc)_k \cong M_2(k)$ by Corollary 2.49. Thus $c(V) = [(-ab, -bc)_k]$. Since this is trivial, we have that $(-ab, -bc)_k \cong (1, -1)_k$, so $(-ab, -bc, -ac) \cong (1, -1, 1)$ by Lemma 2.48. Multiplying by abc gives $\langle a, b, c\rangle \sim \langle -abc, abc, -abc\rangle$, which is isotropic. As $\langle a, b, c\rangle \subseteq V$, V is isotropic.

We have completed the case where $d(V) \in (k^\times)^2$. Assume that $d = d(V) \notin (k^\times)^2$, so $K = k(\sqrt{d})$ is a quadratic extension, and $\sqrt{d} \notin k$. It suffices to show that V is isotropic if and only if $V_K = V \otimes_k K$ is isotropic, as then we can pass to the quadratic extension where $d(V) \in (K^\times)^2$.

If V is isotropic, then clearly V_K is isotropic.

Now suppose V_K is isotropic. Then there exists $u, v \in V$ not both 0 such that $\psi(u + \sqrt{d}v, u + \sqrt{d}v) = 0$. So $\psi(u) + d\psi(v) + 2\sqrt{d}\psi(u, v) = 0$, so $\psi(u) + d\psi(v) = 0$ and $\psi(u, v) = 0$. If $\psi(u) = 0$ or $\psi(v) = 0$ we are done, so we may assume $\psi(u), \psi(v) \neq 0$, and that u, v are linearly independent over k. Then $U = \mathrm{Span}_k(u, dv) \sim \langle \psi(u), -d\psi(u)\rangle \subseteq V$, so $V = U \oplus W$, where W is the complementary space. We have that $d(U) \equiv -d(V)$, so $d(W) \equiv -1$, so $W \sim H$ is isotropic, so V is isotropic. □

3 Quadratic forms over finite fields

Let $k = \mathbb{F}_q$ for q an odd prime (so that $\mathrm{char}\, k \neq 2$). Utilizing the machinery of the previous section, we can now develop a short and sweet classification of quadratic forms over k.

$\mathbb{F}_{q^d}$ is any field extension, the norm map $N : \mathbb{F}_{q^d}^\times \to \mathbb{F}_q^\times$ is surjective. Thus by Corollary 2.49, any quaternion algebra over k is split. In fact we have that $\mathrm{Br}(k) = 0$, but this is a bit harder to prove and we won't need this.

Theorem 3.1.

1. *If V is a regular quadratic space over $\mathbb{F}_q$ of dimension $n \geq 3$, then V is isotropic.*

2. *If V, V' are regular quadratic spaces over $\mathbb{F}_q$ of dimension n, then $V \equiv V'$ if and only if $d(V) \equiv d(V')$.*

   Thus up to equivalence, the only regular quadratic forms are $x_1^2 + \cdots + x_n^2$ and $x_1^2 + \cdots + ux_n^2$ with $u \in \mathbb{F}_q^\times (\mathbb{F}_q^\times)^2$, as $\mathbb{F}_q^\times / (\mathbb{F}_q^\times)^2$ has two elements.

Proof.

1. WLOG we may assume $n = 3$ (as we can always take a 3-dimensional subspace). Then by Theorem 2.52 we have that V is isotropic if and only if $c(V) = [k]$, which is always the case.

2. If $n \leq 3$ we are done by Theorem 2.50, as $c(V) = c(V') = [k]$.
   If $n \geq 4$, then V and V' are isotropic by Part 1, so $V = H \oplus W$ and $V' = H \oplus W'$ with $d(W) \equiv -d(V)$ and $d(W') \equiv -d(V')$, so by induction $W \sim W'$ so $V \sim V'$. □

4 Quadratic forms over p-adic fields

Let $k/\mathbb{Q}_p$ be a finite extension. The classification of quadratic forms over p-adic fields is fairly nice and will allows us to prove things about number fields. First we recall the following theorems from class field theory:

Theorem 4.1.

1. *(Brauer group) There's a canonical isomorphism* $\mathrm{inv}_k : \mathrm{Br}(k) \to \mathbb{Q}/\mathbb{Z}$. *In particular,* $\mathrm{Br}(k)[2] \cong 1/2\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$.

   inv_k *is the* invariant map.

2. *(Artin reciprocity) For any quadratic extension E/k, there's a canonical isomorphism*

$$\mathrm{Art}_k : k^\times / N_{E/k}(E^\times) \cong \mathrm{Gal}(E/k) \tag{4.1}$$

Remark 4.2. Thus if we choose $a \in k^\times \setminus (k^\times)^2$ and $b \in k^\times \setminus N(k(\sqrt{a})^\times)$, then $[(a,b)_k]$ represents the unique non-trivial element of $\mathrm{Br}(k)[2]$ (see Corollaries 2.47 and 2.49).

Lemma 4.3. *Let V, V' be regular quadratic spaces of dimension 3 such that $d(V) \equiv d(V')$. The following are equivalent:*

(i) $V \sim V'$.

(ii) Either V, V' are both isotropic, or both anisotropic.

Proof. (i) → (ii): Done.
(ii) → (i): If V, V' are both isotropic, then $V \cong H \oplus \langle -d(V) \rangle$, so $V \cong V'$. If V, V' are both anisotropic, so that $c(V), c(V') \neq 0$. Then $c(V) = c(V')$ as there is only 1 non-trivial class in $\mathrm{Br}(k)[2]$, so $V \cong V'$ by Theorem 2.50. □

Proposition 4.4.

1. *There exists a unique anisotropic quadratic space W/k of dimension 4. It is $W = \langle 1, -a, -b, ab \rangle$, where $(a,b)_k$ is non-split. W represents every element of $k^\times$.*

2. Any regular quadratic space W' over k of dimension $n \geq 5$ is isotropic.

Proof.

1. Let $A = (a,b)_k$, so that $A = k \oplus P$ where P are the pure quaternions. Let $f : A \to A$ be the map $f(\lambda, \mu) = (\lambda, -\mu)$ for $\lambda \in k, \mu \in P$. We have that $(\lambda + \mu)f(\lambda + \mu) = \lambda^2 - \mu^2$ because λ is a scalar, and hence commutes with μ. So $\psi : (\lambda, \mu) \mapsto \lambda^2 - \mu^2$ is a quadratic form, given by $W = \langle 1, -a, -b, ab \rangle$. It is anisotropic: otherwise $H \subseteq W$, so $W \sim \langle 1, -1, c, -c \rangle \sim H \oplus H$, so $(a,b)_k \cong (-1,1)_k \cong M_2(k)$ would be split by Corollary 2.49.

Let $\alpha, \beta \in A \setminus \{0\}$. We have that $\alpha\beta f(\alpha\beta) = \alpha\beta f(\beta)f(\alpha)\alpha f(\alpha)\beta f(\beta)$ as $f : A \to A^{\mathrm{op}}$ is a k-algebra homomorphism (see the proof of Corollary 2.47), and $f(\alpha) \in k^\times$ is a scalar and hence in the center of A. Thus the map

$$\begin{aligned} A \setminus \{0\} &\to k^\times \\ (\lambda, \mu) &\mapsto (\lambda + \mu) f(\lambda, \mu) \end{aligned} \tag{4.2}$$

is a homomorphism.

We want to show that W represents every element of $k^\times$. We have a k-algebra embedding

$$\begin{aligned} k(\sqrt{a}) &\to A \\ \sqrt{a} &\mapsto x \end{aligned} \tag{4.3}$$

The restriction of the quadratic form ψ to $k(\sqrt{a})$ is $N_{k(\sqrt{a})/k}$, as $(\lambda + \mu x)(\lambda - \mu x) = \lambda^2 - a\mu^2$. Thus W represents every element of $N(k(\sqrt{a})^\times)$, an index 2 subgroup.

Now, for any $c \in k^\times \setminus (k^\times)^2$, then there exists $d \in k^\times \setminus N(k(\sqrt{c})^\times)$, so $(c,d)_k$ is a non-split quaternion algebra over k. Thus $[(a,b)_k] = [(c,d)_k]$, so $(a,b)_k \cong (c,d)_k$ (this follows from part 3 of Definition 2.42), so $\langle 1, -a, -b, ab \rangle \cong \langle 1, -c, -d, cd \rangle$, so W represents every element of $N(k(\sqrt{c})^\times)$, so W represents every norm of every quadratic extension:

$$S \coloneqq \bigcup_{c \in k^\times \setminus (k^\times)^2} N(k(\sqrt{c})^\times) \subseteq \psi(W). \tag{4.4}$$

We need to show that $S = k^\times$. We use the existence theorem from class field theory: any index 2 subgroup of $k^\times$ is of the form $N(k(\sqrt{c})^\times)$ for some $c \in k^\times$. Thus it suffices to show that $k^\times$ is covered by its index 2 subgroups. This is true as $k^\times/(k^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^r$ with $r \geq 2$.

Now, let V be an anisotropic quadratic space of dimension 4 and let $K = k(\sqrt{d(V)})$. Then by Theorem 2.52, we have that $c(V_K) \neq [K]$, and hence $c(V) \neq [k]$ is nontrivial. Suppose $d(V) \not\equiv 1$. Then as $d(V) \in k^\times \setminus (k^\times)^2$, we have that there exists $e \in k^\times$ such that $[(d(V), e)_k]$ is nontrivial, and hence $c(V) = [(d(V), e)_k]$ (see Remark 4.2). Then as $d(V)$ is a square in K, we have that $c(V_K) = [(d(V), e)_K] = [K]$, a contradiction. Thus $d(V) \equiv 1$.

Let $\alpha \in k^\times$ be represented by V. Then we can write $V = \langle \alpha \rangle \oplus V'$, and $W = \langle \alpha \rangle \oplus W'$. As V', W' have the same determinant and are anisotropic of rank 3, so by Lemma 4.3 we have that $V \cong W$.

2. We can assume that $n = 5$ and show that V is isotropic. Let $\alpha \in k^\times$ be represented by V, and write $V = \langle \alpha \rangle \oplus V'$. If V' is isotropic, we are done. If V' is anisotropic, then $V' \cong W$ as in Part 1, so V' represents $-\alpha$, so $V \cong \langle \alpha, -\alpha \rangle \oplus V''$, and $\langle \alpha, -\alpha \rangle \cong H$, so V is isotropic. □

Theorem 4.5. *Let V be a regular quadratic space of dimension $n \geq 1$. Then V is determined up to isomorphism by $d(V)$ and $c(V)$.*

Proof. This is true for any k when $n \leq 3$ by Theorem 2.50.

Suppose $n = 4$. Then V is isotropic if and only if $c(V_K) = [K]$ where $K = k(\sqrt{d(V)})$ by Theorem 2.52. If $d(V) \not\equiv 1$, then V is isotropic by Proposition 4.4, so $V = H \oplus W$, and $d(W) \equiv -d(V)$, and $c(W) = c(V)$. So V is determined. If $d(V) \equiv 1$, then either V is isotropic, so $c(V) = [k]$ and $V = H^2$, or V is anisotropic, and $V \sim \langle 1, -a, -b, ab\rangle$ as in Proposition 4.4.

If $n \geq 5$, then V is isotropic by Proposition 4.4, so $V \sim H \oplus W$ and $d(W) \equiv -d(V)$ and $c(W) = c(V)$, so V is determined by induction. □

Next we will show that every combination of determinant and Clifford invariant does in fact occur.

Theorem 4.6. *Let $n \geq 3$, $d \in k^\times$, and $c \in \mathrm{Br}(k)[2]$. Then there exists a regular quadratic space V over k of dimension n such that $d(V) \equiv d$ and $c(V) = c$.*

This theorem is so nice because when $n \geq 3$, we have that SO_n is a semisimple algebraic group, and we have that $H^1(k, \mathrm{SO}_n)$ classifies the regular quadratic spaces.

We'll use the following formula in the proof, which is valid for any k : If W is a regular quadratic space over k, and $a \in k^\times$, then

$$c(W \oplus \langle a\rangle) = c(W) + \begin{cases} [(a, (-1)^r d(W))_k] & \dim W = 2r+1 \\ [(-a, (-1)^r d(W))_k] & \dim W = 2r \end{cases} \tag{4.5}$$

Proof of Theorem 4.6. First suppose $n = 3$. Then V is isotropic if and only if $c(V) = [k]$. There exist isotropic and anisotropic regular quadratic spaces of dimension 3, so we can freely choose the Clifford invariant. Now, for any $a \in k^\times$ we have that $d(\langle a\rangle \otimes V) \equiv ad(V)$ and $c(\langle a\rangle \otimes V) = c(V)$, so we can pick any $d(V)$.

If $n = 2r + 1 \geq 5$ is odd, let W be a regular quadratic space of dimension $n - 2 \geq 3$. Then $d(W \oplus H) = -d(W)$ and $c(W \oplus H) = c(W)$. By induction we may choose W such that $d(W) \equiv -d$ and $c(W) = c$, so $V = W \oplus H$ does the job.

If $n = 2r \geq 4$ is even, let W be a regular quadratic space of dimension $n - 1 \geq 3$. Then $d(W \oplus \langle 1\rangle) = d(W)$, and

$$\begin{aligned} c(W \oplus \langle 1\rangle) &= c(W) + [(1, (-1)^{r-1} d(W))_k] \\ &= c(W) \end{aligned} \tag{4.6}$$

as 1 is always a norm, so $[(1, (-1)^{r-1}d(W))_k]$ is split by Corollary 2.49. So setting $V = W \oplus \langle 1\rangle$ works. □

In the case $k = \mathbb{Q}_p$, we can define the Hasse invariant of $V = \langle a_1, \ldots, a_n\rangle$, which is

$$\epsilon(V) = \prod_{i<j} (a_i, a_j)_p \tag{4.7}$$

where $(a_i, a_j)_p$ is the Hilbert symbol. For $a, b \in \mathbb{Q}_p$, the Hilbert symbol is defined as $(a, b)_p = 1$ if $z^2 = ax^2 + by^2$ has a nontrivial solutions $(x, y, z) \in \mathbb{Q}_p$ and -1 otherwise. $(a, b)_p = 1$ if and only if b is a norm in $\mathbb{Q}_p(\sqrt{a})$. By Corollary 2.49, we then have that $(a, b)_p = 1$ if and only if $[(a, b)_{Q_p}] = 0$ in $\mathrm{Br}(k)[2] = 1$.

5 Quadratic forms over number fields

Let $k/\mathbb{Q}$ be a finite extension, and let M_k be the set of places of k. We have the following facts from global class field theory.

There's an exact sequence

$$0 \to \mathrm{Br}(k) \xrightarrow{\bigoplus_{v\in M_k} \mathrm{res}_v} \bigoplus_{v\in M_k} \mathrm{Br}(k_v) \xrightarrow{\bigoplus_{v\in M_k} \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 0 \tag{5.1}$$

$$[A] \mapsto ([A_{k_v}])_{v\in M_k} \tag{5.2}$$

inv_k is the *invariant map*. The maps $\mathrm{res}_v : \mathrm{Br}(k) \to \mathrm{Br}(k_v)$ are the natural restriction maps.

If $k_v = \mathbb{C}$, then $\mathrm{Br}(k_v) = 0$ because $\mathbb{C}$ is algebraically closed.

If $k_v = \mathbb{R}$, then $\mathrm{Br}(k_v) = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, with nontrivial element represented by $(-1,-1)_{\mathbb{R}}$ the Hamiltonian quaternions.

In 2-torsion, we have

$$0 \to \mathrm{Br}(k)[2] \to \bigoplus_{v\in M_k} \mathrm{Br}(k_v)[2] \to \frac{1}{2}\mathbb{Z}/\mathbb{Z} \to 0. \tag{5.3}$$

Thus we have a bijection

$$\mathrm{Br}(k)[2] \leftrightarrow \{\text{Finite subsets } S \subseteq M_k \text{ of even cardinality, such that if } v \in S \implies k_v \ncong \mathbb{C}\} \tag{5.4}$$

We need even cardinality as that way our element will be in $\mathrm{Br}(k)[2] = \ker \bigoplus \mathrm{inv}_k$ (we are adding up an even number of $1/2$s). We take $k_v \ncong \mathbb{C}$ as if $k_v \equiv \mathbb{C}$ then $\mathrm{Br}(k_v)$ is trivial, so in order to get a unique representation we just exclude all the complex places.

Explicitly the map is given by

$$[A] \mapsto \{v \in M_k \mid A_{k_v} \text{ is non-split}\} \tag{5.5}$$

If E/k is a quadratic extension, then the Artin map gives an isomorphism

$$\mathrm{Art}_k = \prod_{v\in M_k} \mathrm{Art}_{k_v} : \mathbb{A}_k^\times / k^\times N_{E/k}(\mathbb{A}_E^\times) \xrightarrow{\cong} \mathrm{Gal}(E/k) \tag{5.6}$$

Now, the goal of this section is to prove the following result.

Theorem 5.1 (Hasse-Minkowski)**.** *Let V be a regular quadratic space of dimension $n \geq 1$. Then V is isotropic if and only if $v \in M_k$, $V_{k_v} = V \otimes_k k_v$ is isotropic.*

This theorem is useful as while it is difficult to verify that V is isotropic, V_{k_v} is easily isotropic for all but finitely many places. For the other places, we can compute whether or not V_{k_v} is isotropic using the Clifford invariant and the other local tools developed in the last section.

Proof. The forward direction is trivial.

Now we prove the backwards direction.

If $n = 1$ then nothing is isotropic.

If $n = 2$, then by Theorem 2.52 V is isotropic if and only if $d(V) \equiv -1$. So we need to show that $-d(V) \in (k^\times)^2$ if and only if $-d(V) \in (k_v^\times)^2$ for all $v \in M_k$. We have that $-d(V) \in (k_v^\times)^2$ if and

only if v splits in $k(\sqrt{-d(V)})$. The Chebotarev density theorem says that if $[k(\sqrt{-d(V)}) : k] = 2$, then the primes that split in $k(\sqrt{-d(V)})$ have Dirichlet density $1/2$. So if all places split, then $k(\sqrt{-d(V)}) = k$ and $-d(V) \in (k^\times)^2$.

If $n = 3$, then by Theorem 2.52, V is isotropic if and only if $c(V) = [k]$, if and only if $c(V_{k_v}) = k_v$ for all v by the fundamental exact sequence (5.4), if and only if V_{k_v} is isotropic for all v.

If $n = 4$, then we know that V is isotropic if and only if $c(V_K) = [K]$ where $K = k(\sqrt{d(V)})$. As K is a number field, we may argue as above using the fundamental exact sequence (5.4).

If $n \geq 5$ we argue by induction. We utilize the weak approximation theorem, which states that if $T \subseteq M_k$ is a finite set of places, then $k \hookrightarrow \prod_{v \in T} k_v$ has dense image.

First, choose a decomposition $V = U \oplus W$ with $\dim U = 2$. We assume that V_{k_v} is isotropic for all $v \in M_k$, and we need to show that V is isotropic. If U or W is isotropic we are done, so we may assume that U and W are anisotropic.

Let $S = \{v \in M_k \mid W_{k_v} \text{is anisotropic}\}$. Let W' be any 3-dimensional subspace of W (which exists because $\dim W \geq 3$), and S' the analogue of S for W'. Then $S \subseteq S'$. But $v \in S'$ if and only if $c(W'_{k_v})$ is nontrivial, and by (5.4) this is a finite set of places. Thus S is finite.

Now take some $v \in S$. Then V_{k_v} is isotropic, so we can find $c_v \in k_v^\times$ such that c_v is represented by U_{k_v} and $-c_v$ is represented by W_{k_v}.

We can find $\epsilon > 0$ such that for all $v \in S$ and $d_v \in k_v^\times$, then $|c_v - d_v|_v < \epsilon$ implies that $c_v/d_v \in (k_v^\times)^2$. If v is non-Archimedean, we can do this with Hensel's lemma. If v is archimedean, we take a small ball not containing 0. Then by weak approximation, we can find some $u \in U$ such that for all $v \in S$, $\psi(u,u)/c_v \in (k_v^\times)^2$.

We look at the subspace $ku \oplus W \subseteq V$, which is a regular quadratic of dimension $n-1$ as u is anisotropic. We claim that for all $v \in M_k$, $(ku \oplus W)_{k_v}$ is isotropic. If $v \notin S$, then W_{k_v} is isotropic. If $v \in S$, then $k_v u$ represents c_v by construction, and W_{k_v} represents $-c_v$, so $(ku \oplus W)_{k_v}$ represents 0 and hence is isotropic.

Then by induction, $ku \oplus W$ is isotropic, so V is isotropic. □

We will now derive some consequences of the Hasse-Minkowski theorem.

Theorem 5.2 (Weak Hasse-Minkowski)**.** *Let V, V' be regular quadratic spaces of dimension n. Then $V \sim V'$ if and only if for all $v \in M_k$, $V_{k_v} \sim V'_{k_v}$*

Proof. The forward direction is trivial.

Now suppose that for all $v \in M_k$, $V_{k_v} \cong V'_{k_v}$. We prove the result by induction on the dimension $n \geq 1$.

If $n = 1$, then $V \sim V'$ if and only if $V \oplus (\langle -1 \rangle \otimes V')$ is isotropic. Applying Theorem 5.1 completes the proof.

Now for the inductive step. Let $n > 1$ and choose some $a \in k^\times$ represented by V, and write $V = \langle a \rangle \oplus W$. Note that V' represents a if and only if $V' \oplus \langle -a \rangle$ is isotropic by Corollary 2.11. As $V_{k_v} \sim V'_{k_v}$ for all $v \in M_k$, we have that $V'_{k_v} \oplus \langle -a \rangle \sim V_{k_v} \oplus \langle -a \rangle$ is isotropic over k_v for all $v \in M_k$, so $V' \oplus \langle -a \rangle$ is isotropic by Theorem 5.1. Thus V' represents a, so we can write $V' \sim \langle a \rangle \oplus W'$. If $v \in M_k$, then $V'_{k_v} = \langle a \rangle \oplus W'_{k_v} \sim V_{k_v} = \langle a \rangle \oplus W_{k_v}$. Then applying Witt's cancellation theorem gives $W'_{k_v} \sim W_{k_v}$ for all $v \in M_k$, so by induction $W \sim W'$, so $V \sim V'$. □

Corollary 5.3. *If V, V' are regular quadratic spaces over k of dimension $n \geq 1$. Then $V \sim V'$ if and only if $d(V) \equiv d(V')$, $c(V) = c(V')$, and for all infinite places $v|\infty$ we have that $V_{k_v} \cong V'_{k_v}$.*

Proof. We need to check that $V_{k_v} \sim V'_{k_v}$ for every $v \in M_k$. We already have this for the infinite places. If v is a finite place, then as $d(V) \equiv d(V') \mod (k^\times)^2$ we have that $d(V) \equiv d(V') \mod (k_v^\times)^2$. We also have that the restriction $\mathrm{res}_v\, c(V) = \mathrm{res}_v\, c(V')$, so $c(V_{k_v}) = c(V'_{k_v})$. Then applying Theorem 4.5 gives that $V_{k_v} \sim V'_{k_v}$, so we can apply Theorem 5.1. □

Remark 5.4. We need the condition that $V_{k_v} \sim V'_{k_v}$ at all $v \mid \infty$ as the archimedean places are less well behaved. This is a standard phenomenon in number theory that the archimedean places behave poorly from the perspective of Galois cohomology.

In particular, any regular quadratic space over $\mathbb{R}$ is isomorphic to $\langle 1\rangle^p \oplus \langle -1\rangle^q$ for a unique $p, q \geq 0$. Thus there are $n+1$ regular quadratic spaces over $\mathbb{R}$ of dimension n. But there are 2 choices of Clifford invariant, as $|\operatorname{Br}(\mathbb{R})| = 2$, and there are 2 choices of determinant, as $|\mathbb{R} \times /(\mathbb{R}^\times)^2| = 2$. Thus only knowing $c(V)$ and $d(V)$ is not enough to determine V_{k_v} for v a real place. However, as there is a unique quadratic space of rank n over $\mathbb{C}$, it is always true that $V_{k_v} \sim V'_{k_v}$ if V, V' are regular quadratic spaces of rank n and v is a complex place. Thus we can restrict to only real places in the statement of Corollary 5.3 and in the following theorem.

We can now prove an existence theorem similar to Theorem 4.6.

Theorem 5.5. *Let $n \geq 3$, $d \in k^\times$, $c \in \operatorname{Br}(k)[2]$, and choose for each $v \mid \infty$ a regular quadratic space W_v over k_v of dimension n such that $d(W_v) \equiv d \mod (k_v^\times)$ and $c(W_v) = \mathrm{res}_v(c)$. Then there exists a regular quadratic space V over k such that $d(V) \equiv d \mod (k^\times)^2$, $c(V) = c$ and for all $v \mid \infty$, $V_{k_v} \sim W_v$.*

Remark 5.6.

1. By the previous corollary, any quadratic space V satisfying the above properties is determined uniquely up to isomorphism.
2. If $n = 3$, then the Clifford invariant is a quaternion algebra, so this theorem tells us that any 2-torsion element of the Brauer group is represented by a quaternion algebra.

Proof. First we will define a quadratic space V which satisfies all the conditions above except for the one on the Clifford invariant. Then we will "twist" V to define a quadratic space V' which also satisfies the Clifford invariant condition. The second part will take a bit of muscle.

For all $v \mid \infty$, write $W_v \sim \langle a_{v,1}, \ldots, a_{v,n}\rangle$. Choose $a_1, \ldots, a_n \in k^\times$ such that for all $v \mid \infty$, $a_i/a_{v,i} \in (k_v^\times)^2$ (this is possible by weak approximation, see the proof of Theorem 5.1). Let $V = \langle a_1, \ldots, a_{n-1}, da_1 \cdots a_n\rangle$. Then $d(V) \equiv d \mod (k^\times)^2$, and $V_{k_v} \sim W_v$ for all $v \mid \infty$.

Now, let

$$S = \{v \in M_k \mid c(V_{k_v}) \neq \mathrm{res}_v(c)\}. \tag{5.7}$$

If S is empty we are done. So assume that S is non-empty. We have that

$$S = \{v \in M_k \mid \mathrm{res}_v(c(V) - c) \neq 0\}. \tag{5.8}$$

Thus S is finite and of even cardinality by (5.4).

Choose $\alpha \in k^\times$ such that $\alpha \notin (k_v^\times)^2$ if $v \in S$ and $\alpha \in (k_v^\times)^2$ if $v \mid \infty$. This is possible by weak approximation and because S does not contain any infinite places by construction.

Claim 1: There exists $\beta \in k^\times$ such that $(\alpha, \beta)_{k_v} = [k_v]$ if and only if $v \notin S$.

Proof: By Corollary 2.49, an equivalent statement is that there exists $\beta \in k^\times$ such that for all $v \in M_k$, $\beta \notin N(k_v(\sqrt{\alpha})^\times)$ if and only if $v \in S$.

We show this using the properties of the global Artin map. Let $E = k(\sqrt{\alpha})$. Then $\mathrm{Art}_k = \prod_v \mathrm{Art}_{k_v}$ gives a surjection

$$\mathbb{A}_k^\times / N(\mathbb{A}_E^\times) \to \mathrm{Gal}(E/k) \tag{5.9}$$

with kernel the image of $k^\times$ embedded diagonally in $\mathbb{A}_k^\times$.

We have that

$$\mathbb{A}_k^\times / N(\mathbb{A}_E^\times) = \bigoplus_{v \in M_k} k_v^\times / N(k_v(\sqrt{\alpha})^\times) \tag{5.10}$$

By local class field theory, $k_v^\times / N(k_v(\sqrt{\alpha})^\times)$ is trivial or a cyclic group of order 2 depending on if v splits in E or not (if v splits in E then α is a square in k_v so $k_v(\sqrt{\alpha}) \cong k_v$).

So (5.9) and some other properties of the global Artin map give an exact sequence

$$k^\times \xrightarrow{\varphi} \bigoplus_{\substack{v \in M_k \\ v \text{ not split in } E}} \mathbb{Z}/2\mathbb{Z} \xrightarrow{\Sigma} \mathbb{Z}/2\mathbb{Z} \to 0 \tag{5.11}$$

Then our claim is equivalent to the statement that there exists $\beta \in k^\times$ such that the image of β under φ is $(a_v)_v$, where $a_v = 1$ if $v \in S$ and $a_v = 0$ if $v \notin S$. The claims are equivalent because then $\beta \notin N(k_v(\sqrt{\alpha})^\times)$ if and only if $a_v = 1$, and we want to show that $\beta \notin N(k_v(\sqrt{\alpha})^\times)$ if and only if $v \in S$.

But as the sequence is exact, $(a_v)_v \in \operatorname{im} k^\times$ if and only if $\sum_v a_v = 0$. So Claim 1 holds as $|S|$ is even. □

Now, let $P = \langle 1, -\beta \rangle$ and $P' = \langle \alpha, -\alpha\beta \rangle$. Then $d(P) \equiv d(P') \equiv -\beta$.

Claim 2: P' embeds in $V \oplus P$.

Proof: The same argument as in the proof of the weak Hasse-Minkowski theorem shows that it suffices to check this locally over k_v for all $v \in M_k$, as being represented by a quadratic space is a local condition. In particular, P' embeds in $V \oplus P$ if and only if $\langle \alpha \rangle$ is represented by $V \oplus P$ and $-\alpha\beta$ is represented by W, where $\langle \alpha \rangle \oplus W \subseteq V \oplus P$ is the complement. Thus P' embedding in $V \oplus P$ is equivalent to certain elements being represented by certain quadratic spaces. By Corollary 2.49, an element is represented by a quadratic space if and only if a certain quadratic space is isotropic, and by the Hasse-Minkowski theorem 5.1 being isotropic is a local condition. Thus we can check that P' embeds in $V \oplus P$ locally.

If $v \mid \infty$, then $\alpha \in (k_v^\times)^2$, so $P_{k_v} \sim P'_{k_v}$.

If $v \nmid \infty$, then $\dim V \oplus P \geq 5$, and we know that any regular quadratic space over k_v of dimension at least 4 represents every element of $k_v^\times$. This follows from Proposition 4.4, as an isotropic space represents every element of $k_v^\times$ (by Corollary 2.11, for instance), and we have directly verified the claim for the unique anisotropic space of dimension 4. Thus we can write $(V \oplus P)_{k_v} \sim \langle \alpha \rangle \oplus W$, and W will have dimension at least 4 so we can further write $(V \oplus P)_{k_v} \sim \langle \alpha \rangle \oplus \langle -\alpha\beta \rangle \oplus V'_v \sim P'_{k_v} \oplus V'_v$. Thus P' embeds locally, so it embeds globally. This completes the proof of Claim 2. □

Thus we have that $V \oplus P \sim V' \oplus P'$. We want to verify that V' satisfies the conditions of the theorem. We have that $d(V) \equiv d(V') \mod (k^\times)^2$. If $v \mid \infty$, then $V_{k_v} \sim V'_{k_v}$ by Witt's cancellation theorem as $P_{k_v} \sim P'_{k_v}$. Thus as V satisfies the determinant and infinite place conditions of the theorem, V' does as well.

It remain to check that $c(V') = c$. Using (4.5) we can calculate that

$$\begin{aligned} c(V \oplus P) &= c(V) + c(P) + (\epsilon(n)d(V), -d(P))_k \\ c(V' \oplus P') &= c(V') + c(P) + (\epsilon(n)d(V'), -d(P')) \end{aligned} \tag{5.12}$$

where $\epsilon(n) \in \{\pm 1\}$ only depends on the dimension of the quadratic space. As $d(V) \equiv d(V')$, $d(P) \equiv d(P')$ and $V \oplus P \sim V' \oplus P'$, we have that (recall that the Clifford invariants are all 2-torsion)

$$c(V') = c(V) + c(P) + c(P') = c(V) + c(P') \tag{5.13}$$

as $c(P) = [(1, -\beta)_k] = [k] = 0$ by Corollary 2.49. By Lemma 2.48 we have that $c(P') = [(\alpha, -\alpha\beta)_k] = [(\alpha, \beta)_k]$. Recall the definition of S (5.7). By construction (see Claim 1), we have that

$$S = \{v \in M_k \mid \operatorname{res}_v c(P') \neq [k_v]\} = S. \tag{5.14}$$

Thus for all $v \in M_k$, $\operatorname{res}_v c(V') = \operatorname{res}_v c$. But equivalence in the Brauer group is a local condition (see (5.1)), so $c(V') = c$.

□

Example 5.7. As an application, we can ask which $n \in \mathbb{N}$ are represented by $x^2 + y^2 + z^2$, e.g. are the sum of 3 rational squares?

This is equivalent to determining for which $n \in \mathbb{N}$ $\langle 1, 1, 1, -n\rangle$ is isotropic. By the Hasse-Minkowski theorem, we can check this locally.

Over $\mathbb{R}, \mathbb{C}$ this is always true.

Over $\mathbb{Q}_p$ with p odd, we claim that $\langle 1, 1, 1\rangle$ is isotropic. $\langle 1, 1, 1, \rangle$ is isotropic if and only if $c(\langle 1, 1, 1\rangle) = [\mathbb{Q}_p]$ by Theorem 2.52. We have that $c(\langle 1, 1, 1\rangle) = [(-1, -1)_{\mathbb{Q}_p}]$, so it suffices to show that $(-1, -1)_{\mathbb{Q}_p}$ is split. We verify this by verifying that -1 is a norm in $\mathbb{Q}_p(\sqrt{-1})$ and using Corollary 2.49. If $p \equiv 1 \mod 4$ $\mathbb{Q}_p(\sqrt{-1}) = \mathbb{Q}_p$, so -1 is a norm. If $p \equiv 3 \mod 4$, $\mathbb{Q}_p(\sqrt{-1})$ is the unique unramified quadratic extension $\mathbb{Q}_{p^2}$. But $N(\mathbb{Q}_{p^n}^\times) = p^{n\mathbb{Z}} \times \mathbb{Z}_p^\times$ where n is the unique unramified extension of degree n (this is a standard fact from local fields). So -1 is a norm.

It remains to check $\mathbb{Q}_2$. Over $\mathbb{Q}_2$, $\langle 1, 1, 1, -n\rangle$ is isotropic if $d(\langle 1, 1, 1, -n\rangle) \equiv -n \not\equiv 1 \mod (\mathbb{Q}_2^\times)^2$. This follows from Theorem 4.4, as there is a unique degree 4 anisotropic quadratic form V over $\mathbb{Q}_2$, and it has $d(V) \equiv 1$, so if $d(\langle 1, 1, 1, -n\rangle) \not\equiv 1$ then $\langle 1, 1, 1, -n\rangle$ is isotropic.

If $-n \in (\mathbb{Q}_2^\times)^2$, then $\langle 1, 1, 1, -n\rangle \sim \langle 1, 1, 1, 1\rangle$. We claim that $\langle 1, 1, 1, 1\rangle$ is the unique anisotropic quadratic space of rank 4. From the proof of Theorem 4.4, we have that if $(a, b)_{\mathbb{Q}_2}$ is non-split, then $W = \langle 1, -a, -b, ab\rangle$ is the unique anisotropic quadratic space of rank 4 over $\mathbb{Q}_2$. Thus it suffices to show that $(-1, -1)_{\mathbb{Q}_2}$ is non-split. By Corollary 2.49, it suffices to show that -1 is not a norm in $\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2$. The norm form in $\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2$ is given by $N(x + y\sqrt{-1}) = x^2 + y^2$, and $x^2 + y^2 = -1$ has no solutions modulo 4, so -1 is not a norm.

Thus $n \in \mathbb{N}$ is a sum of 3 rational squares if and only if $-n \notin (\mathbb{Q}_2^\times)^2$. We have that $-n \in (\mathbb{Q}_2^\times)^2$ if and only if $-n = 4^a c$ with $c \in (\mathbb{Z}_2^\times)^2$. Using Hensel's lemma, we can show that $c \in (\mathbb{Z}_2^\times)^2$ if and only if $c \equiv 1 \mod 8$.

Thus $n \in \mathbb{N}$ is a sum of 3 rational squares if and only if n is not of the form $4^a(8b - 1)$.

We also would like to know which $n \in \mathbb{N}$ are a sum of 3 *integer* squares. In order to answer this question, we need to develop the theory of quadratic forms over rings, which we do in the next section.

6 Quadratic forms over rings

The theory of quadratic forms over rings is a bit trickier than over fields and we will define some things from scratch.

Let k be a field of characteristic not equal to 2. Let R be an integral domain with field of fractions $\operatorname{Frac} R = k$.

6.1 Basics

Definition 6.1. A *quadratic form* of rank $n \geq 1$ over R is a polynomial $f(x_1, \ldots, x_n) = \sum A_{ij} x_i x_j$, where $A \in M_{n\times n}(R)$ is a symmetric matrix.

We say that f *represents* $a \in R$ if there exists $\mathbf{b} \in \mathbb{R}^n \setminus 0$ such that $f(\mathbf{b}) = a$.

We say that two quadratic forms f, g are *equivalent* if there exists $P \in \mathrm{GL}_n(R)$ such that $P^t A_f P = A_g$.

Remark 6.2.

1. We can also consider *proper equivalence* of quadratic forms, which is equivalence by an element of $\mathrm{SL}_n(R)$.

2. There are quadratic forms over k which are not quadratic forms over R. The form $x_1 x_2$ over $\mathbb{Q}$ is *not* a quadratic form over $\mathbb{Z}$ because the associated matrix is

$$\begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} \tag{6.1}$$

   However, all the theory developed in this section can be applied to the "form" $x_1 x_2$, so we will not worry too much about this.

Definition 6.3. A *quadratic module* M of rank $n \geq 1$ over R is a pair (M, ψ), where M is a free R-module of rank n and $\psi : M \times M \to R$ is an symmetric R-bilinear form.

A quadratic module M *represents* $a \in R$ if there exists $m \in M$ such that $\psi(m, m) = a$.

A morphism $\alpha : (M, \psi) \to (M', \psi')$ of quadratic modules is a morphism $\alpha : M \to M'$ of R-modules such that for all $m_1, m_2 \in M$, $\psi'(\alpha(m_1), \alpha(m_2)) = \psi(m_1, m_2)$.

Lemma 6.4. *For all $n \geq 1$, there is a a bijection between quadratic forms over R of rank n modulo equivalence and quadratic modules over R of rank n modulo isomorphism.*

Proof. Omitted. Similar to the case for fields. □

Remark 6.5. We can extend scalars to obtain quadratic spaces over fields. For instance, if M is a quadratic module over R, $M \otimes_R k$ is a quadratic space over k.

Two quadratic modules might be equivalent over some extension but not over the base ring. We write $M \sim M'$ or $M \sim_R M'$ to denote isomorphism over R.

Definition 6.6. A quadratic module M has a *determinant* $d(M) \in R/(R^\times)^2$ defined as the determinant of the Gram matrix. Likewise we define $d(f) = \det A_f$ for a quadratic form f. We say that M or the associated form f is *regular* if $d(M) \neq 0$, if and only if $V = M \otimes_R k$ is a regular quadratic space.

However, even if $d(M) \neq 0$ we don't necessarily have $d(M) \in R^\times$ as R is not necessarily a field. We say that M is *unimodular* if $d(M) \in R^\times$, if and only if ψ gives an isomorphism $M \to M^*$.

For the remainder of the course, we will be motivated by the classification of regular quadratic modules over $\mathbb{Z}$. We will also try to determine whether a given quadratic module over $\mathbb{Z}$ represents a given integer. A special case of this question is the integer analogue of Example 5.7. All of this can be generalized to work over the ring of integers of a number field, but we work over $\mathbb{Q}$ for simplicity.

Naive hope: If M, M' are quadratic modules over $\mathbb{Z}$, then $M \sim_{\mathbb{Z}} M'$ if and only if $M_{\mathbb{R}} \sim_{\mathbb{R}} M'_{\mathbb{R}}$ and $M_{\mathbb{Z}_p} \sim_{\mathbb{Z}_p} M'_{\mathbb{Z}_p}$ for all primes p. This is a sort of analogue of the Hasse-Minkowski theorem.

But this is not true! And not even close to being true, even in the simplest cases.

Example 6.7. Let $n \geq 1$ be a squarefree integer with $n \equiv 1 \mod 4$. Consider the set X_n of quadratic forms $f/\mathbb{Z}$ of rank 2, determinant n, such that $f_{\mathbb{R}}$ is positive definite. As the elements of X_k are positive definite, they are all equivalent over $\mathbb{R}$. The group $\mathrm{GL}_2(\mathbb{Z})$ acts on X_n.

Let $E = \mathbb{Q}(\sqrt{-n})$. We know that there are bijections (this is a "well-known classical fact")

$$\mathrm{SL}_2(\mathbb{Z})\backslash X_n \leftrightarrow \mathrm{Cl}(E) \tag{6.2}$$

$$\mathrm{GL}_2(\mathbb{Z})\backslash X_n \leftrightarrow \mathrm{Cl}(E)/\{\pm 1\} \tag{6.3}$$

Here, $\mathrm{Cl}(E)/\{\pm 1\}$ is the set $\mathrm{Cl}(E)$ with each element identified with its inverse. Note that none of the quotients above are group quotients.

We can also show that if $f, g \in X_n$, then $f \sim_{\mathbb{Z}_p} g$ for all p if and only if f, g have the same image in $\mathrm{Cl}(E)/2\,\mathrm{Cl}(E)$. So our "naive hope" is equivalent to asking that the map $\mathrm{Cl}(E)/\{\pm 1\} \to \mathrm{Cl}(E)/2\,\mathrm{Cl}(E)$ is bijective. But this is not true. Gauss showed that $\#\,\mathrm{Cl}(E)/2\,\mathrm{Cl}(E) = 2^r$, where $r = \#\{p \mid n\} = \tau(n)$. Also, by the Brauer Siegel theorem we have that

$$\lim_{n\to\infty} \frac{\log \#\,\mathrm{Cl}(E)}{\log \sqrt{4n}} = 1 \tag{6.4}$$

so the size of $|\,\mathrm{Cl}(E)| \to \infty$ as $n \to \infty$. If we let let n be a prime and let $n \to \infty$, then $\mathrm{Cl}(E)/2\,\mathrm{Cl}(E)$ has 2 elements, but $\mathrm{Cl}(E)/\{\pm 1\}$ has more than 2 elements for n sufficiently large.

Concretely, if $n = 29$, then $\mathrm{Cl}(E) = 6$ and $|\,\mathrm{Cl}(E)/2\,\mathrm{Cl}(E)| = 2$, and $\mathrm{GL}_2(\mathbb{Z})\backslash X_n$ is represented by $x^2 + 29y^2$, $2x^2 + 2xy + 15y^2$, $5x^2 + 2xy + 6y^2$, and $3x^2 + 2xy + 10y^2$. Thus the four forms above split into two equivalence classes in $\mathrm{Cl}(E)/2\,\mathrm{Cl}(E)$.

Thus we can't prove an analogue of the Hasse-Minkowski theorem, so we develop more machinery the failure of the local-global principle

Definition 6.8. Let f be a regular quadratic form over $\mathbb{Z}$. The *genus* of f, denoted by $\mathrm{gen}(f)$, is the set of quadratic forms g over $\mathbb{Z}$ such that $f \sim_{\mathbb{R}} g$ and $f \sim_{\mathbb{Z}_p} g$ for every prime p.

$\mathrm{GL}_n(\mathbb{Z})$ acts on $\mathrm{gen}(f)$, so $\mathrm{gen}(f)$ splits into equivalence classes.

Lemma 6.9. *If $g \in \mathrm{gen}(f)$, then $d(f) = d(g)$ as elements of $\mathbb{Z}/(\mathbb{Z}^\times)^2 = \mathbb{Z}$.*

Proof. If f, g are equivalent locally, then $d(f) \equiv d(g) \mod \mathbb{R}_{>0}$, and $d(f) \equiv d(g) \mod (\mathbb{Z}_p^\times)^2$ for all p. Then $d(f) = d(g)$. This is because equivalence over $\mathbb{R}$ gives that $d(f)$ and $d(g)$ have the same sign, and equivalence over $\mathbb{Z}_p$ gives that they have the same p-divisibility. □

Corollary 6.10. *For any regular quadratic form f, $\mathrm{GL}_n(\mathbb{Z})\backslash \mathrm{gen}(f)$ is finite.*

Proof. For any $d \in \mathbb{Z} \setminus \{0\}$, $n \geq 1$, the set of quadratic forms of fixed determinant d modulo equivalence is finite. This is a consequence of "reduction theory", and we won't prove this. As all the forms in a given genus have the same determinant, we are done. □

Principle: Enumerating genera (the plural of genus) is easy, and a consequence of the Hasse-Minkowski theorem. But computing $\mathrm{GL}_n(\mathbb{Z})\backslash \mathrm{gen}(f)$ is hard, which represents the difficult in working over a ring versus a field. Recalling the key Example 6.7, we have that calculating the number of genera in rank 2 is equivalent to $\mathrm{Cl}(E)/2\,\mathrm{Cl}(E)$, which is fairly easy. But calculating elements in each genus is essentially as difficult as calculating $\mathrm{Cl}(E)$, which is very hard.

Observation: Suppose M, M' are quadratic modules over $\mathbb{Z}$ that correspond to quadratic forms in the same genus. Then $M \otimes_Z \mathbb{R} \sim_{\mathbb{R}} M' \otimes_Z \mathbb{R}$, and $M_{\mathbb{Z}_p} \otimes_{\mathbb{Z}_p} M'_{\mathbb{Z}_p}$. In particular, if $V = M \otimes_Z \mathbb{Q}$ and $V' = M' \otimes_{\mathbb{Z}} \mathbb{Q}$, then $V_{\mathbb{R}} \sim_{\mathbb{R}} V'_{\mathbb{R}}$, and $V_{\mathbb{Q}_p} \sim_{\mathbb{Q}_p} V'_{\mathbb{Q}_p}$ for all p. So then $V \sim_{\mathbb{Q}} V'$ by the weak Hasse-Minkowski theorem 5.2. Let $\alpha : V \to V'$ be the isomorphism defined over $\mathbb{Q}$. Now, V and V' are $\mathbb{Q}$-vector spaces which contain M and M' as quadratic submodules. Then α restricts to an isomorphism of quadratic modules $\alpha^{-1}(M') \to M'$. Thus any quadratic module in the same genus as M is a quadratic submodule of V. This will be one of our guiding principles.

6.2 Lattices

Definition 6.11. Let R be an integral domain with fraction field k, and V a quadratic space over k. An R-lattice $M \subseteq V$ is a free R-submodule of the same rank as V, which spans V as a k-vector space, such that $\psi|_{M\times M}$ takes values in R. M naturally has the structure of a quadratic module over R.

In order to find R-lattices, we can take a basis for V, and check that $\psi|_{M\times M}$ has values in R.

Definition 6.12. Let V be a regular quadratic space over $\mathbb{Q}$ and $M \subseteq V$ a $\mathbb{Z}$-lattice. Then the genus $\mathrm{gen}(M)$ of M is the set of $\mathbb{Z}$-lattices $M' \subseteq V$ such that for all primes p, there's an isomorphism $M_{\mathbb{Z}_p} \sim M'_{\mathbb{Z}_p}$ of quadratic modules over $\mathbb{Z}_p$.

We have that $M_{\mathbb{R}} \sim V_{\mathbb{R}} \sim M'_{\mathbb{R}}$, so equivalence over the reals is automatically satisfied.

If $M, M' \subseteq V$ are R-lattices and we have an isomorphism $\alpha : (M, \psi|_M) \to (M', \psi|_{M'})$ of quadratic modules, then tensoring by k gives

$$\alpha \otimes_R k : M \otimes_R k = V \to M' \otimes_R k = V \in \mathrm{O}(V) \tag{6.5}$$

an element of the orthogonal group of V, as clearly distances are preserved.

Conversely, if $\beta \in \mathrm{O}(V)$, then $\beta(M) \subseteq V$ is another R-lattice, isomorphic to M as a quadratic module over R. Thus the orthogonal group acts on the set of R-lattices in V, and two R-lattices are isomorphic as quadratic modules if and only if they are in the same orbit. This allows us to give the following characterization of the genus:

$$\mathrm{gen}(M) = \{M' \subseteq V \ \mathbb{Z}\text{-lattice} \ \mid \ \forall p, \exists g_p \in O(V_{\mathbb{Q}_p}) \text{ such that } M'_{\mathbb{Z}_p} = g_p(M_{\mathbb{Z}_p})\}. \tag{6.6}$$

This follows from the above discussion as $M'_{\mathbb{Z}_p} \sim M_{\mathbb{Z}_p}$ if and only if such a $g_p \in O(V_{\mathbb{Q}_p})$ exists.

A priori we do not know that the genus of a $\mathbb{Z}$-lattice and the associated quadratic form are the same. The next proposition shows this. Thus if we want to enumerate the equivalence classes in $\mathrm{gen}(f)$, it suffices to enumerate the equivalence classes of lattices in $\mathrm{gen}(M)$. This is the first step towards a group-theoretic description of the equivalence classes of $\mathrm{gen}(f)$, which will eventually lead to a connection with automorphic forms.

Proposition 6.13. *Let V be a regular quadratic space over $\mathbb{Q}$, $M \subseteq V$ a $\mathbb{Z}$-lattice, $e_1, \dots, e_n$ a $\mathbb{Z}$-basis for M, and $f = \sum \psi(e_i, e_j) x_i x_j$ the associated quadratic form over $\mathbb{Z}$. Then there's a bijection between*

1. $\mathrm{O}(V) \backslash \operatorname{gen}(M)$, *the genus of M up to isomorphism of quadratic modules over $\mathbb{Z}$.*
2. $\mathrm{GL}_n(\mathbb{Z}) \backslash \operatorname{gen}(f)$, *the genus of f up to isomorphism of quadratic forms over $\mathbb{Z}$.*

The map is given by

$$\begin{aligned} \operatorname{gen}(M) &\to \operatorname{gen}(f) \\ M' = \operatorname{Span}_{\mathbb{Z}}(e_1', \dots, e_n') &\mapsto f' = \sum \psi(e_i, x_j) x_i x_j \end{aligned} \tag{6.7}$$

Proof. Given $M' \in \operatorname{gen}(M)$, choose a basis $e_1', \dots, e_n'$, and let $f' = \sum \psi(e_i', e_j') x_i x_j$ be the associated quadratic form. If $\gamma \in \mathrm{O}(V)$, then $\gamma M' \in \operatorname{gen}(M)$ has basis $\gamma(e_1'), \dots, \gamma(e_n')$, and the associated quadratic form is the same as $\psi(\gamma e_i', \gamma e_j') = \psi(e_i', e_j')$. Thus we have a well-defined map $\mathrm{O}(V) \backslash \operatorname{gen}(M) \to \mathrm{GL}_n(\mathbb{Z}) \backslash \operatorname{gen}(f)$.

If $M', M'' \in \operatorname{gen}(M)$ give rise to the same quadratic form, then they are isomorphic as quadratic modules by Lemma 6.4, and so by the discussion above they are in the same orbit of the orthogonal group. Thus the map is injective.

Now let $f' \in \operatorname{gen}(f)$. Then there exists a quadratic module N over $\mathbb{Z}$ with basis $b_1, \dots, b_n$ giving rise to the quadratic form f' by Lemma 6.4. As $f' \in \operatorname{gen}(f)$, we have that $N_{\mathbb{R}} \sim V_{\mathbb{R}}$, and $N_{\mathbb{Z}_p} \sim M_{\mathbb{Z}_p}$ for all primes p. In particular, if $V' = N_{\mathbb{Q}}$, then $V'_{\mathbb{R}} \sim V_{\mathbb{R}}$, and $V'_{\mathbb{Q}_p} \sim V_{\mathbb{Q}_p}$ for all p. Then by the weak Hasse-Minkowski Theorem 5.2, there exists an isomorphism $\alpha : V \to V'$. Then $\alpha^{-1}(N) \in \operatorname{gen}(M)$ gives rise to the form f'. □

This is a very useful characterization of the genus, as we will now show.

Proposition 6.14. *Let f be a regular quadratic form over $\mathbb{Z}$ and $a \in \mathbb{Z}$. The following are equivalent:*

(i) f represents a over $\mathbb{R}$ and over $\mathbb{Z}_p$ for all p.

(ii) There exists $f' \in \operatorname{gen}(f)$ which represents a over $\mathbb{Z}$.

Before we prove this proposition, we need a lemma.

Lemma 6.15. *Let V be a quadratic space over $\mathbb{Q}$ and $M \subseteq V$ a $\mathbb{Z}$-lattice. Then there exists a bijection between:*

1. $\{M' \subseteq V \text{ } \mathbb{Z}\text{-lattice}\}$.
2. $\{(M'_p)_p \mid \forall p,\ M'_p \subseteq V_{\mathbb{Q}_p} \text{ is a } \mathbb{Z}\text{-lattice, and for all but finitely many } p,\ M'_p = M_{\mathbb{Z}_p}\}$.

This is a generalization of the fact that the image of the map

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}^{\mathbb{Z}} \\ n &\mapsto v_p(n) \end{aligned} \tag{6.8}$$

has image equal to those tuples which are 0 for all but finitely many indices.

Slogan: Any element of $\mathrm{gen}(M)$ is only finitely many primes away from M.

Slogan: Elements of $\mathrm{gen}(M)$ differ by a denominator.

Proof. The map $1 \to 2$ is given by $M' \mapsto (M'_{\mathbb{Z}_p})_p$.

First we will show the map is well-defined. For each M', we can find N such that $NM \subseteq M' \subseteq \frac{1}{N}M$. This is true because we can find $\gamma \in \mathrm{GL}_n(\mathbb{Q})$ mapping $M \to M'$, and the denominators of γ will be bounded. Thus we have that $M_{\mathbb{Z}_p} = M'_{\mathbb{Z}_p}$ for any $p \nmid N$, as if $p \nmid N$ then $NM_{\mathbb{Z}_p} = M_{\mathbb{Z}_p} = \frac{1}{N}M_{\mathbb{Z}_p}$.

Next we will show injectivity. Once N is fixed (so once the finite set of primes for which $M'_p \neq M_{\mathbb{Z}_p}$ is bounded), M' is determined by $M'/NM \subseteq \frac{1}{N}M/NM$ (this is equivalent to the statement that if $A/H = B/H \subseteq G/H$ then $A = B$). $\frac{1}{N}M/NM$ is a finite abelian group, so it decomposes as a sum of its p-parts:

$$\begin{aligned}\frac{1}{N}M/NM &= \bigoplus_{p|N}(\frac{1}{N}M/NM)[p^\infty] \\ &= \bigoplus p \mid N \frac{1}{N}M_{\mathbb{Z}_p}/NM_{\mathbb{Z}_p}. \end{aligned} \tag{6.9}$$

Also, $M'/NM \subseteq \frac{1}{N}M/NM$ is determined by its p-parts, and

$$M'/NM[p^\infty] = M'_{\mathbb{Z}_p}/NM_{\mathbb{Z}_p}, \tag{6.10}$$

so M' is determined by $(M'_{\mathbb{Z}_p})_p$. Thus if $(M'_{\mathbb{Z}_p})_p = (M''_{\mathbb{Z}_p})_p$ then $M' = M''$, so the map is injective.

Finally we show surjectivity. Given some $(L_p)_p$ in set 2, we can find $N \in \mathbb{N}$ such that for all p,

$$NM_{\mathbb{Z}_p} \subseteq L_p \subseteq \frac{1}{N}M_{\mathbb{Z}_p}. \tag{6.11}$$

This is true because at the primes where $M_{\mathbb{Z}_p} = L_p$, we can take $v_p(N) = 0$. At the finite set of primes where $M_{\mathbb{Z}_p} \neq L_p$, we have that $\frac{1}{p^{e_p}}M_{\mathbb{Z}_p} \subseteq L_p \subseteq p^{e_p}M_{\mathbb{Z}_p}$ for some e_p, and taking $N = \prod p^{e_p}$ gives the desired N. Set $M' = L + NM$, where $L \subseteq \frac{1}{N}M/NM$ is the unique subgroup such that $L/NM[p^\infty] = L_p/NM_{\mathbb{Z}_p}$ for all primes p. Then arguing as above we have that $M'_{\mathbb{Z}_p} = L_p$ for all p. We also need to show that M' is a $\mathbb{Z}$-lattice, so that the form ψ takes integer values on M'. But ψ takes $\mathbb{Z}_p$-values on $L_p = M'_{\mathbb{Z}_p}$ as L_p is a $\mathbb{Z}_p$-lattice, and if $a \in \mathbb{Q}$ then $a \in \mathbb{Z}$ if and only if $a \in \mathbb{Z}_p \subseteq \mathbb{Q}_p$ for all p, so we are done. □

We can now prove the proposition.

Proof of Proposition 6.14. Using Proposition 6.13, we have the following coordinate free formulation:

Let V be a regular quadratic space over $\mathbb{Q}$, $M \subseteq V$ a $\mathbb{Z}$-lattice, and $a \in \mathbb{Z}$. Then we want to show that $M_{\mathbb{Z}_p}$ represents a for all p and $M_{\mathbb{R}}$ represents a if and only if there exists $M' \in \mathrm{gen}(M)$ such that M' represents a.

If there exists $M' \in \mathrm{gen}(M)$ that represents a, then $M'_{\mathbb{Z}_p} \sim M_{\mathbb{Z}_p}$ represents a for all p and $M'_{\mathbb{R}} \sim M_{\mathbb{R}}$ represents a, so we are done.

Now suppose $M_{\mathbb{Z}_p}$ represents a for all p and $M_{\mathbb{R}}$ represents a. By the Hasse-Minkowski theorem we have that V represents a, so there exists $u \in V \setminus \{0\}$ such that $\psi(u, u) = a$.

Let $S = \{p \mid u \notin M_{\mathbb{Z}_p}\}$. Let $e_1, \ldots, e_n$ be a $\mathbb{Z}$-basis for M. Then as $u \in V$, we have that $u = a_1 e_1 + \cdots + a_n e_n$ for some $a_i \in \mathbb{Q}$. Let N be the least common multiple of the denominators of the a_is. Then if $p \nmid N$, $u \in M_{\mathbb{Z}_p}$. Thus S is the set of primes dividing N, so S is a finite set. If $p \in S$, then $M_{\mathbb{Z}_p}$ represents a, so there exists $u_p \in M_{\mathbb{Z}_p} \setminus \{0\}$ such that $\psi(u_p, u_p) = a$. Then by Witt's lemma Theorem 2.14, there exists $g_p \in \mathrm{O}(V_{\mathbb{Q}_p})$ such that $g_p(u_p) = u$.

By Lemma 6.15, there exists a $\mathbb{Z}$-lattice $M' \subseteq V$ such that $M'_{\mathbb{Z}_p} = M_{\mathbb{Z}_p}$ if $p \notin S$ and $M'_{\mathbb{Z}_p} = g_p(M_{\mathbb{Z}_p})$ if $p \in S$. Then by (6.6) we have that $M' \in \mathrm{gen}(M)$.

To complete the proof, we need to show that $u \in M'$, so that M' represents $\psi(u, u) = a$. We have that $u \in V = M \otimes_{\mathbb{Z}} \mathbb{Q}$, so fixing a $\mathbb{Z}$-basis $e'_1, \ldots, e'_n$ for M', we have that $u = b_1 e'_1 + \cdots + b_n e'_n$ for some $b_i \in \mathbb{Q}$, and we have that $u \in M$ if and only if $b_i \in \mathbb{Z}$. We can instead check that $b_i \in \mathbb{Z}_p$ for all p, or equivalently that $u \in M'_{\mathbb{Z}_p}$ for all p. If $p \notin S$, then $u \in M_{\mathbb{Z}_p} = M'_{\mathbb{Z}_p}$. If $p \in S$, then $u_p \in M_{\mathbb{Z}_p}$, and $g_p(u_p) = u$ by construction, so $u \in M'_{\mathbb{Z}_p}$ as $g_p(M_{\mathbb{Z}_p}) = M'_{\mathbb{Z}_p}$ also by construction. □

The previous proposition demonstrates the general Principle 6.1 stated above that to work with quadratic forms over $\mathbb{Z}$ we first enumerate the genera, and then work within each genus.

6.3 Representating integers by a sum of 3 squares

We now demonstrate that we have actually done something useful by returning to the problem of representation of integers by the sum of three integers squares.

Proposition 6.16. *Let p be a prime and $a \in \mathbb{Z}_p \setminus \{0\}$. Then a is represented by $x^2 + y^2 + z^2$ over $\mathbb{Z}_p$ if and only if either p is odd, or $p = 2$ and $-a \notin (\mathbb{Z}_2)^2$.*

Proof. First note that if $b \in \mathbb{Z}_p \setminus \{0\}$, then b is represented by $x^2 + y^2$ if and only if

$$\begin{cases} \text{always} & p \equiv 1 \mod 4 \\ v_p(b) \text{ is even} & p \equiv 3 \mod 4 \\ b \in 2^m(1 + 4\mathbb{Z}_2) \text{ for some } m \geq 0 & p = 2 \end{cases} \tag{6.12}$$

If $p \equiv 1 \mod 4$, we have that $i \in \mathbb{Z}_p$, so we can take $x = (b+1)/2$ and $y = i(b-1)/2$. If $p \equiv 3 \mod 4$ or $p = 2$, this follows from the fact that $x^2 + y^2$ is the norm form for $\mathbb{Z}_p[i]$, so $b \in \mathbb{Z}_p$ is represented if and only if b is a norm. See Example 5.7 for the details.

We use the representation of $x^2 + y^2$ to deduce that of $x^2 + y^2 + z^2$.

If $p \equiv 1 \mod 4$, then $x^2 + y^2 + z^2$ represents $\mathbb{Z}$.

If $p \equiv 3 \mod 4$, then all elements with even valuation are represented by $x^2 + y^2$, so it suffices to show that pu with $u \in \mathbb{Z}_p^\times$. But $pu = (-1 + pu) + 1$, and $(-1 + pu)$ is represented by $x^2 + y^2$, and 1 is represented by z^2, so we are done.

If $p = 2$, we need to check that $3 + 8v$, $2(3 + 8v)$ with $v \in \mathbb{Z}_2$ are represented. This is because we already know that $-a \notin (\mathbb{Z}_2)^2$ is a necessary condition, as it is a necessary condition over $\mathbb{Q}_2$ (see Example 5.7). To show that it is a sufficient condition, we need to check the cases not already covered by $x^2 + y^2$, which are precisely $3 + 8v$ and $2(3 + 8v)$. We have that $3 + 8v = 2 + 8v + 1 = 2(1 + 4v) + 1$. The first term is represented by $x^2 + y^2$, and the second by z^2. Likewise, we have that $2(3 + 4v) = (5 + 8v) + 1$. □

Using Proposition 6.14 and a bit of Hensel's Lemma magic, we have the following corollary:

Corollary 6.17. *If $a \in \mathbb{N}$, then a is represented by $\mathrm{gen}(x^2+y^2+z^2)$ if and only if a is not of the form $4^b(7+8c)$ with $b, c \in \mathbb{Z}$.*

In fact, $\mathrm{gen}(x^2+y^2+z^2)$ has only one element, so a is represented by $x^2+y^2+z^2$ if and only if a is not of the form $4^b(7+8c)$ with $b, c \in \mathbb{Z}$. We will now show this. We will need the following theorem, which we will not prove.

Theorem 6.18 (Minkowski)**.** *Let $C \subseteq \mathbb{R}^n$ be a compact, centrally symmetric (so that $C = -C$), convex subset with $\mathrm{vol}(C) \geq 2^n$. Then $C \cap (\mathbb{Z}^n \setminus \{0\})$ is nonempty.*

Proposition 6.19. $\mathrm{gen}(x^2+y^2+z^2) = \mathrm{GL}_3(\mathbb{Z}) \cdot (x^2+y^2+z^2)$.

Proof. We'll show that if g is a positive definite quadratic form of rank 3 over $\mathbb{Z}$ with $d(g) = 1$, then $g \sim f = x^2+y^2+z^2$. Then as $\mathrm{gen}(x^2+y^2+z^2)$ is a subset of this set of forms, this claim implies the proposition.

Claim 1: It suffices to show that there exists $\mathbf{x} \in \mathbb{Z}^3$ such that $g(\mathbf{x}) = 1$.

Proof: Suppose such an $\mathbf{x} \in \mathbb{Z}^3$ exists. We have that $\mathbb{Q}^3 = (\mathbb{Q}\mathbf{x}) \oplus (\mathbb{Q}\mathbf{x})^\perp$, and if $v \in \mathbb{Z}^3$, then

$$\begin{aligned} v &= (\psi(v,\mathbf{x})\mathbf{x}) + (v - \frac{\psi(v,\mathbf{x})}{\psi(\mathbf{x},\mathbf{x})}\mathbf{x}) \\ &= (\psi(v,\mathbf{x})\mathbf{x}) + (v - \psi(v,\mathbf{x})\mathbf{x}) \end{aligned} \tag{6.13}$$

We have that $v - \psi(v,\mathbf{x})\mathbf{x} \in ((\mathbb{Q}\mathbf{x})^\perp \cap \mathbb{Z}^3)$, so $\mathbb{Z}^3 = (\mathbb{Z}\mathbf{x}) \oplus ((\mathbb{Q}\mathbf{x})^\perp \cap \mathbb{Z}^3)$. $\mathbb{Z}^3 = (\mathbb{Z}\mathbf{x}) \oplus ((\mathbb{Q}\mathbf{x})^\perp \cap \mathbb{Z}^3)$ is a rank 2 positive definite lattice of determinant 1. Any rank 2 positive definite lattice of determinant 1 is equivalent to x^2+y^2, so we have that $g \sim x^2+y^2+z^2$ as desired. □

Thus is suffices to prove the following claim.

Claim 2: there exists $\mathbf{x} \in \mathbb{Z}^3$ such that $g(\mathbf{x}) = 1$.

Proof: We use Minkowski's theorem. Let

$$C_\lambda = \{v \in \mathbb{R}^3 \mid |g(v)|^{1/2} \leq \lambda\}. \tag{6.14}$$

Over $\mathbb{R}$, g is equivalent to $x^2+y^2+z^2$, so C_λ is the image of the unit ball under some linear map with determinant 1. Then $\mathrm{vol}(C_\lambda) = \frac{4}{3}\pi\lambda^3$. We want $\frac{4}{3}\pi\lambda^3 \geq 2^3$, so $\lambda \geq \frac{2}{3\sqrt[3]{\frac{4}{3}\pi}} = 1.24.... < \sqrt{2}$. Choose $\lambda \geq \frac{2}{3\sqrt[3]{\frac{4}{3}\pi}}$. Then Minkowski's Theorem 6.18 implies that there exists $v \in \mathbb{Z}^3 \setminus \{0\}$ such that $|g(v)|^{1/2} < \sqrt{2}$, so $|g(v)| < 2$, so $g(v) = 1$ because g is positive definite and integer valued. This completes the proof of the claim and hence the proposition. □

Proposition 6.19 allows us to give the following strengthening of Corollary 6.17.

Corollary 6.20. *If $a \in \mathbb{N}$, then a is represented by $x^2+y^2+z^2$ if and only if a is not of the form $4^b(7+8c)$ with $b, c \in \mathbb{Z}$.*

Thus we have shown how the theory of genera can be used to solve the representation problem, at least in a special case.

We now study classification of quadratic forms over rings. We first give a group theoretic description of genera.

6.4 Group-theoretic description of genera

Let $M \subseteq V$ be a $\mathbb{Z}$-lattice in a regular quadratic space V. We have that following group schemes/group functors:

$$\begin{aligned} \mathrm{GL}_V : \text{commutative } \mathbb{Q}-\mathsf{alg} &\to \mathsf{Group} \\ R &\mapsto \mathrm{Aut}_R(V \otimes_{\mathbb{Q}} R) \end{aligned} \tag{6.15}$$

$$\begin{aligned} \mathrm{GL}_M : \text{commutative } \mathbb{Z}-\mathsf{alg} = \mathsf{Ring} &\to \mathsf{Group} \\ R &\mapsto \mathrm{Aut}_R(M \otimes_{\mathbb{Z}} R) \end{aligned} \tag{6.16}$$

We have, for example, $\mathrm{GL}_M \times_{\mathrm{Spec}\,\mathbb{Z}} \mathrm{Spec}\,\mathbb{Q} = \mathrm{GL}_V$, and $\mathrm{GL}_V(\mathbb{Q}_p) = \mathrm{GL}(V_{\mathbb{Q}_p})$.

We want to take R to be the ring of finite adeles, which is defined as

$$\begin{aligned} \mathbb{A}^\infty &= \prod_p{}' \mathbb{Q}_p \\ &= \{(x_p)_p \in \mathbb{Q}_p \mid x_p \in \mathbb{Z}_p \text{ for all but finitely many } p\}. \end{aligned} \tag{6.17}$$

We then have that

$$\mathrm{GL}_V(\mathbb{A}^\infty) = \prod_p{}' \mathrm{GL}(V_{\mathbb{Q}_p}) = \{(g_p)_p \in \prod_p \mathrm{GL}(V_{\mathbb{Q}_p}) \mid g_p \in \mathrm{GL}(M_{\mathbb{Z}_p}) \text{ for all but finitely many } p\} \tag{6.18}$$

and the definition is independent of the choice of lattice.

Lemma 6.15 gives a bijection between the set of all lattices $M' \subseteq V$ and the set of tuples $(M''_p)_p$ of $\mathbb{Z}_p$-lattices $M''_p \subseteq V_{\mathbb{Q}_p}$ such that $M''_p = M_{\mathbb{Z}_p}$ for all but finitely p. Thus the $\mathrm{GL}_V(\mathbb{A}^\infty)$ acts transitively on the set of lattices in V by

$$(g_p)_p \cdot (M''_p)_p = (g_p(M''_p))_p \tag{6.19}$$

The action is transitive because we can map any two $\mathbb{Z}_p$-bases to each by some element of $\mathrm{GL}(V_{\mathbb{Q}_p})$, and any two lattices only differ by finitely many primes. The stabilizer will be the set of matrices which do not change M_p for each p, which are

$$\mathrm{Stab}_{\mathrm{GL}_V(\mathbb{A}^\infty)}(M) = \prod_p \mathrm{GL}_M(\mathbb{Z}_p) = \mathrm{GL}_M(\hat{\mathbb{Z}}), \tag{6.20}$$

where $\mathbb{Z} = \prod p = \varprojlim \mathbb{Z}/n\mathbb{Z}$ are the profinite integers. Thus the orbit stabilizer theorem gives a bijection between lattices $M \subseteq V$ and $\mathrm{GL}_V(\mathbb{A}^\infty)/\,\mathrm{GL}_M(\hat{\mathbb{Z}})$.

Furthermore, we know that if $M' \subseteq V$ is a $\mathbb{Z}$-lattice in V, then it lies in $\mathrm{gen}(M)$ if and only if for all p, there exists $g_p \in \mathrm{O}(V_{\mathbb{Q}_p})$ such that $g_p(M_{\mathbb{Z}_p}) = M'_{\mathbb{Z}_p}$. So there's a bijection

$$\begin{aligned} \mathrm{gen}(M) &\Leftrightarrow \mathrm{O}_V(\mathbb{A}^\infty)/\mathrm{O}_M(\hat{\mathbb{Z}}) \\ (g_p(M_{\mathbb{Z}_p}))_p &\leftarrow (g_p)_p \end{aligned} \tag{6.21}$$

This gives a group theoretic description of the genus, and we want to descend to a group theoretic description of the equivalence classes of the genus. By the discussion at the start of Section 6.2,

two lattices are equivalent as quadratic modules over $\mathbb{Z}$ if and only if they are conjugate under the action of the orthogonal group $\mathrm{O}(V)$. So taking quotients gives a bijection

$$\mathrm{O}(V)\backslash \operatorname{gen}(M) \Leftrightarrow \mathrm{O}_V(\mathbb{Q})\backslash \mathrm{O}_V(\mathbb{A}^\infty)/\mathrm{O}_M(\hat{\mathbb{Z}}). \tag{6.22}$$

This gives a purely group-theoretic description of the equivalence classes in the genus. The right hand side is a space which supports automorphic representations, which we will discuss more later.

Now, let's return to classification problem.

6.5 Classification

Let's look at the genera of unimodular $\mathbb{Z}$-lattices $M \subseteq V$. We have the following invariants:

1. The discriminant $d(M) \in \{\pm 1\}$.
2. (r, q)-signature: $V_{\mathbb{R}} \sim_{\mathbb{R}} \langle -1\rangle^r \oplus \langle -1\rangle^q$ (recall the classification of quadratic forms over $\mathbb{R}$).
3. Parity: We say that M is even if for all $v \in M_{\mathbb{Z}_2}$, $\psi(v, v) \in 2\mathbb{Z}_2$. Otherwise it is odd. The module is even if all the diagonal entries are even, and odd otherwise.

Example 6.21. The form $2xy$ corresponding to the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is even and the form $x^2 - y^2$ corresponding to the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ is odd. These two modules are equivalent over $\mathbb{Q}$ and even over $\mathbb{R}$, but they lie in different genera.

These 3 invariants are sufficient to classify all unimodular genera.

Proposition 6.22. *Let $n \geq 3$, $r, q \in \mathbb{Z}_{\geq 0}$ with $r + q = n$. Then*

1. *There exists a unique genus of odd unimodular $\mathbb{Z}$-lattices of signature (r, q).*
2. *There exists a genus of even unimodular $\mathbb{Z}$-lattices if and only if $r \equiv q \mod 8$. In this case, the genus is unique.*

Proof sketch.

1. We need to exhibit a regular quadratic space $V/\mathbb{Q}$ such that there exists an odd unimodular lattice $M \subseteq V$ with $V_{\mathbb{R}} \sim \langle -1\rangle^r \oplus \langle -1\rangle^q$. Then we need to show that any other V' with this property satisfies $V' \sim V$ and that for all p, $\mathrm{O}(V_{\mathbb{Q}_p})$ acts transitively on the unimodular $\mathbb{Z}_p$-lattices in $V_{\mathbb{Q}_p}$, as then all the lattices in V lie in the same genus (see (6.6)). So we will show that V is determined, and then that M is determined.

If $M \subseteq V$ is odd unimodular, then $d(M) \equiv (-1)^q$. In order to show that V is determined, it suffices to show that it is determined locally by the weak Hasse-Minkowski theorem 5.2.

If p is odd, we can use the following version of Hensel's lemma.

Lemma 6.23 (Hensel's lemma for unimodular quadratic forms over $\mathbb{Z}_p$)**.** *If f, g are quadratic forms over $\mathbb{Z}_p$ with p odd, $d(f), d(g) \in \mathbb{Z}_p^\times$, and $f \mod p \sim_{\mathbb{F}_p} g \mod p$, then $f \sim_{\mathbb{Z}_p} g$.*

In Section 3 we determined that quadratic forms over finite fields of characteristic not 2 are classified by their determinant. Thus if such a V and such an M exist, we must have

$$M_{\mathbb{Z}_p} \sim_{\mathbb{Z}_p} \langle 1\rangle^r \oplus \langle -1\rangle^q \tag{6.23}$$

Then tensoring up to $\mathbb{Q}_p$ we have that

$$V_{\mathbb{Q}_p} \sim_{\mathbb{Q}_p} \langle 1\rangle^r \oplus \langle -1\rangle^q \tag{6.24}$$

So if M and V exist, then the determinant is fixed, $V_{\mathbb{R}}$ is fixed, and $V_{\mathbb{Q}_p}$ is fixed for all odd p. We know by Corollary 5.3, 5.5 that V is determined by $d(V)$ and $c(V)$, and we can freely choose $d(V)$ and $c(V)$ as long as they are compatible over $\mathbb{R}$. Thus there's a unique V up to isomorphism such that $d(V) \equiv (-1)^q$, $V_{\mathbb{R}} \sim_{\mathbb{R}} \langle 1\rangle^r \oplus \langle -1\rangle^q$, and $V_{\mathbb{Q}_p} \sim_{\mathbb{Q}_p} \langle 1\rangle^r \oplus \langle -1\rangle^q$ for any odd prime p. At $p = 2$ everything works out also as there is only one choice for the Clifford invariant by (5.4). Thus V is uniquely determined.

To show that this V admits an odd unimodular $\mathbb{Z}$-lattice, by Lemma 6.15 we need to check that $V_{\mathbb{Q}_p}$ admits a unimodular $\mathbb{Z}_p$-lattice for every prime p which is odd for $p = 2$. To show uniqueness, by (6.6) we need to show that locally the $\mathbb{Z}_p$-lattices are unique up to the action of $\mathrm{O}(V_{\mathbb{Q}_p})$.

If p is odd, the existence is clear, and the uniqueness follows from the version of Hensel's lemma stated above. If $p = 2$, we can show that any regular quadratic space W over $\mathbb{Q}_2$ admits a unique $\mathrm{O}(W)$-orbit of odd unimodular $\mathbb{Z}_2$-lattices. To our knowledge, there is not a nice proof of this result, so we won't prove it. This proves part 1.

2. If W is a regular quadratic space of rank n over $\mathbb{Q}_2$, it is a fact that W has an even unimodular $\mathbb{Z}_2$-lattice if and only if $n = 2m$ is even and $W \sim H^m$, or $W \sim H^{m-1} \oplus \left\langle \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \right\rangle$. We can check that in this case, the lattice is unique up to the action of $\mathrm{O}(W)$.

In part 1, we explicitly determined the unimodular lattice at every odd prime, and showed that there was only one choice at $p = 2$, if such a choice existed. We then were saved by the result that any regular quadratic space over $\mathbb{Q}_2$ admits an unique odd unimodular lattice, so such a choice does exist.

But in this case, we need to determine when there exists a regular quadratic space V over $\mathbb{Q}$ such that

1. $V_{\mathbb{R}} \sim \langle 1\rangle^r \oplus \langle -1\rangle^q$
2. $V_{\mathbb{Q}_p} \sim \langle 1\rangle^r \oplus \langle -1\rangle^q$ for all odd primes p
3. $V_{\mathbb{Q}_2} \sim H^m$ or $V_{\mathbb{Q}_2} \sim H^{m-1} \oplus \left\langle \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \right\rangle$.
4. $d(V) \equiv (-1)^q$.

But $H^{m-1} \oplus \left\langle \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \right\rangle$ has determinant 3 so we can remove it immediately. We can compute the Clifford invariant in each case, and we need to decide if the local Clifford invariants come from an element of $\mathrm{Br}(\mathbb{Q})[2]$. If we do this computation, we find that such a V exists if and only if $r \equiv q \bmod 8$, and in this case it is uniquely determined up to isomorphism. Then the work we have done shows that there is a unique genus of even unimodular lattices in V.

□

Let $\mathrm{I}_{r,q}$ denote the unique genus of odd unimodular forms of signature (r,q), and $\mathrm{II}_{r,q}$ denote the unique genus of even unimodular forms of signature (r,q), which exists if and only if $r \equiv q \mod 8$. Classifying equivalence classes within each genus is difficult, and depends on (r,q). We'll introduce the notion of the spin group and the spinor genus, and use them to show that if $r, q \neq 0$, so the form is (positive/negative) definite, then $\mathrm{I}_{r,q}$ and $\mathrm{II}_{r,q}$ have a single equivalence class. In the definite case where $r = 0$ or $q = 0$, computing the equivalence classes is a hard computational problem, and we'll develop a reasonable method of doing so.

Before we do that, we'll give an example to show that computing the genus in the definite case is difficult. In this case, some information is given by the Smith-Minkowski-Siegel mass formula.

Definition 6.24 (Smith-Minkowski-Siegel mass formula)**.** Let $M \subseteq V$ be a $\mathbb{Z}$-lattice, where $V_{\mathbb{R}}$ is positive definite, $n \geq 3$. Then there is a canonical measure, the *Tamagawa measure*, on the group $\mathrm{SO}_V(\mathbb{A})$ with the property that

$$\mathrm{vol}(\mathrm{SO}_V(\mathbb{Q})\backslash \mathrm{SO}_V(\mathbb{A})) = 2 \tag{6.25}$$

Remark 6.25. A measure if a functional on the space of continuous compactly supported functions. It is a fact that any locally compact topological group G has a unique measure (up to rescaling), the *Haar measure*, which is invariant under left translation. If G is compact, then there is a canonical normalization which gives the group volume 1. The group $\mathrm{SO}_V(\mathbb{A})$ is not compact, but there is canonical normalization the Haar measure on this group which works over any number field. Under the Tamagawa measure, the group will have a certain volume, the *Tamagawa number*, which is very difficult to compute.

We want to compute the closely related quantity

$$\#\mathrm{O}_V(\mathbb{Q})\backslash \mathrm{O}_V(\mathbb{A}^\infty)/\mathrm{O}_M(\hat{\mathbb{Z}}) \tag{6.26}$$

as this is the number of equivalence classes of lattices in the genus. We can compute this as some sort of volume. This is a bit tricky as the points of (6.26) don't have measure 1. If we use the Tamagawa measure, we get

$$\sum_{M' \in \mathrm{O}(V)\backslash \mathrm{gen}(M)} \frac{1}{\#\mathrm{O}_{M'}(\mathbb{Z})} = (\star), \tag{6.27}$$

where $(\star)$ is some quantity which we can compute. In the case where $\mathrm{gen}(M) = \mathrm{II}_{n,0}$ with $n \equiv 0 \mod 8$, we have that

$$(\star) = 2^{-n/2} \left| \zeta\left(1 - \frac{n}{2}\right) \prod_{j=1}^{n/2-1} \zeta(1-2j) \right| \tag{6.28}$$

where ζ is the Riemann zeta function. The zeta function terms arise from certain Euler products appearing in the Tamagawa measure formula.

If $n = 8$, we get that

$$(\star) = \frac{1}{2^{14} \cdot 3^5 \cdot 5^2 \cdot 7} = \frac{1}{\#\mathrm{O}_{E_8}(\mathbb{Z})} \tag{6.29}$$

where E_8 is the famous root lattice. Thus $\mathrm{II}_{8,0}$ has a unique equivalence class because the left hand side of the formula is "exhausted". This was first proved by Mordell. We also have that

$$\#(\mathrm{II}_{16,0} \,/\, \sim) = 2 \tag{6.30}$$

as proved by Witt,

$$\#(\mathrm{II}_{24,0} \,/\sim) = 24 \tag{6.31}$$

as proved by Niemier (the Leech lattice is one), and

$$\#(\mathrm{II}_{32,0} \,/\sim) =? \tag{6.32}$$

but we know that it is in the millions, which we can show using the mass formula.

7 Spin groups and spinor genus

Let k be a field of characteristic not 2 and V a regular quadratic space over k of rank $n \geq 3$.

7.1 Spin groups and spinor norms

We start off with a bit of motivation because the spin group is a bit weird. Recall (Proposition 2.13 that $\mathrm{O}(V)$ is generated by simple relfections τ_w, where $w \in V$ is an anisotropic vector.

Proposition 7.1. *Define a map*

$$\begin{aligned} \mathrm{sn} : \mathrm{SO}(V) &\to k^\times/(k^\times)^2 \\ g = \tau_{w_1} \cdots \tau_{w_r} &\mapsto \psi(w_1) \cdots \psi(w_r) \mod (k^\times)^2 \end{aligned} \tag{7.1}$$

Then sn *is a well-defined group homomorphism.*

Even the fact that this is well-defined is a bit surprising. sn is the *spinor norm*, and its existence reflects the existence of the spin group. We will define a few things and then see that the spinor norm emerges naturally from these definitions.

Example 7.2. Assume $k = \mathbb{C}$. Then any finite dimensional irreducible representation of $\mathrm{SO}(V)$ gives rise to a finite dimensional representation of the simple Lie algebra $\mathfrak{so}(V)$ by differentiation. We know that two representations of $\mathrm{SO}(V)$ are isomorphic if and only if the representations of Lie algebras are isomorphic, and we know that we can classify the representations of $\mathfrak{so}(V)$ using the theory of roots and weights (cf. Lie algebras). Associated to the fundamental weights of the Lie algebra we have the *fundamental representations*. There is a fundamental representation of $\mathfrak{so}(V)$ that does not integrate to a representation of $\mathrm{SO}(V)$. If we want to get a representation of a group from this representation of $\mathfrak{so}(V)$, we need to replace $\mathrm{SO}(V)$ by its universal cover. As $\mathrm{SO}(V)$ is a complex algebraic group, its universal cover will have the structure of a complex algebraic group. We call this group the *spin group* $\mathrm{Spin}(V)$.

Now lets return to the case where k is any field of characteristic not equal to 2.

Recall the universal property of the Clifford algebra $C(V)$: maps $C(V) \to A$ are in bijection with maps $\alpha : V \to A$ such that $\alpha(V)^2 = \psi(v, v)$. Taking $\alpha = -1$, which maps $v \mapsto -v$, we get a map

$$\begin{aligned} C(-1) : C(V) &\to C(V) \\ v_1 \cdots v_r &\mapsto (-1)^r v_1 \cdots v_r. \end{aligned} \tag{7.2}$$

Likewise, the natural inclusion $V \hookrightarrow C(V)$ induces a map

$$\begin{aligned}(\cdot)' : C(V) &\to C(V)^{\mathrm{op}} \\ v_1 \cdots v_r &\mapsto v_r \cdots v_1.\end{aligned} \tag{7.3}$$

We then devine $\overline{x} = (C(-1)(x))'$, so that $\overline{v_1 \cdots v_r} = (-1)^r v_r \cdots v_1$.

Definition 7.3. The *Clifford group* is defined as follows:

$$\Gamma_V = \{x \in C(V)^\times \mid \forall v \in V,\ C(-1)(x) v x^{-1} \in V\} \tag{7.4}$$

The *Clifford norm* of an element $x \in \Gamma_V$ is defined as $N(x) = x\overline{x}$.

Lemma 7.4.

1. *Γ_V is a group, which acts on V, so there exists a group homomorphism $\rho : \Gamma_V \to \mathrm{Aut}_k(V)$.*
2. *If $w \in V$ is anisotropic, then $w \in \Gamma_V$, $N(w) = \psi(w, w)$, and for all $v \in V$, $\rho(w)(v) = \tau_w(v)$.*
3. *ρ takes values in $\mathrm{O}(V)$, and gives a surjective homomorphism $\Gamma_V \to \mathrm{O}(V)$ with kernel $k^\times$, and $N : \Gamma_V \to k^\times$ is a homomorphism.*

Proof.

1. This follows from definitions. We clearly have that $1 \in \Gamma_V$, and if $x \in \Gamma_V$ then $x^{-1} \in \Gamma_V$. Note that the action on V is essentially just conjugation twisted by multiplication by $(-1)^r$, and it's easy to see this defines a group action.

2. If $w \in V$ is anisotropic, then $w^2 = \psi(w, w)$, so $w^{-1} = w \cdot \psi(w, w)^{-1}$. Also, if $v \in V$, as $vw + wv = 2\psi(v, w)$, we have that

$$\begin{aligned}C(-1)(w) v w^{-1} &= C(-1)(w) v w \psi(w, w) \\ &= -(2\psi(v, w) - vw) w \psi(w, w)^{-1} \\ &= v - \frac{2\psi(v, w)}{\psi(w, w)} w \\ &= \tau_w(v).\end{aligned} \tag{7.5}$$

Thus $w \in \Gamma_V$, and $\rho(w)(v) = \tau_w(v)$.

Also, we have that $N(w) = w(C(-1)(w))' = -w^2 = -\psi(w, w)$.

3. If $x \in \ker(\rho)$, then for all $v \in V$, we have that $C(-1)(x) v x^{-1} = v$. Thus $C(-1)(x)v = vx$. Thus if $x = x_0 + x_1$, where $x_i \in C_i(V)$, then we have that $C(-1)(x_0) = x_0$ and $C(-1)(x_1) = -x_1$ so

$$x_0 v - x_1 v = v x_0 + v x_1. \tag{7.6}$$

Comparing the $C_0(V)$ and $C_1(V)$ parts of both sides gives $x_0 v = v x_0$ and $x_1 v = -v x_1$. Then as $C(V)$ is generated as an algebra by all $v \in V$, we have that $x_0 \in \mathrm{Cent}_{C_0(V)}(C(V))$, the degree 0 part of the centralizer of $C(V)$. By some standard Clifford algebra computations we can determine that $\mathrm{Cent}_{C_0(V)}(C(V)) = k$, and similarly that $x_1 = 0$, so $x \in k^\times$ as x is nonzero.

Next we check that N takes values in $k^\times$ and is a homomorphism. As we have just shown that the stabilizer of the group action is $k^\times$, it suffices to show that if $x \in \Gamma_V$, then $N(x)$ acts trivially on V.

Let $x \in \Gamma_V$ and $v \in V$. Set $C(-1)(x)vx^{-1} = w$ for some $w \in V$. Then $v = C(-1)(x^{-1})wx$, so $v = x'wC(-1)(x^{-1})' = C(-1)(\overline{x})w(\overline{x})^{-1}$. Thus $C(-1)(\overline{x}x)v(\overline{x}x)^{-1} = C(-1)(\overline{x})w\overline{x}^{-1} = v$, so $\overline{x}x$ acts trivially and $\overline{x}x \in k^\times$. Then $x\overline{x}x = \overline{x}xx$, so $x\overline{x} = \overline{x}x$ as $x \in C(V)^\times$. Thus $N(x) = x\overline{x} = \overline{x}x \in k^\times$. Then $N(xy) = xy\overline{(xy)} = xy\overline{y}\overline{x} = x\overline{x}y\overline{y} = N(x)N(y)$. We frequently utilize that $k^\times$ is in the center of V.

If $x \in \Gamma_V$, $w \in V$ is anisotropic, then

$$\begin{aligned} N(C(-1)(x)wx^{-1}) &= N(C(-1)x)N(w)N(x)^{-1} \\ &= N(w) \\ &= -\psi(w,w) \end{aligned} \tag{7.7}$$

as $N(C(-1)x) = N(x) \in k^\times$. We also have that

$$\begin{aligned} N(C(-1)(x)wx^{-1}) &= N(\rho(x)(w)) \\ &= -\psi(\rho(x)(w), \rho(x)(w)). \end{aligned} \tag{7.8}$$

So $\rho(x)$ acts on V and preserves ψ on the anisotropic vectors. Then it must also preserve ψ on the isotropic vectors, so $\rho(x) \in \mathrm{O}(V)$. ρ is surjective as $\tau_w = \rho(w)$ for w anisotropic, and simple reflections generate the orthogonal group.

□

The above lemma has a lot of parts. To summarize, we have the following diagram with exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & k^\times & \longrightarrow & \Gamma_V & \xrightarrow{\rho} & \mathrm{O}(V) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{sn}} & & \\ & & k^\times & \longrightarrow & k^\times & \longrightarrow & k^\times/(k^\times)^2 & \longrightarrow & 1 \end{array}$$

where the map $k^\times \to k^\times$ on the bottom row is given by $\lambda \mapsto \lambda^2$. sn is the *spinor norm*, it is the unique map which makes the diagram commute. It is calculated as follows.

Any $\gamma \in \mathrm{O}(V)$ can be written as $\tau_{w_1} \cdots \tau_{w_r}$ for some anisotropic $w_i \in V$. The preimage in $\Gamma(V)$ is $w_1 \cdots w_r$, and we have that $N(w_1 \cdots w_r) = (-1)^r \psi(w_1) \cdots \psi(w_r)$. We then have that

$$\mathrm{sn}(\gamma) = \mathrm{sn}(\tau_{w_1} \cdots \tau_{w_r}) = (-1)^r \psi(w_1) \cdots \psi(w_r) \mod (k^\times)^2. \tag{7.9}$$

This completes the proof of Proposition 7.1. □

As a consequence of the surjectivity of ρ, we have that

$$\Gamma_V = \{w_1 \cdots w_r \in C(V) \mid r \geq 0,\ w_i \in V \text{ anisotropic}\}. \tag{7.10}$$

We now define the spin group.

Definition 7.5. The *spin group* $\mathrm{Spin}(V)$ is defined as

$$\mathrm{Spin}(V) = \{x \in \Gamma_V \cap C_0(V) \mid N(x) = 1\}. \tag{7.11}$$

As a consequence of (7.10), we have that

$$\mathrm{Spin}(V) = \{w_1 \cdots w_r \mid r \geq 0 \text{ even}, \psi(w_1) \cdots \psi(w_r) = 1\}. \tag{7.12}$$

Define the map

$$\theta : \mathrm{O}(V) \xrightarrow{\mathrm{sn} \times \det} k^\times/(k^\times)^2 \times \{\pm 1\}. \tag{7.13}$$

Then we have an exact sequence

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathrm{Spin}(V) \xrightarrow{\rho} \mathrm{O}(V) \xrightarrow{\theta} k^\times/(k^\times)^2 \times \{\pm 1\}$$

The $\{\pm 1\}$ arises as the kernel of $\rho : \Gamma_V \to \mathrm{O}(V)$ is $k^\times$, and we have that $k^\times \cap \mathrm{Spin}(V) = \{\pm 1\}$. By exactness, the image of $\mathrm{Spin}(V)$ in $\mathrm{O}(V)$ is the elements of $\mathrm{SO}(V)$ with trivial spinor norm. Thus we have the following exact sequence:

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathrm{Spin}(V) \xrightarrow{\rho} \mathrm{SO}(V) \xrightarrow{\mathrm{sn}} k^\times/(k^\times)^2$$

Remark 7.6. Here is another perspective on the above exact sequence. We can define Spin_V as a linear algebraic group over k. Then we have a short exact sequence of group schemes (not of groups!) over k:

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Spin}_V \longrightarrow \mathrm{SO}_V \longrightarrow 1$$

If we take $\overline{k}$ points, then this will be an exact sequence of groups. But if we just take k-points, then we obtain a connecting homomorphism $\delta : \mathrm{SO}(V) \to H^1(k, \mu_2)$. By Hilbert's theorem 90 we have that $H^1(k, \mu_2) = k^\times/(k^\times)^2$, and we can check that δ is in fact the spinor norm sn.

7.2 Spinor genus

Let V be a regular quadratic space over $\mathbb{Q}$, and let

$$\Omega(V_{\mathbb{Q}_p}) = \rho(\mathrm{Spin}(V_{\mathbb{Q}_p})) = \ker(\mathrm{sn} : \mathrm{SO}(V_{\mathbb{Q}_p}) \to \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2) \subseteq \mathrm{SO}(V_{\mathbb{Q}_p}) \tag{7.14}$$

Definition 7.7. Let $M, M' \subseteq V$ be $\mathbb{Z}$-lattices. We say that M, M' are in the same *spinor genus* if there exists $\gamma \in \mathrm{O}(V)$, and for each prime p, $\omega_p \in \Omega(V_{\mathbb{Q}_p})$ such that $M_{\mathbb{Z}_p} = \gamma\omega_p M'_{\mathbb{Z}_p}$.

Let's show that being in the same spinor genus an equivalence relation. This follows from the fact that $\Omega(V_{\mathbb{Q}_p})$ is a normal subgroup, as it is the kernel of the spinor norm. Suppose $M_{\mathbb{Z}_p} = \gamma\omega_p M'_{\mathbb{Z}_p}$, and $M'_{\mathbb{Z}_p} = \delta\eta_p M''_{\mathbb{Z}_p}$ for all p. Then

$$\begin{aligned} M_{\mathbb{Z}_p} &= \gamma\omega_p\delta\eta_p M''_{\mathbb{Z}_p} \\ &= \gamma\delta\delta^{-1}\omega_p\delta\eta_p M''_{\mathbb{Z}_p}. \end{aligned} \tag{7.15}$$

We have that $\gamma\delta \in \mathrm{O}(V)$ and $\delta^{-1}\omega_p\delta\eta_p \in \Omega_{V_{\mathbb{Q}_p}}$ by normality, so $M \sim M''$.

Remark 7.8. The spinor genus is the set of lattices which differ locally by an element of the spin group and globally by an element of the orthogonal group. We might think that a more natural definition is to only check for local equivalence, but then the spinor genus might not be closed under equivalence (recall that two lattices are equivalent if and only if they differ by an element of the orthogonal group).

If M, M' are in the same spinor genus, they are locally equivalent (they differ by an element of the orthogonal group), so they are in the same genus. Thus $\mathrm{gen}(M)$ is a disjoint union of spinor genera, denoted by $\mathrm{spgen}(M')$. We have a group theoretic description of the genus, and we want to obtain a group theoretic description of the spinor genus. The following result gives this. First, define

$$\Omega_V(\mathbb{A}^\infty) = \left(\prod_p \Omega(V_{\mathbb{Q}_p})\right) \cap \mathrm{O}_V(\mathbb{A}^\infty) \tag{7.16}$$

which is the product of the local Ωs with the adelic finiteness condition imposed by intersecting with $\mathrm{O}_V(\mathbb{A}^\infty)$ (see (6.18)). Also, recalling the definition of the map θ in (7.13), define

$$\theta' = \prod_p{}' \theta : \mathrm{O}_V(\mathbb{A}^\infty) \to \prod_p{}' (\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \times \{\pm 1\}) \tag{7.17}$$

where the product on the right hand side is restricted so that

$$\prod_p{}' (\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \times \{\pm 1\}) = \{(x_p(\mathbb{Q}_p^\times)^2, \epsilon_p)_p \mid x_p \in \mathbb{Z}_p^\times(\mathbb{Q}_p^\times)^2 \text{ for all but finitely many } p\}. \tag{7.18}$$

Proposition 7.9. *Let $M \subseteq V$ be a $\mathbb{Z}$-lattice.*
The following sets are in bijection:

1. *The set of spinor genera in* $\mathrm{gen}(M)$.
2. *The quotient* $\mathrm{O}(V)\backslash \mathrm{O}_V(\mathbb{A}^\infty)/\Omega_V(\mathbb{A}^\infty)\mathrm{O}_M(\hat{\mathbb{Z}})$.
3. *The quotient* $\theta'(\mathrm{O}(V))\backslash\theta'(\mathrm{O}_V(\mathbb{A}^\infty))/\theta'(\mathrm{O}_M(\hat{\mathbb{Z}}))$.

Proof. Recall our work in Section 6.4, and (6.21) in particular.

1⇔2: If $M', M'' \in \mathrm{gen}(M)$, then $M' = g'M$ and $M'' = g''M$ where $g', g'' \in \mathrm{O}_V(\mathbb{A}^\infty)$. By definition, M' and M'' are in the same spinor genus if and only if there exists $\gamma \in \mathrm{O}_V(\mathbb{Q}) = \mathrm{O}(V)$ and $\omega = (\omega_p)_p \in \Omega_V(\mathbb{A}^\infty)$ such that for all p, $M'_{\mathbb{Z}_p} = g'_p M_{\mathbb{Z}_p} = \gamma\omega_p M''_{\mathbb{Z}_p} = \gamma\omega_p g''_p M_{\mathbb{Z}_p}$.

This is true if and only if there exists $\gamma \in \mathrm{O}_V(\mathbb{A}^\infty)$, $\omega = (\omega_p)_p \in \Omega_V(\mathbb{A}^\infty)$, $\kappa = (\kappa_p)_p \in \mathrm{O}_M(\hat{\mathbb{Z}})$ such that $g' = \gamma\omega g''\kappa$, where equality is taken in $\mathrm{O}_V(\mathbb{A}^\infty)$. This follows from the fact that $\mathrm{O}_M(\hat{\mathbb{Z}})$ is the stabilizer of $(M_p)_p$ up to equivalence.

Rearranging gives $g' = \gamma g''(g''^{-1}\omega g'')\kappa$, and since Ω_V is a normal subgroup, M' and M'' are in the same spinor genus if and only if g', g'' have the same image in $\mathrm{O}(V)\backslash \mathrm{O}_V(\mathbb{A}^\infty)/\Omega_V(\mathbb{A}^\infty)\mathrm{O}_M(\hat{\mathbb{Z}})$.

2⇔3: Note that θ' is a group homomorphism with kernel $\Omega_V(\mathbb{A}^\infty)$. So the result follows from one of the elementary group theory isomorphism theorems. □

Remark 7.10. $\mathrm{gen}(M)$ is the union of finitely many equivalence classes, so each spinor genus is the union of finitely many equivalence classes, and there are only finitely many spinor genera in each genus. Thus the group appearing in part 3 of the above proposition is a finite abelian group. It is sort of like the 2-torsion of the class group of a quadratic extension, and computing it should be fairly routine.

The next proposition describes the image of $\mathrm{sn}(\mathrm{SO}(V)) \subseteq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$

Proposition 7.11. *Let V be a regular quadratic space over $\mathbb{Q}$ of dimension $n \geq 4$.*

1. *If $V_{\mathbb{R}}$ is indefinite, then $\mathrm{sn}(\mathrm{SO}(V)) = \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. If $V_{\mathbb{R}}$ is definite, then $\mathrm{sn}(\mathrm{SO}(V)) = \mathbb{Q}_{>0}/(\mathbb{Q}^2_{>0}$.*
2. *If $M \subseteq V$ is a unimodular lattice, then $\mathrm{gen}(M) = \mathrm{spgen}(M)$.*

Proof.

1. Lets assume that $V_{\mathbb{R}}$ is positive definite, the other cases follow similarly. Let $v \in V$ be such that $\psi(v) = \alpha > 0$. Take any $\beta \in \mathbb{Q}_{>0}$. Then $V_{\mathbb{R}}$ represents $\alpha\beta$, and $V_{\mathbb{Q}_p}$ represents $\alpha\beta$ for every prime p by Proposition 4.4. By the Hasse-Minkowski theorem we have that there exists $w \in V$ such that $\psi(w) = \alpha\beta$. Then $\tau_v\tau_w \in \mathrm{SO}(V)$, and $\mathrm{sn}(\tau_v\tau_w) \equiv \psi(v)\psi(w) \equiv \alpha^2\beta \equiv \beta \mod (\mathbb{Q}^\times)^2$.

2. Let $M \subseteq V$ be a unimodular $\mathbb{Z}$-lattice. We claim that for any prime p, $\theta(\mathrm{O}_M(\mathbb{Z}_p)) = \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \times \{\pm 1\}$.

If p is odd, then $M_{\mathbb{Z}_p} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ represents all of $\mathbb{F}_p$. By Hensel's Lemma 6.23, for any $u \in \mathbb{Z}_p^\times$, there exists $v \in M_{\mathbb{Z}_p}$ such that $\psi(v) = u$ (exercise). We have that $\tau_v \in \mathrm{O}(V_{\mathbb{Q}_p})$, and we can check that $\tau_v \in \mathrm{O}_M(\mathbb{Z}_p)$, and that $\theta(\tau_v) = (u(\mathbb{Q}_p^\times)^2, -1)$. It follows that $\theta(\mathrm{O}_M(\mathbb{Z}_p))$, which proves the claim.

If $p = 2$, then we need to be more careful, and we omit details. An easy case is when $M_{\mathbb{Z}_2} = H^{n/2}$.

By Proposition 7.9, the set of spinor genera in $\mathrm{gen}(M)$ is in bijection with

$$\theta'(\mathrm{O}(V))\backslash\theta'(\mathrm{O}_V(\mathbb{A}^\infty))/\theta'(\mathrm{O}_M(\hat{\mathbb{Z}})). \tag{7.19}$$

Recalling the definition of θ' (7.17), this is a subquotient (a quotient of a subgroup) of

$$\mathbb{Q}_{>0}\backslash\left(\prod_p{}'(\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \times \{\pm 1\})\right)\Big/\prod_p(\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \times \{\pm 1\}). \tag{7.20}$$

Here, $\mathbb{Q}_{>0}$ is the diagonal embedding, and $\theta'(\mathrm{O}_V(\mathbb{A}^\infty))$ is a subgroup of the middle term as the middle term is the target of θ'. Thus if we show that (7.20) is trivial then $\mathrm{spgen}(M)$ will have 1 element, so $\mathrm{spgen}(M) = \mathrm{gen}(M)$. The $\{\pm 1\}$ terms all cancel, and after quotienting out by $\mathbb{Z}_p^\times$ we are left with the valuations mod 2, so we have that

$$\left(\prod_p{}'(\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \times \{\pm 1\})\right)\Big/\prod_p(\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \times \{\pm 1\}) \cong \bigoplus_p(\mathbb{Z}/2\mathbb{Z}) \tag{7.21}$$
$$(a_p, \epsilon_p)_p \mapsto (v_p(a_p) \mod 2)_p.$$

Thus it suffices to show that

$$\begin{aligned}\mathbb{Q}_{>0} &\to \bigoplus_p(\mathbb{Z}/2\mathbb{Z}) \\ r &\mapsto (v_p(r) \mod 2)\end{aligned} \tag{7.22}$$

is surjective, which is obvious, as for any $(b_p)_p \in \bigoplus_p(\mathbb{Z}/2\mathbb{Z})$, only finitely many terms are nonzero. □

In general, there are multiple spinor genera in a genus.

The spinor genus is easier to work with than the genus, as the spin group satisfies the strong approximation property.

Definition 7.12. Let G be a linear algebraic group of $\mathbb{Q}$, and $S \subseteq M_{\mathbb{Q}}$ a finite set of places. Then G satisfies the *strong approximation property* relative to S if the map

$$G(\mathbb{Q}) \to \prod_{v \notin S}{}' G(\mathbb{Q}_v) = G(\mathbb{A}^S) \tag{7.23}$$

has dense image.

The strong approximation property is extremely powerful. Here is one elementary application.

Example 7.13. SL_n satisfies the strong approximation property relative to $S = \{\infty\}$.

As a consequence, for any $N \in \mathbb{N}$, the map $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$ is surjective, as we will now show. If $\overline{g} \in \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$, it suffices to show that

$$\mathrm{SL}_n(\mathbb{Q}) \cap U_N \tag{7.24}$$

is nonempty, where

$$U_N \coloneqq \{h \in \mathrm{SL}_n(\hat{\mathbb{Z}}) = \prod_p \mathrm{SL}_n(\mathbb{Z}_p) \ \mid \ \forall p \mid N, \ h \equiv \overline{g} \mod p^{v_p(N)}\}. \tag{7.25}$$

But U_N is an open subgroup of $\mathrm{SL}_n(\mathbb{A}^\infty)$, so as $\mathrm{SL}_n(\mathbb{Q})$ is dense in $\mathrm{SL}_n(\mathbb{A}^\infty)$ by strong approximation, $\mathrm{SL}_n(\mathbb{Q}) \cap U_N$ is nonempty. □

The special orthogonal group does satisfy the strong approximation property, but the spin group does.

Theorem 7.14 (Kneser)**.** *If V is a regular quadratic space over $\mathbb{Q}$ of dimension $n \geq 3$, then Spin_V satisfies the strong approximation relative to S if and only if there exists $v \in S$ such that $V_{\mathbb{Q}_v}$ is isotropic.*

For instance, if $n \geq 5$, this is automatically satisfied by Proposition 4.4.

Strong approximation allows us to prove some nice results about spinor genera, as we now show.

Proposition 7.15. *Suppose $M \subseteq V$ is a $\mathbb{Z}$-lattice of rank $n \geq 3$ such that $V_{\mathbb{R}}$ is indefinite. Then* $\mathrm{spgen}(M)$ *consists of a single element.*

Proof. Set $S = \{\infty\}$. Then as $V_{\mathbb{R}} = V_\infty$ is indefinite, and hence isotropic, strong approximation gives that $\mathrm{Spin}_V(\mathbb{Q}) \subseteq \mathrm{Spin}_V(\mathbb{A}^\infty)$ is a dense subgroup.

If $M' \in \mathrm{spgen}(M)$, then by definition there exists $g = (g_p) \in \mathrm{Spin}_V(\mathbb{A}^\infty)$ such that $M'_{\mathbb{Z}_p} = \gamma\rho(g_p)M_{\mathbb{Z}_p}$. Now, we have that

$$\mathrm{Stab}_{\mathrm{Spin}_V(\mathbb{A}^\infty)}(M_{\hat{\mathbb{Z}}}) = \rho^{-1}(\mathrm{SO}_M(\hat{\mathbb{Z}})) \tag{7.26}$$

is an open subgroup. The translate by g is then an open subset of $\mathrm{Spin}_V(\mathbb{A}^\infty)$, so by strong approximation there exists $\delta \in \mathrm{Spin}_V(\mathbb{Q})$ such that for all p, $\rho(\delta)(M_{\mathbb{Z}_p}) = \rho(g_p)(M_{\mathbb{Z}_p})$. Then $M'_{\mathbb{Z}_p} = \gamma\rho(\delta)M_{\mathbb{Z}_p}$ for all p, so $M' = \gamma\rho(\delta)(M)$. □

Thus we have found an instance where the spinor genus has only one element. Proposition 7.11 gave a situation where the spinor genus was equal to the genus, and Proposition 6.22 gave a classification of unimodular genera. Combining these results gives the following corollary.

Corollary 7.16. *Let $M \subseteq V$ and $M' \subseteq V'$ be unimodular $\mathbb{Z}$-lattices of rank $n \geq 4$ such that $V_{\mathbb{R}}, V'_{\mathbb{R}}$ are indefinite. Then $M \sim M'$ if and only if $V_{\mathbb{R}} \sim V'_{\mathbb{R}}$ and M, M' are either both even or both odd.*

Proof. By Proposition 7.15, it suffices to show that M, M' are in the same spinor genus. But by Proposition 7.11, it suffices to show that M and M' are in the same genus. The result then follows from Proposition 6.22. □

Thus we finally have a criteria to check whether two quadratic modules (or lattices) are equivalent, albeit in a very specific case.

7.3 p-neighbors

Our goal is to develop some sort of classification of unimodular $\mathbb{Z}$-lattices. We have done the case where $V_{\mathbb{R}}$ is indefinite. The case where $V_{\mathbb{R}}$ is definie is much harder. Let's discuss the case where $V_{\mathbb{R}}$ is positive definite, focusing on the genus $\mathrm{II}_{n,0} = \mathrm{II}_n$ of even unimodular lattices of rank n with $n \equiv 0 \mod 8$, living inside the quadratic space $V = \langle 1, \dots, 1 \rangle$. The mass formula (6.28) shows that $\#\mathrm{O}(V) \backslash \mathrm{II}_n \to \infty$ as $n \to \infty$.

The concept of p-neighbors provides a somewhat tractable way to calculate the elements of the genus.

Definition 7.17. Let p be an odd prime. We say that $M, M' \in \mathrm{II}_n$ are *p-neighbors* if $[M : M \cap M'] = p = [M' : M \cap M']$.

Let $N_p(M)$ denote the set of p-neighbors of M.

Proposition 7.18. *Let $M \in \mathrm{II}_n$. There is a bijection*

$$N_p(M) \Leftrightarrow \{[\overline{v}] \in \mathbb{P}(M/pM) \mid \psi(\overline{v}, \overline{v}) \equiv 0 \mod p\} \tag{7.27}$$

Proof. If $M' \in N_p(M)$, then $M/M \cap M' \cong M'/M \cap M' \cong \mathbb{Z}/p\mathbb{Z}$, so they are annihilated by p, so

$$pM \subseteq M \cap M' \subseteq M' \tag{7.28}$$
$$pM' \subseteq M \cap M' \subseteq M \tag{7.29}$$

Then $pM \subseteq M' \subseteq \frac{1}{p}M$, so $M_{\mathbb{Z}_q} = M'_{\mathbb{Z}_q}$ if $q \neq p$ is prime. Consider the map

$$\begin{aligned} M' &\to M/pM \\ m' &\mapsto pm' \mod pM \end{aligned} \tag{7.30}$$

which is well-defined as $M' \subseteq \frac{1}{p}M$ so $pM' \subseteq M$. The image of this map is

$$\begin{aligned} pM'/pM &= pM'/(pM' \cap pM) \\ &= pM'/p(M' \cap M) \\ &= M'/(M' \cap M) \cong \mathbb{Z}/p\mathbb{Z} \end{aligned} \tag{7.31}$$

Choose $m' \in M'$ such that $pm' \in M \setminus pM$, and let $\overline{v} = pm' \mod pM$. We have that $\psi(pm', pm') = p^2\psi(m', m') \equiv 0 \mod p^2$, so $\psi(\overline{v}, \overline{v}) \equiv 0 \mod p$. Choose another $m'' \in M'$ such that $pm'' \in M \setminus pM$ and then set $\overline{w} = pm'' \mod pM$. Then as $pM'/pM \cong \mathbb{Z}/p\mathbb{Z}$, $\overline{v}$ and $\overline{w}$ differ by a scalar. Thus $[\overline{v}] = [\overline{w}]$ as elements of $\mathbb{P}(M/pM)$, so we have a well-defined map between the sets in the statement of the proposition.

Let's show the map is injective. Let $m' \in M$ be such that $pm' \in M \setminus pM$. We first claim that

$$M' = \mathbb{Z}m' + M \cap M' = \mathbb{Z}\frac{1}{p}(pm') + \tilde{M}(pm') \tag{7.32}$$

where

$$\tilde{M}(pm') \coloneqq \{w \in M \mid \psi(pm', w) \equiv 0 \mod p\} \tag{7.33}$$

The first inequality follows from (7.28). The second inequality follows from the fact that both $M \cap M'$ and $\tilde{M}(pm')$ have index p in M, and $M \cap M' \subseteq \tilde{M}(pm')$, so $M \cap M' = \tilde{M}(pm')$. This proves the claim.

Now, given $M', M'' \in N_p(M)$, $m' \in M'$, $m'' \in M''$ such that $pm', pm'' \in M \setminus pM$, suppose that $pm' \equiv pm'' \mod pM$. Then using that $pM \subseteq \tilde{M}(pm')$ and $\tilde{M}(pm') = \tilde{M}(pm'')$, (7.32) gives that $M' = M''$. Thus the map is injective.

Now to show surjectivity. This will be a bit of a sketch. Let $\overline{v} \in M/pM$ such that $\psi(\overline{v}, \overline{v}) \equiv 0 \mod p$. To construct M' it suffices to find $M'_p \subseteq V_{\mathbb{Q}_p}$ such that $[M'_p : M_{\mathbb{Z}_p} \cap M'_p] = p$, $[M_{\mathbb{Z}_p} : M_{\mathbb{Z}_p} \cap M'_p] = p$, and such that if $m'_p \in M'_p \setminus M_{\mathbb{Z}_p}$, then $pm'_p \equiv \overline{v} \mod pM_{\mathbb{Z}_p}$.

To do so, we first split off a copy of the hyperbolic plane: we can find $\overline{w} \in M/pM$ such that $\psi(\overline{v}, \overline{w}) = 1$ and $\psi(\overline{w}, \overline{w}) = 0>$ Then Hensel's lemma says that we can lift $\overline{v}$, $\overline{w}$ to $v, w \in M_{\mathbb{Z}_p}$ such that $\psi(v, v) = 0$, $\psi(v, w) = 1$, $\psi(w, w) = 0$, and $M_{\mathbb{Z}_p} = (\mathbb{Z}_p v \oplus \mathbb{Z}_p w) \oplus N_p$ as we are splitting a lattice with unit determinant off from a lattice with unit determinant.

We can then take $M'_p = \langle \frac{v}{p} \rangle \oplus \langle pw \rangle \oplus N_p$. Then the obvious diagonal matrix which transforms $M_p \to M'_p$ does not change the Gram matrix, and hence is an element of $\mathrm{O}(V_{\mathbb{Q}_p})$, so $M'_p \in \mathrm{gen}(M_{\mathbb{Z}_p})$. □

The next proposition shows that any two elements of II_n are linked by a sequence of p-neighbors.

Proposition 7.19. *Let $M, M' \in \mathrm{II}_n$ and p an odd prime. Then there exists $M = M_0, M_1, \ldots, M_k \in \mathrm{II}_n$ such that*

1. *For all $i = 0, \ldots, k-1$, $M_{i+1} \in N_p(M_i)$.*
2. *$M_k \in \mathrm{O}(V) \cdot M'$.*

Proof. Let $M' \in \mathrm{spgen}(M)$, and recall that $\mathrm{gen}(M) = \mathrm{spgen}(M)$ by Proposition 7.11. Then there exists $\gamma \in \mathrm{O}(V)$ and $g = (g_q)_q \in \mathrm{Spin}_V(\mathbb{A}^\infty)$ such that for all q, $M'(\mathbb{Z}_q) = \gamma\rho(g_q)M_{\mathbb{Z}_q}$. Then $M_{\mathbb{Z}_p}$ is isotropic, so Spin_V satisfies strong approximation with respect to $S = \{p, \infty\}$, so $\mathrm{Spin}_V(\mathbb{Q}) \subseteq \mathrm{Spin}_V(\mathbb{A}^S)$ is dense. By the same argument as in the proof of Proposition 7.15, there exists $\delta \in \mathrm{Spin}_V(\mathbb{Q})$ such that $\rho(\delta)(M_{\mathbb{Z}_q}) = \rho(g_q)(M_{\mathbb{Z}_q})$ if $q \neq p$. Thus $M'_{\mathbb{Z}_q} = \gamma\rho(\delta)M_{\mathbb{Z}_q}$ if $q \neq p$. If we replace M' by $(\gamma\rho(\delta))^{-1}(M')$ (which is equivalent to M' as it is conjugated by an element of the orthogonal group), we have that $M'_{\mathbb{Z}_q} = M_{\mathbb{Z}_q}$ for all $q \neq p$.

Equivalently, we have that $M_{\mathbb{Z}[1/p]} = M'_{\mathbb{Z}[1/p]}$. In this case, we show by induction on $[M : M \cap M']$ that M and M' can be linked by a chain of p-neighbors. If $[M : M \cap M'] = 1$, then $M = M'$ so we are done.

Suppose $[M : M \cap M'] > 1$, and let p^k be the exponent of $M/M \cap M' \cong (M + M')/M'$, so that $p^k M \subset M \cap M'$, but $p^{k-1} M \not\subset M \cap M'$. In particular, we have that $k \geq 1$. Consider the map

$$\begin{aligned} M &\to M'/pM' \\ m &\mapsto p^k m. \end{aligned} \tag{7.34}$$

This is well-defined because $p^k M \subset M \cap M'$. It is a nonzero map as otherwise $p^k M \subset pM'$, so $p^{k-1} M \subset M'$, a contradiction as we are choosing k to be as small as possible.

So there exists $m \in M$ such that $p^k m \in M' \backslash pM'$. Then $\psi(p^k m, p^k m) \equiv 0 \mod p^2$, so arguing as in the proof of Proposition 7.18 we have that

$$M'' \coloneqq \mathbb{Z} p^{k-1} M + \{w \in M' \mid \psi(p^k m, w) \equiv 0 \mod p\} \in N_p(M') \tag{7.35}$$

is a p-neighbor of M'.

We claim that $[M : M \cap M''] < [M : M \cap M']$. If this holds, then we are done by induction. The claim holds if and only if $[M'' : M \cap M''] < [M' : M \cap M'']$, if and only if $[M'' + M : M] < [M' + M : M]$. We have that $M'' + M \subseteq M' + M$, so the claim holds if and only if the inclusion is strict. The strict inclusion follows from the defining formula for M'. □

This proposition is powerful as it allows us to choose *any* odd prime p. Note how strong approximation was essential in all this.

Remark 7.20. The proposition gives an algorithm to enumerate $\mathrm{O}(V) \backslash \mathrm{II}_n$. We start with some "base point" lattice. For example, we can choose

$$E_n = \{\mathbf{x} \in \mathbb{Z}^n \mid \sum x_i \equiv 0 \mod 2\} + \mathbb{Z}(\frac{1}{2}, \dots, \frac{1}{2}). \tag{7.36}$$

We store a list ℓ of elements of II_n. To start we initialize $\ell = (E_n)$ and choose some odd prime p. At each step, given $\ell = (M_1, \dots, M_k)$, we compute all the p-neighbors $N_1, \dots, N_r$ of M_k using Proposition 7.18. We test to see whether any M_i, N_j are equivalent, and add any new equivalence classes to the list ℓ. Then we calculate $\#\mathrm{O}_{M_i}(\mathbb{Z})$, and test to see if the mass formula holds.

Kneser used the above method to classify all unimodular $\mathbb{Z}$-lattices of rank $n \leq 16$.

Example 7.21. Set $n = 24$, and let $v = (0, 1, 2, \dots, 23) \in E_{24}$. Then $\psi(v, v) = \sum_{i=0}^{23} i^2 \equiv 0 \mod 47$. By Proposition 7.18, v is associated to a 47-neighbor $L \in \mathrm{II}_2\, 4$. This L is the *Leech lattice*, the unique $L \in \mathrm{II}_2\, 4$ with no $w \in L$ such that $\psi(w, w) = 2$.

By Proposition 7.18, we have that

$$\#N_p(M) = 1 + p + \cdots + p^{n/2-1}, \tag{7.37}$$

which is quite large. So instead of enumerating every element of $N_p(M)$, we might consider choosing a random element of $N_p(M)$.

Definition 7.22. Let $n \equiv 0 \mod 8$, p an odd prime. Define the graph $G_n(p)$ with vertices $V = \mathrm{O}(V) \backslash \mathrm{II}_n$ and with $[M], [M']$ joined by one edge for each element $M'' \in N_p(M)$ such that $M'' \sim_{\mathbb{Z}} M'$ (thus we allow for self-edges and multiple edges).

Choosing a p-neighbor successively is analogous to taking a random walk on this graph. We can analyze the mixing time of this random walk using the adjacency operator. Set $W = \mathbb{C}[\mathrm{O}(V)\backslash \mathrm{II}_n]$, and define $A_p : W \to W$ by A

$$\begin{aligned} A_p : W &\to W \\ [M] &\mapsto \sum_{M' \in N_p(M)} [M'] \end{aligned} \tag{7.38}$$

It's known that we have "fast" mixing of a random walk if and only if A_p has a "large" spectral gap (the gap between the largest eigenvalue and the second largest eigenvalue).

We can define W, A_p in terms of *automorphic forms*. There are a lot of things in number theory which seem hard to compute explicitly, but automorphic forms allows us to do so anyway. By Proposition 7.9, we have that

$$\mathrm{O}(V)\backslash \mathrm{II}_n \Leftrightarrow \mathrm{O}(V)\backslash \mathrm{O}_V(\mathbb{A}^\infty)/\mathrm{O}_{E_n}(\hat{\mathbb{Z}}) = \mathrm{O}(V)\backslash \mathrm{O}_V(\mathbb{A})/\mathrm{O}_{E_n}(\hat{\mathbb{Z}} \times \mathbb{R}). \tag{7.39}$$

So

$$W \cong \mathbb{C}[\mathrm{O}(V)\backslash \mathrm{O}_V(\mathbb{A})/\mathrm{O}_{E_n}(\hat{\mathbb{Z}} \times \mathbb{R})]. \tag{7.40}$$

This is the space of everywhere unramified, $\mathrm{O}_V(\mathbb{R})$-invariant automorphic forms on $\mathrm{O}(V)$. Under this isomorphism, A_p is identified with a Hecke operator

$$T_p \in C_c\left(\mathrm{O}_{E_n}(\mathbb{Z}_p)\backslash \mathrm{O}_V(\mathbb{Q}_p)/\mathrm{O}_{E_n}(\mathbb{Z}_p)\right) \tag{7.41}$$

where C_c is the space of compactly supported functions on the space, which is fairly well studied. In particular, the desired spectral gap property of A_p is equivalent to a statement about the eigenvalues of T_p, which is equivalent to the Ramanujan conjecture.

Another relevant set of conjectures which are very important to number theorist are the Langlands conjectures. These answer the questions of which eigenvalues of T_p can appear. The Langlands functoriality conjecture posits that all automorphic forms on O_V can be described as "lifts" of automorphic forms from other, better understood groups, such as GL_n.

Let's give some explicit calculations.

Example 7.23. Let $n = 16$. Chenevier-Lannes showed that $\mathrm{O}_V\backslash \mathrm{II}_n = \{[E_{16}, [E_8 \oplus E_8]\}$. In the given basis, we have that

$$A_p = \#N_p \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + (1 + p + p^2 + p^3) \cdot \frac{1 + p^{11} - \tau(p)}{691} \begin{pmatrix} -286 & 405 \\ 286 & -405 \end{pmatrix} \tag{7.42}$$

where τ is the Ramanujan tau function, defined by the generating series

$$\Delta(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{m=1}^{\infty} \tau(m) q^m \tag{7.43}$$

Δ is a modular form on $\mathrm{GL}_2/\mathbb{Q}$, with T_p-eigenvalue $\tau(p)$. The appearance of $\tau(p)$ reflects the relationship between automorphic forms on GL_2 and those on O_V, as conjectured by Langlands functoriality.

For more information see the book of Chenevier and Lannes.

Theorem 7.24. *Let $n \equiv 0 \mod 8$. For $M, M' \in \mathrm{II}_n$, define*

$$N_p(M, M") = \{M'' \in N_p(M) \mid M'' \sim_{\mathbb{Z}} M'\} \tag{7.44}$$

Then "the probability that a random p-neighbor of M is M'" is equal to

$$\frac{\#N_p(M, M')}{\#N_p(M)} = \frac{1/\#O_{M'}(\mathbb{Z})}{m(\mathrm{II}_n)} + \mathrm{O}_n\left(\frac{1}{p}\right) \tag{7.45}$$

where O_n is some unfortunate big O-notation, and

$$m(\mathrm{II}_n) = \sum_{[M'']\in \mathrm{O}_V \backslash \mathrm{II}_n} \frac{1}{\#\mathrm{O}_{M''}(\mathbb{Z})} \tag{7.46}$$

is the mass of the genus.

In particular, when p is large enough, then $G_n(p)$ is complete, so any two vertices have an edge.

Example 7.25. $G_{24}(p)$ is complete if and only if $p \geq 47$.

By doing some number theory in the spirit of what we have described above, Chenevier-Allombot (2024) have extended the classification of all unimodular $\mathbb{Z}$-lattices of rank n to every $n \leq 28$. Instead of randomly choosing a p-neighbor, they search a specific "region" of the graph $G_n(p)$ which is more likely to have undiscovered equivalence classes.