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

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

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 $\mathrm{disc} V \neq 0$.

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
$$V \to \mathrm{Hom}_k(V, k), \quad v \mapsto B(v, -)$$
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

$$\mathrm{rad}(V) := \{v \in V : B(x, v) = 0 \quad \text{for all } x \in V\}.$$

Let V' be *any* subspace of V such that $V = V' \oplus \mathrm{rad}(V)$. Show that V' is regular, and that

$$V = \mathrm{rad}(V) \perp V'.$$

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 $y_r \in U^\perp \backslash W^\perp$, 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 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 $\sigma \in O(V)$. □

The following is an immediate corollary of Witt's Extension theorem.

Theorem 1.28 (Witt's Cancellation Theorem)**.** *Suppose W, W', and V are quadratic spaces with V regular. If $W \perp V \cong W' \perp V$, then $W \cong W'$.*

Proof. The identity map $V \cong V$ is an isometry. By version 1 of Witt's Extension Theorem, this is induced by an isometry $\sigma \in O(W \perp V)$. One then checks that $\sigma|_W$ is an isomorphism from W to W'. □

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* 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.

Theorem 1.29 (Witt's Decomposition Theorem)**.** *If V is any regular quadratic space, then* 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.

1.5 The Orthogonal Group Determines the Form

Remark 1.31. This section was the subject of a question in the first problem set.

Perhaps not surprisingly, we have the following result.

Proposition 1.32. *Suppose Q_1 and Q_2 are two regular quadratic forms on the same vector space V over a field k of characteristic not 2. If $O(V, Q_1) = O(V, Q_2)$, then there exists $\lambda \in k^*$ such that $Q_2 = \lambda Q_1$.*

Proof. We let the corresponding symmetric bilinear forms be B_1 and B_2 respectively. For $v \in V$ with $Q_1(v) \neq 0$, consider the reflection $\tau_v^{(1)}(x) = x - \frac{2B_1(x,v)}{Q(v)}v$. Since $\tau_v^{(1)} \in O(V, Q_1) = O(V, Q_2)$, it preserves B_2. The equation

$$B_2(\tau_v^{(1)}w, \tau_v^{(1)}v) = B_2(w, v)$$

shows that

$$Q_1(v)B_2(v, w) = Q_2(v)B_1(v, w)$$

for all $w \in V$. In particular, this shows that $Q_2(v) \neq 0$ for all $v \in V$ with $Q_1(v) \neq 0$. By exchanging the roles of Q_1 and Q_2, we see that $Q_1(v) \neq 0$ if and only if $Q_2(v) \neq 0$. The previous equation also implies that

$$(kv)^{\perp 1} := \{x \in V : B_1(v, x) = 0\} = \{x \in V : B_2(v, x) = 0\} =: (kv)^{\perp 2}.$$

We now fix $v \in V$ with $Q_1(v) \neq 0$; such a v exists by regularity of Q_1. Let $w \in V$. We claim that

$$Q_2(w) = \frac{Q_2(v)}{Q_1(v)}Q_1(w).$$

If $Q_1(w) = 0$, then $Q_2(w) = 0$ as well and the equation follows easily, so we may suppose that $Q_1(w) \neq 0$ and $Q_2(w) \neq 0$. In particular, we also have

$$Q_1(w)B_2(w,x) = Q_2(w)B_1(w,x)$$

for all $x \in V$. If $B_1(v,w) \neq 0$, it then follows that

$$\frac{Q_2(w)}{Q_1(w)} = \frac{B_2(w,v)}{B_1(w,v)} = \frac{Q_2(v)}{Q_1(v)}.$$

Finally, suppose $B_1(v,w) = 0$. Then $B_2(v,w) = 0$ as well. We have $B_1(v, v+w) = B_1(v,v) = Q_1(v) \neq 0$. By the previous argument, we know that

$$Q_2(v+w) = \frac{Q_2(v)}{Q_1(v)} Q_1(v+w).$$

From $B_1(v,w) = B_2(v,w) = 0$, we then have that

$$Q_2(v) + Q_2(w) = \frac{Q_2(v)}{Q_1(v)} \big(Q_1(v) + Q_1(w)\big),$$

and hence that

$$Q_2(w) = \frac{Q_2(v)}{Q_1(v)} Q_1(w)$$

as claimed. $\square$

Corollary 1.32.1. *Suppose V and W are quadratic spaces over k of the same dimension. Suppose that, under some linear isomorphism $L : V \to W$, the subgroup $O(V) \subset GL(V)$ is carried over via conjugation by L to the subgroup $O(W) \subset GL(W)$. Then $V \cong W$ as quadratic spaces.*

2 Quadratic Forms over $\mathbb{R}, \mathbb{C}$, and $\mathbb{F}_q$.

We are now well-placed to classify all regular quadratic spaces (and thus *all* quadratic forms) over certain fields.

2.1 $k = \mathbb{C}$

This is in fact trivial. Write a regular quadratic space V as

$$V = \langle \mathbb{C}x_1 \rangle \perp \cdots \perp \langle \mathbb{C}x_n \rangle$$

for some choice of orthogonal basis, with $n = \dim V$. Notice that every element of $\mathbb{C}$ has a square root, and so upon replacing x_i with $\frac{1}{\sqrt{Q(x)}} x_i$, we can assume that in fact $Q(x_i) = 1$. Hence,

$$V \cong \langle 1 \rangle \perp \langle 1 \rangle \perp \cdots \perp \langle 1 \rangle .$$

We have thus classified all complex regular quadratic spaces.

Proposition 2.1. *Every regular quadratic space over $\mathbb{C}$ is of the form*

$$\langle 1 \rangle \perp \cdots \perp \langle 1 \rangle .$$

Two regular quadratic spaces over $\mathbb{C}$ are isomorphic if and only if they have the same dimensions.

Notice again that $\langle 1 \rangle$ is universal, since every element of $\mathbb{C}$ has a square root. We thus have the following result.

Proposition 2.2. *Every non-zero regular complex quadratic space is universal.*

In fact, this exact same argument here shows that every regular quadratic space over an algebraically closed field must be of the form $\langle 1 \rangle \perp \cdots \perp \langle 1 \rangle$.

2.2 $k = \mathbb{R}$

Notice that $(\mathbb{R}^*)^2 = \mathbb{R}_{>0}$, the set of positive reals. Any real number is either 0, positive, or negative. This basic fact will allow us to completely determine all regular quadratic spaces over $\mathbb{R}$.

Definition. A real quadratic space V is *positive definite* if $Q(V) \subseteq \mathbb{R}_{>0}$. It is *negative definite* if $Q(V) \subseteq \mathbb{R}_{<0}$. Otherwise, it is said to be *indefinite*.

Now recall that any quadratic space has an orthogonal basis, say

$$V = \langle \mathbb{R}x_1 \rangle \perp \cdots \perp \langle \mathbb{R}x_n \rangle$$

where $n = \dim V$. As we assume V is regular, we know that $Q(x_i) \neq 0$ for all $1 \leq i \leq n$. Since $\mathbb{R}^*/(\mathbb{R}^*)^2$ is a group of order 2, with coset representatives $\{\pm 1\}$, we see that we may take $Q(x_i) \in \{\pm 1\}$ without loss of generality. By reordering, we may suppose that $Q(x_i) = 1$ for $1 \leq i \leq p$, and $Q(x_i) = -1$ for $p+1 \leq i \leq n$. Here, $0 \leq p \leq n$. Thus, we can always decompose any regular real quadratic space as an orthogonal sum of a maximal positive definite space and a maximal negative definite space. We see here that p is the dimension of this maximal positive definite. However, *a priori*, this p could depend on our choice of orthogonal basis.

Lemma 2.3 (Sylvester's Law of Inertia)**.** *The dimension of the maximal positive definite subspace of a real regular quadratic space V is an invariant of V.*

Proof. Suppose P and P' are maximal positive definite subspaces of V, and suppose without loss of generality that $\dim P \leq \dim P'$. By the previous discussion, we know that

$$P = \underbrace{\langle 1 \rangle \perp \cdots \perp \langle 1 \rangle}_{\dim P \text{ times}}$$

and

$$P' = \underbrace{\langle 1 \rangle \perp \cdots \perp \langle 1 \rangle}_{\dim P' \text{ times}}.$$

We thus have an obvious isometry $\iota : P \hookrightarrow P'$ taking the i'th copy of $\langle 1 \rangle$ in P to the i'th copy of $\langle 1 \rangle$ in P'. By Witt's extension theorem, we can find $\sigma \in O(V)$ such that $\sigma|_P = \iota$. Notice that $\sigma^{-1}(P')$ is a positive definite subspace of V such that $P \subseteq \sigma^{-1}(P')$. By maximality of P, we have $P = \sigma^{-1}(P')$. Hence,

$$\dim_{\mathbb{R}} P = \dim_{\mathbb{R}} \sigma^{-1}(P') = \dim_{\mathbb{R}} P',$$

as required. □

By replacing Q with $-Q$, we see that we have also proven the following.

Corollary 2.3.1. *The dimension of the maximal negative definite subspace of a real regular quadratic space V is an invariant of V.*

The above lemma and corollary motivate the following definition.

Definition. The *positive index* $\text{ind}^+ V$ of a regular quadratic space V over $\mathbb{R}$ is the dimension of the maximal positive definite subspace. The *negative index* $\text{ind}^+ V$ of a regular quadratic space V over $\mathbb{R}$ is the dimension of the maximal negative definite subspace.

Clearly, we have $\text{ind}^+ V = \dim V$ if and only if V is positive definite, and $\text{ind}^- = \dim V$ if and only if V is negative definite.

Exercise 2.4. Prove that $\text{ind} V = \min\{\text{ind}^+ V, \text{ind}^- V\}$ and that $\dim V = \text{ind}^+ V + \text{ind}^- V$.

Putting all this together, we have the following.

Theorem 2.5. *Two regular quadratic spaces V and V' over $\mathbb{R}$ are isomorphic if and only if* $\text{ind}^+ V = \text{ind}^+ V'$ *and* $\text{ind}^- V = \text{ind}^- V'$.

Thus, up to isomorphism, there are only $n+1$ isomorphism classes of regular quadratic spaces over $\mathbb{R}$ of dimension n. Every regular quadratic space is the orthogonal sum of a maximal positive definite and a maximal negative definite quadratic space (we consider the zero space as both positive and negative definite). Moreover, V is isotropic if and only if V is indefinite.

Definition. The *signature* of a real regular quadratic space V is the pair of integers $(\mathrm{ind}^+ V, \mathrm{ind}^- V)$.

More generally, we have the following result.

Exercise 2.6. Suppose V and V' are two regular quadratic spaces over $\mathbb{R}$. Then, there exists an isometry $\sigma : V \hookrightarrow V'$ if and only if $\mathrm{ind}^+ V \leq \mathrm{ind}^+ V'$ and $\mathrm{ind}^- V \leq \mathrm{ind}^- V'$.

Using the above classification, the following result is immediate.

Theorem 2.7. *Let V be a regular quadratic space. Then,*

$$Q(V) = \begin{cases} \mathbb{R}_{>0} & \text{if } V \text{ positive definite,} \\ \mathbb{R}_{<0} & \text{if } V \text{ negative definite,} \\ \mathbb{R} & \text{otherwise.} \end{cases}$$

2.3 k a Finite Field

Finally, we consider the case of k a finite field. Then, $k = \mathbb{F}_q$ where q is a prime or a power of a prime. Under our characteristic assumption, we assume q is odd.

Consider the homomorphism

$$\varphi : k^* \to (k^*)^2, \quad x \mapsto x^2.$$

Obviously φ is surjective. Since the roots of $x^2 - 1$ are precisely ± 1 (which are distinct as q is odd), it follows that $\ker \varphi = \{\pm 1\}$. Hence $k^*/(k^*)^2$ is again a group of order 2. Fix a non-trivial coset representative $\epsilon \in k^* \setminus (k^*)^2$.

Lemma 2.8. $\langle \epsilon \rangle \perp \langle \epsilon \rangle \cong \langle 1 \rangle \perp \langle 1 \rangle$.

Proof. Let $V = kx \perp ky$ where $Q(x) = \epsilon = Q(y)$. Now, the sets $(k^*)^2$ and

$$1 - \epsilon(k^*)^2 = \{1 - \epsilon\alpha^2 : \alpha \in k, \alpha \neq 0\}$$

are both finite subsets of k^* of cardinality $\frac{q-1}{2}$. These two sets are also not equal, since $1 \in (k^*)^2$ but $1 \notin 1 - \epsilon(k^*)^2$. It follows that $(1 - \epsilon(k^*)^2) \setminus (k^*)^2$ is non-empty, i.e. there exists $\alpha \in k^*$ such that $1 - \epsilon\alpha^2 \in k^* \setminus (k^*)^2 = \epsilon(k^*)^2$. Thus, we have $1 - \epsilon\alpha^2 = \epsilon\beta^2$, and so $v := \alpha x + \beta y \in V$ and $w = \beta x - \alpha y \in V$ satisfy $Q(v) = 1 = Q(w)$ and $B(v, w) = 0$. Hence, we have $V \cong \langle 1 \rangle \perp \langle 1 \rangle$. □

As before, we can write

$$V = \underbrace{\langle 1 \rangle \perp \cdots \perp \langle 1 \rangle}_{p \text{ times}} \perp \underbrace{\langle \epsilon \rangle \perp \cdots \perp \langle \epsilon \rangle}_{n-p \text{ times}}.$$

By the lemma, we can suppose without loss of generality that $n - p \leq 1$. We have thus proven the following theorem.

Theorem 2.9. *Any regular quadratic space V over a finite field k of odd characteristic has a splitting*

$$V \cong \underbrace{\langle 1 \rangle \perp \cdots \perp \langle 1 \rangle}_{(n-1) \text{ times}} \perp \langle \mathrm{disc} V \rangle.$$

In particular,

1. *there are essentially two regular quadratic spaces over k of given dimension; and*
2. *two regular quadratic spaces over k are isomorphic if and only if they have the same dimension and discriminant.*

Exercise 2.10 (Chevalley's Theorem for Quadratic Polynomials). Show that any regular quadratic space over a finite field of dimension $n \geq 3$ is always isotropic. Hence, or otherwise, prove the $d = 2$ case of the following theorem (this special case was originally due to Dickson).

Theorem (Chevalley (1935)). *Let $n, d \in \mathbb{N}$ be such that $n > d$. Then, every polynomial of total degree d in n variables has a non-trivial zero (i.e. a zero not in $\mathbb{F}_q^n \setminus \{(0, ..., 0)\}$).*

3 Algebraic Invariants

In the previous section, using elementary methods, we were able to completely classify all quadratic spaces over certain nice fields. The classification used some simple invariants of quadratic spaces, such as the dimension, the discriminant, and the index. However, for more general fields, we need more sophisticated invariants.

Throughout this chapter, an algebra is assumed to be both unital and associative (see the appendix).

A *division algebra* over k is an algebra D over k such that for every non-zero element $x \in D$ there exists $y \in D$ such that
$$xy = yx = 1_D.$$
Notice that a commutative division algebra over k is simply a field extension of k. Thus, division algebras are 'non-commutative' field extensions of k.

3.1 Quaternion Algebras

In order to define the Hasse algebra, we need to understand quaternion algebras over k.

Definition. Given a field k and elements $\alpha, \beta \in k^*$, the *quaternion algebra* is the 4-dimensional k-algebra

$$(\alpha, \beta)_k := k \oplus k\mathbf{i} \oplus k\mathbf{j} \oplus k\mathbf{k}$$

where multiplication is defined by the following multiplication table.

	1	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
1	1	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{i}$	$\mathbf{i}$	α	$\mathbf{k}$	$\alpha\mathbf{j}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	β	$-\beta\mathbf{i}$
$\mathbf{k}$	$\mathbf{k}$	$-\alpha\mathbf{j}$	$\beta\mathbf{i}$	$-\alpha\beta$

An element of $(\alpha, \beta)_k^0 := k\mathbf{i} \oplus k\mathbf{j} \oplus k\mathbf{k}$ is called a *pure quaternion*, and an element of k (viewed as an element of the quaternion algebra) is called a *scalar quaternion*.

We say that the k-basis $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ of $(\alpha, \beta)_k$ is the *defining basis* of $(\alpha, \beta)_k$.

The *conjugate* of an element $x := x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k} \in (\alpha, \beta)_k$ is

$$\overline{x} := x_0 - x_1\mathbf{i} - x_2\mathbf{j} - x_3\mathbf{k}.$$

The *norm* and *trace* of x is
$$N(x) = x\overline{x} = (x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2) \in k$$
and $T(x) := x + \overline{x} = 2x_0 \in k$.

One checks that conjugation on any quaternion algebra is a k-linear anti-isomorphism preserving 1. If k' is a field extension of k, then clearly
$$(\alpha, \beta)_k \otimes_k k' \cong (\alpha, \beta)_{k'}.$$

Example 3.1. The classical quaternions $\mathbb{H}$ are $(-1, -1)_{\mathbb{R}}$. This is a division algebra.

Example 3.2. The matrix algebra $M_2(k)$ is a quaternion algebra, isomorphic to $(-1, 1)_k$. A defining basis of this quaternion algebra is $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Conjugation is given by $\overline{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$. Thus, the trace of the quaternion algebra coincides with the usual trace of a matrix and the norm is the determinant.

Remark 3.3. It is possible for $(\alpha, \beta)_k$ to be isomorphic to $(\gamma, \delta)_k$ even if $(\alpha, \beta) \neq (\gamma, \delta)$. For instance, we trivially have
$$(\alpha, \beta)_k \cong (\beta, -\alpha\beta)_k \cong (-\alpha\beta, \alpha)_k$$
by simply permuting $\hat{i}, \hat{j}, \hat{k}$.

Exercise 3.4. Let x be an element of a quaternion algebra. Then x is invertible if and only if $Nx \in k^*$. If this condition is satisfied, then $x^{-1} = (Nx)^{-1}\overline{x}$.

Remark 3.5. In particular, $\mathbf{i}, \mathbf{j}, \mathbf{k}$ are invertible. This is why we require α and β to be both non-zero; otherwise the quaternion algebra starts behaving strangely.

Exercise 3.6. Show that a quaternion x is pure if and only if x^2 is scalar.

Exercise 3.7. An algebra isomorphism of one quaternion algebra onto another sends pure quaternions to pure quaternions, and commutes with conjugation, norms, and traces.

Let $A = (\alpha, \beta)_k$. Recall that the trace of a quaternion algebra is valued in k, and so we have a bilinear map

$$B : A \times A \to k, \quad B(x, y) := \tfrac{1}{2} T(x\overline{y}).$$

A computation shows that the corresponding quadratic form is simply

$$Q : A \to k, \quad Q(x) = N(x).$$

Thus, we can view the underlying k-vector space of A as a quaternary quadratic space. We abuse notation by writing A for the corresponding quadratic space as well. We let A^0 denote the ternary quadratic subspace of pure quaternions. A quick computation shows that $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ is an orthogonal basis for A, and that in this basis we have

$$A \cong \langle 1 \rangle \perp \langle -\alpha \rangle \perp \langle -\beta \rangle \perp \langle \alpha\beta \rangle .$$

Since $\mathrm{disc} A = \alpha^2\beta^2(k^*)^2 = (k^*)^2$, A is a regular quadratic space. The following results show how this quadratic space structure completely determines properties of the quaternion algebra. The proofs of these results are straightforward.

Proposition 3.8. *Let A and B be two quaternion algebras. The following are equivalent.*

1. *A and B are isomorphic as k-algebras.*
2. *A and B are isomorphic as quadratic spaces.*
3. *A and B (the subspace of pure quaternions) are isomorphic as quadratic spaces.*

Proof. That (1) $\implies$ (2) follows simply because the quadratic space structure comes from the algebra structure. If (2) holds, then we have an isomorphism of quadratic spaces

$$\langle 1 \rangle \perp A^0 \cong A \cong B \cong \langle 1 \rangle \perp B^0.$$

Witt's extension theorem then implies (3).

Now suppose (3). Suppose $\sigma : A^0 \cong B^0$ be the given quadratic space isomorphism. Write $A = k1_A \oplus k\mathbf{i}_A \oplus \mathbf{j}_A \oplus \mathbf{k}_A$, and set $x = \sigma(\mathbf{i}_A)$ and $y = \sigma(\mathbf{j}_A)$. Note that x and y are pure quaternions in B.

We show first that $x^2 = \alpha$. Since σ is an isometry, we know that

$$Q_B(x) = Q_B(\sigma\mathbf{i}_A) = Q_A(\mathbf{i}_A) = \mathbf{i}_A\overline{\mathbf{i}_A} = -\mathbf{i}_A^2 = -\alpha.$$

On the other hand, $Q_B(x) = x\overline{x}$ by definition of Q_B. Since x is a pure quaternion, we know that $\overline{x} = -x$ and so $-x^2 = x\overline{x} = -\alpha$. Hence $x^2 = \alpha$. Similarly, it can be checked that $y^2 = \beta$.

Next, as σ is an isometry, we know that

$$\tfrac{1}{2}(x\overline{y} + y\overline{x}) = B_B(x, y) = B_B(\sigma\mathbf{i}_A, \sigma\mathbf{j}_A) = B_A(\mathbf{i}_A, \mathbf{j}_A) = 0,$$

and so $x\overline{y} + y\overline{x} = 0$. However, x and y being pure quaternions means that $\overline{x} = -x$ and $\overline{y} = -y$. We thus see that $xy = -yx$. Since $B = k1_B \oplus B^0$, we can write

$$xy = a1_B + v$$

for some $a \in k$ and some $v \in B^0$. Taking conjugates, we see that

$$a1_B - v = \overline{a1_B + v} = \overline{xy} = \overline{y}\,\overline{x} = (-y)(-x) = yx = -xy = -a1_B - v.$$

Thus $a = 0$, i.e. $xy = -yx$ is a pure quaternion.

Finally, consider the k-linear map $\varphi : A \to B$ given by $\varphi(1_A) = 1_B$, $\varphi(\mathbf{i}_A) = x$, $\varphi(\mathbf{j}_A) = y$, and $\varphi(\mathbf{k}_A) = xy$. We claim that φ is also k-multiplicative. A very tedious computation shows that

$$\varphi(\xi_1 1_A+\xi_2\mathbf{i}_A+\xi_3\mathbf{j}_A+\xi_4\mathbf{k}_A)\varphi(\eta_1 1_A+\eta_2\mathbf{i}_A+\eta_3\mathbf{j}_A+\eta_4\mathbf{k}_A) = \varphi\big((\xi_1 1_A+\xi_2\mathbf{i}_A+\xi_3\mathbf{j}_A+\xi_4\mathbf{k}_A)(\eta_1 1_A+\eta_2\mathbf{i}_A+\eta_3\mathbf{j}_A+\eta_4\mathbf{k}_A)\big)$$

for all $\xi_1, \xi_2, \xi_3, \xi_4, \eta_1, \eta_2, \eta_3, \eta_4 \in k$, and so φ is multiplicative. Hence it is a k-algebra homomorphism. Since A is a quaternion algebra and so is central simple (see the next section), it follows that φ is injective. However A and B have the same dimension, which implies that φ is a k-algebra isomorphism. □

Proposition 3.9. *Let $\alpha, \beta \in k^*$. The following are equivalent.*

1. *$(\alpha, \beta)_k$ is isomorphic as a k-algebra to $(1, -1)_k$.*
2. *$(\alpha, \beta)_k$ is not a division algebra.*
3. *$(\alpha, \beta)_k$ is an isotropic quaternary regular quadratic space.*
4. *$(\alpha, \beta)_k^0$ is isotropic ternary regular quadratic space.*
5. *$\langle\alpha\rangle \perp \langle\beta\rangle$ represents 1.*
6. *$\alpha \in N_{k'/k}(k')$ where $k' := k(\sqrt{\beta})$. (Here, $N_{k'/k}$ denotes the field norm corresponding to a finite field extension k'/k)*

Lemma 3.10 (Basic Manipulation Rules for Quaternion Algebras)**.** *Suppose $\alpha, \beta, \gamma, \lambda, \mu \in k^*$. We have the following algebra isomorphisms:*

- $(1, \alpha)_k \cong (\alpha, -\alpha)_k \cong (\alpha, 1-\alpha)_k \cong (1, -1)_k \cong M_2(k)$.
- $(\beta, \alpha)_k \cong (\alpha, \beta)_k \cong (\alpha\lambda^2, \beta\mu^2)$.
- $(\alpha, \beta)_k \otimes_k (\alpha, \gamma)_k \cong (\alpha, \beta\gamma)_k \otimes_k (1, -1)_k$.

Exercise 3.11. Using Proposition 3.8, classify all quaternion algebras up to isomorphism for $k = \mathbb{R}$, $k = \mathbb{C}$, and for k a finite field.

Exercise 3.12. Prove Proposition 3.9. (*Hint: when is $x \in (\alpha, \beta)_k$ invertible?*)

Exercise 3.13. Prove Lemma 3.10, using Proposition 3.8

Exercise 3.14. Let $u \in (\alpha, \beta)_k^0$.

1. Show that u is anisotropic if and only if u is invertible in the algebra $(\alpha, \beta)_k$.
2. Show that if u is anisotropic, then the reflection τ_u is given by $\tau_u x = -uxu^{-1}$.

3.2 Central Simple Algebras

Quaternion algebras are examples of particularly nice algebras, the central simple algebras.

Definition. A k-algebra A is *central* if the centre

$$Z(A) := \{z \in A : zx = xz \text{ for all } x \in A\}$$

is equal to k (*a priori*, we have $k \subseteq Z(A)$).

Definition. A k-algebra A is *simple* if every k-algebra homomorphism $A \to A'$ to another k-algebra A' is either injective or a constant. In other words, A is simple if A does not contain any non-zero proper two-sided ideal.

Example 3.15. All division algebras are simple. Thus, a central division algebra D over k is a central simple algebra over k.

Example 3.16. $M_n(k)$, for $n \geq 1$, is a central simple algebra.

Example 3.17. If K/k is a field extension, then K is a simple k-algebra. However, the centre of K is K itself. Hence, the only field that is also a central simple k-algebra is k itself.

Proposition 3.18. *Quaternion algebras are central simple algebras.*

Proof. Let A denote the quaternion algebra in question. Suppose $x = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k} \in Z(A)$. A quick computation shows that

$$x\mathbf{i} - \mathbf{i}x = 2(x_2\mathbf{j} + x_3\mathbf{k})\mathbf{i}, \quad x\mathbf{j} - \mathbf{j}x = 2(x_1\mathbf{i} + x_3\mathbf{k})\mathbf{j}, \quad \text{and} \quad x\mathbf{k} - \mathbf{k}x = 2(x_1\mathbf{i} + x_2\mathbf{j})\mathbf{k}.$$

Since $x \in Z(A)$, all of these expressions must be zero, and so we see that $x_1 = x_2 = x_3 = 0$. Thus $x \in k$. Hence, quaternion algebras are central.

Suppose now that $\varphi : A \to A'$ is a k-algebra homomorphism that is not injective nor is the zero map. Then $\varphi(1) = 1$ and so $k \cap \ker\varphi = \{0\}$. Let $x \in \ker\varphi$ be non-zero, which exists as φ is not injective. If $x \in k$ (i.e. if $x_1 = x_2 = x_3 = 0$), we are done. So suppose one of x_1, x_2, x_3 is non-zero, say WLOG that $x_1 \neq 0$. Then, by the previous identities, we have

$$2\varphi\big((x_1\mathbf{i} + x_3\mathbf{k})\mathbf{j}\big) = \varphi(x)\varphi(\mathbf{j}) - \varphi(\mathbf{j})\varphi(x) = 0$$

However, $\mathbf{j}$ is invertible in A, and since φ is assumed non-zero, we see that $\varphi(x_1\mathbf{i} + x_3\mathbf{k}) = 0$. However

$$(x_1\mathbf{i} + x_2\mathbf{k})\mathbf{i} + \mathbf{i}(x_1\mathbf{i} + x_2\mathbf{k}) = 2x_1\mathbf{i}^2,$$

and so $\varphi(2x_1\mathbf{i}^2) = 0$. This is impossible since $x_1 \neq 0$ and so $2x_2\mathbf{i}^2 \in k^*$. $\square$

The following lemma allows us to construct new central simple algebras from old ones.

Lemma 3.19. *If A and B are central simple finite dimensional k-algebras, then so is $A \otimes_k B$.*

Example 3.20. If D is a finite dimensional central division algebra over k and $n \geq 1$, then $M_n(D) \cong M_n(k) \otimes_k D$ is a central simple algebra.

In fact, the famous *Artin-Wedderburn* theorem says that this last example gives us *all* central simple algebras. We only need Wedderburn's contribution to the Artin-Wedderburn theorem.

Theorem 3.21 (Wedderburn)**.** *Let A be a central simple k-algebra of finite dimension over k. Then there is a unique (up to isomorphism) central division algebra D of finite dimension over k and a unique $n \geq 1$ such that $A \cong M_n(D)$.*

For a complete proof, see for instance [OMe73, §52F]

Example 3.22. By Proposition 3.9 and the fact that $(-1, 1)_k \cong M_2(k)$, we see that we have already shown the Artin-Wedderburn theorem for quaternion algebras: every quaternion algebra is either a division algebra, or is isomorphic to $M_2(k)$.

The Artin-Wedderburn theorem allows us to define an equivalence relation on finite-dimensional central simple algebras over k.

Definition. Suppose A and B are central simple algebras over k. Then, A and B are said to be *(Brauer)-equivalent*, written $A \sim_k B$, if their corresponding division algebras (guaranteed by the Artin-Wedderburn Theorem) are isomorphic k-algebras. The *Brauer class* of such an algebra A is the equivalence class of the algebra A under Brauer equivalence; it is written $[A]$.

Brauer equivalence is important for us since Hasse algebras are (finite dimensional) central simple algebras, and it turns out that the Brauer class of the Hasse algebra is very useful invariant of a regular quadratic space.

Example 3.23. $(1, -1)_k \sim_k k$.

Example 3.24. In Lemma 3.10, one of the isomorphisms can be rewritten as $(\alpha, \beta)_k \otimes_k (\alpha, \gamma)_k \sim_k (\alpha, \beta\gamma)_k$.

Since $\dim_k M_n(D) = n^2 \dim_k D$, the following lemma is obvious.

Lemma 3.25. *If $A \sim_k A'$ for two central simple k-algebras A and A' such that $\dim_k A = \dim_k A'$, then $A \cong A'$.*

We also have the following.

Lemma 3.26. *Suppose A, A', B, B' are central simple k-algebras of finite-dimension. If $A \sim_k A'$ and $B \sim_k B'$, then $A \otimes_k B \sim_k A' \otimes_k B'$.*

Definition. For a field k, the *Brauer group* $\mathrm{Br}(k)$ is the set of Brauer classes of finite dimensional central simple algebras over k.

By the previous lemma, it is clear that tensor products of k-algebras yields a commutative associative binary operation on $\mathrm{Br}(k)$. Since $A \otimes_k k \cong A$ for any algebra A, it follows that the Brauer equivalence class of k acts as the identity on $\mathrm{Br}(k)$. We have the following non-trivial proposition.

Proposition 3.27. *For any finite dimensional central simple k-algebra A, the opposite algebra A^{op} is a finite dimensional central simple k-algebra satisfying $A \otimes_k A^{op} \cong M_n(k)$ for some $n \geq 1$.*

Corollary 3.27.1. $\mathrm{Br}(k)$ *is an abelian* group *under the tensor product.*

Example 3.28. $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$, generated by the Brauer class of the usual quaternions $(-1,-1)_{\mathbb{R}}$.

Example 3.29 (Wedderburn's Little Theorem). $\mathrm{Br}(k) = 0$ for k a finite field.

Example 3.30. $\mathrm{Br}(\mathbb{C}) = 0$.

This justifies our use of the term 'Brauer group' for $\mathrm{Br}(k)$. Brauer groups (and their generalisations) play an important role in algebraic geometry and number theory. For us however, we are only interested in the subgroup of the Brauer group generated by the Brauer classes of quaternion algebras, i.e. the Brauer classes of those central simple algebras that are a tensor product of finitely many quaternion algebras.

Notice first that the Brauer class of $(\alpha, \beta)_k$ has order 2 in $\mathrm{Br}(k)$; indeed, we have

$$(\alpha, \beta)_k \otimes_k (\alpha, \beta)_k \sim_k (\alpha, \beta^2)_k \cong (\alpha, 1)_k \cong M_2(k).$$

It turns out we have a kind of converse.

Theorem 3.31 (Merkurjev-Suslin)**.** *The subgroup of the Brauer group $\mathrm{Br}(k)$ generated by the Brauer classes of quaternion algebras over k is $\mathrm{Br}(k)[2]$, the subgroup of those elements of $\mathrm{Br}(k)$ of order 2.*

3.3 The Hasse Algebra

3.3.1 Construction

Suppose V is a regular n-ary quadratic space over k. Fix an orthogonal basis for the moment, and suppose

$$V \cong \langle \alpha_1 \rangle \perp \cdots \perp \langle \alpha_n \rangle$$

in this basis. Let $d_i := \alpha_1 \cdots \alpha_i$. Write

$$SV := \bigotimes_{i=1}^{n} (\alpha_i, d_i)_k.$$

This is clearly a finite dimensional central simple algebra, since each of the $(\alpha_i, d_i)_k$ are such.

Definition. The *Hasse algebra* of V is the k-algebra SV.

Clearly, $[SV] \in \mathrm{Br}(k)[2]$.

As of now, the Hasse algebra still depends on the choice of orthogonal basis. We now show that the Hasse algebra is an honest invariant of V.

Lemma 3.32. *Let X, Y be two orthogonal bases for V. Then, there is a chain of orthogonal bases $X = X_0, X_1, ..., X_{r-1}, X_r = Y$ in which each X_i is obtained by altering at most two adjacent basis vectors of X_{i-1}.*

Proof. We prove the lemma by induction on n. The lemma is trivial if $n \leq 2$, so suppose $n \geq 3$. Write $Y = \{y_1, ..., y_n\}$. Let $\mathcal{C}$ be the set of all orthogonal bases X' such that there exists a chain of orthogonal bases $X = X_0, X_1, ..., X_r = X'$ where each X_i is obtained by altering at most two adjacent basis vectors of X_{i-1}. We want to show that $Y \in \mathcal{C}$. It is clear that $\mathcal{C}$ is non-empty, for instance since $X \in \mathcal{C}$.

First, pick $X' \in \mathcal{C}$ such that, writing $y_1 = \sum_{x \in X'} c_x x$, the set of all $x \in X'$ with $c_x \neq 0$ has minimal cardinality (i.e., in the coordinates with respect to X', the vector y_1 has the least number of non-zero coordinates). Write $X' = \{x_1, ..., x_n\}$, ordered in such a way so that

$$y_1 = \alpha_1 x_1 + \cdots + \alpha_p x_p$$

where $\alpha_i \neq 0$ for $1 \leq i \leq p$. We claim that $p = 1$. Suppose not. If $p = 2$, notice that

$$Q(\alpha_1 x_1) + Q(\alpha_2 x_2) = Q(y_1) \neq 0$$

by regularity of V. If $p \geq 3$, then $Q(\alpha_3 x_3) \neq 0$ (we have $Q(x_3) \neq 0$ by regularity). It follows that

$$\frac{1}{2}\Big(\big(Q(\alpha_1 x_1) + Q(\alpha_3 x_3)\big) + \big(Q(\alpha_2 x_2) + Q(\alpha_3 x_3)\big) - \big(Q(\alpha_1 x_1) + Q(\alpha_2 x_2)\big)\Big) = Q(\alpha_3 x_3) \neq 0,$$

and so at least one of $Q(\alpha_1 x_1) + Q(\alpha_3 x_3), Q(\alpha_2 x_2) + Q(\alpha_3 x_3), Q(\alpha_1 x_1) + Q(\alpha_2 x_2)$ is non-zero. Without loss of generality, we may thus suppose that $Q(\alpha_1 x_1) + Q(\alpha_2 x_2) \neq 0$ with $p \geq 2$.

Set $\overline{x}_1 = \alpha_1 x_1 + \alpha_2 x_2$, $\overline{x}_2 = x_2 - \frac{B(\overline{x}_1, x_2)}{Q(\overline{x}_1)} \overline{x}_1$. Then $\overline{X}' := \{\overline{x}_1, \overline{x}_2, x_3, ..., x_n\}$ is obtained from X' by changing at most two vectors, and so $\overline{X}' \in \mathcal{C}$. However, y_1 has exactly $p-1$ coordinates non-zero in $\overline{X}'$. This contradicts the minimality of X' and p. Hence, we have $p = 1$.

We have thus shown that there exists a basis $X' \in \mathcal{C}$ such that $y_1 \in X'$. Write $X' = \{y_1, z_2, ..., z_n\}$. Then we have

$$kz_2 \perp \cdots \perp kz_n = ky_1 \perp \cdots \perp ky_n =: V'$$

with $\dim V' = n - 1$. By the inductive hypothesis, there exists a chain of the required type from $\{z_2, ..., z_n\}$ to $\{y_2, ..., y_n\}$. There thus exists a chain of the required type from X to Y, i.e. $Y \in \mathcal{C}$. $\square$

Proposition 3.33. *SV, up to isomorphism, does not depend on the choice of orthogonal basis.*

Proof. For $n = 1$, the result is obvious, so we suppose $n > 1$. We need to compare SV in two orthogonal bases $x_1, ..., x_n$ and $x'_1, x'_2, x'_3, ..., x'_n$. Write

$$V \cong \langle \alpha_1 \rangle \perp \langle \alpha_2 \rangle \perp \cdots \perp \langle \alpha_n \rangle \qquad \text{and} \qquad V \cong \langle \alpha'_1 \rangle \perp \langle \alpha'_2 \rangle \perp \langle \alpha'_3 \rangle \perp \cdots \perp \langle \alpha'_n \rangle$$

in these two bases. By the previous lemma, it suffices to suppose that $x_j = x'_j$ for $j \neq i, i+1$, for some $1 \leq i \leq n-1$. We must have $kx_i \perp kx_{i+1} \cong kx'_i \perp kx'_{i+1}$. Note that $\alpha_i \alpha_{i+1}$ and $\alpha'_i \alpha'_{i+1}$ are both the discriminant of this binary quadratic space, and so $\alpha_i \alpha_{i+1} = \alpha'_i \alpha'_{i+1} \lambda^2$ for some $\lambda \in k^*$. Writing $d_j = \alpha_1 \cdots \alpha_j$ and $d'_j = \alpha'_1 \cdots \alpha'_j$, we then see that $d_j = d'_j$ for $1 \leq j < i$ and $d_j = d'_j \lambda^2$ for $i+1 \leq j \leq n$. Thus, we have

$$\otimes_{1 \leq j \leq n, j \neq i, i+1} (\alpha_i, d_i)_k \cong \otimes_{1 \leq j \leq n, j \neq i, i+1} (\alpha'_i, d'_i)_k.$$

It remains to show that

$$(\alpha_i, d_i)_k \otimes_k (\alpha_{i+1}, d_{i+1})_k \cong (\alpha'_i, d'_i)_k \otimes_k (\alpha'_{i+1}, d'_{i+1})_k.$$

Now, using Lemma 3.10 throughout, we have

$$\begin{aligned}
(\alpha_i, d_i)_k \otimes_k (\alpha_{i+1}, d_{i+1})_k &= (\alpha_i, d_{i-1}\alpha_i)_k \otimes_k (\alpha_{i+1}, d_{i-1}\alpha_i\alpha_{i+1})_k \cong (\alpha_i, -d_{i-1})_k \otimes_k (\alpha_{i+1}, -d_{i-1}\alpha_i)_k \\
&\sim_k (\alpha_i, -d_{i-1})_k \otimes_k (\alpha_{i+1}, \alpha_i)_k \otimes_k (\alpha_{i+1, -d_{i-1}})_k \\
&\cong (\alpha_i \alpha_{i+1}, -d_{i-1})_k \otimes_k (\alpha_i, \alpha_{i+1})_k.
\end{aligned}$$

Similarly

$$(\alpha'_i, d'_i)_k \otimes_k (\alpha'_{i+1}, d'_{i+1})_k \sim_k (\alpha_i \alpha_{i+1} \lambda^2, -d_{i-1})_k \otimes_k (\alpha'_i, \alpha'_{i+1})_k \cong (\alpha_i \alpha_{i+1}, -d_{i-1})_k \otimes_k (\alpha'_i, \alpha'_{i+1})_k.$$

However, notice that $(\alpha_i, \alpha_{i+1})_k \cong (\alpha'_i, \alpha'_{i+1})_k$ since $kx_i \perp kx_{i+1} \cong kx'_i \perp kx'_{i+1}$ (see also Proposition 3.8). Since these are the same binary space, we have $(\alpha_i, \alpha_{i+1})_k \cong (\alpha'_i, \alpha'_{i+1})_k$. Hence, we see that

$$(\alpha_i, d_i)_k \otimes_k (\alpha_{i+1}, d_{i+1})_k \sim_k (\alpha'_i, d'_i)_k \otimes_k (\alpha'_{i+1}, d'_{i+1})_k.$$

Since both sides have dimension 4 over k, they are isomorphic, and we are done. $\square$

The following exercises show how to manipulate the Hasse algebra.

Exercise 3.34. Let $V = \langle \alpha_1 \rangle \perp \cdots \langle \alpha_n \rangle$. Show that

$$SV \sim_k \bigotimes_{1 \le i \le j \le n} (\alpha_i, \alpha_j)_k.$$

Exercise 3.35. Let K/k be any field extension. Show that

$$S(V \otimes_k K) \cong SV \otimes_k K.$$

Exercise 3.36. Suppose U and W are regular subspaces of V such that $V = U \perp W$. Show that

$$SV \sim_k SU \otimes_k (\mathrm{disc}U, \mathrm{disc}W)_k \otimes_k SW.$$

(Since $(\alpha\lambda^2, \beta\mu^2)_k \cong (\alpha, \beta)_k$, the quaternion algebra $(\mathrm{disc}U, \mathrm{disc}W)_k$ makes sense up to isomorphism.)

3.3.2 Applications

We now use the Hasse algebra (or, more specifically, the Brauer class $[SV] \in \mathrm{Br}(k)[2]$ of the Hasse algebra), to prove some classification results.

Theorem 3.37. *Suppose V and W are regular n-ary quadratic spaces with $1 \le n \le 3$. Then V is isomorphic to W as a quadratic space if and only if*

$$\dim V = \dim W \ (= n), \quad \mathrm{disc}V = \mathrm{disc}W, \quad SV \sim_k SW.$$

Proof. For $n = 1$, the quadratic space is completely determined by the discriminant, and so the theorem is trivial. Of course, we have already shown the necessity of these invariants. We thus need to prove sufficiency, i.e. we assume $\mathrm{disc}V = \mathrm{disc}W$ and $SV \sim_k SW$.

Suppose $n = 3$. If $\mathrm{disc}V = \alpha(k^*)^2$, then by replacing Q_V and Q_W by $\frac{1}{\alpha}Q_V$ and $\frac{1}{\alpha}Q_W$ respectively, we see that it suffices to assume $\mathrm{disc}V = \mathrm{disc}W = 1$. Write

$$V \cong \langle -\alpha \rangle \perp \langle -\beta \rangle \perp \langle \alpha\beta \rangle \quad \text{and} \quad W \cong \langle -\gamma \rangle \perp \langle -\delta \rangle \perp \langle \gamma\delta \rangle.$$

We thus have $V \cong (\alpha, \beta)_k^0$ and $W \cong (\gamma, \delta)_k^0$ as ternary quadratic spaces over k. However, one can compute that

$$(-1, -1)_k \otimes_k SV \sim_k (\alpha, \beta)_k.$$

Similarly $(-1, -1)_k \otimes_k SW \sim_k (\gamma, \delta)_k$. Since $SV \sim_k SW$, we thus have $(\alpha, \beta)_k \sim_k (\gamma, \delta)_k$. For dimension reasons, we thus have $(\alpha, \beta)_k \cong (\gamma, \delta)_k$ and hence that $V \cong W$.

Finally, suppose $n = 2$. Since V and W have the same invariants, one can check that so so $V \perp \langle 1 \rangle$ and $W \perp \langle 1 \rangle$. Thus, by the previous argument, we have $V \perp \langle 1 \rangle \cong W \perp \langle 1 \rangle$. By Witt's cancellation theorem, we have $V \cong W$. $\square$

Exercise 3.38. Show that a regular ternary quadratic space over k is isotropic if and only if $SV \sim_k (-1, -1)_k$.

Theorem 3.39. *Suppose k has the property that every regular quinary quadratic space over k is isotropic. Let V and W be any regular quadratic spaces over k. Then $V \cong W$ if and only if*

$$\dim V = \dim W, \quad \mathrm{disc}V = \mathrm{disc}W, \quad SV \sim_k SW.$$

Proof. As before, we just need to prove sufficiency. Let $n = \dim V = \dim W$. We use induction on n. The case of $n \le 3$ the result holds without the assumption on k. So assume $n \ge 4$. Since $V \perp \langle -1 \rangle$ is a regular space of dimension at least 5, by our assumption on k, $V \perp \langle -1 \rangle$ is isotropic. Exercise 1.18 implies that V represents 1. We thus have a splitting $V \cong V' \perp \langle 1 \rangle$ for some $n-1$ dimensional regular quadratic space V'. It is easy to see that $[SV] = [SV']$ and $\mathrm{disc}V = \mathrm{disc}V'$. Similarly, we can write $W = W' \perp \langle 1 \rangle$ for W' a regular $n-1$ dimensional space with $[SW] = [SW']$ and $\mathrm{disc}W = \mathrm{disc}W'$. Thus we see that $[SV'] = [SW']$ and $\mathrm{disc}V' = \mathrm{disc}W'$. By induction, it follows that $V' \cong W'$ and thus $V \cong W$. $\square$

4 Quadratic Spaces over the p-Adics

4.1 Valuations and Complete Fields

Definition. A *valuation* on a field k is a map $|.| : k \to \mathbb{R}_{\geq 0}$ satisfying the following three axioms.

(V1) $|\alpha| = 0$ if and only if $\alpha = 0$.

(V2) $|\alpha\beta| = |\alpha| \cdot |\beta|$ for all $\alpha, \beta \in k$.

(V3) (*triangle inequality*) $|\alpha + \beta| \leq |\alpha| + |\beta|$ for all $\alpha, \beta \in k$.

A valuation is said to be *non-archimedean* (or is an *ultrametric*) if it further satisfies

(V3') $|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$ for all $\alpha, \beta \in k$.

If a valuation does not satisfy (V3'), then it is said to be *archimedean.*

A *valuated field* is simply a field equipped with a valuation.

Remark 4.1. It is easy to see that (V3') implies (V3).

Example 4.2. Let k be any subfield of $\mathbb{C}$ (say $k = \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$ for instance). Then the usual absolute value is a valuation on k, often denoted by $|.|_\infty$. It is an archimedean valuation.

Example 4.3. Consider $k = \mathbb{Q}$ and fix a prime p. Then, we define $|.|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ by

$$\left| p^r \frac{a}{b} \right|_p = p^{-r}$$

where $r \in \mathbb{Z}$, and $a, b \in \mathbb{Z}$ are such that $\gcd(a, b) = 1$ and $p \nmid a, b$. This is the *p-adic valuation.* One checks that this is a non-archimedean valuation.

In fact, for any number field K and any prime ideal $\mathfrak{p}$ of its ring of integers $\mathcal{O}_K$, we can similarly define a non-archimedean valuation $|.|_\mathfrak{p}$ on K.

Example 4.4. Given any field k, we have the *trivial valuation* $|.|_{triv}$ defined by $|0|_{triv} = 0$ and $|\alpha|_{triv} = 1$ for $\alpha \neq 0$.

Now, notice that (V1) and (V3) imply that $d(x, y) := |x - y|$ is a metric on the field K. In particular, we have a nice topology on k. However this topology can behave unexpectedly for non-archimedean fields; for instance, any point in a ball of a certain radius is the centre of the ball.

Definition. A valuated field k is said to be *complete* if k equipped with the induced metric is complete as a metric space.

Example 4.5. The fields $\mathbb{R}$ and $\mathbb{C}$ equipped with $|.|_\infty$ are complete. The trivial valuation is always complete.

We have some obvious properties that one can check immediately.

Lemma 4.6. *Let k be a field with a valuation $|.|$.*

1. $|1| = 1 = |-1|$.
2. *k is a* topological field*, i.e. addition, multiplication, negation, and inverses are all continuous with respect to the induced topology on k.*
3. *If $|.|$ is non-archimedean and $|\alpha| \neq |\beta|$ for $\alpha, \beta \in k$, then $|\alpha + \beta| = \max\{\alpha, \beta\}$.*
4. *If $|.|$ is non-archimedean and $\alpha_1, ..., \alpha_r \in k$ are such that $|\alpha_i| < |\alpha_1|$ for $2 \leq i \leq r$, then*
$$|\alpha_1 + \cdots + \alpha_r| = |\alpha_1|.$$
5. *$|.|$ is non-archimedean if and only if the set $\{|n| : n \in \mathbb{Z}\}$ is bounded (here, we view $\mathbb{Z} \to k$ via $1 \mapsto 1_k$).*

Exercise 4.7. Prove the above lemma.

Recall that given any metric space (X, d), there exists a unique metric space $(\widetilde{X}, \widetilde{d})$, called the *completion* of X, such that $X \hookrightarrow \widetilde{X}$ is a dense subset of $\widetilde{X}$ and such that $\widetilde{d}|_X = d$. Since a valuation induces a metric structure on the underlying field k, we can embed k as a dense subset of a unique metric space $(\widetilde{k}, \widetilde{d})$. Identifying $k \subset \widetilde{k}$, we can then define $\widetilde{|.|} : \widetilde{k} \to \mathbb{R}_{\geq 0}$ via $\widetilde{|\alpha|} = \widetilde{d}(0, \alpha)$ for all $\alpha \in \widetilde{k}$.

Proposition 4.8. *In the above setting, the field structure on k extends to induce a field structure on the metric space completion $\widetilde{k}$, so that $\widetilde{k}$ is a topological field containing k. The map $\widetilde{|.|} : \widetilde{k} \to \mathbb{R}_{\geq 0}$ is in fact a valuation. It is non-archimedean if and only if the original valuation $|.|$ on k was non-archimedean.*

Thus, any valuated field $(k, |.|)$ can be embedded as a dense subset of a complete valuated field $(\widetilde{k}, |.|)$.

While the proof is omitted, it follows by tedious checking using the usual construction of $\widetilde{k}$ as an equivalence class of sequences in k. See for example the proof in [Cas78, Chapter 3, Lemma 1.2].

Definition. The completion $\mathbb{Q}_p$ of $\mathbb{Q}$ equipped with the valuation $|.|_p$ from Example 4.3 is called the *field of p-adic numbers.*

Finally, let us discuss equivalence of valuations.

Definition. Two valuations on a field k are said to be *equivalent* if they induce the same topology on k.

Exercise 4.9. Suppose $|.|$ is a valuation on k equivalent to the trivial valuation. Then, show that $|.|$ is in fact the trivial valuation as well.

Exercise 4.10. Suppose $|.|, |.|'$ are two valuations on a field k. Prove that the following are equivalent.

1. $|.|'$ and $|.|$ are equivalent valuations.
2. For any $\alpha \in k$, we have $|\alpha|' < 1$ if and only if $|\alpha| < 1$.
3. There exists $\rho > 0$ such that $|\alpha|' = |\alpha|^\rho$ for all $\alpha \in k$.

Definition. An equivalence class of valuations on a field k not containing the trivial valuation is called a *place* of k.

Remark 4.11. Most often, this terminology is usually reserved for k a *global field*, i.e. for k a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p[t]$ for p prime.

We now list some important results on valuations and places of a field. Since the proofs are not really relevant, we shall omit them. Chapter 1 of [OMe73] contains all the proofs.

Proposition 4.12. *There is exactly one archimedean place on $\mathbb{Q}$, corresponding to the usual archimedean valuation $|.|_\infty$ on $\mathbb{Q}$.*

Definition. The unique archimedean place on $\mathbb{Q}$ is referred to as the *infinite* place on $\mathbb{Q}$.

Theorem 4.13 (Weak Approximation). *Suppose $|.|_i$ (for $1 \leq i \leq r$) are a finite number of inequivalent non-trivial valuations on a field k. For each $1 \leq i \leq r$, fix $\alpha_i \in k$. Then, for every $\epsilon > 0$ there exists $\alpha \in k$ such that $|\alpha - \alpha_i|_i < \epsilon$ for $1 \leq i \leq r$.*

Theorem 4.14 (Ostrowski). *Up to isomorphism of complete valuated fields, there are exactly two complete archimedean fields, namely $\mathbb{R}$ and $\mathbb{C}$.*

Definition. The *ordinary absolute value* on a complete archimedean field k is the valuation on k coinciding with the usual absolute value on $\mathbb{R}$ or $\mathbb{C}$ under any isomorphism $k \cong \mathbb{R}$ or $k \cong \mathbb{C}$.

An archimedean valuation $|.|$ on k is *real* (resp. *complex*) if the completion of k is $\mathbb{R}$ (resp. $\mathbb{C}$).

Definition. A complete field is said to be a *local field* if the valuation is not the trivial valuation and the topology is locally compact (i.e. every element has a compact neighbourhood).

Proposition 4.15. *The only local fields of characteristic 0 are $\mathbb{R}$, $\mathbb{C}$, or finite field extensions of $\mathbb{Q}_p$. The valuations in the non-archimedean case are* discrete, *i.e. the image in $\mathbb{R}_{\geq 0}$ of the field under the valuation is a discrete set.*

Theorem 4.16 (Ostrowski)**.** *The only places on $\mathbb{Q}$ are the (archimedean) infinite place, and the (non-archimedean) places corresponding to the p-adic valuations $|.|_p$. Moreover, $|.|_p$ is not equivalent to $|.|_q$ if and only if $p \neq q$.*

A Modules and Algebras

A.1 Modules

Let R be a commutative ring with identity.

Definition. An *R-module* is an abelian group $(M, +)$ equipped with a 'multiplication by R' map

$$\cdot : R \times M \to M$$

such that, for all $r, s \in R$ and all $x, y \in M$ we have

- $r \cdot (x + y) = r \cdot x + r \cdot y$,
- $(r + s) \cdot x = r \cdot x + s \cdot x$,
- $(rs) \cdot x = r \cdot (s \cdot x)$, and
- $1 \cdot x = x$.

Example A.1. Modules over a field are called vector spaces.

Example A.2. All abelian groups are $\mathbb{Z}$-modules.

Definition. A *submodule* of an R-module M is a subgroup $N \subset M$ such that $r \cdot n \in N$ for all $r \in R$ and all $n \in N$. Clearly, a submodule is an R-module in its own right.

Given a submodule N of a module M, we can form the quotient of abelian groups M/N. We may equip this quotient group by the following action of R:

$$r \cdot (m + N) = rm + N.$$

One can then check that M/N equipped with this R-action is itself an R-module. Thus we can take quotients of modules.

Definition. A *homomorphism of R-modules* from M to N is a homomorphism of abelian groups $f : M \to N$ such that $f(rx) = rf(x)$ for all $x \in M$ and all $r \in R$. An *isomorphism* is a bijective homomorphism.

Definition. A module M is *finitely generated* if there exists a finite collection of elements $x_1, ..., x_n \in M$ such that for any $x \in M$ there exists $c_i \in R$ such that

$$x = c_1x_1 + c_2x_2 + \cdots + c_nx_n.$$

A module M is *free* if there exists a collection $S \subset M$ (possibly infinite) that forms a *basis* for M, i.e. every $x \in M$ can be written as

$$x = \sum_{y \in S} c_y y$$

for unique choices of $c_y \in R$, where $c_y = 0$ for all but finitely many $y \in S$.

Example A.3. R^n is a finitely generated free module. In fact, every finitely generated free module is isomorphic to R^n for some n.

Definition. Suppose S is any subset of an R-module M. The *R-submodule generated by S* is defined to be

$$\langle S \rangle := \bigcap_{N \supseteq S} N$$

where N runs through all submodules of M containing S.

Concretely, we have

$$\langle S\rangle = \left\{\sum_{i=1}^{k} r_i x_i : k \in \mathbb{N}, r_i \in R, x_i \in S\right\}.$$

A.2 Algebras

As usual, we let R be a commutative ring. However, we will only need the case where R is a field.

Definition. An *R-algebra* A is an R-module equipped with a binary operation (multiplication)

$$\cdot : A \times A \to A$$

such that, for any $r, s \in R$ and any $x, y, z \in A$, we have

- $(x + y) \cdot z = x \cdot z + y \cdot z$,
- $x \cdot (y + z) = x \cdot y + x \cdot z$,
- $(ax) \cdot (by) = (ab)(x \cdot y)$.

An R-algebra A is *associative* if the above binary operation also satisfies $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x, y, z \in A$.

An R-algebra A is *commutative* if the above binary operation also satisfies $x \cdot y = y \cdot x$ for all $x, y \in A$.

An R-algebra A is *unital* if there exists an element $1_A \in A$ such that $1_A \cdot x = x \cdot 1_A = x$ for all $x \in A$.

Example A.4. For any commutative ring R, the matrices $M_n(R)$ are an associative unital R-algebra.

Example A.5. If S is any ring with R as a subring, then S is a associative R-algebra. If S is commutative and with identity, then S is a commutative associative unital R-algebra. Thus, for instance, $\mathbb{C}$ is a 2-dimensional commutative associative unital $\mathbb{R}$-algebra.

For us, most of the algebras tend to be unital and associative.

Definition. Given two R-algebras A and B, a *homomorphism of R-algebras* is a homomorphism of R-modules $f : A \to B$ further satisfying $f(x \cdot y) = f(x) \cdot f(y)$.

Thus, given any rings S_1 and S_2 both containing a commutative ring R, a homomorphism $S_1 \to S_2$ of rings is a homomorphism of R-algebras if and only if it acts as the identity on R.

A.3 Tensor Products

We shall define tensor products using a *universal property*. Again, R is a commutative ring.

Definition. Suppose M and N are R-modules. The *tensor product of M and N* is an R-module $M \otimes_R N$ equipped with a bilinear map $\otimes : M \times N \to M \otimes_R N$ satisfying the following universal property: For any R-module T with a bilinear map $B : M \times N \to T$, there exists a unique morphism $f : M \otimes_R N \to T$ of R-modules satisfying

$$B(m, n) = f(m \otimes n)$$

for all $m \in M$ and $n \in N$.

$$\begin{tikzcd}
M \times N \arrow[d, "- \otimes -"'] \arrow[dr, "B"] & \\
M \otimes_R N \arrow[r, dashed, "\exists! f"'] & T
\end{tikzcd}$$

Due to the universal property, if the tensor product exists it is unique up to unique isomorphism. That it exists can be checked easily via the following construction:

Let X be the free R-module generated by $M \times N$. Let Y be the submodule of X generated by all elements of X of the form

$$(m_1 + m_2, n) - (m_1, n) - (m_2, n), \quad (m, n_1 + n_2) - (m, n_1) - (m, n_2), \quad \text{and} \quad (rm, n) - (m, rn).$$

Then one can check that X/Y satisfies the universal property of tensor products, so that $M \otimes_R N = X/Y$. Thus, as a set, $M \otimes_R N$ consists of finite-linear combination of formal symbols $m \otimes n$, where the symbol $- \otimes -$ satisfies

$$(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n, \quad m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2, \quad \text{and} \quad r(m \otimes n) = (rm) \otimes n = m \otimes (rn).$$

We have a lot of straightforward properties of tensor products:

Proposition A.6. *Let R be a commutative ring, and M, N, L are R-modules. Then, we have the following canonical isomorphisms of R-modules:*

1. $M \otimes_R R \cong M$*;*
2. $M \otimes_R N \cong N \otimes_R M$*;*
3. $L \otimes_R (M \otimes_R N) \cong (L \otimes_R M) \otimes_R N$*.*
4.

It also turns out that the tensor product of finitely generated R-modules is also finitely generated.

Now suppose S is a commutative associative unital R-algebra. In particular, it is an R-module, so that we can form the tensor product $M \otimes_R S$ with any R-module M. We can equip $M \otimes_R S$ with an S-action by defining

$$s \cdot (m \otimes t) := m \otimes (st)$$

and then extending linearly. In this way, $M \otimes_R S$ is an S-module. This process of producing S-modules from R-modules is called *base-change*. One can think of base-change as simply a change in coefficients. For instance, we have

$$M_n(R) \otimes_R S \cong M_n(S) \quad \text{and} \quad R^n \otimes_R S \cong S^n.$$

In fact, for us, just these two facts is more than enough.

Proposition A.7. *Suppose L is an R-module, and M and N are S-modules for a commutative associative unital R-algebra S. We then have the following canonical isomorphism*

$$L \otimes_R (M \otimes_S N) \cong (L \otimes_R M) \otimes_S N$$

if M is an S-module then it is also an R-module by simply restricting to the image of R in S.

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.