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

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

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 $H = \langle(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix})\rangle$ 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 $\sigma \in O(V)$. □

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* $\mathrm{ind}V$ 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.

Theorem 1.29 (Witt's Decomposition Theorem)**.** *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.

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. □

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

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

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

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* $\mathrm{ind}^+V = \mathrm{ind}^+V'$ *and* $\mathrm{ind}^-V = \mathrm{ind}^-V'$.

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

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

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 $2x_2\mathbf{i}^2 \in k^*$. □

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. $Y \in \mathcal{C}$. □

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

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

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. □

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

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

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 $1 \leq n \leq 3$. 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 $V \cong W$. □

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 $n \leq 3$ the result holds without the assumption on k. So assume $n \geq 4$. 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 $V \cong W$. □

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 $p \neq q$.*

4.2 Non-Archimedean Local Fields

We now take an in-depth look at non-archimedean local fields of characteristic 0. The most basic example of such a field is $\mathbb{Q}_p$ for p a prime.

Let K be a non-archimedean local field with valuation $|.|$. Set

$$\mathcal{O}_K := \{\alpha \in K : |\alpha| \leq 1\},$$
$$\mathfrak{m}_K := \{\alpha \in K : |\alpha| < 1\}.$$

Definition. $\mathcal{O}_K$ is called the *ring of integers* of K.

Example 4.17. The ring of integers of $\mathbb{Q}_p$ is denoted by $\mathbb{Z}_p$, the ring of *p-adic integers*. One can check that $\mathfrak{m}_{\mathbb{Q}_p} = p\mathbb{Z}_p$.

Proposition 4.18. *The subset $\mathcal{O}_K$ is actually a subring of K, and $\mathfrak{m}_K$ is a maximal ideal of $\mathcal{O}_K$. In fact, $\mathcal{O}_K$ is a local ring, with unique maximal ideal $\mathfrak{m}_K$.*

This result justifies calling $\mathcal{O}_K$ the 'ring of integers' of K. Since $\mathcal{O}_K$ is a local ring, it is in particular a PID. The group $\mathcal{O}_K^*$ of units of $\mathcal{O}_K$ satisfies $\mathcal{O}_K^* = \mathcal{O}_K \setminus \mathfrak{m}_K$, and so $|u| = 1$ for all units u of $\mathcal{O}_K$.

Definition. A *uniformiser* of K is any generator of the principal ideal $\mathfrak{m}_K$.

The *residue field* of K is the field $\kappa_K := \mathcal{O}_K/\mathfrak{m}_K$. The canonical projection map $\mathcal{O}_K \to \kappa_K$ is denoted by $\alpha \mapsto \overline{\alpha}$.

It is a fact that κ_K is a finite field for K a non-archimedean local field. In particular, it has characteristic p for some prime p. This is often referred to as the *residue characteristic*.

Example 4.19. A uniformiser of $\mathbb{Q}_p$ is p. The residue field of $\mathbb{Q}_p$ is $\mathbb{F}_p$.

Pick a uniformiser π. One can check easily that every non-zero element $\alpha \in K^*$ can be written as

$$\alpha = \pi^r \cdot u$$

for some $u \in \mathcal{O}_K^*$ and some $r \in \mathbb{Z}$. This decomposition is unique for a fixed choice of π. This integer r is often referred to as the *order* of α, written $r = \mathrm{ord}_K \alpha$.

In particular, the valuation is discretely valued in the sense that the image of the group homomorphism

$$|.| : K^* \to \mathbb{R}_{>0}$$

is cyclic and generated by $|\pi|$. Notice that $|\pi| \in \mathbb{R}_{>0}$ only depends on $|.|$ and not on our choice of uniformiser. Since we only care about valuations up to equivalence, it doesn't matter what the exact value of $|\pi|$ is. We can thus choose a specific normalization.

Definition. The valuation $|.|$ of a non-archimedean local field is said to be *normalised* if $|\pi| = \frac{1}{\#\kappa_K}$ for any uniformiser π.

It is clear that any non-archimedean local field has a unique normalised valuation.

Example 4.20. The usual p-adic valuation $|.|_p$ introduced previously is the normalised valuation of $\mathbb{Q}_p$.

Proposition 4.21. *Let S be any set of coset representatives of $\mathcal{O}_K/\mathfrak{m}_K$ (in particular, S is in bijection with κ_K). Suppose that the coset representative of $0 + \mathfrak{m}_K$ in $\mathcal{O}_K$ is chosen to be 0. Let π be a uniformiser of K.*

Then, any element $\alpha \in \mathcal{O}_K$ can be written uniquely as

$$\alpha = \sum_{i \geq 0} c_i \pi^i$$

for $c_i \in S$ (here, the power series converges with respect to the valuation $|.|$).

In particular, every element of $\mathbb{Z}_p$ is of the form $\sum_{i \geq 0} c_i p^i$ for a unique choice $c_i \in \{0, 1, 2, ..., p-1\}$.

Proof Sketch. We prove the special case for $\mathbb{Z}_p$. Set $S = \{0, 1, 2, ..., p-1\}$. Let $\alpha \in \mathbb{Z}_p$ be fixed. Then $\overline{\alpha} \in \mathbb{F}_p$, and so we can find a unique $c_0 \in S$ such that $\overline{\alpha} = \overline{c}_0$. This is equivalent to $\alpha - c_0 \in p\mathbb{Z}_p$, and so we write $\alpha = c_0 + p\alpha_1$ for a unique $\alpha_1 \in \mathbb{Z}_p$. We can continue this process with α_1, and write $\alpha_1 = c_1 + p\alpha_2$ for a unique $c_1 \in S$ and unique $\alpha_2 \in \mathbb{Z}_p$. Continuing, we have $\alpha_2 = c_2 + p\alpha_3$, $\alpha_3 = c_3 + p\alpha_4$, etc. The result follows. □

The following theorem gives an easy way to construct elements of $\mathcal{O}_K$.

Theorem 4.22 (Hensel's Lemma)**.** *Suppose K is a non-archimedean local field with valuation $|.|$. Let $f(x) \in \mathcal{O}_K[x]$ be a polynomial. Suppose there exists $\alpha \in \mathcal{O}_K$ such that $|f(\alpha)| < |f'(\alpha)|^2$. Then, there exists $\beta \in \mathcal{O}_K$ such that $\beta - \alpha \in \mathfrak{m}_K$ and such that $f(\beta) = 0$.*

Here, $f'(x)$ denotes the formal derivative of a polynomial $f \in \mathcal{O}_K[x]$. We omit the proof, though a proof for the case of $K = \mathbb{Q}_p$ is given in [Cas78].

Corollary 4.22.1 (Local Square Theorem)**.** *Suppose $\alpha \in \mathcal{O}_K^*$ is such that $|\alpha - 1| < |4|$. Then α is a perfect square in $\mathcal{O}_K^*$, i.e. $\alpha = \beta^2$ for some $\beta \in \mathcal{O}_K^*$.*

In particular, if $\alpha \in \mathbb{Z}_p$ satisfies

$$|\alpha - 1|_p \leq \begin{cases} \frac{1}{p} & \text{if } p \text{ odd,} \\ \frac{1}{8} & \text{if } p = 2, \end{cases}$$

then α is a perfect square in $\mathbb{Z}_p$.

Proof. This follows immediately from Hensel's Lemma applied to the polynomial $f(x) = x^2 - \alpha$. □

The following corollary is left as an exercise.

Corollary 4.22.2. *Suppose K is a non-archimedean local field with uniformiser π, and let $\alpha \in K^*$. Then $\alpha \in (K^*)^2$ if and only if $r := \operatorname{ord}_K \alpha$ is even and $\overline{(\alpha/\pi^r)} \in \kappa_K$ is a perfect square.*

Exercise 4.23. Using Hensel's Lemma, prove Corollary 4.22.2.

Corollary 4.22.2, along with some basic modular arithmetic, gives us the following result.

Corollary 4.23.1.

- *$\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 = \langle 2 \rangle \times \langle -1 \rangle \times \langle 5 \rangle$ is isomorphic as a group to $(\mathbb{Z}/2\mathbb{Z})^3$.*
- *for p an odd prime, let $r \in \mathbb{Z}$ be any choice of quadratic non-residue (i.e. $\overline{r} \notin (\mathbb{F}_p^*)^2$). Then $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 = \langle p \rangle \times \langle r \rangle$ is isomorphic as a group to $(\mathbb{Z}/2\mathbb{Z})^2$.*

In fact, one can use Hensel's Lemma to prove the following generalisation of the previous corollary.

Corollary 4.23.2. *If K has odd residue characteristic, then $\mathcal{O}_K^*/(\mathcal{O}_K^*)^2$ is a group of order 2. Thus, $K^*/(K^*)^2$ is a group of order 4.*

Remark 4.24. For K a non-archimedean local field with residue characteristic equal to 2, it turns out that the group $K^*/(K^*)^2$ has order $4(\#\kappa_K)^{\operatorname{ord}_K 2}$.

Exercise 4.25. Show that $\mathbb{Z}_2^* = (\mathbb{Z}_2^*)^2 \cup 3(\mathbb{Z}_2^*)^2 \cup 5(\mathbb{Z}_2^*)^2 \cup 7(\mathbb{Z}_2^*)^2$. If $\alpha \in \mathbb{Z}_2^*$ and $a \in \{1, 3, 5, 7\}$, show moreover that $\alpha \in a(\mathbb{Z}_2^*)^2$ if and only if $\alpha \equiv a \pmod 8$.

Exercise 4.26. Suppose p is odd. Let $a_1, a_2, a_3 \in \mathbb{Q}_p$ be such that $|a_1|_p = |a_2|_p = |a_3|_p$. Show that the quadratic space $V = \langle a_1 \rangle \perp \langle a_2 \rangle \perp \langle a_3 \rangle$ is regular and isotropic.

With the theory of non-archimedean local fields somewhat set up, we now go back to studying quadratic spaces over non-archimedean local fields. If the residue characteristic is odd, then the we already know everything about quadratic forms over the residue field. Due to results like Hensel's lemma, we should be able to deduce facts about quadratic spaces over such non-archimedean local fields. However, for residue characteristic 2, we have no such hope. Quadratic forms behave very strangely in characteristic 2, and so we need to modify the previous strategy to understand quadratic forms over such non-archimedean local fields.

This motivates distinguishing non-archimedean local fields into two types.

Definition. A non-archimedean local field is said to be a *dyadic local field* if its residue characteristic is odd. Otherwise, it is said to be *non-dyadic local field*.

Note that K is dyadic if and only if $0 < |2| < 1$.

4.3 Quaternion Algebras over Non-Archimedean Local Fields

Suppose that K is a non-archimedean local field of characteristic 0; for instance, $K = \mathbb{Q}_p$. Let $\mathcal{O}_K$ be its ring of integers, $\mathfrak{m}_K$ its unique maximal ideal, and $\kappa_K = \mathcal{O}_K/\mathfrak{m}_K$ its residue field. Set $e = \operatorname{ord}_K 2$; then $e = 0$ for K non-dyadic while $e \geq 1$ for K dyadic.

Recall the Brauer group; we know that $\operatorname{Br}(K)[2]$ contains the Brauer class of all quaternion algebras. It turns out we can determine $\operatorname{Br}(K)$ completely.

Theorem 4.27 ((Corollary of) Local Class Field Theory)**.** $\mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$.

Corollary 4.27.1. $\mathrm{Br}(K)[2] \cong \mathbb{Z}/2\mathbb{Z}$.

In particular, local class field theory implies that there are exactly two division algebras over K, namely K itself and another non-commutative division algebra. We try to prove this fact directly, without using local class field theory.

Definition. Call a unit $\Delta \in \mathcal{O}_K^*$ *distinguished* if $\Delta + \mathfrak{m}_K^{2e}$ is a square in the ring $\mathcal{O}_K/\mathfrak{m}_K^{2e}$, but Δ is not a square in $\mathcal{O}_K/\mathfrak{m}_K^{2e+1}$.

In other words, $\Delta \in \mathcal{O}_K^*$ is distinguished if there exists $\epsilon \in \mathcal{O}_K^*$ with $\Delta - \epsilon^2 \in \mathfrak{m}_K^{2e}$, but no such ϵ exists that satisfies $\Delta - \epsilon^2 \in \mathfrak{m}_K^{2e+1}$.

Example 4.28. If K is non-dyadic, we know already that $\kappa_K^*/(\kappa_K^*)^2$ is of order 2, and it is easy to see that $\Delta \in \mathcal{O}_K^*$ is such that $\overline{\Delta} \notin (\kappa_K^*)^2$.

Example 4.29. If $K = \mathbb{Q}_2$, we can take $\Delta = 5$, since $5 \equiv 1 \pmod 4$ is a square, but 5 is not a square in $\mathbb{Z}/8\mathbb{Z}$.

Lemma 4.30. *$\Delta(\mathcal{O}_K^*)^2$ is an invariant of the field K, i.e. given any other distinguished unit $\Delta' \in \mathcal{O}_K^*$, there exists $\epsilon \in \mathcal{O}_K^*$ such that $\Delta' = \Delta\epsilon^2$.*

Proof. For K non-dyadic, this simply follows from the fact that $\mathcal{O}_K^*/(\mathcal{O}_K^*)^2$ is a group of order 2. Suppose $K = \mathbb{Q}_2$. Then $e = 1$. If Δ is any distinguished element, then Δ is a square modulo 4 but not modulo 8. Thus $\Delta \equiv 1 \pmod 4$ and $\Delta \not\equiv 1 \pmod 8$. These two imply that $\Delta \equiv 5 \pmod 8$, and hence that $\Delta \in 5(\mathbb{Z}_2^*)^2$. □

Remark 4.31 (for those who know algebraic number theory). In short, it turns out that Δ is distinguished if and only if $K(\sqrt{\Delta})$ is a quadratic unramified extension of K. In particular, since there is a unique quadratic unramified extension of K, it actually follows immediately that $\Delta(K^*)^2$ is an invariant of the field K.

Lemma 4.32. *Let V be a binary quadratic space over K. Let $\Delta \in \mathcal{O}_K$ denote any distinguished unit. Suppose $\mathrm{disc}V = \pi u(K^*)^2$ for some uniformiser π of K and some $u \in \mathcal{O}_K^*$. If $\gamma \in K^*$, then V represents either γ or $\gamma\Delta$, but not both.*

Proof. By replacing the quadratic form Q with $\frac{1}{\gamma}Q$, we may assume without loss of generality that $\gamma = 1$. Since $\mathrm{disc}V = \pi u(k^*)^2$, we can write $V = \langle\epsilon\rangle \perp \langle\delta\pi\rangle$ for some $\epsilon, \delta \in \mathcal{O}_K^*$.

Let us show that V represents at least one of 1 or Δ. For K non-dyadic, we know already that $\mathcal{O}_K^* = (\mathcal{O}_K^*)^2 \sqcup \Delta(\mathcal{O}_K^*)^2$, and so $\langle\epsilon\rangle$ represents either 1 or Δ. We now prove this for $K = \mathbb{Q}_2$, so that $\Delta \in 5(\mathbb{Z}_2^*)^2$. It suffices to assume that $\epsilon \in \{1, 3, 5, 7\}$. If $\epsilon = 1$ or $\epsilon = 5$, the claim follows immediately. We claim that $\epsilon \in \{3, 7\}$ cannot occur. Write $\epsilon_1 = \frac{\epsilon-1}{2}$. Choose $\lambda \in \mathbb{Z}_2^*$ such that $\lambda^2\delta \equiv -\epsilon_1 \pmod 2$. One can then compute that V represents $1 + 2\epsilon_1 + 2\delta\lambda^2$. However, $1 + 2\epsilon_1 + 2\delta\lambda^2 \equiv 1 \pmod 4$, and we are done.

We now need to show that V cannot represent both 1 and Δ simultaneously. Suppose it did. Then we would be able to write

$$V \cong \langle 1\rangle \perp \langle\pi u\rangle \cong \langle\Delta\rangle \perp \langle\Delta\pi u\rangle.$$

Thus $\Delta = \xi^2 + \eta^2\pi u$ for some $\xi, \eta \in K$. Then

$$1 = |\xi^2 + \eta^2\pi u| = \max\{|\xi|^2, |u\pi\eta^2|\}.$$

It follows that ξ has to be a unit and η an integer. Hence, $\Delta/\xi^2 = 1 + u\pi\beta^2$ for some $\beta \in \mathcal{O}_K$. For $K = \mathbb{Q}_2$, this is impossible, since the right hand side is $1 \pmod 8$ whereas the left hand side is $5 \pmod 8$. For K dyadic, this implies that $\overline{\Delta} \in (\kappa_K^*)^2$, which is impossible. □

Proposition 4.33. *Let π be any uniformiser and Δ any distinguished unit of K. Any quaternion algebra is isomorphic to either $M_2(k) \cong (\pi, 1)_K$ or to the division algebra $(\pi, \Delta)_K$.*

Proof. Lemma 4.32 says that $\langle\pi\rangle \perp \langle\Delta\rangle$ does not represent 1. It follows from Proposition 3.9 that $(\pi, \Delta)_K$ is a division algebra. By Proposition 3.9 again, it suffices to show that a quaternion algebra A that is also a division

algebra must be Brauer equivalent (thus isomorphic) to $(\pi, \Delta)_K$. In fact, what we will show is that the Brauer class of any quaternion algebra lies in the cyclic subgroup of $\mathrm{Br}(K)$ generated by $[(\pi, \Delta)_K]$. Since this subgroup is of order 2, the result would then follow.

Let us first compute $[(\epsilon, \delta)_K]$ for $\epsilon, \delta \in \mathbb{Z}_p^*$. For K non-dyadic, we claim that $\langle \epsilon \rangle \perp \langle \delta \rangle$ represents 1. If $\epsilon = 1$, we are done, so suppose $\epsilon = \Delta$. For K non-dyadic, we already know that binary forms over κ_K are universal, and so there exists $\xi, \eta \in \mathcal{O}_K$ such that $\Delta\xi^2 + \delta\eta^2 \equiv 1 \pmod{\pi}$. By the local square theorem, it follows that $\Delta\xi^2 + \delta\eta^2$ is a square, and hence $\langle \Delta \rangle \perp \langle \delta \rangle$ represents 1.

Now suppose $K = \mathbb{Q}_2$. Since $5(1)^2 + \delta(2)^2 \equiv 1 \pmod{8}$ for any $\delta \in \mathbb{Z}_2^*$, the local square theorem implies that $\langle 5 \rangle \perp \langle \delta \rangle$ represents 1. Thus $(5, \delta)_{\mathbb{Q}_2} \cong (1, 2)_{\mathbb{Q}_2}$. It remains to check the case of $(a, b)_{\mathbb{Q}_2}$ for $a, b \in \{3, 7\}$. By computing discriminants and Hasse algebras, and appealing to Theorem 3.37, one can check that

$$\langle -3 \rangle \perp \langle -3 \rangle \perp \langle 9 \rangle \cong \langle -3 \rangle \perp \langle -7 \rangle \perp \langle 21 \rangle \cong \langle -7 \rangle \perp \langle -7 \rangle \perp \langle 49 \rangle \cong \langle -2 \rangle \perp \langle -5 \rangle \perp \langle 10 \rangle .$$

Proposition 3.8 then implies that

$$(3, 3)_{\mathbb{Q}_2} \cong (3, 7)_{\mathbb{Q}_2} \cong (7, 7)_{\mathbb{Q}_2} \cong (2, 5)_{\mathbb{Q}_2}.$$

Hence, in all cases, we see that any quaternion algebra over $\mathbb{Q}_2$ is Brauer equivalent to either $(1, 2)_{\mathbb{Q}_2}$ or $(5, 2)_{\mathbb{Q}_2}$.

We now consider quaternion algebras of the form $(\epsilon, \pi)_K$. For K non-dyadic, either ϵ is a square or Δ times a square, and we are done. So suppose $K = \mathbb{Q}_2$. We just need to check whether $(3, 2)_{\mathbb{Q}_2}$ and $(7, 2)_{\mathbb{Q}_2}$ are Brauer equivalent to either $(1, 2)_{\mathbb{Q}_2}$ or $(5, 2)_{\mathbb{Q}_2}$. However, note that

$$[(7, 2)_{\mathbb{Q}_2}] = [(15, 2)_{\mathbb{Q}_2}] = [(3, 2)_{\mathbb{Q}_2}][(5, 2)_{\mathbb{Q}_2}]$$

so that we just need to check whether $[(3, 2)_{\mathbb{Q}_2}] \in \{[(1, 2)_{\mathbb{Q}_2}], [(5, 2)_{\mathbb{Q}_2}]\}$. However, using Theorem 3.37 and Proposition 3.8, it can be checked that $(3, 2)_{\mathbb{Q}_2} \cong (5, 2)_{\mathbb{Q}_2}$.

Let us now consider the general case, where K may be either dyadic or non-dyadic. Suppose $A = (\alpha, \beta)_K$. Write $\alpha = \epsilon\pi^a$ and $\beta = \delta\pi^b$ for $a, b \in \mathbb{Z}$ and $\epsilon, \delta \in \mathcal{O}_K^*$. By Lemma 3.10, we may suppose without loss of generality that $a, b \in \{0, 1\}$. Using Lemma 3.10 again, we see that the Brauer class $[A]$ is a product (in $\mathrm{Br}(K)$) of Brauer classes of the form $[(\epsilon, \delta)_K]$ or $[(\epsilon, \pi)_K]$ for units $\epsilon, \delta \in \mathcal{O}_K^*$. By the previous special cases, we see that $[A]$ is in the cyclic subgroup of $\mathrm{Br}(K)$ generated by $[(\pi, \Delta)_K]$. □

Corollary 4.33.1. *Assuming the Merkurjev-Suslin theorem,* $\mathrm{Br}(K)[2] \cong \mathbb{Z}/2\mathbb{Z}$.

4.4 Hilbert Symbols and Hasse Symbols

We maintain the notation set up in the previous section. The results of the previous section motivates the following definition.

Definition. The *Hilbert Norm Residue Symbol* $[\alpha, \beta]_K$ for $\alpha, \beta \in K^*$ is defined to be

$$[\alpha, \beta]_K := \begin{cases} 1 & \text{if } (\alpha, \beta)_K \sim_K (\pi, 1)_K, \\ -1 & \text{if } (\alpha, \beta)_K \sim_K (\pi, \Delta)_K. \end{cases}$$

Remark 4.34. The above definition holds for *any* local field of characteristic 0.

As a result of Proposition 3.9, we have the following.

Proposition 4.35. *Suppose $\alpha, \beta \in K^*$. Then $[\alpha, \beta]_K = 1$ if and only if there exists $\xi, \eta \in K$ such that $\alpha\xi^2 + \beta\eta^2 = 1$.*

Remark 4.36. This proposition gives a very elementary criterion to determine the Brauer class of any quaternion algebra over K.

Remark 4.37. In most references, the description of the Hilbert symbol given in the proposition is taken as the definition of the Hilbert symbol. One then shows the interpretation in terms of quaternion algebras.

One can now rewrite a lot of previous results on quaternion algebras in terms of the Hilbert residue symbol.

Lemma 4.38. *Suppose K is a non-archimedean local field*

1. $[1,\alpha]_K = [\alpha,-\alpha]_K = [\alpha,1-\alpha]_K = 1$ *for any* $\alpha \in K^*$.
2. $[\beta,\alpha]_K = [\alpha,\beta]_K = [\alpha\lambda^2,\beta\mu^2]_K$ *for any* $\alpha,\beta,\lambda,\mu \in K^*$.
3. $[\alpha,\beta]_K[\alpha,\gamma]_K = [\alpha,\beta\gamma]_K$ *for any* $\alpha,\beta,\gamma \in K^*$
4. $[\alpha,\beta]_K = [\alpha,-\alpha\beta]_K$ *for* $\alpha,\beta \in K^*$. *In particular,* $[\alpha,\alpha]_K = [\alpha,-1]_K$ *for* $\alpha \in K^*$.
5. *If K is non-dyadic, π is a uniformiser of K and Δ a distinguished unit, then* $[\pi,\Delta]_K = -1$.
6. *If K is non-dyadic, then for any* $\epsilon,\delta \in \mathcal{O}_K^*$, *we have* $[\epsilon,\delta] = 1$.

Notice that one can compute any Hilbert norm residue symbol by using just the rules given in the previous lemma.

Thus, the Hilbert norm residue symbol gives a nice and clean way to compute the Brauer equivalence class of any central simple K-algebra that happens to be a tensor product of quaternion algebras. In particular, it gives us a quick way to compute Hasse algebras.

Definition. Suppose V is a regular quadratic space over a local ring K (of characteristic 0). The *Hasse Symbol*

$$h(V) := \begin{cases} 1 & \text{if } SV \sim_K (\pi,1)_K, \\ -1 & \text{if } SV \sim_K (\pi,\Delta)_K. \end{cases}$$

As before, we can translate properties of the Hasse algebra into properties of the Hasse symbol. For instance, if $V = \langle\alpha_1\rangle \perp \cdots \perp \langle\alpha_n\rangle$, then

$$h(V) = \prod_{1\le i\le j\le n} [\alpha_i,\alpha_j]_K \in \{\pm 1\}.$$

More generally, if $V = U \perp W$ then

$$h(V) = [\mathrm{disc}U, \mathrm{disc}W]_k h(U)h(W).$$

We have an interpretation of the Hilbert norm residue symbol in terms of the quadratic reciprocity law from elementary number theory. Suppose p is an odd prime. Recall the *Legendre symbol* $(\frac{a}{p})$ for $a \in \mathbb{Z}$ prime to p: we set $(\frac{a}{p}) = 1$ if a is a square modulo p, and we set $(\frac{a}{p}) = -1$ otherwise. By the local square theorem, notice that a is a square modulo p if and only if $a \in \mathbb{Z}_p^*$ is a perfect square.

Lemma 4.39. *Suppose $a,b \in \mathbb{Z}$ are integers prime to p. Then* $[a,b]_{\mathbb{Q}_p} = 1$, *and that* $[a,p]_{\mathbb{Q}_p} = (\frac{a}{p})$. *If* $a = -1$, *we have* $[-1,p]_{\mathbb{Q}_p} = (-1)^{\frac{1}{2}(p-1)}$.

Lemma 4.40. *Suppose $a,b \in \mathbb{Z}$ are odd integers. Then* $[a,b]_{\mathbb{Q}_2} = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$ *and* $[a,2]_{\mathbb{Q}_2} = (-1)^{\frac{a^2-1}{8}}$

Exercise 4.41. Prove Lemma 4.39 and Lemma 4.40.

Recall the original quadratic reciprocity law.

Theorem (Quadratic Reciprocity)**.** *Suppose p and q are distinct odd primes. Then, we have*

$$(\tfrac{p}{q})(\tfrac{q}{p}) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}, \quad (\tfrac{-1}{p}) = (-1)^{\frac{p-1}{2}}, \quad \text{and} \quad (\tfrac{2}{p}) = (-1)^{\frac{1}{8}(p^2-1)}.$$

This law can now be recast in terms of the Hilbert symbols. The formulae for $(\frac{-1}{p})$ and $(\frac{2}{p})$ have already been proven.

Theorem 4.42 (Quadratic Reciprocity)**.** *Suppose p and q are distinct odd primes. Then, we have*

$$[p,q]_{\mathbb{Q}_p}[p,q]_{\mathbb{Q}_q} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

4.5 Classifying All Quadratic Spaces over Non-Archimedean Local Fields

Let us now attempt to classify all quadratic spaces over a non-archimedean local field K. Fix a uniformiser π and a distinguished unit Δ of K. As usual, $\mathcal{O}_K$ is the ring of integers of K. First, we study binary spaces.

Lemma 4.43. *A regular binary quadratic space V over K represents $\beta \in K^*$ if and only if*

$$[\beta, -\text{disc}V]_K = h(V)[-1, \text{disc}V]_K.$$

Proof. Write $V = \langle \alpha_1 \rangle \perp \langle \alpha_2 \rangle$. Then V represents β if and only if $\langle \alpha_1/\beta \rangle \perp \langle \alpha_2/\beta \rangle$ represents 1. By Proposition 4.35, this is true if and only if $[\alpha_1\beta, \alpha_2\beta]_K = 1$. Now, a quick computation shows that

$$[\alpha_1\beta, \alpha_2\beta]_K = [\alpha_1, \alpha_2]_K[\alpha_1, \beta]_K[\alpha_2, \beta]_K[\beta, \beta]_K = [\alpha_1, \alpha_2]_K[\beta, \alpha_1]_K[\beta, \alpha_2]_K[\beta, -1]_K = [\alpha_1, \alpha_2]_K[\beta, -\text{disc}V]_K.$$

On the other hand, note that

$$h(V) = [\alpha_1, \alpha_2]_K[\alpha_1, \alpha_1]_K[\alpha_2, \alpha_2]_K = [\alpha_1, \alpha_2]_K[\alpha_1, -1]_K[\alpha_2, -1]_K = [\alpha_1, \alpha_2]_K[-1, \text{disc}V]_K.$$

Thus

$$h(V)[\alpha_1\beta, \alpha_2\beta]_K = [\beta, -\text{disc}V]_K[-1, \text{disc}V]_K,$$

and so the result follows. □

Corollary 4.43.1. *If V is a regular anisotropic binary quadratic space over K and $1 \in Q(V)$, then $Q(V \setminus \{0\})$ is an index 2 subgroup of K^*.*

Proof. As $1 \in Q(V)$, the lemma says $h(V)[-1, \text{disc}V]_K = 1$. We have a group homomorphism $K^* \to \{\pm 1\}, \gamma \mapsto [-\text{disc}V, \gamma]_K$. The lemma then clearly implies that the kernel of this homomorphism is $Q(V) \cap K^* = Q(V \setminus \{0\})$. This map is surjective since $\text{disc}V \neq -(K^*)^2$, for otherwise $V \cong \langle 1 \rangle \perp \langle -1 \rangle$ is isotropic. □

Corollary 4.43.2. *If $\text{disc}V = -\Delta(K^*)^2$, then $Q(V \setminus \{0\})$ can only be either $\mathcal{O}_K^*(K^*)^2$ or $\pi\mathcal{O}_K^*(K^*)^2$.*

Proof. If K is non-dyadic, then the corollary follows easily since $[\pi, \Delta]_K = -1$ and $[\epsilon, \Delta]_K = 1$ for all $\epsilon \in \mathcal{O}_K^*$. Suppose now that $K = \mathbb{Q}_2$, by scaling, suppose without loss of generality that $1 \in Q(V)$. Since any isotropic regular binary space must be the hyperbolic plane with discriminant $-(\mathbb{Q}_2^*)^2$, it follows that V is anisotropic. Hence, by the proof of the previous corollary, $Q(V \setminus \{0\})$ is the kernel of the map $\gamma \mapsto [5, \gamma]_{\mathbb{Q}_2}$. A computation shows that this kernel is precisely $\mathbb{Z}_2^*(\mathbb{Q}_2^*)^2$. □

Corollary 4.43.3. *If V and W are regular anisotropic binary spaces with $Q_V(V) \subseteq Q_W(W)$, then $V \cong W$.*

Proof. By scaling Q_V and Q_W appropriately, we may suppose without loss of generality that $1 \in Q(V) \subseteq Q(W)$. By the previous corollary, it follows that $Q_V(V) = Q_W(W)$. By the lemma (or the proof of the previous corollary), we thus have $[\beta, -\text{disc}V]_K = [\beta, -\text{disc}W]_K$ for all $\beta \in K^*$. It follows that $\text{disc}V\text{disc}W = (K^*)^2$, which implies that $\text{disc}V = \text{disc}W$ in $K^*/(K^*)^2$. The lemma then implies that $h(V) = h(W)$ as well. By Theorem 3.37, we thus have $V \cong W$. □

Lemma 4.44. *Suppose K is non-dyadic and $V = \langle \epsilon_1 \rangle \perp \cdots \perp \langle \epsilon_n \rangle$ for units $\epsilon_1, ..., \epsilon_n \in \mathcal{O}_K^*$, with $n \geq 3$. Then V is isotropic.*

Exercise 4.45. Prove Lemma 4.44.

With these lemmas out of the way, we can now classify anisotropic quaternary regular spaces.

Proposition 4.46. *Let V be any anisotropic regular quaternary quadratic space over K. Then*

$$V \cong \langle 1 \rangle \perp \langle -\Delta \rangle \perp \langle \pi \rangle \perp \langle -\pi\Delta \rangle$$

where π is a uniformiser of K and Δ a distinguished unit.

Proof. Write $V = U_1 \perp U_2$ for regular binary quadratic spaces. As V is anisotropic, U_1 and U_2 are anisotropic. If $Q(U_1 \setminus \{0\}) \subseteq \mathcal{O}_K^*(K^*)^2$, then $Q(U_1 \setminus \{0\}) = \mathcal{O}_K^*(K^*)^2$ and $U_1 \cong \langle 1\rangle \perp \langle -\Delta\rangle$ by the corollaries of Lemma 4.43. If $Q(U_2 \setminus \{0\}) \cap \mathcal{O}_K^*(K^*)^2 \neq \emptyset$, then $-Q(U_1 \setminus \{0\}) \cap Q(U_2 \setminus \{0\}) \neq \emptyset$. This would imply that $U_1 \perp U_2$ is isotropic, a contradiction. Thus $Q(U_2 \setminus \{0\}) \subseteq K^* \setminus \mathcal{O}_K^*(K^*)^2 = \pi\mathcal{O}_K^*(K^*)^2$. It follows that $U_2 \cong \langle \pi\rangle \perp \langle -\pi\Delta\rangle$ by the corollaries of Lemma 4.43, and we are done. Similarly, we are done if $Q(U_1 \setminus \{0\}) \subseteq \pi\mathcal{O}_K^*(K^*)^2$.

Thus, we may suppose that $Q(U_1 \setminus \{0\})$ and $Q(U_2 \setminus \{0\})$ are neither contained in $\mathcal{O}_K^*(K^*)^2$ nor $\pi\mathcal{O}_K^*(K^*)^2$, i.e. both U_1 and U_2 represent (some) units as well as some uniformisers (possibly not π itself). In particular, we have a decomposition

$$V \cong \underbrace{\langle \epsilon_1\rangle \perp \langle \epsilon_2\pi\rangle}_{U_1} \perp \underbrace{\langle \epsilon_3\rangle \perp \langle \epsilon_4\pi\rangle}_{U_2}$$

for some $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4 \in \mathcal{O}_K^*$. In particular, $\mathrm{disc}U_1$ and $\mathrm{disc}U_2$ are both uniformisers (times $(K^*)^2$). By Lemma 4.32, it follows that U_1 represents Δ_1 for $\Delta_1 \in \{1, \Delta\}$ while U_2 represents $-\Delta_2$ for $\Delta_2 \in \{1, \Delta\}$. we thus have a binary subspace U of V isomorphic to $\langle \Delta_1\rangle \perp \langle -\Delta_2\rangle$. We cannot have $\Delta_1 = \Delta_2$ since otherwise $U_1 \perp U_2$ is isotropic. Thus, $\Delta_1\Delta_2 = \Delta$, and so $\mathrm{disc}U = -\Delta$. Thus we have found a regular binary subspace U of V with $Q(U \setminus \{0\})$ either $(\mathcal{O}_K^*)(K^*)^2$ or $\pi(\mathcal{O}_K^*)(K^*)^2$, and we are done by the previous argument (where we use the splitting $V = U \perp U^\perp$). □

Corollary 4.46.1. *Every regular quaternary quadratic space over K is universal.*

Proof. We already know that regular isotropic spaces are universal, so we just need to see that a regular anisotropic quaternary space is universal. By the proposition, it suffices to show that $V = \langle 1\rangle \perp \langle -\Delta\rangle \perp \langle \pi\rangle \perp \langle -\pi\Delta\rangle$ is universal. However, we see that $Q(\langle 1\rangle \perp \langle -\Delta\rangle)$ represents $\{0\} \cup \mathcal{O}_K^*(K^*)^2$ while $Q(\langle \pi\rangle \perp \langle -\pi\Delta\rangle)$ represents $\{0\} \cup \pi\mathcal{O}_K^*(K^*)^2$, and hence $Q(V) = K$ as required. □

The significance of the work we have done is to establish the hypothesis on K required by Theorem 3.39.

Corollary 4.46.2. *Every regular quadratic space of dimension $n \geq 5$ over K is isotropic.*

Proof. We can write a regular quadratic space of dimension ≥ 5 as $U \perp W$ for W regular quaternary, and $\dim_K U = n - 4$. By the previous corollary, W is universal, and so $-Q(U \setminus \{0\}) \subseteq Q(W)$. Thus $U \perp W$ is isotropic. □

Theorem 3.39 is now applicable, and so we immediately get the following classification theorem for free!

Theorem 4.47. *Two regular quadratic spaces V and W over a non-archimedean local field are isomorphic if and only if*

$$\dim V = \dim W, \quad \mathrm{disc}V = \mathrm{disc}W, \quad \textit{and} \quad h(V) = h(W).$$

Exercise 4.48. Suppose U and V are regular quadratic spaces over a non-archimedean local field, and let $r := \dim V - \dim U \in \{0, 1, 2\}$. Show that there exists an isometry $U \hookrightarrow V$ if and only if

$$V \cong \begin{cases} U & \text{if } r = 0, \\ U \perp \langle \mathrm{disc}U \cdot \mathrm{disc}V\rangle & \text{if } r = 1, \\ U \perp H & \text{if } r = 2. \end{cases}$$

Here, H is the hyperbolic plane.

The previous theorem says that there are at most $2\#\big(K^*/(K^*)^2\big)$ regular quadratic spaces over K of fixed dimension (2 choices for the Hasse invariant, and $\#\big(K^*/(K^*)^2\big)$ number of choices for the discriminant). Are all of these possibilities actually realisable as a quadratic space over K? To answer this question, we need the following lemma.

Lemma 4.49. *Suppose U and V are regular quadratic spaces over a non-archimedean local field. If $\dim V - \dim U \geq 3$, there always exists an isometry $U \hookrightarrow V$.*

Proof. We proceed by induction on $\dim U$. For $\dim U = 0$ (so $U = \{0\}$) this is trivial, so suppose $\dim U =: m \geq 1$. Write $U = \langle \alpha_1 \rangle \perp \cdots \perp \langle \alpha_m \rangle$. Then $\dim V \geq m + 3 \geq 4$, so V is universal by Corollary 4.46.1. In particular, $\alpha_m \in Q(V)$, so we can write $V = \langle \alpha_m \rangle \perp V'$ for some V'. By induction, we can find an isometry

$$\langle \alpha_1 \rangle \perp \cdots \perp \langle \alpha_{m-1} \rangle \hookrightarrow V'.$$

Hence $U \hookrightarrow V$. □

Theorem 4.50. *Fix $n \geq 3$, $d \in K^*/(K^*)^2$, and $h \in \{\pm 1\}$. There exists a regular quadratic space V over K with invariants $\dim V = n$, $\mathrm{disc} V = d$, and $h(V) = h$.*

For $n = 2$, there exists a binary regular quadratic space V over K with invariants $\mathrm{disc} V = d$ and $h(V) = h$ if and only if either $d \neq -(K^*)^2$ or $h = [-1, -1]_K$.

Proof. Necessity follows immediately. Suppose $n \geq 3$. Take $V' = \langle 1 \rangle \perp \cdots \perp \langle 1 \rangle \perp \langle d \rangle$. If $h(V') = h$, then we may take $V = V'$ and we are done. So suppose $h(V') = -h$. Write $U = \langle 1 \rangle \perp \langle \pi \rangle$ and $U' = \langle \Delta \rangle \perp \langle \pi \Delta \rangle$. By Lemma 4.49, there exists a map $U' \hookrightarrow U \perp V'$. Thus, we must have a splitting $U' \perp V \cong U \perp V'$. Computing invariants, we see that $\mathrm{disc} V = \mathrm{disc} V' = d$ and $h(V) = -h(V') = h$ as required.

Now suppose $n = 2$. If $h(V) = [d, -1]_K$, then we may simply take $V = \langle 1 \rangle \perp \langle d \rangle$. In particular, we have covered the case of $d = -(K^*)^2$ and $h = [-1, -1]_K$. We may thus suppose that $d \neq -(K^*)^2$ and that $h = -[d, -1]_K$. There exists $\alpha \in K^*$ such that $[\alpha, -d] = -1$. Write $V = \langle \alpha \rangle \perp \langle \alpha d \rangle$. Clearly $\mathrm{disc} V = d$. It can now be checked that $h(V) = -[d, -1]_K = h$. □

Exercise 4.51. Write down a complete list of all isomorphism classes of regular quadratic spaces over $\mathbb{Q}_p$ for p a prime. (*Hint: For an arbitrary prime $p \equiv 1 \pmod 4$, you will not be able to write down Δ explicitly.*)

5 Quadratic Spaces over $\mathbb{Q}$

In this section, we now study quadratic spaces over $\mathbb{Q}$. It turns out that most of our work is already done, by the p-adic case!

For those who are interested in quadratic spaces over arbitrary number fields, the last sub-section has a brief discussion in which all proofs are omitted. Those who are interested should read [OMe73, §64-66].

Throughout, p will denote a prime or ∞, and we set $\mathbb{Q}_\infty := \mathbb{R}$. We often write '$p \leq \infty$ is a prime' to mean that either p is an honest prime number, or $p = \infty$. The honest prime numbers are often referred to as the finite primes, to distinguish it from the 'infinite prime' $p = \infty$.

5.1 Local Invariants

Suppose V is a regular quadratic space over $\mathbb{Q}$. We then have the $\mathbb{Q}_p$-vector space $V_p := V \otimes_{\mathbb{Q}} \mathbb{Q}_p$, and the quadratic form Q on V extends to a quadratic form on V_p via

$$Q_p : V_p = V \otimes_{\mathbb{Q}} \mathbb{Q}_p \to \mathbb{Q}_p, \quad v \otimes \alpha \mapsto \alpha^2 Q(v).$$

In a fixed basis $V = \mathbb{Q}x_1 \perp \cdots \perp Qx_n$, we clearly have

$$V_p = \mathbb{Q}_p x_1 \perp \cdots \perp \mathbb{Q}_p x_n.$$

Obviously $\dim_{\mathbb{Q}_p} V_p = \dim_{\mathbb{Q}} V$.

For each finite p, we have the discriminant $\mathrm{disc} V_p \in \mathbb{Q}_p/(\mathbb{Q}_p^*)^2$ and the Hasse invariant $h(V_p) \in \{\pm 1\}$. We set

$$\mathrm{disc}_p V := \mathrm{disc} V_p \quad \text{and} \quad h_p(V) := h(V_p).$$

Of course, at the global level, we also have the discriminant $\mathrm{disc} V \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ and the Hasse algebra SV. Let us see how these global invariants are related to the local ones.

Composing the obvious inclusion map $\mathbb{Q}^* \hookrightarrow \mathbb{Q}_p^*$ with the projection $\mathbb{Q}_p^* \to \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$, we have the group homomorphism $\mathbb{Q}^* \to \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$. Clearly $(\mathbb{Q}^*)^2$ lies in the kernel of this homomorphism, and hence we get a map

$$\mathbb{Q}^*/(\mathbb{Q}^*)^2 \to \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2.$$

As $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, one can check that the above map is surjective. It is easily seen that $\mathrm{disc}_p V$ is the image of $\mathrm{disc} V$ under the above map.

To see how the Hasse algebra SV is related to the local invariants, recall that $SV \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong S(V_p)$, and so the Brauer class of $SV \otimes_{\mathbb{Q}} \mathbb{Q}_p$ in $\mathrm{Br}(\mathbb{Q}_p)$ is determined by $h_p(V)$. These p-adic Hasse invariants for varying p turn out to be related to each other. Recall the Hilbert symbols $[\alpha, \beta]_{\mathbb{Q}_p} \in \{\pm 1\}$ which describe the isomorphism $\mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Z}/2\mathbb{Z}$. Since $\mathbb{Q} \subset \mathbb{Q}_p$ for all p, we of course have the Hilbert symbols $[a, b]_p := [a, b]_{\mathbb{Q}_p} \in \{\pm 1\}$ for $a, b \in \mathbb{Q}$ over all finite primes p. Since $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ as well, we can also define the Hilbert symbol over $\mathbb{R}$ as before:

$$[x, y]_{\mathbb{R}} = \begin{cases} 1 & \text{if } (x, y)_{\mathbb{R}} \cong M_2(\mathbb{R}), \\ -1 & \text{if } (x, y)_{\mathbb{R}} \cong (-1, -1)_{\mathbb{R}}. \end{cases}$$

As before, we have $[x, y]_{\mathbb{R}} = 1$ if and only if there exist $z, w \in \mathbb{R}$ such that $xz^2 + yw^2 = 1$. Hence, $[x, y]_{\mathbb{R}} = 1$ if and only if one of x or y is positive, and is -1 if and only if both x and y are negative.

We thus have Hilbert symbols $[a, b]_p$ for all primes $p \leq \infty$ and for all $a, b \in \mathbb{Q}^*$.

Theorem 5.1 (Hilbert Reciprocity)**.** *Let $a, b \in \mathbb{Q}^*$ be arbitrary. Then for almost all primes p, we have $[a, b]_p = 1$, and we have*

$$\prod_{p \leq \infty} [a, b]_p = 1.$$

Remark 5.2. The fact that $[a, b]_p = 1$ for almost all p guarantees that the product $\prod_{p \leq \infty} [a, b]_p = 1$ is well-defined.

Proof. Recall that there are only finitely many primes p such that $|ab|_p = 1$. In particular, for almost all p, both a and b are p-adic units. By Lemma 4.38(6), we then have $[a, b]_p = 1$ for almost all $p \geq 3$. In particular, the map

$$\mathbb{Q}^* \times \mathbb{Q}^* \to \{\pm 1\}, (a, b) \mapsto \prod_{p \leq \infty} [a, b]_p$$

is a well-defined group homomorphism. Since $\mathbb{Q}^*$ is the product of $\{\pm 1\}$ times the free abelian group generated by the primes, it suffices to show that $\prod_{p \leq \infty} [a, b]_p = 1$ whenever a and b are primes or -1.

Suppose first that a and b are prime numbers. In particular, they are positive. Then $[a, b]_p = 1$ for all primes $p \notin \{a, b\}$ (by Lemma 4.38(6) again), as well as for $p = \infty$. Thus $\prod_{p \leq \infty} [a, b]_p = [a, b]_a [a, b]_b [a, b]_2$. By quadratic reciprocity, we have $[a, b]_a [a, b]_b = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$, which by Lemma 4.40 is also $[a, b]_2$.

Now suppose that $b = -1$. If a is a prime, then $\prod_{p \leq \infty} [a, -1]_p = [a, -1]_a [a, -1]_2$. By Lemma 4.40 and Lemma 4.39, both $[a, -1]_a$ and $[a, -1]_2$ are equal to $(-1)^{\frac{a-1}{2}}$. If $a = -1$ as well, then $\prod_{p \leq \infty} [-1, -1]_p = [-1, -1]_2 = 1$ by Lemma 4.40. □

Since $h_p(V)$ is a product of Hilbert symbols, we have the following.

Corollary 5.2.1. *For any regular quadratic space V over $\mathbb{Q}$, we have $h_p(V) = 1$ for almost all primes p, and*

$$\prod_{p \leq \infty} h_p(V) = 1.$$

Here, we set

$$h_\infty(V) := \begin{cases} 1 & \text{if } S(V_\infty) \cong M_2(\mathbb{R}), \\ -1 & \text{if } S(V_\infty) \cong (-1, -1)_{\mathbb{R}}. \end{cases}$$

Remark 5.3. More generally, notice that tensoring with $\mathbb{Q}_p$ induces a map $\mathrm{Br}(\mathbb{Q}) \to \mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$. This map is called the *local invariant map* and often denoted by $\mathrm{inv}_p : \mathrm{Br}(\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}$. Hilbert reciprocity then immediately follows from the following hard theorem of global class field theory.

Theorem. There is a short exact sequence

$$0 \to \mathrm{Br}(\mathbb{Q}) \xrightarrow{\sum_p \mathrm{inv}_p} \bigoplus_{p \leq \infty} \mathrm{Br}(\mathbb{Q}_p) \xrightarrow{\sum} \mathbb{Q}/\mathbb{Z} \to 0.$$

Here, we set $\mathrm{Br}(\mathbb{R}) = (\frac{1}{2}\mathbb{Z})/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$.

Now consider $p = \infty$, i.e. $V_\infty = V \otimes_{\mathbb{Q}} \mathbb{R}$. We have the two invariants $\mathrm{ind}^+ V_\infty$ and $\mathrm{ind}^- V_\infty$, giving the dimensions of a maximal positive definite and a maximal negative definite subspace of the real space V_∞. We write these two invariants as simply $\mathrm{ind}^+ V$ and $\mathrm{ind}^- V$.

Exercise 5.4. Show that $h_\infty(V) = (-1)^{\frac{1}{2}\mathrm{ind}^- V(\mathrm{ind}^- V - 1)}$.

From the above discussion, the following is fairly obvious.

Proposition 5.5. *If V and W are regular quadratic spaces that are isomorphic over $\mathbb{Q}$, then $\dim_{\mathbb{Q}} V = \dim_{\mathbb{Q}} W$, $\mathrm{ind}^+ V = \mathrm{ind}^+ W$, $\mathrm{ind}^- V = \mathrm{ind}^- W$, and for any finite prime p we have $\mathrm{disc}_p V = \mathrm{disc}_p W$ and $h_p(V) = h_p(W)$.*

Remark 5.6. By Corollary 5.2.1, in practice we only need to check that $h_P(V) = h_p(W)$ for only finitely many primes p.

It turns out that the converse is true as well!

5.2 The Hasse-Minkowski Theorem

In this section, we prove the Hasse-Minkowski Theorem (or, to be more precise, Minkowski's contribution to the theorem).

Theorem 5.7 (Hasse-Minkowski for $\mathbb{Q}$)**.** *Suppose V and W are regular quadratic spaces over $\mathbb{Q}$. Then $V \cong W$ if and only if $V_p \cong W_p$ for all primes $p \leq \infty$.*

Corollary 5.7.1. *Suppose that V and W are regular quadratic spaces over $\mathbb{Q}$. Then $V \cong W$ if and only if $\dim_{\mathbb{Q}} V = \dim_{\mathbb{Q}} W$, $\mathrm{ind}^+ V = \mathrm{ind}^+ W$, $\mathrm{ind}^- V = \mathrm{ind}^- W$, and for any finite prime p we have $\mathrm{disc}_p V = \mathrm{disc}_p W$ and $h_p(V) = h_p(W)$.*

As described in the overview, the Hasse-Minkowski theorem is an example of a *local-global principle*. A local-global principle, at least in the case of number theory over characteristic 0, is any result that says that to check something 'globally' (over $\mathbb{Q}$, or over arbitrary number fields), it suffices to check 'locally' (i.e. over $\mathbb{Q}_p$ over all p, or more generally over all completions of number fields). Of course, local-global principles don't often hold, as we shall see with $\mathbb{Z}$ later on. Studying local-global principles, or obstructions to local-global principles, is pretty much what arithmetic geometry is all about.

We prove the Hasse-Minkowski theorem by proving the following (mild) generalisation.

Proposition 5.8. *Suppose V and W are regular quadratic spaces over $\mathbb{Q}$ with $\dim_{\mathbb{Q}} V \leq \dim_{\mathbb{Q}} W$. Then there exists an isometry $V \hookrightarrow W$ if and only if there exist isometries $V_p \hookrightarrow W_p$ for all primes $p \leq \infty$.*

We will prove Proposition 5.8 by proving the *strong Hasse principle*. The strong Hasse principle is also a local global principle. The proof of the strong Hasse principle is actually greatly simplified in the ternary and quaternary cases if we pass to a quadratic extension of $\mathbb{Q}$ and then use non-trivial results from algebraic number theory (for instance, in the ternary case, we need a result from global class field theory). For convenience, we give an elementary proof using only results proven (or left as an exercise) above. We first need a technical lemma.

Lemma 5.9. *Let P be a finite set of primes $p \leq \infty$. Suppose $\infty \in P$. For $p \in P$, let $t_p \in \mathbb{Q}_p^*$ be given. Then there is a $t \in \mathbb{Q}^*$ and a prime $p_0 \notin P$ such that*

- *$t \in t_p(\mathbb{Q}_p^*)^2$ for all $p \in P$,*
- *$|t|_p = 1$ for all $p \notin (P \cup \{p_0\})$.*

Proof. Write ϵ_∞ to be the sign of t_∞, i.e. $\epsilon_\infty \in \{\pm 1\}$ such that $\epsilon_\infty t_\infty \in \mathbb{R}_{>0}$. Write $P \setminus \{\infty\} = \{p_1, ..., p_r\}$. For each $1 \leq i \leq r$, write $t_{p_i} = p_i^{r_i} s_i$ for $s_i \in \mathbb{Z}_{p_i}^*$ and $r_i \in \mathbb{Z}$. Pick any finite prime p_0 not in P satisfying the congruences

$$\epsilon p_0 \prod_{1 \leq j \leq r, j \neq i} p_j^{r_j} \equiv s_i \,(\mathrm{mod}\, p_i^{e_i})$$

where $e_i = 1$ if p_i odd, and $e_i = 3$ if $p_i = 2$. By the Chinese remainder theorem this is equivalent to asking that $p_0 \notin P$ satisfy a single congruence $p_0 \equiv a \,(\mathrm{mod}\, m)$ for $\gcd(a, m) = 1$. Such a prime exists by the following theorem of Dirichlet.

Theorem. *Given any $m \in \mathbb{N}$ and any $a \in \mathbb{Z}$ relatively prime to m, there exists infinitely many primes p such that $p \equiv a \,(\mathrm{mod}\, m)$.*

With p_0 so defined, set

$$t = \epsilon_p p_0 \prod_{i=1}^{r} p_i^{r_i} \in \mathbb{Q}.$$

Clearly $t \in \mathbb{Z}_p^*$ for all $p \notin P \cup \{p_0\}$. One checks, by our choice of p_0 and by the local square theorem, that $t \in t_p(\mathbb{Q}_p^*)^2$ for all $p \in P$. □

Theorem 5.10 (The Strong Hasse Principle for $\mathbb{Q}$)**.** *A regular quadratic space V over $\mathbb{Q}$ is isotropic if and only if V_p is isotropic for all primes $p \leq \infty$.*

Proof. Necessity is obvious. So suppose V is a regular n-ary quadratic space over $\mathbb{Q}$ such that V_p is isotropic for all primes $p \leq \infty$. In particular $n \geq 2$. Fix an orthogonal basis $x_1, ..., x_n$ for V with respect to which we have

$$V \cong \langle a_1 \rangle \perp \cdots \perp \langle a_n \rangle$$

for integers $a_i \in \mathbb{Q}$.

First suppose $n = 2$. Then V_p is the hyperbolic plane for all $p \leq \infty$; in particular, we have $\mathrm{disc}_p V = -(\mathbb{Q}_p^*)^2$ for all primes p. Thus $-a_1 a_2$ is a square in $\mathbb{Q}_p$ for all finite primes p, and $-a_1 a_2 > 0$. It follows that $-a_1 a_2$ is a square in $\mathbb{Q}$, so that $\mathrm{disc} V = -(\mathbb{Q}^*)^2$. Corollary 1.17.2 then implies that V is isotropic.

Now suppose $n = 3$. By scaling Q, we may suppose that $a_1 = 1$, so that $V \cong \langle 1 \rangle \perp \langle a_2 \rangle \perp \langle a_3 \rangle$, where without loss of generality a_2, a_3 are square-free integers. We prove the $n = 3$ case by induction on $m := |a_2| + |a_3|$. For $m = 2$, we have $V \cong \langle 1 \rangle \perp \langle \pm 1 \rangle \perp \langle \pm 1 \rangle$. Isotropy at $\mathbb{R}$ implies that $V \ncong \langle 1 \rangle \perp \langle 1 \rangle \perp \langle 1 \rangle$, and so we see that V is isotropic over $\mathbb{Q}$. Now suppose $m \geq 3$. For any $p | a_3$, we have by isotropy at V_p that $-a_2$ is represented by $\langle 1 \rangle \perp \langle a_3 \rangle$, so that $-a_2$ is a square modulo p. Thus $-a_2$ is a square modulo $\prod_{p | a_3} p = a_3$. In particular, we can find $t \in \mathbb{Z}$ with $|t| \leq \frac{1}{2}|a_3|$ such that $t^2 = -a_2 + a_3 a_3' u^2$ for some non-zero squarefree $a_3' \in \mathbb{Z}$ and some $u \in \mathbb{Z}$. The inequality $|t| \leq \frac{1}{2}|a_3|$ implies that $|a_3'| < |a_3|$. For any prime $p \leq \infty$, suppose $\xi, \eta \in \mathbb{Q}_p$ satisfy $1 + a_2 \xi^2 + a_3 \eta^2 = 0$. Then

$$1 + a_2 \left(\frac{\xi t - 1}{t + \xi a_2} \right)^2 + a_3' \left(u\eta \frac{t^2 + a_2}{t + \xi a_2} \right)^2 = 0,$$

and so $V' = \langle 1 \rangle \perp \langle a_2 \rangle \perp \langle a_3 \rangle$ is isotropic at all $p \leq \infty$. By induction, V' is isotropic over $\mathbb{Q}$, and so there exist $x, y \in \mathbb{Q}$ such that

$$1 + a_2 x^2 + a_3' y^2 = 0.$$

It follows that

$$1 + a_2 \left(\frac{xt - 1}{t + x a_2} \right)^2 + a_3 \left(\frac{y(t^2 + a_2)}{u(t + \xi a_2)} \right)^2 = 0$$

and hence V is isotropic at $\mathbb{Q}$. The $n = 3$ is thus established.

Let us now do the $n = 4$ case. Since V_p is isotropic for all $p \leq \infty$, there exists $t_p \in \mathbb{Q}_p^*$ such that $t_p \in Q(\mathbb{Q}_p x_1 \perp \mathbb{Q}_p x_2)$ and $-t_p \in Q(\mathbb{Q}_p x_3 \perp \mathbb{Q}_p x_4)$. Let P' be the set of all (finite) primes dividing $2a_1 a_2 a_3 a_4$, and let $P = \{\infty\} \cup P'$. By Lemma 5.9, there exists $t \in \mathbb{Q}^*$ and a prime p_0 such that $t \in t_p(\mathbb{Q}_p^*)^2$ for all $p \in P$ and $|t|_p = 1$ for all $p \notin P \cup \{p_0\}$. Consider the two ternary spaces over $\mathbb{Q}$

$$U_1 := \langle a_1 \rangle \perp \langle a_2 \rangle \perp \langle -t \rangle \quad U_2 := \langle a_3 \rangle \perp \langle a_4 \rangle \perp \langle t \rangle .$$

The construction of t implies that U_1 and U_2 are both isotropic for all $p \in P$. For all primes $p \notin P \cup \{p_0\}$ (which are, in particular, odd), we have $a_1, a_2, -t \in \mathbb{Z}_p^*$, and so U_1 is isotropic at p by Lemma 4.44. Similarly U_2 is isotropic at p for all such $p \notin P \cup \{p_0\}$. Hence U_1 and U_2 are isotropic at p for all $p \neq p_0$ (including the infinite place). In particular, $\langle a_1 \rangle \perp \langle a_2 \rangle$ over $\mathbb{Q}_p$ represents t. It follows from Proposition 4.35 that U_1 is isotropic at p if and only if $[a_1 t, a_2 t]_p = 1$. Thus we know that $[a_1 t, a_2 t]_p = 1$ for all $p \neq p_0$. However, by Hilbert reciprocity, we have

$$\prod_{p \leq \infty} [a_1 t, a_2 t]_p = 1,$$

which forces $[a_1 t, a_2 t]_{p_0} = 1$ as well. Thus U_1 is isotropic at p_0 as well. Similarly U_2 is isotropic at p_0 is isotropic as well. Hence, the ternary spaces U_i are isotropic at all places of $\mathbb{Q}$, and so by the strong Hasse principle for $n = 3$ (proven above), the U_i are isotropic over $\mathbb{Q}$. In particular, $\mathbb{Q}x_1 \perp \mathbb{Q}x_2$ represents t and $\mathbb{Q}x_3 \perp \mathbb{Q}x_4$ represents $-t$. It follows that V is isotropic.

We are now left with the case of $n \geq 5$. We prove by induction on n for $n \geq 2$, where the base cases of $n = 2, 3, 4$ is done above. Now suppose $n \geq 5$. Set $U = \mathbb{Q}x_1 \perp \mathbb{Q}x_2$ and $W = \mathbb{Q}x_3 \perp \cdots \perp \mathbb{Q}x_n$ so that $V = U \perp W$. Then $V_p = U_p \perp W_p$ for all $p \leq \infty$. Let T denote the set of primes $p \leq \infty$ such that W_p is anisotropic. By Lemma 4.44, we have $p \notin T$ whenever p is a finite prime not dividing $2a_1 a_2 \cdots a_n$, and so T is a finite set. If T is empty, then W is locally isotropic everywhere, and by the inductive hypothesis W is isotropic over $\mathbb{Q}$, and we are done. So suppose T is non-empty. Pick $\mu_p \in \mathbb{Q}_p^*$ at each $p \in T$ such that $\mu_p \in Q(U_p)$ and $-\mu_p \in Q(W_p)$; such a $\mu_p \in \mathbb{Q}_p$ exists by isotropy of V_p; we can guarantee $\mu_p \neq 0$ since either U_p is anisotropic as well, or U_p is isotropic and thus universal. Write $\mu_p = Q(\xi_p x_1 + \eta_p x_2)$ for some $\xi_p, \eta_p \in \mathbb{Q}_p$ for all $p \in T$. By the weak approximation theorem (see Theorem 4.13), we can find $\xi, \eta \in \mathbb{Q}$ with ξ close to ξ_p and η close to η_p (under $|.|_p$) for each $p \in T$. Set $\mu = Q(\xi x_1 + \eta x_2)$. By making $|\xi - \xi_p|_p$ and $|\eta - \eta_p|_p$ small enough, we may make μ arbitrarily close to μ_p for all $p \in T$. Thus we can make $|\mu \mu_p^{-1} - 1|_p < \epsilon$ for all $p \in T$, for any arbitrary $\epsilon > 0$.

However, one can check that $(\mathbb{Q}_p^*)^2$ is an open subset of $\mathbb{Q}_p$, and so by making ϵ small enough we can guarantee $\mu \in \mu_p (\mathbb{Q}_p^*)^2$. Thus $-\mu \in Q(W_p)$ for all $p \in T$. We already have $-\mu \in Q(W_p)$ for $p \notin T$ by isotropy of W_p at p. Hence, the $n-1$-dimensional subspace $V' := \langle \xi x_1 + \eta x_2 \rangle \perp W$ of V is isotropic over $\mathbb{Q}_p$ for all primes $p \leq \infty$. The induction hypothesis then implies that V' is isotropic over $\mathbb{Q}$, and so V is isotropic over $\mathbb{Q}$. □

Proof of Proposition 5.8. First suppose $\dim V = 1$, say $V = \langle \alpha \rangle$. Then α is represented by W for all p, and so $\langle -\alpha \rangle \perp W$ is isotropic at all p. By the strong Hasse principle, $\langle -\alpha \rangle \perp W$ is isotropic over $\mathbb{Q}$, and so W represents α over $\mathbb{Q}$. We thus have an isometry $V = \langle \alpha \rangle \hookrightarrow W$. We now proceed by induction on $\dim V$.

Pick any anisotropic $x \in V$. We have isometries $\mathbb{Q}_p x \hookrightarrow V_p \hookrightarrow W_p$ for all primes $p \leq \infty$, and so by the 1-dimensional case we have an isometry $\mathbb{Q}x \hookrightarrow W$. Since x is anisotropic, we have splittings $V = \langle x \rangle \perp V'$ and $W = \langle x \rangle \perp W'$. For each prime $p \leq \infty$, using Witt's extension theorem, we get isometries $V_p' \hookrightarrow W_p'$. The inductive hypothesis implies that there is an isometry $V' \hookrightarrow W'$ over $\mathbb{Q}$. Hence we have an isometry $V \hookrightarrow W$. □

Exercise 5.11. Show that the spaces $\langle 1 \rangle \perp \langle 1 \rangle \perp \langle 1 \rangle \perp \langle 1 \rangle$ and $\langle b \rangle \perp \langle b \rangle \perp \langle b \rangle \perp \langle b \rangle$ are isomorphic over $\mathbb{Q}$ for all $b \in \mathbb{Q}^*$.

Exercise 5.12. Consider the three quadratic forms

$$f = x_1^2 + x_2^2 + 16x_3^2 - x_4^2, \quad g = 3x_1^2 + 7x_2^2 - 4x_3 x_4, \quad \text{and} \quad h = 2x_1^2 + 2x_2^2 + 5x_3^2 - 16x_4^2 - 2x_2 x_3 - 2x_1 x_3.$$

Which of these forms are isotropic over $\mathbb{Q}$? Are any of these isomorphic to each other?

Exercise 5.13. Suppose V and W are regular quadratic spaces over $\mathbb{Q}$ with $V_\infty \cong W_\infty$. Suppose that there exists a finite prime p_0 such that $V_p \cong W_p$ for all primes $p \neq p_0$. Show that $V \cong W$.

5.3 Prescribing Local Behaviour

As in the case of local fields, now that we have a set of invariants for a quadratic space that determine it up to isomorphism, one can of course ask whether such a quadratic space exists for a prescribed set of invariants. This is the content of the following.

Theorem 5.14. *Let $n \geq 1$. Suppose, for each prime $p \leq \infty$, we are given a regular n-ary quadratic space U_p over $\mathbb{Q}_p$. Then, there exists a regular n-ary quadratic space V over $\mathbb{Q}$ such that $V_p \cong U_p$ for all primes $p \leq \infty$ if and only if*

1. *there exists $d_0 \in \mathbb{Q}^*$ such that $\mathrm{disc}U_p = d_0(\mathbb{Q}_p^*)^2$ for all p,*
2. *$h(U_p) = 1$ for almost all p, and*
3. *$\prod_{p \leq \infty} h(U_p) = 1$, where we define $h(U_\infty)$ as the image of $S(U_\infty)$ under $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.*

This V is necessarily unique (by Hasse-Minkowski).

Proof. Necessity is clear from what has been discussed before. We proceed by induction on n. If $n = 1$, we may simply take $V = \langle d_0 \rangle$. So suppose $n \geq 2$. So suppose we are given U_p satisfying the above constraints. Let $P = \{\infty, 2\} \cup P'$ where P' is the set of all odd finite primes p such that either $|d_0|_p \neq 1$ or $h(U_p) = -1$. This is a finite set by condition (2) and the fact that $d_0 \in \mathbb{Q}$. For each $p \in P$ fix $t_p \in \mathbb{Q}_p^*$ such that $t_p \in Q_{U_p}(U_p)$.

Suppose first that $n = 2$. Lemma 5.9 guarantees the existence of $t \in \mathbb{Q}^*$ and a prime $p_0 \notin P$ such that $t \in t_p(\mathbb{Q}_p^*)^2$ for all $p \in P$ and $|t|_p = 1$ for $p \notin P \cup \{p_0\}$. Set $V = \langle t \rangle \perp \langle d_0 t \rangle$. We clearly have $\mathrm{disc}_p V = d_0(\mathbb{Q}_p^*)^2 = \mathrm{disc}U_p$ for all $p \leq \infty$. Notice that $h_p(V) = [t,t]_p[t, d_0t^2]_p = [t,-1]_p[t,d_0]_p = [t,-d_0]_p$. A computation checks that $h_p(V) = h(U_p)$ for all $p \in P$. For $p \notin P \cup \{\infty\}$, one easily checks that $h_p(V) = 1 = h(U_p)$. Hilbert reciprocity then forces $h_{p_0}(V) = h(U_{p_0})$. Hence $V_p \cong U_p$ by Theorem 4.47.

Now suppose $n \geq 3$. As a result of the weak approximation theorem and the fact that $(\mathbb{Q}_p^*)^2$ is open in $\mathbb{Q}_p^*$, we can find $t \in \mathbb{Q}^*$ such that $t \in t_p(\mathbb{Q}_p^*)^2$ for all $p \in P$. We thus have $t \in Q_{U_p}(U_p)$ for all $p \in P$. For all $p \notin P$, we have $|d_0|_p = 1$ and $h(U_p) = 1$. Theorem 4.47 implies that $U_p \cong \langle 1 \rangle \perp \cdots \perp \langle 1 \rangle \perp \langle d_0 \rangle$, and so Lemma 4.44 implies that U_p is isotropic. In particular, it is universal, and so $t \in Q(U_p)$ for all $p \notin P$. Hence, for all primes $p \leq \infty$, we have $U_p \cong \langle t \rangle \perp U_p'$ for some $n-1$ dimensional regular quadratic space U_p' over $\mathbb{Q}_p$.

Notice that for all p, $\mathrm{disc}U_p' = (d_0 t)(\mathbb{Q}_p^*)^2$ where $d_0 t \in \mathbb{Q}$. Next, we have $h(U_p) = [t, d_0 t]_p h(U_p')$. In particular, for almost all odd p, we have $[t, d_0 t]_p = 1$ as t and d_0 are p-adic primes. We also have $h(U_p) = 1$ for almost all p. Hence $h(U_p') = 1$ for almost all p. Hilbert reciprocity (and its corollary) then implies that $\prod_p h(U_p') = 1$. Thus, the U_p' satisfy the conditions of the theorem, and so by the induction hypothesis there exists V' over $\mathbb{Q}$ such that $V_p' \cong U_p'$. We may then take $V = \langle t \rangle \perp V'$. □

Combining the above theorem with what we know about quadratic spaces over local fields, we have the following.

Corollary 5.14.1. *Let $n \geq 2$ and $0 \leq q \leq n$ be given integers. For each finite prime p, suppose we are given $d_p \in (\mathbb{Q}_p^*)/(\mathbb{Q}_p^*)^2$ and $h_p \in \{\pm 1\}$. Then, there exists a unique regular n-ary quadratic space V over $\mathbb{Q}$ satisfying*

$$\mathrm{ind}^+ V = q, \quad h_p(V) = h_p \ \forall\, p \quad \text{and} \quad \mathrm{disc}_p V = d_p \ \forall\, p$$

if and only if the following conditions hold:

1. *for each (finite) prime p, either $n \geq 3$, or $d_p \neq -(\mathbb{Q}_p^*)^2$, or $h_p = [-1,-1]_{\mathbb{Q}_p}$;*
2. *there exists $d \in \mathbb{Q}^*$ such that $d_p = d(\mathbb{Q}_p^*)^2$ for all finite primes p, and $(-1)^{n-q} d \in \mathbb{R}_{>0}$;*
3. *$h_p = 1$ for almost all p; and*
4. *$\prod_p h_p = (-1)^{\frac{1}{2}(n-q)(n-q-1)}$ (the product beign over all finite primes p).*

5.4 Quadratic Spaces over General Number Fields

Remark 5.15. This section is for those who are interested in the theory of quadratic spaces over number fields. In particular, I will be assuming some basic knowledge of algebraic number theory. This section was not covered in class, and may be safely skipped.

Let K be a number field. Each finite place v of K corresponds to a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, while each infinite place corresponds to either a real embedding $K \hookrightarrow K_v = \mathbb{R}$, or a complex embedding $K \hookrightarrow K_v = \mathbb{C}$. Given a

regular n-ary quadratic space V over K, we can assign the local invariants

$$h_{\mathfrak{p}}(V) = h(V \otimes_K K_{\mathfrak{p}}) \quad \text{and} \quad \operatorname{disc}_{\mathfrak{p}} V = \operatorname{disc}(V \otimes_K K_{\mathfrak{p}})$$

at primes $\mathfrak{p}$ of $\mathcal{O}_K$, and for the real places v we have

$$\operatorname{inv}_v^+ V := \operatorname{inv}^+(V \otimes_K \mathbb{R}) \quad \text{and} \quad \operatorname{inv}_v^- V := \operatorname{inv}^-(V \otimes_K \mathbb{R}).$$

We also have the Hilbert symbols $[a,b]_{\mathfrak{p}} := [a,b]_{K_{\mathfrak{p}}}$ associated to each $\mathfrak{p}$.

5.4.1 Hilbert Reciprocity

We still still have Hilbert reciprocity.

Theorem. *For almost all $\mathfrak{p}$, we have $[a,b]_{\mathfrak{p}} = 1$. Also,*

$$\left(\prod_{v \text{ real}} [a,b]_{\mathbb{R}}\right) \cdot \left(\prod_{\mathfrak{p}} [a,b]_{\mathfrak{p}}\right) = 1.$$

Unlike over $\mathbb{Q}$, the proof of Hilbert reciprocity for general K requires class field theory. It is a direct corollary of the short exact sequence

$$0 \to \operatorname{Br}(K) \xrightarrow{\sum_v \operatorname{inv}_v} \bigoplus_v \operatorname{Br}(K_v) \xrightarrow{\sum} \mathbb{Q}/\mathbb{Z} \to 0$$

where

$$\operatorname{Br}(K_v) = \begin{cases} \mathbb{Q}/\mathbb{Z} & \text{if } v \text{ finite,} \\ (\frac{1}{2}\mathbb{Z})/\mathbb{Z} & \text{if } v \text{ real,} \\ \{1\} & \text{if } v \text{ complex.} \end{cases}$$

Exactness on the right is trivial, exactness in the middle is a result of class field theory, and exactness on the left is the *Albert–Brauer–Hasse–Noether theorem.*

However, we can also reformulate Hilbert reciprocity in terms of classical class field theory. We recall some of the statements.

1. (*Kummer Theory*) Let $n \geq 2$. Suppose K is a number field containing all n'th roots of unity. Let Δ be a subgroup of $K^*/(K^*)^n$, and write $\Delta^{\frac{1}{n}} := \{\sqrt[n]{a} : a \in K, a(K^*)^n \in \Delta\}$. Set $L = K(\Delta^{\frac{1}{n}})$. Then L is a finite extension, and there is a natural bijection

   $$\Delta \cong \operatorname{Hom}(\operatorname{Gal}(L/K), \mathbb{C}) = \operatorname{Hom}(\operatorname{Gal}(L/K), \mu_n(\mathbb{C})), \quad b(K^*)^n \mapsto \chi_b$$

   where $\mu_n(\mathbb{C})$ is the group of n'th roots of unity in $\mathbb{C}$.

2. (*Local Class Field Theory - Artin Reciprocity*) Suppose L/K is a finite abelian extension of non-archimedean local fields, and let $N_{L/K} : L \to K$ be the field norm. Then, there exists a canonical isomorphism (the *local Artin reciprocity map*)

   $$\operatorname{Art}_{L/K} : K^*/N_{L/K}(L^*) \xrightarrow{\sim} \operatorname{Gal}(L/K).$$

   Write $\operatorname{Art}_{L/K}(a) := \operatorname{Art}_{L/K}\big(a \cdot N_{L/K}(L^*)\big)$. It turns out that the local Artin reciprocity map sends all uniformisers to the Frobenius map in $\operatorname{Gal}(L/K)$, while $\operatorname{Art}_{L/K}$ maps any unit to the identity.

3. (A part of *Artin's Global Reciprocity Law*) Suppose K is a global field, and L a finite (Galois) abelian extension of K. For each valuation v of K, fix a valuation w of L above v. If v is non-archimedean, we already have a map

   $$\operatorname{Art}_{L_w/K_v} : K_v^* \to \operatorname{Gal}(L_w, K_v) \subset \operatorname{Gal}(L/K).$$

   For v real and w complex, we define a map

   $$\operatorname{Art}_{L_w/K_v} : K_v^* \to \mathbb{Z}/2\mathbb{Z} = \operatorname{Gal}(L_w, K_v) \subset \operatorname{Gal}(L/K)$$

   that takes positive reals to the identity and negative reals to complex conjugation. In all other cases, we have $L_w = K_v$ and we define $\operatorname{Art}_{L_w/K_v}$ to be the trivial map.

In this set up, it turns out that for any $a \in K^*$, we have $\mathrm{Art}_{L_w/K_v}(a)$ is the identity in $\mathrm{Gal}(L/K)$ for almost all v. Moreover, we have the following product in Gal(L/K):

$$\prod_v \mathrm{Art}_{L_w/K_v}(a) = 1.$$

Now suppose K is a global field and $\mathfrak{p}$ is a prime. In the notation of statement (1), take $\Delta = K_\mathfrak{p}^*/(K_\mathfrak{p}^*)^n$ itself and set $L = K_\mathfrak{p}(\Delta^{1/n})$. It turns out that $N_{L/K}(L^*) = (K^*)^n$. Set

$$[\alpha, \beta]_{K_\mathfrak{p}}^{(n)} := \chi_\beta\Big(\mathrm{Art}_{L/K}(\alpha)\Big) \in \mu_n.$$

These are the *n'th order Hilbert Symbols on* $K_\mathfrak{p}$. It turns out that the second order Hilbert symbol corresponds precisely to the Hilbert symbol defined previously in the context of quaternions. Hilbert reciprocity immediately follows from statements (2) and (3) above.

5.4.2 Hasse-Minkowski

We still have the Hasse-Minkowski theorem.

Theorem. *Suppose V and W are regular quadratic spaces over the number field K. Then $V \cong W$ over K if and only if $V \otimes_K K_v \cong W \otimes_K K_v$ over K_v for all places v of K.*

Remark 5.16. Minkowski only proved the case $K = \mathbb{Q}$, and Hasse generalised to arbitrary number fields.

The proof of the Hasse-Minkowski theorem for general number fields follows that of $\mathbb{Q}$. Indeed, one first proves the following.

Theorem (Strong Hasse Principle)**.** *Suppose V is a regular quadratic space over a number field K. Then V is isotropic over K if and only if $V \otimes_K K_v$ is isotropic over K_v for all places v of K.*

The proof of the strong Hasse principle over number fields mostly follows as in the case of $\mathbb{Q}$, except in the ternary and quaternary cases. In these two cases, one needs to argue slightly differently (see [OMe73, Theorem 66:1]). For instance, in the ternary case, one replaces the use of Dirichlet's theorem on primes in arithmetic progression with some basic results from class field theory. Once the strong Hasse principle is established, the Hasse-Minkowski theorem follows in exactly the same way as in the case of $\mathbb{Q}$.

We can also prescribe local behaviour as before. The theorem carries over *mutatis mutandis*.

Theorem. *Let $n \geq 1$ and K a number field. Suppose, for each place v of K, we are given a regular n-ary quadratic space U_v over K_v. Then, there exists a regular n-ary quadratic space V over K such that $V \otimes_K K_v \cong U_v$ for all places v of K if and only if*

1. *there exists $d_0 \in K^*$ such that $\mathrm{disc} U_v = d_0(K_v^*)^2$ for all places v,*
2. *$h(U_v) = 1$ for almost all places v, and*
3. *$\prod_v h(U_v) = 1$.*

This V is necessarily unique (by Hasse-Minkowski).

The proof for general number fields is again slightly different. As before, instead of Dirichlet's theorem on primes in arithmetic progression, one uses some facts from class field theory (see [OMe73, §72]).

6 Lattices over Principal Ideal Domains

We now consider the study of quadratic forms over *rings*, not fields. The simple fact that distinguishes the theory of quadratic forms over rings from over fields is that one can always divide by non-zero elements in a field. In general rings, this does not hold, which complicates the theory significantly. However, we stick to integral domains; by embedding into the fraction field, we can then use results that we have proven over fields to obtain results over rings.

In this section, we will mostly be concerned with quadratic forms over PIDs. The general theory of lattices does extend to arbitrary Dedekind domains. Recall that Dedekind domains are integral domains in which every non-zero proper ideal factors uniquely as a product of prime ideals. The main example of Dedekind domains are the rings of integers $\mathcal{O}_K$ for K a number field. PIDs are also Dedekind domains. See [OMe73, Chapter VIII] for details on the general theory of lattices over Dedekind domains.

Throughout this section, let R be a PID with fraction field K.

6.1 Necessary Results About PIDs

Before introducing the theory of lattices over PIDs, let us recall some basic definitions and facts about PIDs that we will need. For proofs, see pretty much any book on abstract ring theory.

Definition. A *PID* (or *principal ideal domain*) is an integral domain R in which every ideal of R is principal (i.e. generated by a single element).

Examples include all local rings, $\mathbb{Z}$, $k[x]$ for k a field, etc.

Definition. A prime element $\pi \in R$ is an element of R such that $\pi|\alpha\beta$ implies that $\pi|\alpha$ or $\pi|\beta$.

Lemma 6.1. *Every prime element π is irreducible, i.e. if $\pi = \alpha\beta$ for $\alpha, \beta \in R$, then one of α or β is a unit in R.*

Proposition 6.2. *Every PID is a UFD. In other words, for any $\alpha \in R \setminus \{0\}$, there exist prime elements $\pi_1, ..., \pi_r$ (unique up to permutation and multiplication by units) such that $\alpha = \pi_1 \cdots \pi_r$.*

Corollary 6.2.1. *For any $\alpha \in K^*$, there exist distinct prime elements $\pi_1, ..., \pi_r$ in R and integers $a_1, ..., a_r \in \mathbb{Z} \setminus \{0\}$ such that $\alpha = \epsilon\pi_1^{a_1} \cdots \pi_r^{ar}$ for some $\epsilon \in R^*$. Moreover, the π_i are unique up to multiplication by units and up to reordering, the a_i are unique, and r is unique.*

Definition. A *fractional ideal of R* is an R-submodule $\mathfrak{a} \subset K$ such that $\alpha\mathfrak{a}$ is an honest ideal of R for some $\alpha \in R$ (possibly equal to R itself).

In particular, both $\{0\}$ and R are fractional ideals of R. Also, every ideal of R is a fractional ideal. Since by definition every ideal of R is principal, the previous corollary implies the following.

Lemma 6.3. *Every fractional ideal in a PID R is of the form αR for some α in the fraction field of R. This α is unique up to multiplication by a unit.*

We will also need the following structure theorem for finitely generated modules over PIDs.

Theorem 6.4 (Structure Theorem of Finitely Generated Modules over PIDs)**.** *Suppose M is a finitely generated module over a PID R.*

- *There is a direct sum decomposition*
$$M \cong R^n \oplus M^{tor}$$
into a free module R^n for a unique $n \geq 0$ and the submodule
$$M^{tor} := \{m \in M : am = 0 \text{ for some } a \in R \setminus \{0\}\}$$
consisting of all torsion elements of M. This $n \geq 0$ is called the rank *of M, and*
- *Every R-submodule of M is also a finitely generated R-module.*

6.2 Abstract Lattices

Suppose V is *any* vector space over K, i.e. we do take any quadratic space structure on V.

Definition. A *lattice* (over R) is an R-submodule L of V such that there exists a K-basis $x_1, ..., x_n$ of V satisfying $L = Rx_1 + Rx_2 + \cdots + Rx_k$ for some $1 \leq k \leq n$. The lattice is said to be *full* if L spans V. The basis $x_1, ..., x_n$ of V above is said to be *adapted to L*.

In particular, $\{0\}$ is a lattice. Clearly, the rank of a lattice satisfies

$$\text{rank} L = k = \dim_K KL$$

where k is as in the definition above. Notice that any lattice L is always a full lattice in the subspace KL of V. Given any $\alpha \in K$, we define $\alpha L := \{\alpha x : x \in L\}$. Clearly αL is a lattice if L is a lattice.

The structure theorem (Theorem 6.4) gives us the following characterisation of lattices.

Proposition 6.5. *Suppose M is a R-submodule of V. The following are equivalent.*

1. *M is finitely generated over R.*
2. *M is a lattice.*
3. *For any given full lattice L, there exists a non-zero $\alpha \in R$ such that $\alpha M \subseteq L$.*
4. *$M \subseteq Rx_1 + \cdots + Rx_n$ for some basis $x_1, ..., x_n$ of V.*

Proof. (4) $\implies$ (1) follows immediately from the structure theorem, noting that $Rx_1 + \cdots + Rx_n$ is a finitely generated R module. (3) $\implies$ (4) follows by simply taking $L := Rx_1 + \cdots + Rx_n$ for any basis of V, and then replacing x_i with $\frac{1}{\alpha}x_i$.

We now show (1) $\implies$ (2). Since V is obviously torsion free over R, so is M. The structure theorem then implies that M is free, i.e. $M = Rx_1 + \cdots + Rx_m$ for some $x_1, ..., x_m \in M \subset V$ that are linearly independent over R. If any non-trivial K-linear combination of $x_1, ..., x_m$ is zero, then by clearing denominators we would get a non-trivial R-linear combination of $x_1, ..., x_m$ equalling 0. It follows that $x_1, ..., x_m$ are linearly independent over K. Hence M is a lattice.

It remains to show (2) $\implies$ (3). Write $L = Rx_1 + \cdots + Rx_n$ and $M = Ry_1 + \cdots + Ry_m$. Each y_i can be written as $x_i = \sum_j a_{ij}x_j$. There exists $\alpha \in R$ such that $\alpha a_{ij} \in R$ for all i, j (we are just clearing denominators). Hence $\alpha y_i \in L$ for all i, and thus $\alpha M \subseteq L$. □

Corollary 6.5.1. *Suppose U is a subspace of V, and L is an R-submodule of U. Then, L is a lattice in U if and only if L is a lattice in V.*

This corollary in particular allows us to often assume lattices are full without loss of generality.

Corollary 6.5.2. *$L \cap M$ is a lattice in V whenever L and M are lattices in V.*

We define

$$M + N := \{m + n : m \in M, n \in N\} \subseteq V.$$

Corollary 6.5.3. *$L + M$ is a lattice in V whenever L and M are lattices in V. Moreover, $L + M$ is full whenever at least one of L or M is full.*

Exercise 6.6. Prove Corollary 6.5.1, Corollary 6.5.2, and Corollary 6.5.3.

The following identities are clear:

$$\alpha(M \cap N) = (\alpha M) \cap (\alpha N), \quad (\alpha + \beta)M = \alpha M + \beta N, \quad \text{and} \quad \alpha(M + N) = \alpha M + \alpha N.$$

Now suppose L is a lattice, and $x \in KL$ is non-zero. Then $L \cap Kx$ is a rank 1 lattice in KL, and so $L \cap KL = Ry$ for some $y \in L \cap Kx$. Writing $y = \alpha x$ for $\alpha \in K$, we have $L \cap Kx = \alpha Rx$. Thus, given any $x \in KL$ we can find a fractional ideal $\mathfrak{a}$ of R such that $\mathfrak{a} \cdot x = L \cap Kx$.

Definition. Suppose $x \in KL$ is non-zero. Then, $\alpha \in K^*$ is a *coefficient of x in L* if $R(\alpha x) = L \cap Kx$.

Lemma 6.7. *Suppose $x \in KL \setminus \{0\}$ for L a lattice. Consider the set*

$$\mathfrak{c}_x := \{\beta \in K : \beta x \in L\}.$$

Then $\mathfrak{c}_x$ is a fractional ideal, and $\mathfrak{c}_x = \alpha R$ if and only if α is a coefficient of x in L. In particular, $x \in L$ if and only if $R \subseteq \mathfrak{c}_x$.

In particular, it follows that the coefficient of x in L is uniquely defined up to multiplication by a unit of R.

Exercise 6.8. Prove Lemma 6.7.

Definition. The ideal $\mathfrak{c}_x$ given in Lemma 6.7 is called the *coefficient ideal of x in L*. We denote the coefficient ideal by $\mathfrak{c}_x^L$ (or $\mathfrak{c}_x$ if the lattice is known).

Note that the coefficient ideal of x in L is a fractional ideal.

Exercise 6.9. Show that $\alpha(\mathfrak{c}_{\alpha x}) = \mathfrak{c}_x$.

Lemma 6.10. *Suppose $L = Rx_1 + \cdots + Rx_n$ is a full lattice of V. Let $x \in V \setminus \{0\}$ be arbitrary, and write $x = \alpha_1 x_1 + \cdots + \alpha_n x_n$. Then,*

$$\mathfrak{c}_x = \bigcap_{1 \leq i \leq n, \alpha_i \neq 0} (\alpha_i^{-1} R).$$

Exercise 6.11. Prove Lemma 6.10.

Definition. Suppose L is a lattice. A vector $x \in KL$ is a *maximal vector of L* if the coefficient of x in L is a unit. In other words, x is a maximal vector of L if $\alpha x \in L$ holds if and only if $\alpha \in R$.

Thus, all basis vectors of a lattice are maximal vectors.

Exercise 6.12. Suppose $x \in V$ is a maximal vector of a lattice L. Show there exists a basis $x_1, ..., x_n$ of V adapted to L such that $x_1 = x$.

Exercise 6.13. Suppose $x_1, ..., x_n$ is a basis for V, and let L be a full lattice. Then, $x_1, ..., x_n$ is a basis for L if and only if x_i is a maximal vector of L for all $1 \leq i \leq n$.

Proposition 6.14. *Suppose the PID R has the property that R/π is a finite field for all prime elements π of R. Then, between any two lattices $M \subseteq L$ of the same rank, there exist only finitely many lattices N such that $M \subseteq N \subseteq L$.*

Remark 6.15. This assumption on R holds for $R = \mathbb{Z}_p$ and for $R = \mathbb{Z}$, which are the cases we are most interested in.

Proof. Without loss of generality we suppose L and M are full. Then L/M is a finitely generated R-module. Suppose $x + M \in L/M$. By Proposition 6.5, there exists $\alpha \in R \setminus \{0\}$ such that $\alpha L \subseteq M$, and so $\alpha(x + M) = M \in L/M$. Thus $x + M$ is a torsion element. Hence, L/M is a torsion module, and so by the structure theorem, we can write

$$L/M \cong (R/\gamma_1) \times \cdots (R/\gamma_r)$$

for unique r and unique $\gamma_i \in R \setminus \{0\}$ such that $\gamma_{i+1} | \gamma_i$ for $1 \leq i \leq r$. By the assumption on R, and the fact that each γ_i has a unique factorization into finitely many primes, it follows that each of R/γ_i are finite sets. Thus L/M is a finite R-module. Hence, there can only be finitely many lattices N such that $M \subseteq N \subseteq L$. □

6.3 Quadratic Lattices

6.3.1 Classes

Now suppose L is a regular lattice. If $\sigma \in O(V)$, then $\sigma(L)$ is also a (regular) lattice. Clearly, $Q(\sigma L) = Q(L)$, so that the elements of R represented by L is the same as those represented by $\sigma(L)$. We thus want to identify $\sigma(L)$ and L as belonging to the same equivalence class, and we thus want to classify the equivalence classes of lattices in V. This leads to the following definition.

Definition. The *class* of a lattice L, denoted $\mathrm{cls}(L)$, is the set of all full lattices K in V such that $\sigma(K) = L$ for some $\sigma \in O(V)$. The *proper class* of a lattice, denoted $\mathrm{cls}^+(L)$, is the subset of $\mathrm{cls}(L)$ consisting of those full lattices K such that $\sigma(K) = L$ for $\sigma \in SO(V)$.

Definition. The *group of automorphisms of a lattice* $O(L)$ is the subset of $O(V)$ consisting of those $\sigma \in O(V)$ such that $\sigma(L) = L$. We denote by $SO(L)$ the subgroup $SO(L) := O(L) \cap SO(V)$.

Clearly $O(L)$ and $O(K)$ are isomorphic as groups whenever K and L are in the same class; indeed, $O(\sigma L) = \sigma O(L)\sigma^{-1}$. Notice also that $SO(L)$ need not be a proper subgroup of $O(L)$; indeed, it is possible for $SO(L) = O(L)$ in some cases.

Lemma 6.16. *Suppose L is a full lattice on V. Then $\mathrm{cls}L = \mathrm{cls}^+L$ if and only if $SO(L)$ is a proper subgroup of $O(L)$ (necessarily a normal index 2 subgroup).*

Proof. We already have $\mathrm{cls}^+L \subseteq \mathrm{cls}L$. So suppose $K \in \mathrm{cls}L$, and write $K = \sigma L$ for $\sigma \in O(V)$. If $\sigma \in SO(V)$, we are done, so suppose $\det\sigma = -1$. Since $SO(L)$ is a proper subgroup, there exists a $\tau \in O(L)$ such that $\det(\tau) = -1$. Then $\sigma\tau(L) = \sigma(L) = K$, and $\det(\sigma\tau) = 1$. Hence $K \in \mathrm{cls}^+(L)$. □

Exercise 6.17. Show that there exists a natural bijection between $\mathrm{cls}L$ and $O(V)/O(L)$, such that under this bijection the subset cls^+L is in bijection with $SO(V)/SO(L) \hookrightarrow O(V)/O(L)$.

Exercise 6.18. If $\dim V$ is odd, show that $\mathrm{cls}L = \mathrm{cls}^+L$.

6.3.2 Orthogonal Splittings

Recall that, given lattices $L_1, ..., L_r$ in V, we can form the lattice $L = L_1 + \cdots + L_r$. We say that this sum is *direct*, written $L = L_1 \oplus + \cdots \oplus L_r$, if every element in L can be expressed uniquely as a sum $x_1 + \cdots + x_r$ for $x_i \in L_i$ (this is just the definition of a direct sum of R-modules).

Definition. Suppose $L = L_1 \oplus \cdots \oplus L_r$, and suppose that $B(x_i, x_j) = 0$ for all $x_i \in L_i$ and $x_j \in L_j$, for all $i \neq j$. Then we write $L = L_1 \perp \cdots \perp L_r$, and say that L has an *orthogonal splitting* into the components $L_1, ..., L_r$. We say that the L_i *split* L.

Clearly,

$$K(L_1 \perp \cdots \perp L_r) = KL_1 \perp \cdots \perp KL_r.$$

Notice that if V and W are regular quadratic spaces containing lattices L and M respectively, then $L \perp M$ makes sense as a lattice in $V \perp W$. We thus sometimes abuse notation by writing $L = L_1 \perp L_2$ for any arbitrary lattices L_1 and L_2 (even if they do not live in the same quadratic space), by considering L, L_1, L_2 as lattices in $KL = KL_1 \perp KL_2$.

If L is a full lattice in V, and suppose V has a basis $x_1, ..., x_n$, we can form the matrix $A = (B(x_i, x_j))_{i,j}$ as before. We have $V = \langle A \rangle$. We will write $L = \langle A \rangle$ to denote that $L = Rx_1 + \cdots + Rx_n$. In particular, we can consider a rank 1 lattice $\langle \alpha \rangle = Rx$ where x satisfies $Q(x) = 0$. We say that $x_1, ..., x_n$ is an *orthogonal basis* for L if

$$L = Rx_1 \perp \cdots \perp Rx_n.$$

Unlike in the case of a quadratic space, not all lattices have an orthogonal basis!

Finally, a comment on regularity.

Definition. A lattice L is *regular* if KL is a regular quadratic space.

Throughout, we will assume that L is regular. The following exercise shows that this assumption is harmless (see also Exercise 1.16).

Exercise 6.19. For any lattice L in any quadratic space V, set

$$\mathrm{rad}(L) = \{x \in L, B(x, v) = 0 \; \forall \; v \in L\}.$$

Recall also the subspace $\mathrm{rad}(V)$ from Exercise 1.16.

1. Show that $\mathrm{rad}(L)$ is a lattice in V.
2. Show that $\mathrm{rad}(KL) = K\mathrm{rad}(L)$ and that $\mathrm{rad}L = L \cap \mathrm{rad}(KL)$.
3. Show that L is a regular lattice if and only if $\mathrm{rad}(L) = \{0\}$.

4. Show $\text{rad}(L \perp M) = \text{rad}(L) \perp \text{rad}(M)$.

5. Given any lattice L in V, show that there exists a regular lattice M in V such that $L = M \perp \text{rad}(L)$.

6.4 Invariants of Lattices

We now construct various invariants of a lattice.

Consider the following lemma.

Lemma 6.20. *Suppose $L = Rx_1 + \cdots + Rx_k$ is a lattice in V. Consider any $y_1, ..., y_k \in KL$. Then $y_1, ..., y_k$ is a basis for L if and only if we have $y_i = \sum_j a_{ij}x_j$ where $(a_{ij}) \in GL_k(R)$ (importantly, $\det(a_{ij}) \in R^*$).*

Proof. Since $y_i \in KL$, we can write $y_i = \sum_j a_{ij}x_j$ for $a_{ij} \in K$. Notice that $y_1, ..., y_k$ is a basis for L if and only if all the $a_{ij} \in R$ and if there exists $b_{ij} \in R$ such that $x_i = \sum_j b_{ij}y_j$. In particular, it follows that $y_1, ..., y_k$ is a basis for L if $(a_{ij}) \in GL_k(R)$ since we may take $b_{ij} = (a_{ij})^{-1}$. On the other hand, if we can find such a $(b_{ij}) \in M_k(R)$, then we have $x_i = \sum_j \left(\sum_h b_{ih}a_{hj}\right) x_j$. Linear independence implies that $(a_{ij})(b_{ij}) = I_k$ in $M_k(R)$, and so $(a_{ij}) \in GL_k(R)$. □

Thus, we see that the matrices $X = (B(x_i, x_j))_{i,j}$ and $Y = (B(y_i, y_j))_{i,j}$ satisfy $Y = A^tXA$ where $A = (a_{ij})_{i,j} \in GL_k(R)$ is in the lemma above. Thus $\det Y = u^2 \det X$ for some $u \in R^*$. Since we are assuming our spaces to be regular, we also know that $\det X \neq 0$. This motivates the following definition.

Definition. The *discriminant* of a full regular lattice L in V, written $\text{disc}L$, is the class $(\det X)(R^*)^2 \in K^*/(R^*)^2$. For any regular lattice L in V, by considering L as a sublattice of KL, we can thus define $\text{disc}L$.

Since $R^* \subset K^*$, note that $(\text{disc}L)(K^*)^2 = \text{disc}(KL)$. We also clearly have $\text{disc}(\alpha L) = \alpha^{2r}\text{disc}L$ where $r = \text{rank}L$.

Also, since $\text{disc}L$ can be considered as an element of K^* up to multiplication by (the square of) a unit, it follows that the fractional ideal $(\text{disc}L)R$ is well-defined. This fractional ideal is sometimes referred to as the *volume* of L.

Lemma 6.21. *Suppose L and M are regular lattices of the same rank with $M \subseteq L$. Then $(\text{disc}M) \cdot R \subset (\text{disc}L) \cdot R$, i.e. $\text{disc}M/\text{disc}L \in R/(R^*)^2$. Moreover, $\text{disc}M/\text{disc}L \in R^*/(R^*)^2$ if and only if $L = M$.*

Proof. Without loss of generality, suppose L and M are full. Write $L = Rx_1 + \cdots + Rx_n$. Set $X = (B(x_i, x_j))_{i,j}$ (so $L = \langle X \rangle$). Write $M = Ry_1 + \cdots + Ry_n$; then there exists $C \in M_n(R)$ with entries in R such that

$$(y_1, ..., y_n) = (x_1, ..., x_n)C.$$

Set $Y = (B(y_i, y_j))_{i,j} \in M_n(K)$. A computation shows that $Y = C^tXC$. Hence $\det Y = (\det C)^2 \det X$ with $\det C \in R$. The first result follows. The second statement follows from the fact that $\det C \in R^*$ if and only if $C \in GL_n(R)$. □

Since $\text{disc}(\sigma L) = \text{disc}L$, we have the following corollary.

Corollary 6.21.1. *Suppose L is a full regular lattice. If $\sigma \in O(V)$ satisfies $\sigma L \subseteq L$, then $\sigma L = L$ and so $\sigma \in O(L)$.*

Related to the discriminant are the following two invariants.

Definition. The *scale* of a regular lattice L, written $\mathfrak{s}L$, is the fractional ideal of R generated by $B(x, y)$ for $x, y \in L$. The *norm* of a lattice L, written $\mathfrak{n}L$, is the fractional ideal of R generated by $Q(L)$.

Again, by regularity of KL we see that $\mathfrak{s}L$ and $\mathfrak{n}L$ are non-zero fractional ideals of R, i.e. $\mathfrak{s}L = s(L) \cdot R$ and $\mathfrak{n}L = n(L) \cdot R$ for some $s(L), n(L) \in K^*$. Moreover, these elements $s(L)$ and $n(L)$ of K^* are well-defined only up to R^*.

If $L = Rx_1 + \cdots + Rx_r$, notice that

$$\mathfrak{s}L = \sum_{1 \le i \le j \le r} B(x_i, x_j) \cdot R \quad \text{and} \quad \mathfrak{n}L = Q(x_1)R + \cdots + Q(x_r)R + 2\mathfrak{s}L$$

as fractional ideals of R. In particular, $2\mathfrak{s}L \subseteq \mathfrak{n}L \subseteq \mathfrak{s}L$.

The following properties of the discriminant, scale, and norm of a lattice follow from the definitions, and are left as exercises.

Lemma 6.22. *Suppose V and W are regular quadratic spaces. Let L be a full lattice in V, M a full lattice in W, and write $N = L + M$ for the corresponding full lattice in $V \perp W$. Then,*

$$\mathfrak{s}N = \mathfrak{s}L + \mathfrak{s}M \quad \text{and} \quad \mathfrak{n}N = \mathfrak{n}L + \mathfrak{n}M.$$

Lemma 6.23. $\mathfrak{s}(\alpha L) = \alpha^2(\mathfrak{s}L)$ *and* $\mathfrak{n}(\alpha L) = \alpha^2(\mathfrak{n}L)$.

Lemma 6.24. *Let M be a non-zero lattice in the regular quadratic space V. Then, there exists a full lattice L on V split by M (i.e. $L = M \perp J$ for some lattice J in V) with the same scale and norm as M.*

Lemma 6.25. *Suppose L is a lattice of rank r. Then,* $\mathrm{disc}L \subset (\mathfrak{s}L)^r$ *(viewing* $\mathrm{disc}L$ *as a coset in $K^*/(R^*)^2$). In other words,* $(\mathrm{disc}L)s(L)^{-r} \in R/R^*$.

Exercise 6.26. Prove Lemma 6.23, Lemma 6.24, and Lemma 6.25.

6.5 Modular Lattices

Suppose L is a regular lattice of rank r. Write $\mathrm{disc}L = \alpha(R^*)^2$. We know that $\alpha \in (\mathfrak{s}L)^r$.

Definition. Suppose $\alpha \in K^*$. A regular lattice L is *α-modular* if $(\mathrm{disc}L)R = \alpha R$ and $(\mathfrak{s}L)^r = \alpha R$ (so that $s(L) = \alpha R^*$). A lattice is *unimodular* if it is 1-modular.

Clearly βL is $\beta^2\alpha$-modular whenever L is α-modular. The lattice Rx with $x \in V$ anisotropic is always $Q(x)$-modular.

Lemma 6.27. *Write $L = \langle X \rangle$ for $X \in M_r(K)$. Then L is unimodular if and only if $X \in GL_r(R)$.*

Exercise 6.28. Prove Lemma 6.27.

Given a lattice L, consider

$$L^\# := \{x \in KL : B(x, y) \in R \; \forall \; y \in L\}.$$

This is the *dual lattice*. One can check easily that if $L = Rx_1 + \cdots + Rx_r$ and $y_i \in KL$ is such that $B(y_i, x_j) = \delta_{ij}$ (the Kronecker delta), then

$$L^\# = Ry_1 + \cdots + Ry_n.$$

Hence $L^\#$ is an honest lattice. One can compute that $K(L^\#) = KL$, $(L^\#)^\# = L$, $(\alpha L)^\# = \alpha^{-1}L^\#$ for any $\alpha \in K^*$, and $(L \perp M)^\# = L^\# \perp M^\#$. A simple computation shows that $\mathrm{disc}L^\# = (\mathrm{disc}L)^{-1}$, i.e. if we write $\mathrm{disc}L = \alpha(R^*)^2$ for $\alpha \in K^*$, then $\mathrm{disc}L^\# = \alpha^{-1}(R^*)^2$.

Proposition 6.29. *Suppose L is a non-zero regular lattice. The following are equivalent.*

1. *L is α-modular.*
2. *$\alpha L^\# = L$.*
3. *$B(x, L) = \alpha R$ for every maximal vector x in L.*

Proof. Suppose L is α-modular. Then $B(L, \alpha^{-1}L) \subseteq R$ so that, by definition, $\alpha^{-1}L \subseteq L^\#$. On the other hand, since $\mathrm{disc}L = \alpha^r(R^*)^2$ we have

$$\mathrm{disc}(\alpha^{-1}L) = \alpha^{-2r}\mathrm{disc}L = \alpha^{-r}(R^*)^2 = (\mathrm{disc}L)^{-1} = \mathrm{disc}L^\#.$$

By Lemma 6.21, it follows that $\alpha^{-1}L = L^{\#}$. Hence (1) $\implies$ (2). On the other hand, if (2) holds, so that $B(L,L) = B(L, \alpha L^{\#}) \subseteq \alpha R$ and thus $\mathfrak{s}L \subseteq \alpha R$. Further, we have

$$\mathrm{disc}L = \mathrm{disc}(\alpha L^{\#}) = \alpha^{2r}\mathrm{disc}(L^{\#}) = \alpha^{2r}(\mathrm{disc}L)^{-1}.$$

Hence $\mathrm{disc}L = \alpha^r (R^*)^2$. Since $(\mathrm{disc}L)(R^*) \subset \mathfrak{s}L$, we see that $\mathfrak{s}L = \alpha R$, and we are done.

Now suppose $\alpha L^{\#} = L$, and let x be a maximal vector. We have $B(x, L^{\#}) \subseteq R$ by definition of $L^{\#}$, so that $B(x,L) \subseteq \alpha R$. As x is maximal, we can find a basis $x_1, ..., x_n$ of KL with $x_1 = x$ such that $L = Rx_1 + \cdots + Rx_n$. Let $y_1, ..., y_n$ be the dual basis of KL, i.e. y_i satisfies $B(y_i, x_j) = \delta_{ij}$. Then $L^{\#} = Ry_1 + \cdots + Ry_n$. Hence,

$$\alpha R \supseteq B(x,L) \supseteq B(x, R\alpha y_1) = \alpha B(x, y_1)R = \alpha R.$$

Thus (2) $\implies$ (3).

Finally, suppose (3). Since any basis vector for L is also maximal, it is easy to see that $\mathfrak{s}L = \alpha R$. In particular, $B(\alpha^{-1}L, L) \subseteq R$. It follows from the definition of the dual that $\alpha^{-1}L \subseteq L^{\#}$. Now suppose $y \in KL \setminus L$, so that $y = \beta x$ for some x maximal in L with $\beta \notin R$. Then, we have $B(y,L) = \beta B(x,L) = \alpha\beta R$, which is not contained in αR as $\beta \notin R$. In particular, we see that no vector in $KL \setminus L$ can lie in $\alpha L^{\#}$, and hence $\alpha L^{\#} \subseteq L$. Statement (2) follows. □

Proposition 6.30. *Suppose L is a regular lattice and J is a α-modular sublattice of L. Then J splits L (i.e. $L = J \perp M$ for some sublattice M of L) if and only if $B(J,L) \subseteq \alpha R$.*

Proof. If $L = J \perp M$, then we see that $B(J,L) = B(J,J) \subseteq \mathfrak{s}L = \alpha R$. So suppose that $B(J,L) \subseteq \alpha R$. By regularity, we write $KL = KJ \perp W$ for some subspace W of V. Write $M = L \cap W$. We claim that $L = J \perp M$. We already have $J \perp M \subseteq L$. Suppose $x \in L$. Write $x = y + z$ for $y \in KJ$ and $z \in W$. Then $B(y,J) = B(x,J) \subseteq B(L,J) \subseteq \alpha R$. It follows that $\frac{1}{\alpha}y \in J^{\#}$. By Proposition 6.29, we have $y \in J$. Hence $z = x - y \in L$ as well, and we are done. □

The definition of $\mathfrak{s}L$ implies the following corollary.

Corollary 6.30.1. *If J is an α-modular sublattice of L, where $\mathfrak{s}L = \alpha R$, then J splits L.*

Corollary 6.30.2. *If L is a α-modular lattice and x is an isotropic vector in L, then there exists a binary lattice J splitting L and containing x.*

Proof. Let $x_1, ..., x_n$ be a basis for KL with $x_1 = x$. By scaling $x_2, ..., x_n$, we suppose that $x_1, ..., x_n$ is a basis for L. Let $y_1, ..., y_n$ be a dual basis to $x_1, ..., x_n$ (i.e. $B(x_i, y_j) = \delta_{ij}$), so that $L^{\#} = Ry_1 + \cdots + Ry_n$. We have $\alpha L^{\#} = L$. Take $J = Rx + R\alpha y_1$; this is clearly a binary sublattice of L containing x. A quick computation shows that $\mathrm{disc}J = \alpha^2 (R^*)^2$. Also, we have $\mathfrak{s}J \subseteq \mathfrak{s}L \subseteq \alpha R$. Hence J is α-modular as well, and so splits L by the proposition. □

Remark 6.31. Note the similarity to Corollary 1.17.1.

Suppose L is a non-zero regular lattice, and suppose $\alpha \in K^*$. Define

$$L^{\alpha} := \{x \in L : B(x,L) \subseteq \alpha R\}.$$

Lemma 6.32. *For L a non-zero regular lattice, the following holds.*

1. *L^{α} is a lattice with $\mathfrak{s}(L^{\alpha}) \subseteq \alpha R$.*
2. *$L^{\alpha} = L$ if and only if $\mathfrak{s}(L) \subseteq \alpha R$.*
3. *$L^{\alpha} = \alpha L^{\#} \cap L$.*
4. *$\beta L^{\alpha} \subseteq L^{\alpha\beta} \subseteq L^{\alpha}$ for all $\beta \in R \setminus \{0\}$.*
5. *If L is α-modular, then $L^{\alpha\beta} = \beta L$ and $L^{\alpha/\beta} = L$ for all $\beta \in R \setminus \{0\}$.*

Exercise 6.33. Prove Lemma 6.32.

7 Lattices over Rings of Integers of Local Fields

We will now consider lattices over $\mathcal{O}_K$, where K is a non-archimedean local field with valuation $|.|$ and uniformiser π. Since $\mathcal{O}_K$ is a local ring, it is a PID. Moreover, every fractional ideal of $\mathcal{O}_K$ is of the form $\pi^r\mathcal{O}_K$ for $r \in \mathbb{Z}$; this makes the theory significantly simpler. This simple fact, for instance, implies the following very useful facts.

Lemma 7.1. *If $x, y \in L$ are such that $|B(x,y)|$ is the largest, then $B(L,L) = B(x,y)\mathcal{O}_K = \mathfrak{s}L$.*

Lemma 7.2. *If $x \in L$ is such that $|Q(x)|$ is the largest, then $\mathfrak{n}L = Q(x)\mathcal{O}_K$.*

In keeping with Section 4, in this section we will again restrict ourselves to non-dyadic fields and to $\mathbb{Q}_2$ only, for simplicity. However, the theory for $\mathbb{Q}_2$ carries over pretty much verbatim to any *2-adic field*, i.e. any dyadic field K where 2 is a uniformiser of K.

There are significant complications if the dyadic field is not 2-adic. A simple reason is that $2\mathfrak{s}L \subseteq \mathfrak{n}L \subseteq \mathfrak{s}L$; if K is 2-adic, this double inequality immediately implies that $\mathfrak{n}L = \mathfrak{s}L$ or $\mathfrak{n}L = 2\mathfrak{s}L$. If K were not 2-adic, other cases would need to be considered. For the general theory over dyadic local fields, see [OMe73, §93].

7.1 Automorphisms of a Lattice

Suppose L is a lattice on the regular quadratic space V over K.

Lemma 7.3. *Let u be any maximal anisotropic vector of L. Then $\tau_u \in O(L)$ if and only if $2B(u,L) \subseteq Q(u)\mathcal{O}_K$.*

Proof. If $\tau_u L = L$, then $\frac{2B(u,x)}{Q(u)}u = x - \tau_u x \in L$ for all $x \in L$. Since u is a maximal vector of L, we have $2\frac{B(u,x)}{Q(u)} \in \mathcal{O}_K$ as required. On the other hand, if $2B(u,L) \subseteq Q(u)\mathcal{O}_K$, then $\tau_u x = x - \frac{2B(u,x)}{Q(u)}u \in L$. Hence $\tau_u L \subseteq L$, and so $\tau_u \in O(L)$. □

Lemma 7.4. *$O(L)$ contains a symmetry of V.*

Proof. Suppose $u \in L$ with $Q(u)\mathcal{O}_K = \mathfrak{n}L$; in particular, u is anisotropic. We claim that u is a maximal vector. Since $u \in L$, we already have $R \subseteq \mathfrak{c}_u$. So suppose $\alpha \in \mathfrak{c}_u$ so that $\alpha u \in L$. Then $\alpha^2 Q(u) = Q(\alpha u) \in \mathfrak{n}L = Q(u)\mathcal{O}_K$, which implies $\alpha^2 \in \mathcal{O}_K$. Hence $\alpha \in \mathcal{O}_K$. It follows that $\mathfrak{c}_u = \mathcal{O}_K$, and so u is maximal. Since

$$2B(u,L) \subseteq 2\mathfrak{s}L \subseteq \mathfrak{n}L = Q(u)\mathcal{O}_K,$$

the condition of Lemma 7.3 is met and hence $\tau_u \in O(L)$. □

In particular, we see that $SO(L) \neq O(L)$. Lemma 6.16 yields the following.

Corollary 7.4.1. *We have* $\mathrm{cls}L = \mathrm{cls}^+L$.

Thus, any two lattices that are equivalent are properly equivalent. This is useful!

7.2 Jordan Decomposition

Suppose L is a non-zero regular lattice. If there exists $x \in L$ with $Q(x)\mathcal{O}_K = \mathfrak{s}L$, then $J = \mathcal{O}_K x$ is a $s(L)$-modular sublattice of L.. On the other hand, suppose $Q(x)\mathcal{O}_K \subset \mathfrak{s}L$ for all $x \in L$. Then we may pick $x, y \in L$ with $B(x,y)\mathcal{O}_K = \mathfrak{s}L$. Take $J = \mathcal{O}_K x + \mathcal{O}_K y$. Since $|B(x,y)| > |Q(x)|, |Q(y)|$, the quantity $Q(x)Q(y) - B(x,y)^2$ is non-zero, and it follows that J is a regular binary lattice. This also implies that $\mathfrak{s}J = B(x,y)\mathcal{O}_K = \int L$ and that $(\mathrm{disc}J)\mathcal{O}_K = B(x,y)^2\mathcal{O}_K = (\mathfrak{s}L)^2$. Hence J is actually as binary $s(L)$-modular sublattice of L. The upshot is that we can always find a rank 1 or rank 2 $s(L)$-modular sublattice J of L. By Proposition 6.30, it follows that

$$L = J_1 \perp \cdots \perp J_2$$

where each of the J_i are rank 1 or 2 modular sublattices of L.

Definition. A *Jordan splitting/decomposition* of a lattice L is an orthogonal splitting $L = L_1 \perp \cdots \perp L_r$ where each of the L_i are modular, and $\mathfrak{s}L_1 \supset \cdots \supset \mathfrak{s}L_r$.

By grouping the various J_i according to their scales, we immediately get the following.

Lemma 7.5. *Every non-zero regular lattice over $\mathcal{O}_K$ has a Jordan splitting.*

We will now study to what extent the Jordan splitting is unique.

Recall the lattice L^α for $\alpha \in K^*$.

Lemma 7.6. *Suppose $L = L_1 \perp \cdots \perp L_r$ is a Jordan decomposition, and let $\alpha \in K^*$. Then $\mathfrak{s}L^\alpha = \alpha R$ if and only if L_i is α-modular for some i. Otherwise, if none of the L_i are α-modular, we have $\mathfrak{s}L^\alpha \subset \alpha\mathcal{O}_K$.*

Proof. Notice that, as a consequence of Lemma 6.32 and the fact that $\alpha\mathcal{O}_K \subseteq \beta\mathcal{O}_K$ if and only if $|\alpha| \leq |\beta|$, for a β-modular lattice L the lattice L^α is α-modular if and only if $\alpha = \beta$; otherwise, it is γ-modular for some γ with $|\gamma| < |\alpha|$.

Now suppose α is as in the statement of the lemma. We already know that $\mathfrak{s}L^\alpha \subseteq \alpha\mathcal{O}_K$, and that

$$L^\alpha = L_1^\alpha \perp \cdots \perp L_t^\alpha.$$

If L_i is not α-modular, then L_i^α will be γ-modular for $|\gamma| < |\alpha|$. On the other hand, if L_i^α is α-modular, then $L_i^\alpha = L_i$. Since $\mathfrak{s}L^\alpha$ is the ideal generated by $\mathfrak{s}_i L^\alpha$, the result follows. □

In fact, this proof shows that if there is an α-modular component L_i in the Jordan decomposition of L, then L_i will occur first in a Jordan decomposition for L^α.

Proposition 7.7. *Suppose L is a lattice over $\mathcal{O}_K$ with two Jordan splittings $L = L_1 \perp \cdots \perp L_t$ and $L = M_1 \perp \cdots \perp M_T$. Then $t = T$, and for $1 \leq i \leq t$ we have $\mathfrak{s}L_i = \mathfrak{s}M_i$, $\mathfrak{n}L_i = \mathfrak{n}M_i$, and $\mathrm{rank}L_i = \mathrm{rank}M_i$.*

Proof. Suppose that there is an α-modular component in the first Jordan splitting. The previous lemma implies that $\mathfrak{s}L^\alpha = \alpha\mathcal{O}_K$, and so (once again by the previous lemma) one of the components in the second Jordan splitting is α-modular. The converse also holds, i.e. if there is an α-modular component in the second Jordan splitting, then there is an α-modular component in the first Jordan splitting. In particular, we see that $t = T$ and that $\mathfrak{s}L_i = \mathfrak{s}M_i$ for $1 \leq i \leq t$.

Now suppose $1 \leq i \leq t$, and take $\alpha\mathcal{O}_K = \mathfrak{s}L_i = \mathfrak{s}M_i$. Since L_i and M_i are the first components in Jordan decompositions of L^α, we may suppose without loss of generality that $i = 1$. By scaling B, we may also suppose that $\mathfrak{s}L = \mathcal{O}_K$. Consider the K-linear map $\phi : KL_1 \to KM_1$ defined as the composition

$$KL_1 \hookrightarrow KL_1 \perp \cdots \perp KL_t = KL = KM_1 \perp \cdots \perp KM_t \twoheadrightarrow KM_1.$$

Notice that ϕ satisfies $\phi(L_1) \subseteq M_1$. Since $\mathfrak{s}(M_2 \perp \cdots \perp M_t) = \mathfrak{s}M_2 \subset \mathfrak{s}M_1 = \mathcal{O}_K$, we see that $B(z, z') \equiv 0 \,(\mathrm{mod}\,\pi)$ for all $z, z' \in M_2 \perp \cdots \perp M_t$. Thus, for all $x, x' \in L_1$, we have

$$B(\phi x, \phi x') \equiv B(x, x') \,(\mathrm{mod}\,\pi).$$

Suppose $\phi x = 0$ for some non-zero $x \in KL_1$. By scaling x, we may suppose x is a maximal vector of L_1. As L_1 is assumed unimodular, Proposition 6.29 implies that $B(x, y) = 1$ for some $y \in L_1$. Then, we have

$$1 = B(x, y) \equiv B(\phi x, \phi y) = 0 \,(\mathrm{mod}\,\pi),$$

which is impossible. Hence ϕ is injective. It follows that $\dim KL_1 \leq \dim KM_1$. By symmetry, it follows that $\dim KL_1 = \dim KM_1$ and hence that $\mathrm{rank}L_1 = \mathrm{rank}M_1$.

If K is non-dyadic, we are done as $\mathfrak{n}L_i = \mathfrak{s}L_i$. So we may suppose that K is 2-adic. Suppose $\mathfrak{n}L_1 = \mathcal{O}_K = \mathfrak{s}L_1$. We can thus find $x \in L_1$ with $Q(x) = \epsilon$ for some $\epsilon \in \mathcal{O}_K^*$. Then $Q(\phi x) \equiv Q(x) = \epsilon \,(\mathrm{mod}\,\pi)$ which implies that $Q(\phi x) \in \mathcal{O}_K^*$. Hence $\mathcal{O}_K \subseteq \mathfrak{n}M_1 \subseteq \mathfrak{s}M_1 = \mathcal{O}_K$, so that $\mathfrak{n}M_1 = \mathcal{O}_K$. By symmetry, we thus see that $\mathfrak{n}L_1 = \mathcal{O}_K$ if and only if $\mathfrak{n}M_1 = \mathcal{O}_K$. As $2\mathcal{O}_K \subseteq \mathfrak{n}L_1 \subseteq \mathcal{O}_K$ and 2 is a uniformiser of K, it follows that $\mathfrak{n}L_1 = \mathfrak{n}L_2$. □

Definition. Suppose L and M are lattices over $\mathcal{O}_K$ with Jordan decompositions $L = L_1 \perp \cdots \perp L_t$ and $M = M_1 \perp \cdots \perp M_T$. We say that these Jordan decompositions are of *the same Jordan type* if $t = T$ and if for $1 \leq i \leq t$ we have $\mathfrak{s}L_i = \mathfrak{s}M_i$, $\mathfrak{n}L_i = \mathfrak{n}M_i$, and $\mathrm{rank}L_i = \mathrm{rank}M_i$

We have thus shown that two Jordan decompositions of the same lattice must be of the same Jordan type.

7.3 K non-dyadic

For K non-dyadic, we have $2 \in \mathcal{O}_K^*$. This simple fact simplifies the entire theory of non-dyadic fields. Indeed, notice that $2\mathfrak{s}L \subseteq \mathfrak{n}L \subseteq \mathfrak{s}L$ implies that $\mathfrak{s}L = \mathfrak{n}L$. In particular, we can find $x \in L$ such that $Q(x)\mathcal{O}_K = \mathfrak{s}L$. From the proof of Lemma 7.5, it follows that L has an orthogonal basis, i.e.

$$L = \mathcal{O}_K x_1 \perp \mathcal{O}_K x_2 \perp \cdots \perp \mathcal{O}_K x_n.$$

Lemma 7.8. *If L is a unimodular lattice, there exists $\epsilon \in \mathcal{O}_K^*$ such that*

$$L \cong \langle 1 \rangle \perp \cdots \perp \langle 1 \rangle \perp \langle \epsilon \rangle .$$

Proof. Since L has an orthogonal basis, and since L is unimodular, Lemma 6.27 implies that we can write $L = \langle \epsilon_1 \rangle \perp \cdots \perp \langle \epsilon_n \rangle$ for $\epsilon_i \in \mathcal{O}_K^*$. Set $\epsilon = \epsilon_1 \cdots \epsilon_n$. It follows from Theorem 4.47 and a quick computation of Hasse invariants that

$$KL \cong \langle 1 \rangle \perp \langle 1 \rangle \perp \cdots \perp \langle \epsilon \rangle .$$

We can thus find a full lattice $M \cong \langle 1 \rangle \perp \cdots \perp \langle 1 \rangle \perp \langle \epsilon \rangle$ on KL. We claim that $M \cong L$. We prove this by induction on $n = \dim KL = \text{rank}L = \text{rank}M$.

If $n = 1$, this is trivial. Suppose $n \geq 2$. Since any space of dimension ≥ 2 is universal over the finite field κ_K, we may find $\alpha_1, ..., \alpha_n \in \mathcal{O}_K$ such that

$$\epsilon_1 \alpha_1^2 + \cdots + \epsilon_n \alpha_n^2 \equiv 1 \,(\text{mod}\, \pi).$$

We cannot have all of $\alpha_1, ..., \alpha_n \equiv 0 \,(\text{mod}\, \pi)$, so reordering if necessary we may suppose $\alpha_1 \in \mathcal{O}_K^*$. An application of Hensel's lemma to the polynomial

$$\epsilon_1 x^2 + (\epsilon_2 \alpha_2^2 + \cdots + \epsilon_n \alpha_n^2) - 1$$

implies that, upon modification of α_1, we can write $\epsilon_1 \alpha_1^2 + \cdots + \epsilon_n \alpha_n^2 = 1$. Thus there exists $x \in L$ such that $Q(x) = 1$, and so we have $L = \mathcal{O}_K x \perp L'$ for L' a rank $n-1$ unimodular lattice with discriminant $\epsilon(\mathcal{O}_K^*)^2$. By the induction hypothesis, $L' \cong \langle 1 \rangle \perp \cdots \perp \langle 1 \rangle \perp \langle \epsilon \rangle$, and the claim follows. □

Since $\mathcal{O}_K^*/(\mathcal{O}_K^*)^2$ is a group of order 2, the following corollary is obvious.

Corollary 7.8.1. *There are only two classes of unimodular lattices of given dimension over a non-dyadic local field.*

Theorem 7.9. *Suppose L and M are lattices of the same Jordan type on the regular quadratic space V over K. Consider Jordan splittings*

$$L = L_1 \perp \cdots \perp L_t \quad \text{and} \quad M = M_1 \perp \cdots \perp M_t.$$

Then $\text{cls}L = \text{cls}M$ *if and only if* $\text{disc}L_i = \text{disc}M_i$ *for all* $1 \leq i \leq t$.

Proof. If $\text{cls}L = \text{cls}M$, we may suppose without loss of generality that $L = M$. Consider a specific i. Scaling B, we may suppose that the modular lattices L_i and M_i are in fact unimodular. Then L_i and M_i are the first components of Jordan decompositions for L^1, and so we may suppose $i = 1$ without loss of generality.

Now, from the proof of Proposition 7.7, there is a K-linear isomorphism $\phi : KL_1 \to KM_1$ with $\phi(L_1) \subseteq \phi(M_1)$ and such that $B(\phi x, \phi y) \equiv B(x, y) \,(\text{mod}\, \pi)$ for all $x, y \in L_1$. Fix a specific basis for L_1 in which the discriminant is $\epsilon \in \mathcal{O}_K^*$. We then see that $\text{disc}(\phi L_1) \equiv \text{disc}L_1 \,(\text{mod}\, \pi)$, and so $\text{disc}(\phi L_1)\epsilon^{-1} \equiv 1 \,(\text{mod}\, \pi)$. The local square theorem then implies that $\text{disc}(\phi L_1) = \epsilon(\mathcal{O}_K^*)^2$ as well. It follows from Lemma 6.21that $\phi L_1 = M_1$. In particular, we see that $\text{disc}M_1 = \text{disc}L_1$.

Conversely, suppose that $\text{disc}L_i = \text{disc}M_i$ for all $1 \leq i \leq t$. Since L_i and M_i are both modular of the same scale and discriminant, it follows from Lemma 7.8 that $KL_i \cong KM_i$, and under this isometry, L_i is sent to M_i. Combining these isometries for all i, we get $\sigma \in O(V)$ such that $\sigma L = M$, and the result follows. □

Corollary 7.9.1. *Every non-zero regular lattice L over a non-dyadic field has a unique Jordan decomposition. Moreover, two lattices in the same quadratic space with the same Jordan decomposition must be in the same class.*

In other words, the Jordan decomposition uniquely determines the lattice, and vice versa.

Corollary 7.9.2. *Fix $\Delta \in \mathcal{O}_K^*$ a quadratic non-residue in κ_K. If L is a regular non-zero lattice, then there exist unique*

- *positive integers $t \geq 1$ and $m_1, ..., m_t \geq 1$ with $m_1 + \cdots + m_t = \mathrm{rank} L$,*
- *integers $e_1, ..., e_t \in \mathbb{Z}$ with $e_1 < \cdots < e_t$, and*
- *$\epsilon_i \in \{0, 1\}$ for $1 \leq i \leq t$,*

such that

$$L \cong \underbrace{\langle \pi^{e_1} \rangle \perp \cdots \perp \langle \pi^{e_1} \rangle}_{m_1 - 1 \text{ of them}} \perp \langle \Delta^{\epsilon_1} \pi^{e_1} \rangle \perp \cdots \perp \underbrace{\langle \pi^{e_t} \rangle \perp \cdots \perp \langle \pi^{e_t} \rangle}_{m_t - 1 \text{ of them}} \perp \langle \Delta^{\epsilon_t} \pi^{e_t} \rangle .$$

Corollary 7.9.3. *Suppose L is unimodular. We have $Q(L) \supseteq \mathcal{O}_K^*$ if $\dim L \geq 2$, and $Q(L) = \mathcal{O}_K$ for $\dim L \geq 3$.*

Exercise 7.10. Prove Corollary 7.9.3.

We have thus completely classified quadratic forms over $\mathcal{O}_K$ for K non-dyadic!

Proposition 7.11. *Suppose L is a full lattice in the n-ary regular quadratic space V over K. Then, every element of $O(L)$ is the product of at most $2n - 1$ reflections in $O(L)$.*

Proof. We proceed by induction on n. The statement for $n = 1$ is trivial, so we suppose $n \geq 2$. By suitably changing Q, we may suppose that $\mathfrak{s} L = \mathcal{O}_K$. Pick $\sigma \in O(L)$. Fix $y \in L$ with $Q(y) \in \mathcal{O}_K^*$ (such a y exists as $\mathfrak{s} L = \mathcal{O}_K$). From

$$Q(y - \sigma y) + Q(y + \sigma y) = 4Q(y) = 4\epsilon \in \mathcal{O}_K^*$$

it follows that one of $Q(y - \sigma y)$ or $Q(y + \sigma y)$ is a unit. If $Q(y - \sigma y) \in \mathcal{O}_K^*$, then $\tau_{y - \sigma y} \in O(L)$ by Lemma 7.3, and this reflection satisfies $\tau_{y-\sigma y} y = \sigma y$. On the other hand, if $Q(y + \sigma y) \in \mathcal{O}_K^*$, then a computation shows that $\tau_y, \tau_{y+\sigma y} \in O(L)$ and that

$$\tau_{y+\sigma y} \tau_y y = \sigma y.$$

Thus, in any case, we can find $\rho \in O(L)$ that is the product of at most two reflections such that $\sigma y = \rho y$. Since $\mathcal{O}_K y$ is unimodular, we have $L = \mathcal{O}_K y \perp L'$ with $\mathrm{rank} L' = n - 1$, and $(\rho^{-1}\sigma)|_{KL'} \in O(L')$. Since $\rho^{-1}\sigma$ is a product of at most $2n - 3$ reflections by the induction hypothesis, it follows that σ is the product of at most $2n - 1$ reflections. □

Exercise 7.12. Show that, if L is a binary regular lattice, then every element of $O(L)$ is in fact the product of at most 2 reflections. Hence, show that for $\mathrm{rank} L \geq 2$, every element of $O(L)$ is the product of at most $2n - 2$ reflections.

7.4 $K = \mathbb{Q}_2$

Remark 7.13. Rather than developing the theory of lattices for general dyadic fields as in [OMe73], I have chosen to take the simpler and cleaner route given in [Cas78].

Recall as before that any non-zero regular lattice L has a decomposition $L \cong J_1 \perp \cdots \perp J_r$ where J_i is a rank 1 or rank 2 modular lattice. The only possible rank 1 lattices over $\mathbb{Z}_2$ must clearly be one of the following

$$\langle 2^e \rangle , \langle 3 \cdot 2^e \rangle , \langle 5 \cdot 2^e \rangle , \text{ or } \langle 7 \cdot 2^e \rangle ,$$

for some $e \in \mathbb{Z}$. Let us now study rank 2 unimodular lattices.

Proposition 7.14. *If L is a binary unimodular lattice, then L is of the form*

$$\langle \epsilon_1 \rangle \perp \langle \epsilon_2 \rangle , \quad \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle , \quad \text{or} \quad \left\langle \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \right\rangle ,$$

where $\epsilon_1, \epsilon_2 \in \mathbb{Z}_2^*$ are some units.

Proof. Suppose first that $\mathfrak{n}L = \mathfrak{s}L = \mathbb{Z}_2$. Then there exists $x \in L$ with $Q(x) \in \mathbb{Z}_2^*$. Then $\mathbb{Z}_2 x$ is unimodular, and we have a splitting $L = \mathbb{Z}_2 x \perp \mathbb{Z}_2 y$ for some $y \in L$. Since $\mathfrak{s}L = \mathbb{Z}_2$, it follows that $L \cong \langle \epsilon_1 \rangle \perp \langle \epsilon_2 \rangle$ for some units ϵ_1, ϵ_2.

So we may thus suppose that $\mathfrak{n}L = 2\mathbb{Z}_2$. Pick $x, y \in L$ such that $B(x,y) \in \mathbb{Z}_2^*$. Since $\mathfrak{n}L = 2\mathbb{Z}_2$, it follows that $x \neq y$ and that $Q(x), Q(y) \in 2\mathbb{Z}_2$. Set $\delta := Q(x)Q(y) - B(x,y)^2$; we have

$$|\delta|_2 = \max\{|Q(x)|_2 |Q(y)|_2, 1\} = 1$$

since $B(x,y) \in \mathbb{Z}_2^*$. Hence, $\mathrm{disc}(\mathbb{Z}_2 x + \mathbb{Z}_2 y)\mathbb{Z}_2 = \mathbb{Z}_2 = (\mathrm{disc} L)\mathbb{Z}_2$, and so Lemma 6.21 implies that $L = \mathbb{Z}_2 x + \mathbb{Z}_2 y$.

Suppose that $Q(x) \in 2\mathbb{Z}_2^*$ and $Q(y) \in 2\mathbb{Z}_2^*$. By scaling x we may suppose that $Q(x) = 2a$ for some $a \in \{\pm 1, \pm 3\}$, and by scaling y we can assume that $B(x,y) = 1$. Write $Q(y) = 2b\epsilon^2$ for $\epsilon \in \mathbb{Z}_2^*$ and $b \in \{\pm 1, \pm 3\}$. Consider the polynomial

$$p(x) = (4ba^2\epsilon^2 - a)x^2 + (1 - 4ab\epsilon^2)x + b\epsilon^2 - 1.$$

We have $p'(x) = 1 - 4ab\epsilon^2 + 2x(4ba^2\epsilon^2 - a)$, and so $|p'(x)|_2 = 1$. Since $p(1) \equiv -a + 1 + b\epsilon^2 - 1 \equiv 0 \pmod 2$ (as all of a, b, ϵ are 2-adic units, and so are all $1 \pmod 2$), Hensel's Lemma then implies the existence of $\beta \in \mathbb{Z}_2^*$ such that $p(\beta) = 0$. With this choice of β, one can check that

$$Q\big(\beta x + (1 - 2a\beta)y\big) = 2 \quad \text{and} \quad B\big(\beta x + (1 - 2a\beta)y, x\big) = 1.$$

Thus, by replacing y with $1 - 2a\beta$, we may suppose that $Q(y) = 2$. One then checks that $L = \mathbb{Z}_2 x' + \mathbb{Z}_2 y$ where $Q(x') = 2$ and $B(x', y) = 1$ for $x' := (1 - 2\alpha)x + \alpha y$ where $\alpha \in \mathbb{Z}_2^*$ is one of the roots of the polynomial

$$a(1 - 2x)^2 + x^2 + x(1 - 2x) - 1 = 0.$$

Hence, we see that $L \cong \langle \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right) \rangle$.

On the other hand, suppose that one of $Q(x)$ or $Q(y)$ is divisible by 4, say without loss of generality that $4 | Q(y)$. By scaling x by a unit, we may suppose that $B(x,y) = 1$ as usual. Let ξ be a root of the polynomial

$$p(t) = \frac{Q(y)}{2}\big(1 - Q(x)t\big)^2 + \frac{Q(x)}{2}t^2 + t\big(1 - Q(x)t\big)$$

such that $\xi \equiv 0 \pmod 2$; since $p(0) = \frac{1}{2}Q(y) \equiv 0 \pmod 2$ and $p'(0) = 1 - Q(y)Q(x)$, one such ξ exists by Hensel's Lemma. Then, one can check that $L = \mathbb{Z}_2 x' + \mathbb{Z}_2 y'$ with $Q(x') = 0 = Q(y')$ and $B(x', y') = 1$, where

$$x' := \big(1 - \tfrac{1}{2}Q(x)\xi\big)\, x - \tfrac{1}{2}Q(x)(1 - Q(y)\xi)y \quad \text{and} \quad y' := \xi x + (1 - Q(y)\xi)y.$$

The result follows. □

We have thus proven the following.

Corollary 7.14.1. *The class of any regular lattice L over $\mathbb{Z}_2$ contains a lattice which is an orthogonal direct sum of the following types of rank 1 or 2 lattices:*

$$\langle 2^e \rangle, \langle 3 \cdot 2^e \rangle, \langle 5 \cdot 2^e \rangle, \langle 7 \cdot 2^e \rangle, \langle 2^e \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle, \text{ and } \langle 2^e \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right) \rangle$$

where $e \in \mathbb{Z}$.

However, such an orthogonal direct sum need not be unique. See the following exercises for example.

Exercise 7.15. Show the following equivalences, where $u \in \{1, 3, 5, 7\}$ can be arbitrary.

$$\langle 1 \rangle \perp \langle 1 \rangle \cong \langle 5 \rangle \perp \langle 5 \rangle; \quad \langle 1 \rangle \perp \langle 2 \rangle \cong \langle 3 \rangle \perp \langle 6 \rangle; \quad \langle 1 \rangle \perp \langle 4 \rangle \cong \langle 5 \rangle \perp \langle 20 \rangle; \quad \langle u \rangle \perp \langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle \cong \langle u \rangle \perp \langle 1 \rangle \perp \langle -1 \rangle;$$

$$\langle u \rangle \perp \langle \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right) \rangle \cong \langle 3u \rangle \perp \langle -u \rangle \perp \langle -u \rangle; \qquad \langle \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right) \rangle \perp \langle \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right) \rangle \cong \langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle \perp \langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle.$$

Given two Jordan decompositions, one can indeed figure out quickly whether two are the same or not. However, due to the tedious and unilluminating nature of the proof, and since we won't have any need for it, we shall skip it. See [OMe73, §93G] for the proof.

Let L and M be full lattices in a regular quadratic space over $\mathbb{Q}_2$. Suppose they have Jordan decompositions

$$L = L_1 \perp \cdots \perp L_t \quad \text{and} \quad M = M_1 \perp \cdots \perp M_t$$

of the same Jordan type (so that $\mathrm{rank} L_i = \mathrm{rank} M_i$, $\mathfrak{s}_i := \mathfrak{s}L_i = \mathfrak{s}M_i$, and $\mathfrak{n}_i := \mathfrak{n}L_i = \mathfrak{n}M_i$). Recall that, in a Jordan decomposition, the L_i (and M_i) are ordered so that

$$\mathfrak{s}_1 \supseteq \mathfrak{s}_2 \supseteq \cdots \supseteq \mathfrak{s}_t.$$

Set

$$L_{(i)} := L_1 \perp \cdots \perp L_i \quad \text{and} \quad M_{(i)} := M_1 \perp \cdots \perp M_i.$$

Notice that $L_{(t)} = L$ and $M_{(t)} = M$. Let $d_i^L, d_i^M \in \mathbb{Q}_2^*$ be chosen so that $\mathrm{disc} L_{(i)} = d_i^L(\mathbb{Z}_2^*)^2$ and $\mathrm{disc} M_{(i)} = d_i^M(\mathbb{Z}_2^*)^2$. Note that d_i^L and d_i^M are uniquely determined up to multiplication by a square of a unit. Finally, set $u_i = \mathrm{ord}_2 \mathfrak{n}_i$ and $v_i = \mathrm{ord}_2 \mathfrak{s}_i$, so that $\mathfrak{n}_i = 2^{u_i}\mathbb{Z}_2$, $\mathfrak{s}_i = 2^{v_i}\mathbb{Z}_2$, and $v_i \leq u_i \leq v_i + 1$.

Theorem 7.16. *With the notation as above, we have* $\mathrm{cls} L = \mathrm{cls} K$ *if and only if the following conditions hold for each* $1 \leq i \leq t-1$*:*

- $d_i^L/d_i^M \in \mathbb{Z}_2^*$ *and* $d_i^L/d_i^M \equiv 1 \pmod{2^{u_i+u_{i+1}-2v_i}}$
- *there exists an isometry* $\mathbb{Q}_2 L_{(i)} \hookrightarrow \mathbb{Q}_2 M_{(i)} \perp \langle 2^{u_i} \rangle$ *whenever* $2u_i \leq u_{i+1}$.

Remark 7.17. John Conway and Neil Sloane in Chapter 15 of their book [CS13] give a different characterisation that turns out to be more computationally efficient and easier to work with. Since that would require introducing new notation, we will not go into any details here.

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.

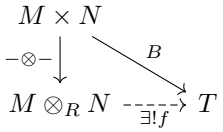
A.3 Tensor Products

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 $n \in N$.



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.