Arithmetic Theory of Quadratic Forms

Lecture Notes for Harvard Summer Tutorial 2023

Kush Singhal

3 July - 11 August 2023

Contents

Notation

- $\mathbb{Q}$ denotes the field of rational numbers, and $\mathbb{Z}$ its ring of integers.
- $\mathbb{N}$ denotes the set of positive integers (in particular, we use the convention that $0 \notin \mathbb{N}$).
- Unless otherwise specified, the letter p is always going to denote a prime.
- For $a, b, n \in \mathbb{Z}$, we write $a \equiv b \pmod{n}$ to mean $n|(b-a)$.
- $\mathbb{F}_p$ denotes the finite field with p elements, i.e. $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$.
- $\mathbb{R}$ denotes the field of real numbers.
- $\mathbb{Q}_p$ will denote the field of p-adic numbers, and $\mathbb{Z}_p$ the ring of p-adic integers.
- Throughout, a ring will be assumed to be unital and commutative. An algebra over a ring will always be assumed to be unital and associative.
- Given a ring R, we write R^* to be the group of units of R. For instance, for k a field, we have $k^* = k\backslash\{0\}$.
- If V and W are vector spaces over k, then $\mathrm{Hom}_k(V, W)$ denotes the k-vector space of all k-linear maps $T : V \to W$. We let $GL(V)$ denote the group of all invertible k-linear maps $T : V \to V$. We write $M_n(k)$ and $GL_n(k)$ for $M(k^n)$ and $GL(k^n)$ respectively.
- For a matrix A, we denote its transpose by A^t.
- The phrase 'almost all' will always mean 'all but finitely many'.

0 Overview

This tutorial is about *quadratic forms*, i.e. quadratic homogeneous polynomials in n variables over various fields and rings. Given a quadratic form, say

$$f(x, y, z) = x^2 + y^2 + 3z^2 + 4xy$$

we can ask a few basic questions:

Q1) Can we understand the set of real numbers/rational numbers/p-adic numbers/integers that can be *represented* by f? More generally, for R some ring or field, which $a \in R$ can be written as

$$f(x, y, z) = a$$

for $x, y, z \in R$?

This question of course has many sub-questions, two examples being:

(a) Is the above set non-empty, i.e. can we find even one such $a \in R$?

(b) Is there an easy way to tell whether $a \in R$ can be represented by f without finding explicit solutions in x, y, z?

Q2) Can we classify quadratic forms? For instance, is there some (relatively) small set S of quadratic forms such that if we can answer the above question for all $f \in S$, then we can actually answer the above question for all quadratic forms?

Q3) Fixing $n \in \mathbb{Z}$, say, can we find the number of solutions to $f(x, y, z) = n$ for $x, y, z \in \mathbb{Z}$? Is the number of solutions finite or infinite? If the number of solutions is finite, can we write down a formula in the variable n?

In this tutorial, we try to answer the above three questions for quadratic forms over $\mathbb{Q}$ and $\mathbb{Z}$. We will see however that in trying to answer the question for the 'global field' $\mathbb{Q}$, we need to in fact answer the above questions for the *completions* of $\mathbb{Q}$, i.e. for $\mathbb{R}$ and for the p-adic numbers. This is the *local-global principle*. This principle is present everywhere in number theory, and guides how much modern research is done. The idea itself is simple: in order to study some object over $\mathbb{Q}$, we try to instead understand this object over each prime individually, and then try to stitch this 'local' information together to gain information about the original 'global' object over $\mathbb{Q}$. The prototypical example of a local-global principle is the *Hasse-Minkowski Theorem* for quadratic forms.

Another key idea is to use linear algebra and geometry to answer the above questions. The basic idea is that quadratic forms correspond to bilinear forms, which behave like inner products in some ways. By exploiting this analogy with inner products on vector space, we will develop a linear algebraic theory of *quadratic spaces* and *lattices*. This theory will lead to deeper insights into quadratic forms. Of course, it should be kept in mind that this will always be an analogy: one can develop the entire theory without having to mention vector spaces at all (indeed, this is what is done in [Cas78]). However, the linear-algebraic theory allows us to state things cleanly, and is a useful source of motivation and intuition.

Finally, towards the end of the tutorial, in our attempt to answer the third question above, we will see how the interplay between analytic and algebraic number theory gives us very explicit results about the number of representations by quadratic forms. This will culminate in the *Siegel-Weil mass formula*.

Of course, the entire story above can be generalised to number fields K and their ring of integers $\mathcal{O}_K$. In fact, we can even generalise the theory to function fields. The Hasse-Minkowski theorem extends to this setting as well, as will pretty much all of the algebraic theory.

For the sake of concreteness, I have decided to stick to $\mathbb{Q}$ and $\mathbb{Z}$ rather than general number fields. However, I will still make brief remarks about the theory over general number fields. Thus, if you are interested in the theory over an arbitrary number field, I would encourage you to read through the remarks I make. Those who are not familiar with the language of number fields may safely skip such remarks. I've tried to state results in as much generality as I can without having to add unnecessary complications.

Let us look at a concrete classical example to get a sense for the kind of results we're after. The binary quadratic form $f = x^2 + y^2$ was first studied by Fermat, and then by Gauss, Jacobi, and a whole litany of other famous number theorists. Fermat gave a complete answer for the first question.

Theorem 0.1 (Fermat)**.** *An odd prime is a sum of two integer squares if and only if it is 1 modulo 4. In our terminology, a prime p is represented by the binary quadratic form $f = x^2 + y^2$ over $\mathbb{Z}$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$.*

Corollary 0.1.1. *A number $n \in \mathbb{N}$ is represented by $x^2 + y^2$ over $\mathbb{Z}$ if and only if in the prime factorisation $n = p_1^{k_1} \cdots p_r^{k_r}$ for n, the exponent k_i must be even whenever $p_i \equiv 3 \pmod 4$.*

The second question was answered by Gauss in his *Disquisitiones Arithmeticae*. His general body of work on binary quadratic forms is a little too big for this section, but we will satisfy ourselves with the following result just to illustrate a positive answer to the second question above.

Theorem 0.2 (Gauss)**.** *Let $a, b, c \in \mathbb{Z}$, and set $f(x, y) = ax^2 + bxy + c^2$. Then there exist $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ with $\alpha\delta - \beta\gamma = 1$ and*

$$f(\alpha x + \beta y, \gamma x + \delta y) = x^2 + y^2$$

if and only if $b^2 - 4ac = -4$.

Finally, let us give an answer to the third question for $f = x^2 + y^2$ over $\mathbb{Z}$. Jacobi proved the following result using a very clever argument involving formal power series. However, from the modern perspective, this statement is a direct result of the Siegel-Weil Mass Formula.

Theorem 0.3 (Jacobi)**.** *Let $r(n)$ denote the number of integer solutions (x, y) to $x^2 + y^2 = n$. Then,*

$$r(n) = 4 \left(\sum_{d|n, d \equiv 1 \pmod 4} 1 - \sum_{d|n, d \equiv 3 \pmod 4} 1 \right),$$

i.e. $\frac{1}{4} r(n)$ is the difference between the number of divisors of n congruent to 1 modulo 4, minus the number of divisors of n congruent to 3 modulo 4.

We will revisit all of the above theorems above later on in the tutorial.

The main reference for the algebraic theory of quadratic forms is the excellent book by Timothy O'Meara [OMe73]. However, this book is quite old and so a lot of the notation and terminology is outdated. O'Meara also works over general number fields rather than just $\mathbb{Q}$. Another good reference is Cassels [Cas78]; the advantage with him is that he only works over $\mathbb{Q}$. For a computational point of view, as well as for applications in error correcting codes and so on, [CS13] is an excellent book. For the latter part on the Siegel-Weil Mass Formula, I don't know of any good complete expository references. I will thus mostly be following [Gar14] and [Li23] for the proof of the Siegel-Weil mass formula, and a variety of modern papers for applications of the formula.

Finally, a word on exercises. I have sprinkled a lot of exercises throughout the notes. These exercises are usually results from one of the references whose proof was straightforward enough. Quite a few of the exercises are extremely easy and can be proved within a couple of lines; most exercises should be easy enough!

1 Quadratic Spaces

Let us first introduce the basic language and terminology of quadratic forms. As mentioned in the overview, our approach is going to be a linear algebraic one, so that we can exploit some of the algebra and geometry inherent in quadratic forms.

Throughout, k is going to denote a field of characteristic not 2.

1.1 Definitions

Recall that a symmetric bilinear form B on a finite dimensional k-vector space V is a mapping

$$B : V \times V \to k$$

such that $B(ax+by,z) = aB(x,z) + bB(y,z)$ for $a,b \in k$ and $x,y,z \in V$, and such that $B(x,y) = B(y,x)$ for $x,y \in V$.

Remark 1.1. Alternatively, a symmetric bilinear form is an element of $\mathrm{Sym}^2(V^*)$.

Given a symmetric bilinear form B on a vector space V, we can set

$$Q : V \to k, \quad Q(x) := B(x,x).$$

Definition. A *quadratic space (over k)* is a finite dimensional vector space V over k equipped with a symmetric bilinear form B.
The *quadratic form* on V associated to B is the above map Q.
The quadratic space is said to be *n-ary* if the underlying space has dimension n. We say a quadratic space is *unary*, *binary*, *ternary*, *quaternary* for $n = 1, 2, 3, 4$ respectively.

We can of course recover the symmetric bilinear form from its corresponding quadratic form via the identity

$$B(x,y) = \frac{1}{2}\left(Q(x+y) - Q(x) - Q(y)\right).$$

Thus we can define a quadratic space by simply defining the associated quadratic form on the vector space.

Example 1.2. If V is a quadratic space, then for any $W \subset V$ a k-linear subspace of V we can restrict the quadratic form Q_V of V to W to get a new quadratic space $(W, Q_V|_W)$. The inclusion map $i : W \hookrightarrow V$ is an isometry.

Example 1.3. Classically, a quadratic form is supposed to be a homogeneous degree 2 polynomial in n variables. We can recover this notion here. Indeed, if $f \in k[x_1, ..., x_n]$ is a degree 2 homogeneous polynomial, then we can simply take $V = k^n$ and define the quadratic form

$$Q(v) = f(v_1, ..., v_n)$$

for $v = (v_1, ..., v_n) \in k^n$.

Example 1.4. Suppose $A \in M_n(k)$ is a symmetric matrix. Then, we can equip $V = k^n$ by the symmetric bilinear form

$$B(x,y) = x^t A y$$

where we view $x, y \in k^n$ as column vectors. This n-ary quadratic space is denoted by $\langle A \rangle$ in [OMe73].

Example 1.5. For $a \in k$, we can define a quadratic space by equipping the 1-dimensional space k by the quadratic form

$$Q_a(b) = ab^2$$

for $b \in k$. This quadratic space will be denoted by $< a >$. Notice that this coincides with the previous example; of course, we have $M_1(k) = k$ and $< a >$ defined here is precisely the quadratic space defined in the above example.

We can also define maps between quadratic spaces, in the obvious way.

Definition. A morphism of quadratic spaces $\sigma : (V, B_V) \to (W, B_W)$ over k is a k-linear map $\sigma : V \to W$ such that $B_W(\sigma v_1, \sigma v_2) = B_V(v_1, v_2)$ for $v_1, v_2 \in V$.

Equivalently, a morphism of quadratic spaces is a k-linear map that preserves the quadratic forms.

Definition. An *isometry* is a morphism of quadratic spaces that is injective.
Two quadratic spaces are *isomorphic* if there exists a surjective isometry between them.
For a quadratic space (V, Q), the *orthogonal group attached to* V, denoted by $O(V, Q)$, is the subgroup of $GL(V)$ consisting of isometries. If the Q is known, we can simply write $O(V)$.

Remark 1.6 (for those who know about reductive group schemes). $O(V)$ is the set of k-points of a certain reductive group scheme over k. In fact, the functor $R \mapsto O(V \otimes_k R)$ is an algebraic group, say denoted by $\mathbf{O}(V)$.

Example 1.7. By fixing a basis $x_1, ..., x_n$ for V, we can write

$$A = \big(B(x_i, x_j)\big)_{1 \leq i,j \leq n},$$

and then we see easily that $V \cong \langle A \rangle$. This is is the *Gram matrix of* V *(with respect to the basis* $x_1, ..., x_n$*).*

Example 1.8. Suppose $A, A' \in M_n(k)$ are symmetric matrices. Then $\langle A \rangle \cong \langle A' \rangle$ if and only if there exists $X \in GL_n(k)$ such that $A' = XAX^t$.

In particular, in the second example above, we see that $\det A' = (\det A)(\det X)^2$. This leads to the following definition.

Definition. The *discriminant* $\mathrm{disc}V$ of a quadratic space V is the element of $\{0\} \cup k^*/(k^*)^2$ given by $(\det A)(k^*)^2$ for any symmetric matrix A such that $V \cong \langle A \rangle$.

It is clear that the discriminant is an invariant of a quadratic space, i.e. $\mathrm{disc}V = \mathrm{disc}V'$ if $V \cong V'$. Note that multiplication of discriminants makes sense.

Finally, recall that we are interested in the set $Q(V)$, motivating the following definitions.

Definition. Let (V, Q) be a quadratic space. An element $a \in k$ is said to be *represented by* Q (or sometimes *represented by* V if the quadratic form on V is clear) if there exists $v \in V$ such that $Q(v) = a$.
A quadratic space is *universal* if $Q(V) = k$, i.e. every element of k is represented by the quadratic form on V.

It is easy to see that a is represented by a quadratic space (V, Q_V) if and only if there is an isometry $(< a >, Q_a) \hookrightarrow (V, Q_V)$.

Even though a quadratic space is a vector space with extra structure, as usual we often abuse notation and say that 'V is a quadratic space over k', when we really mean that V is a vector space over k equipped with a symmetric bilinear form B_V and corresponding quadratic form Q_V. If the vector space is clear from context, we sometimes omit the V from the subscript.

Now that we have a symmetric bilinear form on a vector space, we can try to generalise various notions from an introductory linear algebra course.

Definition. Let V be a quadratic space. Suppose $v, w \in V$. We say that v, w are *orthogonal* (with respect to the quadratic space structure on V) if $B(v, w) = 0$.

Given two subspaces $W_1, W_2 \subset V$ such that $V = W_1 \oplus W_2$ as k-vector spaces, we say that V is the *orthogonal sum of* W_1 *and* W_2, written $V = W_1 \perp W_2$, if every vector in W_1 is orthogonal to every vector in W_2.

Given a subspace $W \subset V$, we write $W^\perp$ to be the subspace of all $v \in V$ such that v is orthogonal to w for all $w \in W$.

A basis $v_1, ..., v_n$ is said to be *orthogonal* if v_i is orthogonal to v_j for all $i \neq j$.

These definitions satisfy various familiar/obvious properties, all of which are left as an exercise.

Exercise 1.9. Suppose V is a quadratic space. Then V always admits an orthogonal basis.

Exercise 1.10. If $V \cong \langle A_1 \rangle \perp \langle A_2 \rangle \perp \cdots \perp \langle A_r \rangle$ for symmetric matrices A_i, then

$$V \cong \left\langle \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{pmatrix} \right\rangle.$$

Exercise 1.11. If $V \cong W_1 \perp W_2$ then $\mathrm{disc}(V) = \mathrm{disc}(W_1)\mathrm{disc}(W_2)$.

1.2 Regularity and Isotropy

However, unlike in Euclidean geometry, in a general quadratic space V with quadratic form Q it is possible for there to exist non-zero $v \in V$ such that $Q(v) = 0$. Thus we have a few extra definitions.

Definition. A quadratic space V is *regular* if $\text{disc}V \neq 0$.

The following exercises give all the key properties of regular spaces; the proofs involve simply unwinding definitions and shouldn't be too difficult.

Exercise 1.12. Let V be a quadratic space with quadratic form Q. Show that the following are equivalent.

1. V is regular.
2. The usual k-linear map
$$V \to \text{Hom}_k(V, k), \quad v \mapsto B(v, -)$$
is an isomorphism.
3. If $w \in V$ and $B(v, w) = 0$ for all $v \in V$, then $w = 0$.
4. $V^\perp = \{0\}$.
5. If $x_1, ..., x_n$ are an orthogonal basis for V, then $Q(x_i) \neq 0$ for all x_i.

Show also that if V is regular, then $(W^\perp)^\perp = W$ for any subspace $W \subset V$.

Exercise 1.13. If W is a regular subspace of a (possibly not regular) quadratic space V, then show that $V = W \perp W^\perp$, and that if $V = W \perp W'$ for some other subspace W' of W, then $W' = W^\perp$.

Exercise 1.14. If V is a regular quadratic space, show that all morphisms of quadratic spaces $V \to W$ are actually isometries, i.e. must be injective.

Exercise 1.15. Suppose V is a regular quadratic space. Let W be a subspace. Show that the following are equivalent:

1. W is regular;
2. $W^\perp$ is regular;
3. $W \cap W^\perp = \{0\}$;
4. $V = W \oplus W^\perp$.

Exercise 1.16. Suppose V is any quadratic space. Consider the subspace
$$\text{rad}(V) := \{v \in V : B(x, v) = 0 \quad \text{for all } x \in V\}.$$
Let V' be *any* subspace of V such that $V = V' \oplus \text{rad}(V)$. Show that V' is regular, and that
$$V = \text{rad}(V) \perp V'.$$

Hence, show that every non-zero quadratic form $f \in k[x_1, ..., x_n]$ is of the form
$$f = h(a_{11}x_1 + \cdots + a_{1n}x_n, ..., a_{r1}x_1 + \cdots + a_{rn}x_n)$$
for some $1 \leq r \leq n$, some regular quadratic form $h \in k[y_1, ..., y_r]$, and some $A = (a_{ij}) \in GL_n(k)$.

This last exercise shows that we only need to look at regular quadratic spaces.

Definition. Let V be a quadratic space.

A vector $v \in V$ is *isotropic* if v is non-zero but $Q(v) = 0$. Otherwise, v is said to be *anisotropic*.

A subspace W of V is *isotropic* if there exists an isotropic vector in W. Otherwise, if every vector of W is anisotropic, we say that W is *anisotropic*.

The following is the most important example of an isotropic quadratic space.

Definition. A binary quadratic space is said to be a *hyperbolic plane* if it is isomorphic to $\langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle$.

Notice that the discriminant of the hyperbolic plane is $-1 \cdot (k^*)^2$, and so the hyperbolic plane is regular. It is also clearly isotropic.

Proposition 1.17. *Every isotropic regular quadratic space V contains a hyperbolic plane as a subspace.*

Proof. Let $v \in V$ be an isotropic vector. Since an isotropic quadratic space is by definition regular, by Exercise 1.12 we can find $w' \in V$ such that $B(v, w') \neq 0$. Replacing w' with $\frac{1}{B(v,w')}w'$ if necessary, we can assume that $B(v, w') = 1$. Now consider

$$w = w' - \frac{Q(w')}{2}v.$$

An easy computation shows that $Q(w) = 0$ and $B(v, w) = 1$. We then see that the subspace spanned by v and w is a hyperbolic plane. □

The above proof in fact established something stronger.

Corollary 1.17.1. *Every isotropic vector in a regular quadratic space is contained in a hyperbolic plane.*

Corollary 1.17.2. *The following are equivalent for a binary quadratic space V:*

1. *V is regular isotropic;*
2. *V is the hyperbolic plane; and*
3. *$\mathrm{disc}V = -(k^*)^2$.*

Proof. (1) $\Leftrightarrow$ (2) is immediate from the theorem. (2) $\implies$ (3) is a direct computation. So suppose (3). As $\mathrm{disc}V = -1$, V is regular, and so $Q(V) \neq \{0\}$. Let $\alpha \in Q(V) \setminus \{0\}$ and let $x \in V$ such that $Q(x) = \alpha$. By regularity, $V = kx \perp ky$ for some $y \in V$. Now $\mathrm{disc}V = -(k^*)^2$ implies that $-\alpha Q(y)$ is a non-zero square in k, and so after scaling y we can write $Q(y) = -\alpha$. One then checks that $Q(\frac{x+y}{2}) = 0 = Q(\frac{x-y}{\alpha})$ and $B(\frac{x+y}{2}, \frac{x-y}{\alpha}) = 1$, so that V is isomorphic to the hyperbolic plane. □

Corollary 1.17.3. *Any isotropic regular quadratic space is universal.*

Proof. By the lemma, it suffices to prove that the hyperbolic plane $H = \langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle$ is universal. However this is easy, since for any $a \in k$ we can take $v = (\frac{1}{2}, a)$ so that

$$Q(v) = \begin{pmatrix} \frac{1}{2} & a \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{2} \\ a \end{pmatrix} = a.$$

□

Corollary 1.17.4. *Let V be a regular quadratic space, and let $x_1, ..., x_r$ be r linearly independent vectors in V. Suppose that $B(x_i, x_j) = 0$ for all $1 \leq i, j \leq r$. Then, there exist subspaces $H_i \subset V$ such that $x_i \in H_i$, each H_i is a hyperbolic plane, and $H_i \subseteq H_j^{\perp}$ for all $i \neq j$ (so that $H_1 \perp \cdots \perp H_r$ is a $2r$-dimensional subspace of V).*

Proof. The proof is by induction on r. For $r = 1$, this is Corollary 1.17.1. So suppose $r > 1$. Let $U = kx_1 \perp \cdots \perp kx_{r-1}$ and $W = U \perp kx_r$. By assumption, $Q(W) = \{0\}$. Now, we have $U \subset W$ and so $W^{\perp} \subset U^{\perp}$. Pick $y_r \in U^{\perp} \setminus W^{\perp}$, and take $H_r = kx_r + ky_r$. A quick computation checks that H_r is a hyperbolic plane containing x_r and that $x_i \in H_r^{\perp}$ for $1 \leq i \leq r-1$. Applying the inductive hypothesis to $H_r^{\perp}$, we have $H_1 \perp \cdots \perp H_{r-1} \subseteq H_r^{\perp}$ with $x_i \in H_i$ and H_i a hyperbolic plane, and the collection $H_1, ..., H_r$ satisfies the lemma. □

We have already made some progress towards answering **Q1** from before!

The following exercises are also corollaries of the above lemma.

Exercise 1.18. Let V be a regular quadratic space over k and $a \in k$. Then V represents a if and only if $\langle -a \rangle \perp V$ is isotropic.

Exercise 1.19. Let U be a regular ternary subspace of a regular quaternary space V such that $\mathrm{disc}V = 1$. Then V is isotropic if and only if U is isotropic.

1.3 Reflections and Rotations

There is a special family of isometries in $O(V)$ for V a regular quadratic space.

Definition. Fix an anisotropic vector $x \in V$. The *reflection* (aka *symmetry*) attached to x is the map $\tau_x : V \to V$ given by

$$\tau_x y := y - \frac{2B(x,y)}{Q(x)}x.$$

Remark 1.20. In [OMe73], reflections mean something else entirely, while he refers to τ_x as symmetries. However, I think the term reflection is quite common nowadays.

It is easy to check that $\tau_x \in O(V)$, that it is an involution (i.e. $\tau_x^2 = 1$), and that $\det \tau_x = -1$ for all anisotropic $x \in V$. Notice also that $\tau_x(x) = -x$, and that $\tau_x(v) = v$ whenever $B(v,x) = 0$. Thus, τ_x can be viewed as the reflection through the subspace $(kx)^\perp$ of V orthogonal to x. It is easy to see that $\tau_{\lambda x} = \tau_x$ for any $\lambda \in k^*$.

Exercise 1.21. Suppose $\sigma \in O(V)$ and $x \in V$ is anisotropic. Then, $\tau_{\sigma x} = \sigma \tau_x \sigma^{-1}$.

Now, recall that we have a group homomorphism $\det : GL(V) \to k^*$ for any k-vector space V. Since $O(V) \subset GL(V)$, we have the group homomorphism

$$\det|_{O(V)} : O(V) \to k^*.$$

Exercise 1.22. The image of $\det|_{O(V)}$ is the subgroup $\{\pm 1\} \subset k^*$.

Definition. The *special orthogonal group* $SO(V)$ attached to a quadratic space V is the kernel of $\det|_{O(V)}$, i.e. it is the subgroup of isometries of determinant 1.

We can now prove the following.

Theorem 1.23 (Cartan-Dieudonné)**.** *Every isometry $\sigma \in O(V)$ of a regular n-ary quadratic space is a product of at most n reflections, (here, the identity is considered to be the product of 0 reflections).*

Before we establish this theorem, we need a couple of lemmas. The first is left as an exercise.

Exercise 1.24. Suppose V is a quadratic space, and $W \subseteq V$ a subspace such that $Q(W) = \{0\}$. Then, show that $W \subseteq W^\perp$.

This second lemma is the technical heart of the proof.

Lemma 1.25. *Suppose V is as in the statement of the theorem. Suppose $\sigma \in O(V)$ satisfies the condition that $\sigma x - x$ is non-zero and isotropic whenever $x \in V \setminus \{0\}$ is anisotropic. Then, $n \geq 4$, n is even, and $\sigma \in SO(V)$.*

Proof. Suppose there exists anisotropic $x \in V$ such that σx is not linearly independent from x. We must have $\sigma x = \pm x$, and so either $\sigma x - x$ is zero or it is anisotropic, thus violating the given assumption on σ. Thus x and σx must be linearly independent whenever x is anisotropic. In particular, $n \neq 1$.

If $n = 2$, then as $\mathrm{disc}V \neq 0$ we can pick an anisotropic $x \in V$. Since $x, \sigma x$ are linearly independent, V has a basis given by x and $\sigma x - x$. However since $\sigma x - x$ is isotropic, a simple calculation shows $Q(x) = B(x, \sigma x)$, and so we see that

$$B(\sigma x - x, ax + b(\sigma x - x)) = 0$$

for all $a, b \in k$. This contradicts the regularity of V.

We now suppose that $n \geq 3$. Let $y \in V$ be isotropic; then there exists a hyperbolic plane $H \subset V$ with $y \in H$ and $V = H \perp H^\perp$. Since H is regular, $H^\perp$ is regular, and so there exists an anisotropic $z \in H^\perp$. Thus, for any $a \in k^*$, we see that $Q(y + az) \neq 0$. By our assumption on σ, we have $Q(\sigma z - z) = 0$ and

$$Q(\sigma(y + az) - y - az) = 0.$$

A simple computation then shows that

$$Q(\sigma y - y) + 2aB(\sigma y - y, \sigma z - z) = 0$$

for all $a \in k^*$. Thus $Q(\sigma y - y) = 0$. Since $Q(\sigma y - y) = 0$ for $y \in V$ anisotropic anyway, it thus follows that $Q(\sigma y - y) = 0$ for all $y \in V$.

In particular, the subspace $W = (\sigma - 1)(V)$ satisfies $Q(W) = \{0\}$. A computation now shows that

$$B(x, \sigma y - y) = -B(\sigma x - x, y) = 0$$

for all $x \in V$ and all $y \in W^\perp$. By the regularity of V, we then have $\sigma y = y$ for all $y \in W^\perp$. Since $\sigma y - y \neq 0$ for y anisotropic, it then follows that every element of $W^\perp$ is isotropic. By Exercise 1.24 we have $W \subseteq W^\perp$ and $W^\perp \subseteq (W^\perp)^\perp$. However, V is regular, and so $(W^\perp)^\perp = W$, and thus $W^\perp = W$.

As $\sigma|_{W^\perp} = 1$ and $W = \mathrm{im}(\sigma - 1)$, it follows that

$$n = \dim_k \ker(\sigma - 1) + \mathrm{rank}(\sigma - 1) = \dim W^\perp + \dim W = 2 \dim W.$$

Hence n is even. As a consequence of Corollary 1.17.4, we then have a $n/2$-dimensional subspace U of V such that $Q(U) = \{0\}$ and $V = W \oplus U$. We have $(\sigma - 1)(U) \subseteq W = W^\perp$ so that $\sigma(u) = u + L(u)$ for some linear map $L : U \to W^\perp$. Since $\sigma|_W$ is the identity as well, the matrix of σ is of block form $\left(\begin{smallmatrix} I & * \\ 0 & I \end{smallmatrix}\right)$, which has determinant 1. □

We can now prove the theorem.

Proof of Theorem 1.23. We proceed by induction on n. For $n = 1$, we have $O(V) = \{1_V, -1_V\}$ where -1_V is a reflection, and so we are done. We can thus suppose $n > 1$. If there exists an anisotropic $x \in V$ such that $\sigma x = x$, then $\sigma|_{(kx)^\perp}$ has image contained in $(kx)^\perp$ where $\dim_k (kx)^\perp = n - 1$ (since x anisotropic), and we can apply the inductive hypothesis to $\sigma|_{(kx)^\perp} \in O((kx)^\perp)$ and write $\sigma|_{(kx)^\perp)} = \tau_{y_1} \cdots \tau_{y_r}$ for $r \leq n - 1$ vectors $y_i \in (kx)^\perp$. Since $B(x, y_i) = 0$ for all $1 \leq i \leq r$, it follows that $\tau_{y_1} \cdots \tau_{y_r}(x) = x$ as well, and hence we have the equality

$$\sigma = \tau_{y_1} \cdots \tau_{y_r}$$

in $O(V)$.

Next, suppose that we can find an anisotropic $x \in V$ such that $Q(\sigma x - x) \neq 0$. Then, a quick calculation shows that $\tau_{\sigma x - x}\sigma$ fixes x. As x is anisotropic, the image of $\tau_{\sigma x - x}\sigma$ lies in $(kx)^\perp$, and as before $\tau_{\sigma x - x}\sigma$ is a product of at most $n - 1$ reflections. Multiplying by $\tau_{\sigma x - x}$ on both sides it follows that σ is the product of at most n reflections.

Finally, we can suppose that σ is such that $\sigma x \neq x$ and $Q(\sigma x - x) = 0$ whenever $x \in V$ is anisotropic. By Lemma 1.25, we know that $n \geq 4$ is even and $\sigma \in SO(V)$. Let $y \in V$ be an arbitrary anisotropic vector, and consider $\tau_y \sigma$. Since $\det(\tau_y \sigma) = -1$ as $\det \tau_y = -1$, by Lemma 1.25 again $\tau_y \sigma$ cannot satisfy the hypothesis of the lemma. In particular, we are in one of the previous two cases, and so $\tau_y \sigma$ is the product of r reflections with $r \leq n$. However n is even, whereas the number of reflections r must be odd as

$$-1 = \det(\tau_y \sigma) = (-1)^r.$$

Hence $r \leq n - 1$, and so by multiplying by τ_y we see that σ is the product of at most n reflections. □

We now have a bunch of corollaries, all of which are left as an exercise.

Corollary 1.25.1. *Suppose σ can be expressed as a product of n-reflections. Then, σ can be expressed as a product of n reflections with the first (or last) symmetry chosen arbitrarily.*

Corollary 1.25.2. *If σ is a product of r symmetries, then the dimension of its fixed space (i.e. of $\ker(\sigma - 1)$) is at least $n - r$.*

1.4 Witt's Theorems, and Index of Quadratic Spaces

We now give two powerful theorems of Witt.

Theorem 1.26 (Witt's Extension Theorem (version 1))**.** *Suppose $V_1, V_2 \subseteq V$ are regular subspaces of the (possibly not regular) quadratic space V. Suppose $\rho : V_1 \to V_2$ is an isomorphism of quadratic spaces. Then, there exists $\sigma \in O(V)$ such that $\sigma|_{V_1} = \rho$.*

Proof. Pick an anisotropic $x \in V_1$. Then there exists $\sigma' \in O(V)$ such that $\sigma'(\rho x) = x$; indeed, either $Q(\rho x - x) \neq 0$ in which case we can take $\sigma' = \tau_{\rho x - x}$, or $Q(\rho x - x) = 0$ in which case we must have $Q(\rho x + x) \neq 0$ (as $Q(x) \neq 0$) and we can take $\sigma' = \tau_{\rho x}\tau_{\rho x + x}$. By replacing ρ and V_2 with $\sigma'\rho$ and $\sigma' V_2$ respectively, we may as well assume that $x \in V_1 \cap V_2$ and that $\rho x = x$.

If $\dim V_1 = 1$, we are done already as $V_1 = V_2 = kx$. Otherwise, we use induction on $\dim V_1$. Let $W = (kx)^\perp$, and take $V_i' := W \cap V_i$. As $x \in V_1 \cap V_2$, one checks that $\rho|_{V_1'} : V_1' \to V_2'$ is surjective, and thus an isomorphism. Since x is anisotropic, we have $\dim_k V_1' \leq \dim_k V_1 - 1$. By the induction hypothesis, there exists $\sigma_1 \in O(W)$ such that $\sigma_1|_{V_1'} = W$. The map $\sigma \in GL(V)$ given by $\sigma x = x$ on kx and by $\sigma = \sigma_1$ on W is an isometry, so that $\sigma \in O(V)$ as required. □

Theorem 1.27 (Witt's Extension Theorem (version 2))**.** *Suppose V is a regular quadratic space, and U is any subspace of V with an isometry $\rho : U \hookrightarrow V$. Then, there exists an isomorphism $\sigma \in O(V)$ such that $\sigma|_U = \rho$.*

Proof. Write $U = U_0 \perp U_r$ where $Q(U_0) = \{0\}$ and U_r is regular. Let $x_1, ..., x_r$ be a basis for U_0. By Corollary 1.17.4 applied to $U_0 \subseteq U_r^\perp$, there is a $2r$-dimensional space $H = H_1 \perp \cdots \perp H_r$ with each H_i a hyperbolic plane and $x_i \in H_i$. As H is regular, we can write $U_r^\perp = H \perp W$ for some $W = H$. We thus have a splitting $V = H \perp W \perp U_r$ where each of H, W, U_r are regular.

Now, we can do the same thing for $\rho(U)$. We thus write $V = H' \perp W' \perp \rho(U_r)$ where $H', W', \rho(U_r)$ are all regular with $(\rho(U_r))^\perp = H' \perp W'$, and where $H' = H_1' \perp \cdots \perp H_r'$ with each H_i' a hyperbolic plane containing ρx_i. We can easily define an extension $\hat{\rho}_i : H_i \to H_i'$ of $\rho|_{kx_i} : kx_i \to k\sigma x_i$. Glueing these $\hat{\rho}_i$s together along with $\rho|_{U_r} : U_r \to \rho(U_r)$, we get an isomorphism $\hat{\rho} : H \perp U_r \to H' \perp \rho(U_r) \subset V$. By version 1 of Witt's extension theorem, noting that $H \perp U_r$ and $H' \perp \sigma(U_r)$ are regular, we can find the required extension $\sigma \in O(V)$. □

Theorem 1.28 (Witt's Lemma)**.** *Let V, V' be isomorphic quadratic spaces and $W \subseteq V, W' \subseteq V'$ isomorphic subspaces of V and V'. Suppose that W (thus W') is regular. Then $W^\perp$ is isomorphic to $(W')^\perp$.*

Proof. Without loss of generality, suppose $V = V'$. Then the isometry $W \xrightarrow{\sim} W'$ extends to an element $\sigma \in O(V)$. Then σ takes $W^\perp$ to $(W')^\perp$. □

The above theorems now allow us to define a new invariant of a regular quadratic space. Indeed, by Witt's extension theorems, any two maximal subspaces M, M' of V with $Q(M) = \{0\} = Q(M')$ must be isomorphic. Thus, the dimension of the maximal subspace M of V with $Q(M) = \{0\}$ is independent of the choice of M.

Definition. The *index* $\mathrm{ind}V$ of a regular quadratic space V is the k-dimension of the maximal subspace M of V satisfying $Q(M) = \{0\}$.

We have another interpretation. By Corollary 1.17.4, we can write

$$V = H_1 \perp \cdots \perp H_r \perp V'$$

where each of the H_i are hyperbolic planes and where V' is either 0 or is anisotropic. Witt's Lemma implies that the number r of such hyperbolic planes does not depend on how we do the splitting (i.e. it is an invariant of V) and that V' is unique up to isomorphism. It is easy to check that in fact $r = \mathrm{ind}V$.

We have thus proven the following lemma.

Lemma 1.29. *If V is any regular quadratic space, then* $\mathrm{ind}V$ *satisfies* $0 \leq \mathrm{ind}V \leq \frac{1}{2}\dim_k V$.
There exist $H_1, ..., H_{\mathrm{ind}V} \subset V$ hyperbolic planes such that

$$V = H_1 \perp \cdots \perp H_{\mathrm{ind}V} \perp V'$$

for a unique (up to isomorphism) subspace $V' \subset V$ that is either 0 or (regular and) anisotropic.

In this sense, the index of a regular quadratic space measures how far the space is from being anisotropic. If the index is 0, then the space is anisotropic.

Exercise 1.30. Suppose V is a regular quadratic space such that we have a decomposition

$$V = H_1 \perp \cdots \perp H_r \perp V'$$

where V' is either 0 or anisotropic, and $0 \leq r \leq \frac{1}{2} \dim V$. Show, using Witt's extension theorem, that this r does not depend on the above decomposition of V. Hence, show that $r = \mathrm{ind} V$.

This exercise shows that the index is precisely the number of hyperbolic planes showing up as orthogonal factors in V.

References

[Cas78] John William Scott Cassels. *Rational quadratic forms*. Courier Dover Publications, 1978.

[CS13] John Horton Conway and Neil James Alexander Sloane. *Sphere packings, lattices and groups*. Vol. 290. Springer Science & Business Media, 2013.

[Gar14] Paul Garrett. *Proof of a Simple Case of the Siegel-Weil Formula*. 2014. URL: `https://www-users.cse.umn.edu/~garrett/m/v/easy_siegel_weil.pdf`.

[Li23] Chao Li. "From sum of two squares to arithmetic Siegel–Weil formulas". In: *Bulletin of the American Mathematical Society* (2023).

[OMe73] O. Timothy O'Meara. *Introduction to Quadratic Forms*. Springer-Verlag, New York, 1973.