Questions in the Theory of Orthogonal Shimura Varieties

Andrew Fiori

Doctor of Philosophy

Department of Mathematics and Statistics

McGill University

Montreal, Quebec

June 30, 2013

A thesis submitted to McGill University
in partial fulfilment of the requirements for a Ph.D. degree

Acknowledgements

There are a great number of people whose help, support and guidance over the past few years have made it possible for me to complete this thesis. Firstly, I would like to thank my supervisor, Eyal Goren. Without his mathematical guidance, the suggestions for areas to look into, as well as all the help along the way, none of this would have been possible.

I would like next to thank my various professors, my fellow students and other colleagues. The great many things I have learned from all of you, as well as the environment for mathematical study you create, have been a great asset.

I would like to thank specifically Eva Bayer, the chief editor for my first submitted paper, for her patience and many suggestions which will be as valuable in my future as they were with improving the original manuscript.

I would also like to thank my friends and family: without the distractions and support they are able to provide I do not think I could have maintained sufficient sanity to complete this project.

I would particularly like to thank Victoria de Quehen who qualifies as both a good friend, fellow student and beyond the great asset she has been in both of those capacities has also been invaluable as a proofreader. I would like also to thank specifically the various other people who read and commented on various drafts of this text. In addition to those already mentioned these are my friends Juan Ignacio Restrepo and Cameron Franc.

Finally, I would like to thank the Mathematics and Statistics Department at McGill, the Institut des Sciences Mathematique as well as the National Science and Engineering and Research Council for their financial support during this time.

Abstract

We investigate a variety of questions in the theory of Shimura varieties of orthogonal type. Firstly we provide a general introduction in the theory of these spaces. Secondly, motivated by the problem of understanding the special points on Shimura varieties of orthogonal type we give a characterization of the maximal algebraic tori contained in orthogonal groups over an arbitrary number field. Finally, motivated by the problem of computing dimension formulas for spaces of modular forms, we compute local representation densities of lattices focusing specifically on those arising from Hermitian forms by transfer.

Resumé

Le but de cette thèse est l'exploration d'une variété de questions sur les variétés de Shimura de type orthogonal. On commence par une introduction à la théorie de ces espaces. Àpres, dans le but de caractériser les points spéciaux sur les variétés de Shimura de type orthogonal, on décrit les tores algébriques maximaux dans les groupes orthogonaux. Finalement, dans le but d'obtenir des formules explicites pour la dimension des espaces de formes modulaires sur les variétés de Shimura de type orthogonal, on trouve des formules pour les densités locales des réseaux. On se concentre sur les réseaux qui proviennent de la restriction de formes Hermitiennes.

TABLE OF CONTENTS

CHAPTER 1
Introduction

The primary motivation for this thesis has been to understand various aspects of orthogonal Shimura varieties. The study of these orthogonal symmetric spaces and their modular forms fits into the larger picture of automorphic forms on Shimura varieties. This topic has connections to the study of Galois representations and the Langlands conjectures. There are connections to explicit class field theory via the values of modular forms at special points. Moreover, the Gross-Zagier theorem [GZ86], which allows for the construction of non-torsion points on elliptic curves, has natural conjectural generalizations in this context, see for example the work of [BY06]. Understanding this phenomenon remains an important open question.

Modular forms have been both a successful tool and object of study in number theory for some time. As a result various generalizations also became objects of interest. An axiomatic treatment of many of these generalizations was given by Deligne in [Del71]. In his article he defines the notions of Shimura varieties. These Shimura varieties are highly related to Hermitian symmetric spaces, and are classified into families in much the same way. Although many of these families have already been well studied, those we will investigate have received less attention. The orthogonal Shimura varieties are precisely the generalizations that come from replacing the classical upper half plane by an orthogonal symmetric spaces associated to a quadratic form of signature (2,n). Though these spaces have been known for some time, many aspects of them have yet to be studied extensively and at present remain mysterious. It is only recently that results coming out of the Fields Medal work of Borcherds, in particular his work in [Bor95], have renewed interest in the structure of these spaces. Borcherds' contribution to the theory was to define a lift of classical modular forms on the upper half plane to modular forms on these orthogonal spaces. This lifting allows for the construction of special divisors together with Green functions that are objects of great interest in Arakelov theory. The work of various people, especially Brunier, Kudla, Rapoport and Yang (see [BKY12, Kud04, KR99]) have led to strong conjectures about the intersection theory of divisors on these spaces.

The bulk of the original results contained in this thesis are contained in two papers:

1. *The Characterization of Special Points on Orthogonal Symmetric Spaces* and
2. *Representation Densities for Hermitian Lattices.*

These appear in this thesis as Chapters 3 and 4 respectively. The first paper was published, in a format similar to what appears here, in [Fio12]. The second has not yet been submitted, and it may be restructured into shorter papers before being submitted.

Though the results of both of these chapters have applications outside the realm of orthogonal Shimura varieties, they are both motivated by the study of particular aspects of these spaces. The concrete relation of these chapters to orthogonal Shimura varieties is discussed in more detail in Chapter 2.

The first of the two papers characterizes which number fields can be associated to the algebraic tori in orthogonal groups. The application of this result in the study of orthogonal Shimura varieties is that it gives a characterization of the fields that are associated to the special points of these Shimura varieties. The results of this paper motivate our interest in a certain class of quadratic forms, that we call Hermitian and it is these Hermitian forms on lattices that are the motivation for our second paper.

Our second paper focuses on computing the arithmetic volume of the orthogonal groups associated to Hermitian lattices. These volumes, which are computed by way of representation densities, determine the lead term in a Riemann-Roch formula for dimensions of spaces of modular forms, but are also of independent interest. Though the primary motivation of the paper is the study of Hermitian lattices over the rational numbers, along the way we produce general formulas for computing representation densities over arbitrary number fields, as well as proving several structure theorems for the transfer of lattices. These latter results are of interest outside the study of Shimura varieties.

Aside from Chapters 3 and 4 which contain these papers, Chapter 2 is also fairly substantial. It can be viewed as either the background material necessary to understand the relation of the aforementioned chapters to the appropriate problem in the theory of orthogonal Shimura varieties, or a survey of the general theory of modular forms on Hermitian symmetric domains with an emphasis on the orthogonal case. Though most of the content of this background chapter is not new, the details of at least some aspects of the discussion are not known to appear in the literature.

A discussion of some further avenues of research are discussed in our conclusion (Chapter 5).

CHAPTER 2
Background And Motivation

The main purpose of this chapter is to explain the connection between the later chapters of this thesis and questions concerning orthogonal Shimura varieties. The connection for the content of Chapter 3 is made apparent in Section 2.6.3, whereas the connection for the content of Chapter 4 is made apparent in Section 2.4.4. The main purpose of the other sections in this chapter is to provide sufficient background on orthogonal Shimura varieties to properly explain these connections. Strictly speaking we provide more background than is needed.

The primary object of interest in this document are Shimura varieties of orthogonal type. In order to give a satisfactory definition of these one needs the terminology and notation of the theory of Hermitian symmetric spaces [Hel01], quadratic spaces and orthogonal groups [O'M00, Lam05, Ser73]. Note that Chapter 4 contains information about lattices, while Chapter 3 gives a basic overview of Clifford algebras. To put it in the right context one should perhaps also have access to the basic notions of Shimura varieties [Mil05, Del71].

It is our intent in this chapter to give a survey of the basic theory of orthogonal symmetric spaces. Other references include [Fio09, Bru08]. The sections of this chapter are organized as follows.

(2.1) Introduces key notations and results for orthogonal groups.

(2.2) Covers the key notions of Hermitian symmetric domains.

(2.3) Provides a basic definition of modular forms.

(2.4) Surveys the problem of computing dimension formulas for spaces of modular forms via the Hirzebruch-Mumford proportionality theorem (see [Mum77]).

(2.5) Discusses the ramification structures between different levels introducing two interesting classes of cycles on orthogonal Shimura varieties.

(2.6) Introduces the notions of Shimura varieties, special points and special fields.

2.1 Basics of Orthogonal Groups

It is natural to assume that the reader has a basic understanding of quadratic spaces. Thus, the main purpose of this section is to introduce our notation.

Definition 2.1.1. Let R be an integral domain, and K be its field of fractions. Given a finitely generated R-module V, a **quadratic form** on V is a mapping $q : V \to K$ such that:

1. $q(r\vec{x}) = r^2 q(\vec{x})$ for all $r \in K$ and $\vec{x} \in V$, and
2. $B(\vec{x}, \vec{y}) := q(\vec{x} + \vec{y}) - q(\vec{x}) - q(\vec{y})$ is a bilinear form.

Given such a pair (V, q), we call V a **quadratic module** over R. The quadratic module V is said to be **regular** or **non-degenerate** if for all $\vec{x} \in V$ there exists $\vec{y} \in V$ such that $B(\vec{x}, \vec{y}) \neq 0$.

Remark. Given an R module V and a bilinear form $b : V \times V \to K$ we have an associated quadratic form $q(\vec{x}) = b(\vec{x}, \vec{x})$. Note that $B(\vec{x}, \vec{y}) = 2b(\vec{x}, \vec{y})$.

Definition 2.1.2. We define the **Clifford algebra** and the **even Clifford algebra** to be respectively:

$$\mathrm{C}_q := \bigoplus_k V^{\otimes k} / (\vec{v} \otimes \vec{v} - q(\vec{v})) \text{ and } \mathrm{C}_q^0 := \bigoplus_k V^{\otimes 2k} / (\vec{v} \otimes \vec{v} - q(\vec{v})).$$

They are isomorphic to matrix algebras over quaternion algebras. We denote the standard involution $\vec{v}_1 \otimes \cdots \otimes \vec{v}_m \mapsto \vec{v}_m \otimes \cdots \otimes \vec{v}_1$ by $v \mapsto v^*$. To a quadratic form q we will associate the following algebraic groups:

$$\begin{aligned} \mathrm{O}_q(R') &= \{g \in \mathrm{GL}(V \otimes_R R') \mid q(\vec{x}) = q(g(\vec{x})) \text{ for all } x \in V \otimes_R R'\} \\ \mathrm{SO}_q(R') &= \{g \in \mathrm{O}_q(R') \mid \det(g) = 1\} \\ \mathrm{GSpin}_q(R') &= \{g \in (\mathrm{C}_q^0 \otimes_R R')^\times \mid gVg^{-1} \subset V\} \\ \mathrm{Spin}_q(R') &= \{g \in \mathrm{GSpin}_q(R') \mid g \cdot g^* = 1\}. \end{aligned}$$

Proposition 2.1.3. *Given a quadratic form q we have a short exact sequence of algebraic groups:*

$$0 \to \underline{\mathbb{Z}/2\mathbb{Z}} \to \mathrm{Spin}_q \to \mathrm{SO}_q \to 0.$$

Over a number field k, with $\Gamma = \mathrm{Gal}(\overline{k}/k)$, this becomes the long exact sequence:

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathrm{Spin}_q(k) \to \mathrm{SO}_q(k) \xrightarrow{\theta} H^1(\Gamma, \mathbb{Z}/2\mathbb{Z}) \to \dots.$$

*The map θ is called the **spinor norm**.*

Notation 2.1.4. We have the following standard invariants of (V, q):

- Whenever V is free over R we shall denote by $D(q)$ the **discriminant** of q, that is, $D(q) = \det(b(\vec{v}_i, \vec{v}_j)_{i,j})$ for some choice of basis $\{\vec{v}_1, \dots, \vec{v}_n\}$.
- We shall denote by $H(q)$ (or $H_R(q), H_{\mathfrak{p}}(q)$) the **Hasse invariant** of q, that is, if over the field of fractions K of R we may express $q(\vec{x}) = \sum_i a_i x_i^2$ then $H(q) = \prod_{i<j}(a_i, a_j)_K$. Here $(a, b)_K$ denotes the Hilbert symbol (see [Ser73, Ch. III] and [Ser79, Ch. XIV]).
- We shall denote by $W(q)$ the **Witt invariant** of q, that is, the class in $\mathrm{Br}(K)$ of C_q when $\dim(V)$ is odd or of C_q^0 when $\dim(V)$ is even.
- For a real place, $\rho : R \to \mathbb{R}$, we shall denote by $(r_\rho, s_\rho)_\rho$ the **signature** of q at ρ. Here r_ρ denotes the dimension of the maximal positive-definite subspace of $V \otimes_\rho \mathbb{R}$ and s_ρ denotes the dimension of the maximal negative-definite subspace of $V \otimes_\rho \mathbb{R}$.

2.2 Hermitian Symmetric Spaces

In this section we briefly recall some key results about Hermitian symmetric spaces. A good reference on this topic is [Hel01]. Most of what we will use can also be found in [BJ06, Sec I.5], or [AMRT10, Sec. 3.2].

Definition 2.2.1. A **symmetric space** is a Riemannian manifold $\mathcal{D}$ such that for each $x \in \mathcal{D}$ there exists an isometric involution s_x of $\mathcal{D}$ for which x is locally the unique fixed point. We say that $\mathcal{D}$ is **Hermitian** if $\mathcal{D}$ has a complex structure making $\mathcal{D}$ Hermitian.

Example. The standard example of this is the upper half plane:

$$\mathbb{H} = \{x + iy \in \mathbb{C} \mid y > 0\}.$$

It is a consequence of the definition that we have:

Theorem 2.2.2. *Fix $x \in \mathcal{D}$, $G = \mathrm{Isom}(\mathcal{D})^0$, $K = \mathrm{Stab}_G(x)$ and let s_x act on G by conjugation then $\mathcal{D} \simeq G/K$ and $(G^{s_x})^0 \subset K \subset G^{s_x}$. Moreover, given any real Lie group G, an inner automorphism $s : G \to G$ of order 2, and K such that $(G^s)^0 \subset K \subset G^s$, then the manifold $\mathcal{D} = G/K$ is a symmetric space.*

See [Hel01, Thm. IV.3.3].

Theorem 2.2.3. *A symmetric space $\mathcal{D} = G/K$ is Hermitian if and only if the centre $Z(K)$ of K has positive dimension. Moreover, if $\mathcal{D}$ is irreducible then $Z(K)^0 = \mathrm{SO}_2(\mathbb{R})$.*

See [Hel01, Thm. VIII.6.1].

There are three main types of symmetric spaces:

1. Compact Type: In general these come from compact Lie groups G.
2. Non-Compact Type: In general these arise when K^0 is the maximal compact connected Lie subgroup of G, or equivalently when s_x is a Cartan involution.
3. Euclidean Type: These generally arise as quotients of Euclidean space by discrete subgroups.

The definitions of these types can be made precise by looking at the associated Lie algebras.

Claim. *Every symmetric space decomposes into a product of the three types listed above.*

See [Hel01, Ch. V Thm. 1.1].

For $\mathcal{D}$ a Hermitian symmetric space of the non-compact type, one often considers the following objects (see [Hel01] for details):

- The Lie algebra $\mathfrak{g}$ of G.
- The Lie sub-algebra $\mathfrak{k} \subset \mathfrak{g}$ of K.
- The Killing form $B(X, Y) = \mathrm{Tr}(\mathrm{Ad}(X) \circ \mathrm{Ad}(Y))$ on $\mathfrak{g}$.
- The orthogonal complement $\mathfrak{p}$ of $\mathfrak{k}$ under B is identified with the tangent space of $\mathcal{D}$.
- The centre $Z(K)$ of K and its Lie algebra $\mathfrak{u}$.
- A map $h_0 : \mathrm{SO}_2 \to Z(K) \subset K \subset G$ such that K is the centralizer of h_0.
- The element $s = \mathrm{Ad}(h_0(e^{i\pi/2}))$ induces the Cartan involution whereas the element $J = \mathrm{Ad}(h_0(e^{i\pi/4}))$ induces the complex structure.

Through these one can construct:

- A G-invariant metric on $\mathcal{D}$ (via B and the identification of the tangent space of $\mathcal{D}$ with $\mathfrak{p}$).
- The dual Lie algebra $\mathfrak{g}^* = \mathfrak{k} \oplus i\mathfrak{p}$. This is the Lie algebra of $\breve{G}$ the compact real form of G.
- The ideals $\mathfrak{p}_+, \mathfrak{p}_- \subset \mathfrak{p}_\mathbb{C}$ which are the eigenspaces of $\mathfrak{u}$.
- The parabolic subgroups $P_\pm$ associated respectively to $\mathfrak{p}_\pm$.
- The embeddings $\mathcal{D} = G/K \hookrightarrow G_\mathbb{C}/K_\mathbb{C}P_- \simeq \breve{G}/K \simeq \breve{\mathcal{D}}$.

There exists a duality between the compact and non-compact types, that is, if $\mathcal{D}$ is of the compact type, there exists a dual symmetric space $\breve{\mathcal{D}}$ such that $\mathcal{D} \hookrightarrow \breve{\mathcal{D}}$.

2.2.1 The O(2,n) Case

We now discuss the example of the Hermitian symmetric spaces in which we are most interested. That is those associated to quadratic spaces of signature $(2, n)$. Other references on this topic include [Fio09, Bru08, Bru02].

Let (V, q) be a quadratic space over $\mathbb{Q}$. Then $V(\mathbb{R}) := V \otimes \mathbb{R}$ has signature (r, s) for some choice of r, s. The maximal compact subgroup of $\mathrm{O}_q(\mathbb{R})$ is $K \simeq \mathrm{O}_r(\mathbb{R}) \times \mathrm{O}_s(\mathbb{R}) \subset \mathrm{O}_q(\mathbb{R})$ and $\mathrm{O}_q(\mathbb{R})/K$ is a symmetric space. These only have complex structures (and thus are Hermitian) if one of r or s is 2. Since interchanging r and s does not change the orthogonal group (it amounts to replacing q by $-q$) we will assume that $r = 2$. We wish to construct the associated symmetric spaces along with its complex structure in this case.

Remark. For much of the following discussion only the $\mathbb{R}$-structure will matter, and as such, the only invariants of significance are the values r and s. However, when we must consider locally symmetric spaces and their compactifications the $\mathbb{Q}$-structure, and potentially the $\mathbb{Z}$-structure, will become relevant.

The Grassmannian

Let (V, q) be of signature $(2, n)$. We consider the Grassmannian of 2-dimensional subspaces of $V(\mathbb{R})$ on which the quadratic form q restricts to a positive-definite form, namely:

$$\mathrm{Gr}(V) := \{v \subset V \mid \dim(v) = 2, q|_v > 0\}.$$

By Witt's extension theorem (see [Ser73, Thm. IV.3]), the group $G = \mathrm{O}_q(\mathbb{R})$ will act transitively on $\mathrm{Gr}(V)$. If we fix $v_0 \in \mathrm{Gr}(V)$ then its stabilizer K_{v_0} will be a maximal compact subgroup. Indeed, since this group must preserve both the plane and its orthogonal complement we have $K_{v_0} \simeq \mathrm{O}_2 \times \mathrm{O}_n$. Thus $\mathrm{Gr}(V) = G/K_{v_0}$ realizes a symmetric space.

Remark. Though this is a simple and useful realization of the space, it is not clear from this construction what the complex structure should be.

The Projective Model

We consider the complexification $V(\mathbb{C})$ of the space V and the projectivization $P(V(\mathbb{C}))$. We then consider the zero quadric:

$$N := \{[\vec{v}] \in P(V(\mathbb{C})) \mid b(\vec{v}, \vec{v}) = 0\}.$$

It is a closed algebraic subvariety of projective space. We now define:

$$\kappa := \{[\vec{v}] \in P(V(\mathbb{C})) \mid b(\vec{v}, \vec{v}) = 0, b(\vec{v}, \overline{\vec{v}}) > 0\}.$$

This is a complex manifold of dimension n consisting of 2 connected components.

Remark. One must check that these spaces are in fact well defined, that is, that the conditions do not depend on a representative $\vec{v}$. Indeed $b(c\vec{v}, c\vec{v}) = c^2 b(\vec{v}, \vec{v})$ and $b(c\vec{v}, \overline{c\vec{v}}) = c\bar{c} b(\vec{v}, \overline{\vec{v}})$.

Remark. The orthogonal group $\mathrm{O}_q(\mathbb{R})$ acts transitively on κ. In order to see this we reformulate the condition that $\vec{v} = X + iY \in V(\mathbb{C})$ satisfies $[\vec{v}] \in \kappa$ as follows. We observe that:

$$b(X + iY, X + iY) = b(X, X) - b(Y, Y) + 2ib(X, Y) \text{ and}$$
$$b(X + iY, X - iY) = b(X, X) + b(Y, Y).$$

It follows from the conditions $b(X+iY, X+iY) = 0$ and $b(X+iY, X-iY) > 0$ that:

$$[\vec{v}] \in \kappa \Leftrightarrow b(X, X) = b(Y, Y) > 0 \text{ and } b(X, Y) = 0.$$

We thus have that $\mathrm{O}_q(\mathbb{R})$ acts on κ. To show that it acts transitively we appeal to Witt's extension theorem to find $g \in \mathrm{O}_q(\mathbb{R})$ taking $X \mapsto X'$ and $Y \mapsto Y'$. This isometry g then maps $[\vec{v}] \mapsto [\vec{v}']$.

Consider the subgroup $O_q^+(\mathbb{R})$ of elements whose spinor norm equals the determinant. This consists of those elements which preserve the orientation of any, and hence all, positive-definite planes. The group $O_q^+(\mathbb{R})$ preserves the 2 components of κ whereas $O_q \setminus O_q^+(\mathbb{R})$ interchanges them. Pick either component of κ and denote it κ^+.

Proposition 2.2.4. *The assignment* $[\vec{v}] \mapsto v(\vec{v}) := \mathbb{R}X + \mathbb{R}Y$ *gives a real analytic isomorphism* $\kappa^+ \to \mathrm{Gr}(V)$.

This is a straightforward check (see [Fio09, Lem. 2.3.38]).

The Tube Domain Model

Pick e_1 an isotropic vector in $V(\mathbb{R})$ and pick e_2 such that $b(e_1, e_2) = 1$. Define $\mathcal{U} := V \cap e_2^\perp \cap e_1^\perp$. We then may express elements of $V(\mathbb{C})$ as $(a, b, \vec{y})$, where $a, b \in \mathbb{C}$ and $\vec{y} \in \mathcal{U}$. Thus

$$V = \mathbb{Q}e_1 \oplus \mathbb{Q}e_2 \oplus \mathcal{U}$$

and $\mathcal{U}$ is a quadratic space of type $(1, n-1)$.

Definition 2.2.5. We define the tube domain

$$\mathbb{H}_q := \{\vec{y} \in \mathcal{U}(\mathbb{C}) \mid q(\Im(\vec{y})) > 0\},$$

where $\Im(\vec{y})$ is the imaginary part of the complex vector $\vec{y}$. We also define the open cone:

$$\Omega = \{\vec{y} \in \mathcal{U}(\mathbb{R}) \mid q(\vec{y}) > 0\},$$

as well as, the map Φ from $\mathcal{U}(\mathbb{C}) \to \mathcal{U}(\mathbb{R})$ given by $\Phi(\vec{y}) = \Im(\vec{y})$ so that $\mathbb{H}_q = \Phi^{-1}(\Omega)$.

Proposition 2.2.6. *The map* $\psi : \mathbb{H}_q \to \kappa$ *given by* $\psi(\vec{y}) \mapsto [-\frac{1}{2}(q(\vec{y}) + q(e_2)), 1, \vec{y})]$ *is biholomorphic.*

This is a straight forward check (see [Fio09, Lem. 2.3.40]).

Remark. The space $\mathbb{H}_q$ has 2 components. To see this suppose q has the form $q(x_1, ..., x_n) = a_1x_1^2 - a_2x_2^2 - ... - a_nx_n^2$ with $a_i > 0$. The condition imposed by $q(\Im(Z)) > 0$ gives us two components corresponding to $z_1 > 0$ and $z_1 < 0$. Under the map ψ one of these corresponds to κ^+. We shall label that component $\mathbb{H}_q^+$.

Via the isomorphism with κ, we see that we have a transitive action of $\mathrm{O}_q^+(\mathbb{R})$ on $\mathbb{H}_q$. One advantage to viewing the symmetric space under this interpretation is that it corresponds far more directly to some of the more classically constructed symmetric spaces such as the upper half plane.

Conjugacy Classes of Morphisms $\mathbb{S} \to \mathrm{O}_{2,n}$

We now give the interpretation of the space as a Shimura variety (see Section 2.6).

We may (loosely) think of Shimura varieties as elements of a certain conjugacy classes of morphisms:

$$h : (\mathbb{S} = \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)) \to \mathrm{GO}_{2,n}$$

satisfying additional axioms. In particular, we are interested in those morphisms where the centralizer:

$$Z_{\mathrm{GO}}(h(\mathbb{S})) = Z(\mathrm{GO}_{2,n}) \cdot K \simeq \mathbb{G}_m \cdot (\mathrm{O}_2 \times \mathrm{O}_n).$$

We get a bijection between such maps and our space as follows:

Given an element $\langle \vec{x}, \vec{y} \rangle \in \mathrm{Gr}(V)$ we consider the morphism $h(re^{i\theta})$ defined by specifying that it acts as $\begin{pmatrix} r^2\cos(2\theta) & r^2\sin(2\theta) \\ -r^2\sin(2\theta) & r^2\cos(2\theta) \end{pmatrix}$ on the span$(\vec{x}, \vec{y})$ and trivially on its orthogonal complement.

Conversely, given h in the conjugacy class of such a morphism we may take $[\vec{v}] \in \kappa^+$ to be the eigenspace of $r^2(\cos(2\theta) + i\sin(2\theta))$.

The following claim is a straightforward check.

Claim. *These two maps are inverses.*

Note that the two components correspond to swapping the (non-trivial) eigenspaces of h.

Realization as a Bounded Domain

For this section we will assume that:

$$\tilde{A} = \begin{pmatrix} 0 & 0 & 1 & 0 & \\ 0 & 0 & 0 & 1 & \\ 1 & 0 & 0 & 0 & \\ 0 & 1 & 0 & 0 & \\ & & & & A \end{pmatrix}$$

is the matrix for our quadratic form. This is not in general possible over $\mathbb{Q}$ if $n \leq 4$. For the purpose of most of this discussion we work over $\mathbb{R}$ and this fact is not a problem. However, it must be accounted for if ever rational structures are to be used. In order to compute the bounded domain, we must work with the Lie algebra, and this is slightly easier if we change the basis using the matrix:

$$\begin{pmatrix} 1 & 0 & 1 & 0 & \\ 0 & 1 & 0 & 1 & \\ 1 & 0 & -1 & 0 & \\ 0 & 1 & 0 & -1 & \\ & & & & 1_{n-2} \end{pmatrix}$$

so that the matrix for the quadratic form is:

$$\hat{A} = \begin{pmatrix} 2 & 0 & 0 & 0 & \\ 0 & 2 & 0 & 0 & \\ 0 & 0 & -2 & 0 & \\ 0 & 0 & 0 & -2 & \\ & & & & A \end{pmatrix} = \begin{pmatrix} 2 & 0 & \\ 0 & 2 & \\ & & A' \end{pmatrix}.$$

We compute that the Lie algebra $\mathfrak{so}_{\hat{A}}$ is $\begin{pmatrix} W & Z' \\ Z & Y \end{pmatrix}$, where $W \in \mathrm{M}_{2,2}$ is skew-symmetric, $Y \in \mathrm{M}_{n,n}$ is in $\mathfrak{so}_{A'}$, $Z \in \mathrm{M}_{2,n}$, and $Z' = -Z^t A'/2$. We conclude that the eigenspaces for the action of the centre of $\mathfrak{k}$ on $\mathfrak{p}_{\mathbb{C}}$ are $\mathfrak{p}_\pm$ are $\begin{pmatrix} 0 & Z' \\ Z & 0 \end{pmatrix}$,

where $Z = \begin{pmatrix} \vec{z}^t & \mp i\vec{z}^t \end{pmatrix}$ and $Z' = -Z^t A'/2$.

In order to compute the exponential of the Lie algebra we observe that the square of this matrix is equal to

$$-\frac{1}{2}\begin{pmatrix} Z^t A' Z & 0 \\ 0 & 0 \end{pmatrix} = -\frac{\vec{z}^t A' \vec{z}}{2}\begin{pmatrix} 1 & \mp i & \\ \mp i & -1 & \\ & & 0 \end{pmatrix},$$

and that its cube is the zero matrix. We thus have that $P_\pm$ is

$$\begin{pmatrix} 1_2 - \frac{1}{4}Z^t A' Z & -\frac{1}{2}Z^t A' \\ Z & 1_n \end{pmatrix},$$

where $Z = \begin{pmatrix} \vec{z}^t & \mp i\vec{z}^t \end{pmatrix}$.

After undoing the change of basis $P_\pm$ becomes:

$$1_{n+2} + \frac{1}{2}\begin{pmatrix} 0 & -iz_1-z_2 & 2z_1 & -iz_1+z_2 & -\vec{z_3}A' \\ iz_1+z_2 & 0 & -iz_1-x_2 & 2-iz_2 & i\vec{z_3}A' \\ -2z_1 & iz_1-z_2 & 0 & -iz_1+z_2 & -\vec{z_3}A' \\ iz_1-z_2 & 2iz_2 & -iz_1-z_2 & 0 & i\vec{z_3}A' \\ \vec{z_3}^t & -i\vec{z_3}^t & \vec{z_3}^t & -i\vec{z_3}^t & 0 \end{pmatrix} - \frac{\vec{z}^t A' \vec{z}}{8}\begin{pmatrix} 1 & -i & 1 & -i & \\ -i & -1 & -i & -1 & \\ 1 & -i & 1 & -i & \\ -i & -1 & -i & -1 & \\ & & & & 0 \end{pmatrix},$$

where $\vec{z_3} = (z_3, z_4, \ldots, z_{n-2})$. The action of this matrix on κ^+ takes $[1 : i : 1 : i : \vec{0}]$ to:

$$\Psi(\vec{z}) = [(1, i, 1, i, \vec{0}) + 2(z_1, z_2, -z_1, -z_2, \vec{z_3}) - \tfrac{1}{2}\vec{z}^t A' \vec{z}(1, -i, 1, -i, \vec{0})] \in N.$$

One may check that this is an injective map. We thus conclude that $\mathcal{D}$ is the bounded domain:

$$\{(z_1, z_2, \vec{z_3}) \subset P_+ |\text{ conditions }\}.$$

The conditions are computed by pulling them back from $P(V(\mathbb{C}))$. The resulting conditions can be expressed as:

$$4 + 4\vec{z}A'\overline{\vec{z}^t} + \left|\vec{z}A'\vec{z}^t\right|^2 > 0 \text{ and}$$
$$4 - \left|\vec{z}A'\vec{z}^t\right|^2 > 0.$$

We have the following maps between these models:

$$\Psi : \text{Bounded} \to \text{Projective}$$
$$\Psi^{-1} : \text{Projective} \to \text{Bounded}$$
$$\Upsilon : \text{Bounded} \to \text{Tube Domain}$$
$$\Upsilon^{-1} : \text{Tube Domain} \to \text{Bounded}$$

The definition of the map Ψ is implicit in the above computations.

Set $s(\vec{z}) = 1 - 2z_1 - \frac{1}{2}\vec{z}A'\vec{z}^t$ then Υ is defined by:

$$y_1 = \frac{i + 2z_2 + i\vec{z}A'\vec{z}^t}{s(\vec{z})},$$
$$y_2 = \frac{i - 2z_2 + i\vec{z}A'\vec{z}^t}{s(\vec{z})} \text{ and}$$
$$y_i = \frac{2z_i}{s(\vec{z})} \text{ for } i > 2.$$

To define an inverse to Υ set:

$$\vec{y}' = (\tfrac{1}{4}(iy_1 + iy_2 + \vec{y}A''\vec{y}^t), \tfrac{1}{4}(y_1 - y_2), -\tfrac{1}{4}(iy_1 + iy_2 + \vec{y}A''\vec{y}^t), -\tfrac{1}{4}(y_1 - y_2), \vec{y}_3).$$

Now set:

$$r(\vec{y}) = \frac{\vec{y}A''\vec{y}^t}{(\vec{y}')A''(\vec{y}')^t}.$$

Notice that $r(\Upsilon(\vec{z})) = 1 - 2z_1 - \frac{1}{2}\vec{z}A'\vec{z}^t$. We can therefore define Υ^{-1} via:

$$z_1 = \tfrac{1}{4}r(\vec{y})(\vec{y}A'\vec{y}^t + i(y_1 + y_2)) + 1,$$
$$z_2 = \tfrac{1}{4}r(\vec{y})(y_1 - y_2) \text{ and}$$
$$z_i = r(\vec{y})y_i \text{ for } i > 2.$$

2.2.2 Boundary Components and the Minimal Compactification

Locally symmetric spaces are often non-compact. It is thus often useful while studying them to construct compactifications. We present here some of the most basic notions of this very rich theory. For more details see [Hel01, BJ06, AMRT10, Nam80].

Definition 2.2.7. Consider a Hermitian symmetric domain $\mathcal{D}$ realized as a bounded domain in P_+. We say $x, y \in \overline{\mathcal{D}}$ are in the same **boundary component** if there exist maps:

$$\varphi_j : \mathbb{H} \to \overline{\mathcal{D}} \quad j = 1, \ldots, m$$

with $\varphi_j(\mathbb{H}) \cap \varphi_{j+1}(\mathbb{H}) \neq \emptyset$, and there exist $x', y' \in \mathbb{H}$ such that $\varphi_1(x') = x$ and $\varphi_m(y') = y$.

We say that two boundary components F_1, F_2 are adjacent if $\overline{F_1} \cap \overline{F_2} \neq 0$.

Theorem 2.2.8. *The boundary components of the Hermitian symmetric domain $\mathcal{D}$ are the maximal sub-Hermitian symmetric domains in $\overline{\mathcal{D}}$. Moreover, they satisfy the following:*

- *The group G acts on boundary components preserving adjacency.*
- *The closure $\overline{\mathcal{D}}$ can be decomposed as $\overline{\mathcal{D}} = \sqcup_\alpha F_\alpha$, where the F_α are boundary components.*
- *For each boundary component F_α there exists a map:*

$$\varphi_\alpha : \mathrm{SL}_2(\mathbb{R}) \to G$$

inducing a map

$$f_\alpha : \overline{\mathbb{H}} \to \overline{\mathcal{D}}$$

such that $f_\alpha(i) = o$ (for the fixed base point $o = K$) and $f_\alpha(i\infty) \in F_\alpha$.

See [AMRT10, Thm. 1,2 Sec 3.3].

Theorem 2.2.9. *There is a bijective correspondence between the collection $\{F_\alpha\}$ of boundary components and the collection of real "maximal" parabolic* *subgroups P_α of $G = \mathrm{Aut}(\mathcal{D})$. (By "maximal" we mean that for each simple factor G_i of G the restriction to the factor is either maximal or equal to G_i).*

Explicitly we have $P_\alpha = \{g \in G \mid gF_\alpha = F_\alpha\}$. Moreover, $F_\alpha \subset \overline{F}_\beta$ if and only if $P_\alpha \cap P_\beta$ is a parabolic subgroup.

See [AMRT10, Prop. 1,2 Sec 3.3].

Definition 2.2.10. We say F_α is a **rational** boundary component if P_α is defined over $\mathbb{Q}$. We define the space:

$$\mathcal{D}^* = \bigcup_{rational} F_\alpha.$$

Theorem 2.2.11. *Let $\Gamma \subset G(\mathbb{Q})$ be an arithmetic subgroup. There exists a topology on $\mathcal{D}^*$ such that the quotient $\overline{X}^{Sat} := \Gamma\backslash\mathcal{D}^*$ has the structure of a normal analytic space.*

We call $\overline{X}^{Sat}$ the minimal Sataké compactification of $\Gamma\backslash\mathcal{D}$.

See [BJ06, Sec. III.3].

Remark. The topology one should assign may become more apparent once we introduce other compactifications.

2.3 Modular Forms

We give now a simplified notion of modular forms. More general and precise definitions can be found in any of [Bor66, Mum77, BB66].

Definition 2.3.1. Let $\mathcal{Q}$ be the image of $\mathcal{D} = G/K$ in the projective space $\check{\mathcal{D}} = G_{\mathbb{C}}/P^-$ and let $\tilde{\mathcal{Q}}$ be the cone over $\mathcal{Q}$. A **modular form** f for Γ of weight k on $\mathcal{D}$ can be thought of as any of the equivalent notions:

1. A function on $\tilde{\mathcal{Q}}$ homogeneous of degree $-k$ which is invariant under the action of Γ.
2. A section of $\Gamma\backslash(\mathcal{O}_{\check{\mathcal{D}}}(-k)|_{\mathcal{D}})$ on $\Gamma\backslash\mathcal{D}$.
3. A function on $\mathcal{Q}$ which transforms with respect to the k^{th} power of the factor of automorphy under Γ.

To be a **meromorphic** (resp. **holomorphic**) modular form we require that f extends to the boundary and that it be meromorphic (resp. holomorphic). One may also consider forms which are holomorphic on the space but are only meromorphic on the boundary.

Remark. The condition at the boundary depends on understanding the topology, a concept we have not yet defined. There is an alternative definition in terms of Fourier series. Let $\mathcal{U}_\alpha$ be the centre of the unipotent radical of P_α and set $U_\alpha = \Gamma \cap \mathcal{U}_\alpha$. This group is isomorphic to $\mathbb{Z}^m$ for some m and the function f is invariant under its action. The boundary condition can be expressed by saying the non-trivial Fourier coefficients (which are indexed by elements of U_α^*), are contained in a certain self-adjoint cone $\Omega_\alpha \subset \mathcal{U}_\alpha^*$.

The following is what is known as the Koecher principle (see for example [Fre90]).

Claim. *If the codimension of all of the boundary components is at least* 2*, then every form which is holomorphic on* $\mathcal{D}$ *extends to the boundary as a holomorphic modular form.*

This result is a consequence of results about extending functions on normal varieties.

Theorem 2.3.2 (Baily-Borel)**.** *Let* $M(\Gamma, \mathcal{D})$ *be the graded ring of modular forms then*

$$\overline{X}^{BB} := \mathrm{Proj}(M(\Gamma, \mathcal{D}))$$

is the Baily-Borel compactification of X*. Moreover, this is isomorphic to the minimal Sataké compactification as an analytic space*

See [BB66] and [BJ06, III.4].

2.3.1 The O(2,n) Case

Specializing the previous section to the orthogonal case we can use the following definition for modular forms.

Definition 2.3.3. Let $\overline{\kappa}^+ = \{\vec{v} \in V(\mathbb{C}) \mid [\vec{v}] \in \kappa^+\}$ be the cone over κ^+. Let $k \in \mathbb{Z}$, and χ be a character of Γ. A meromorphic function on $\overline{\kappa}^+$ is a **modular form** of weight k and character χ for the group Γ if it satisfies the following:

1. F is homogeneous of degree $-k$, that is, $F(c\vec{v}) = c^{-k}F(\vec{v})$ for $c \in \mathbb{C}-\{0\}$.
2. F is invariant under Γ, that is, $F(g\vec{v}) = \chi(g)F(\vec{v})$ for any $g \in \Gamma$.
3. F is meromorphic on the boundary.

If F is holomorphic on $\overline{\kappa}^+$ and on the boundary then we call F a holomorphic modular form. In this case $\mathcal{U}_\alpha$ and Ω_α are precisely those introduced for the tube domain model (see Section 2.2.1).

Remark. The Koecher principle implies condition (3) is automatic if the dimension of maximal isotropic subspace is less than n. Noting that for type $(2, n)$ the Witt rank is always at most 2, we see that the Koecher principle often applies.

Remark. One of the best sources of examples of modular forms for these orthogonal spaces is the Borcherds lift (see [Bor95, Bru04, Bru02] for more details). The Borcherds lift, which may be defined via a regularized theta integral, takes nearly holomorphic vector-valued modular forms for the upper half plane and constructs modular forms on an orthogonal space. The forms constructed this way have well understood weights, levels, and divisors. One can also consider other types of forms (for example Eisenstein series, Poincare series and theta series).

2.4 Dimension Formulas for Spaces of Modular Forms

One very natural question which remains unanswered about modular forms on orthogonal symmetric spaces is that of giving explicit formulas for the dimensions of spaces of modular forms on these spaces. These types of formulas have a wide variety of applications, both computational and theoretical. This problem has been extensively studied in lower dimensional cases where exceptional isomorphisms exist between the orthogonal Shimura varieties and other classical varieties. In particular, the (2,1)-case corresponds to the classical modular and Shimura curves and the (2,2)-case corresponds to Hilbert modular surfaces. Many results are known for these cases (see for example [DS05, Ch. 3] and [Fre90, Ch. 2]). Additionally, the split (2,3)-case corresponds to a Siegel space where the work of Tsushima (see [Tsu80]) gives us dimension formulas. The only work in the general case is that of [GHS08]. They are able to compute asymptotics for the dimensions as one changes the weight for several higher dimension cases. The standard approach to this type of problem and the one we intend to discuss is that which has been used successfully in the above listed cases.

The first tool we shall discuss is the Riemann-Roch formula.

2.4.1 Hirzebruch-Riemann-Roch Theorem

Before discussing the theorem we shall quickly survey the objects involved in the statement of this theorem. Most of what we say can be found in [Har77, Appendix A]. More thorough treatments exist, both from a more topological approach [Hir66] or algebraic approach [BS58].

What the Hirzebruch-Riemann-Roch theorem fundamentally is about is a formula for the Euler characteristic in terms of the values of intersection pairings between certain cycles and cocycles. We will say very little about what this means. Two good references for this material are [Ful98, Ful84].

The Euler Characteristic

Theorem 2.4.1 (Serre). *Let X be a projective scheme over a Noetherian ring A and let $\mathcal{O}_X(1)$ be a very ample invertible sheaf on X over* $\mathrm{Spec}(A)$. *Let $\mathcal{E}$ be a coherent sheaf on X. Then the following properties hold:*

1. *For each $i \geq 0$ the ith cohomology $H^i(X, \mathcal{E})$ is a finitely generated A-module.*
2. *There exists an n_0 such that $H^i(X, \mathcal{E}(n)) = 0$ for all $i > 0$ and $n \geq n_0$.*

See [Har77, III.5.2].

Definition 2.4.2. Let X be a projective scheme over k and let $\mathcal{E}$ be a coherent sheaf on X we define the **Euler characteristic** of $\mathcal{E}$ to be:

$$\chi(\mathcal{E}) = \sum_i (-1)^i \dim_k H^i(X, \mathcal{E}).$$

Proposition 2.4.3. *Let X be a projective scheme over k, let $\mathcal{O}_X(1)$ be a very ample invertible sheaf on X over k, and let $\mathcal{E}$ be a coherent sheaf on X. There exists $P(z) \in \mathbb{Q}[z]$ such that $\chi(\mathcal{E}(n)) = P(n)$ for all n. We call P the **Hilbert polynomial** of $\mathcal{E}$ relative to $\mathcal{O}_X(1)$.*

See [Har77, Thm. I.7.5 and Ex. 2.7.6].

Theorem 2.4.4 (Hirzebruch-Riemann-Roch)**.** *For a locally free sheaf $\mathcal{E}$ of rank r on a non-singular projective variety X of dimension n we have the following formula for the Euler characteristic:*

$$\chi(\mathcal{E}) = \deg(\mathrm{ch}(\mathcal{E}).\,\mathrm{td}(\mathcal{T}_X))_n.$$

The statement is from [Har77, A.4.1]. For the proof see [BS58].

Corollary 2.4.5. *Consider a locally free sheaf $\mathcal{E}$ of rank r on a smooth projective variety X of dimension n. There exists a 'universal polynomial' Q such that:*

$$\begin{aligned}\chi(\mathcal{E}) &= Q(c_1(\mathcal{E}), \dots, c_r(\mathcal{E}); c_1(\Omega_X^1), \dots, c_n(\Omega_X^1)) \\ &= \sum_{i=0}^{n} \sum_{|\alpha|=i} \sum_{|\beta|=n-i} a_{\alpha,\beta} c^\beta(\mathcal{E}) \cdot c^\alpha(\Omega_X^1),\end{aligned}$$

where α, β are partitions of $i, n-i$, and the $a_{\alpha,\beta}$ are integers which depend only on α, β, n.

Proof. This follows from the observation that the Tod and Chern characters are universal polynomials in the Chern classes. □

2.4.2 Kodaira Vanishing

In order to effectively apply this theorem to computing dimensions of H^0s, one needs to know that, for the line bundle in question, the higher cohomology vanishes. To this end we have the following results.

Theorem 2.4.6 (Kodaira)**.** *If X is a non-singular projective variety of dimension n and L is an ample line bundle on X then:*

$$H^i(X, L^{\otimes(-m)}) = 0 \text{ for all } m > 0, i < n.$$

The statement is [Har77, Rem. III.7.15]. For the proof see [Kod53].

Corollary 2.4.7. *If X is a non-singular projective variety of dimension n and L is an ample line bundle on X then:*

$$H^i(X, L^{\otimes(m)} \otimes \Omega^1_X) = 0 \text{ for all } m > 0, i > 0.$$

This follows immediately from the previous result by Serre duality (see [Har77, III.7 and III.7.15]).

2.4.3 Hirzebruch-Proportionality

In order to effectively apply the Riemann-Roch theorem to the situation of locally symmetric spaces there are a number of key issues that must be overcome. The first is that one must be working with a line bundle on a projective variety. It is not immediately apparent that modular forms should be sections of such a bundle and this should not be assumed lightly. The second is how to actually compute the various intersection pairings that make up the Riemann-Roch formula. Both of these problems have at least partial solutions coming out of the theory of toroidal compactifications (see [AMRT10, Mum77]).

Notation 2.4.8. Throughout this section we will be using the following notation. Let $\mathcal{D} = G/K$ be a Hermitian symmetric domain of the non-compact type and let $\breve{\mathcal{D}} = G^c/K$ be its compact dual. Each of these has the induced volume form coming from the identification of tangent spaces at a base point with part of the Lie algebra $\mathfrak{p}_{\mathbb{C}} \subset \mathfrak{g}_{\mathbb{C}}$.

Let $\Gamma \subset \mathrm{Aut}(\mathcal{D})$ be a neat arithmetic subgroup with finite covolume and let $X = \Gamma \backslash \mathcal{D}$ be the corresponding locally symmetric space. We will denote by $\overline{X}$ a choice of smooth toroidal compactification and by $\overline{X}^{BB}$ the Baily-Borel compactification.

Definition 2.4.9. We then define the **Hirzebruch-Mumford volume** to be:

$$\mathrm{Vol}_{HM}(X) = \frac{\mathrm{Vol}(X)}{\mathrm{Vol}(\check{\mathcal{D}})}.$$

Proposition 2.4.10. *Given a G-equivariant analytic vector bundle E_0 on $\mathcal{D}$ there exists:*

- *an analytic vector bundle $\check{E}$ on $\check{D}$ which agrees with E_0 on $\mathcal{D}$,*
- *an analytic vector bundle E on X with an induced Hermitian metric, and*
- *a unique extension $\overline{E}$ to $\overline{X}$ such that the induced metric is a good singular metric on $\overline{X}$.*

See [Mum77, Thm 3.1].

Theorem 2.4.11. *Using the notation of the previous proposition. For each partition α of $n = \dim(X)$ the associated Chern numbers $c^{\alpha}(\overline{E})$ and $c^{\alpha}(\check{E})$ satisfy the following relation:*

$$c^{\alpha}(\check{E}) = (-1)^{\dim(X)} \mathrm{Vol}_{HM}(X) c^{\alpha}(\overline{E}).$$

See [Mum77, Thm 3.2].

Geometric Modular Forms

We now give a definition of the spaces in which we are interested.

Definition 2.4.12. Given a representation $\rho : K \to \mathrm{GL}_n$ we define a bundle E_ρ on $\mathcal{D}$ via

$$E_\rho = K \backslash (G \times_\rho \mathbb{C}^n).$$

We define a ρ**-form** on X to be a Γ-equivariant section of E_ρ such that the induced map $\tilde{f} : G \to \mathbb{C}^n$ satisfies:

$$\left|\tilde{f}(g)\right| \leq C \, ||g||_G^n$$

for some $n > 1, C > 0$. The norm $||g||$ is defined as in [Bor66, Sec. 7] as $\mathrm{Tr}(\mathrm{Ad}(s(g))^{-1} \cdot \mathrm{Ad}(g))$, where s is a Cartan involution.

We say a ρ-form is **holomorphic** if it is a holomorphic section of:

$$\breve{E}_\rho = K_{\mathbb{C}} P_+ \backslash (G_{\mathbb{C}} \times_\rho \mathbb{C}^n)$$

on the inclusion of $E \hookrightarrow \breve{E}$.

Proposition 2.4.13. *The vector space of holomorphic ρ-forms is precisely:*

$$H^0(\overline{X}, \overline{E_\rho}),$$

where $\overline{X}$ is a smooth toroidal compactification of X and $\overline{E}_\rho$ the unique extension of E_ρ to $\overline{X}$.

See [Mum77, Prop 3.3].

Proposition 2.4.14. *Consider the case $\breve{E} = \Omega^1_{\breve{\mathcal{D}}}$ so that $E = \Omega^1_{\mathcal{D}}$. In this case*

$$\overline{E} = \Omega^1_{\overline{X}}(\log)$$

is the bundle whose sections near a boundary of k intersecting hyperplanes are of the form:

$$\sum_{i=1}^{k} a_i(z) \tfrac{dz_i}{z_i} + \sum_{i=k+1}^{n} a_i(z) dz_i.$$

See [Mum77, Prop 3.4.a].

Proposition 2.4.15. *Consider the case $\breve{E} = \Omega^n_{\breve{\mathcal{D}}}$ so that $E = \Omega^n_{\mathcal{D}}$ is the canonical bundle of $\mathcal{D}$. In this case*

$$\overline{E} = f^*(\mathcal{O}_{\overline{X}^{BB}}(1))$$

is the pullback of an ample line bundle on the Baily-Borel compactification. The sections of $\mathcal{O}_{\overline{X}^{BB}}(n)$ *are the modular forms of weight* n*.*

See [Mum77, Prop 3.4.b].

Corollary 2.4.16. *Suppose* $n' = \dim(\overline{X}^{BB} - X)$*, then for all* $k > n'$ *the cycle* $[\Omega^1_{\overline{X}}(\log)]^k$ *is supported on* X*.*

Proof. This is true for the ample line bundle on $\overline{X}^{BB}$ for which $\Omega^1_{\overline{X}}(\log)^k$ is the pull back. Hence the statement is true for $\Omega^1_{\overline{X}}(\log)^k$. □

Corollary 2.4.17. *For* $X = \Gamma\backslash\mathcal{D}$ *a locally symmetric space, the modular forms are:*

$$M_k(\Gamma) = H^0(\overline{X}, \Omega^n_{\overline{X}}(\log)^k)$$

is the space of modular forms of weight k *level* Γ *for* G*. Furthermore the cusp forms are:*

$$S_k(\Gamma) = H^0(\overline{X}, \Omega^n_{\overline{X}}(\log)^{k-1} \otimes \Omega^n_{\overline{X}}).$$

Computing Dimensions

We now describe how to compute dimensions for spaces of modular forms.

Proposition 2.4.18. *Suppose* D *is a cycle on* $\overline{X}$ *supported entirely on* X*, then*

$$D \cdot c^\alpha(\Omega_{\overline{X}}(\log)) = D \cdot c^\alpha(\Omega_{\overline{X}}).$$

This follows from the properties of the Chern classes.

Lemma 2.4.19. *Suppose* Q *is the universal polynomial of Corollary 2.4.5 then:*

$$\begin{aligned} E_{\overline{X}}(\ell) := \ & Q(\ell c_1(\Omega^1_{\overline{X}}(\log)); c_1(\Omega^1_{\overline{X}}(\log)), \ldots, c_n(\Omega^1_{\overline{X}}(\log))) \\ & \qquad - Q(\ell c_1(\Omega^1_{\overline{X}}); c_1(\Omega^1_{\overline{X}}(\log)), \ldots, c_n(\Omega^1_{\overline{X}})) \\ = & \sum_{i=0}^{n'} \ell^i [c_1(\Omega^1_{\overline{X}}(\log))^i] \sum_{|\alpha|=n-i} b_\alpha (c^\alpha(\Omega^1_{\overline{X}}) - c^\alpha(\Omega^1_{\overline{X}}(\log))) \end{aligned}$$

for constants b_α *which depend only on* α *and not on* X*.*

Proof. This is a direct application of Corollary 2.4.16 and Proposition 2.4.18. □

Theorem 2.4.20. *Consider* $(\Omega^n_{\check{\mathcal{D}}})^{-1}$ *the ample line bundle on* $\check{\mathcal{D}}$ *and let*

$$P_{\check{\mathcal{D}}}(\ell) = \sum_i \dim(H^i(\check{\mathcal{D}}, (\Omega^n_{\check{\mathcal{D}}})^{-1}))$$

be the associated Hilbert polynomial. Suppose Γ *is a neat arithmetic subgroup and* $\overline{X}$ *is a smooth toroidal compactification of* $X = \Gamma\backslash\mathcal{D}$ *with* $n' = \dim(\overline{X}^{BB} - X)$*. Then for* $\ell \geq 2$ *we have:*

$$\dim(S_\ell(\Gamma)) = \mathrm{Vol}_{HM}(X) P_{\check{\mathcal{D}}}(\ell - 1) - E_{\overline{X}}(\ell).$$

See [Mum77, Prop 3.5].

Remark. A remark is in order on the issue of the *weight* of a modular form. The *weight* ℓ in the above theorem is what is known as the geometric weight. This differs from the arithmetic weight by a factor of $\dim(X)$.

Notation 2.4.21. Denote the boundary of X by $\Delta = \overline{X} - X$ and write $[\Delta] = \sum [D_i]$ as a decomposition into its irreducible components $[D_i]$. Denote by Δ_k the kth elementary symmetric polynomial in the $[D_i]$. Moreover, for α a partition denote by $\Delta^\alpha = \prod_\ell \Delta_{\alpha_\ell}$.

Proposition 2.4.22. *Let* $\overline{X}$ *be an* n *dimensional complex manifold and suppose* $\Delta = \overline{X} \setminus X$ *is a reduced normal crossings divisor. Denoting by* $\Omega^1_{\overline{X}}(\log)$ *the subsheaf of* $\Omega_{\overline{X}}$ *with* log-*growth near* Δ*. Then:*

$$c_j(\Omega^1_{\overline{X}}) = \sum_{i=0}^{j} c_i(\Omega^1_{\overline{X}}(\log))\Delta_{j-i}.$$

Proof. This is proven is slightly more generality in [Tsu80, Prop 1.2] for the tangent bundle. It follows from considering the following two exact sequences:

$$0 \longrightarrow \Omega^1_{\overline{X}}(\log) \longrightarrow \Omega^1_{\overline{X}} \longrightarrow \oplus \mathcal{O}_{D_i}(D_i) \longrightarrow 0,$$

$$0 \longrightarrow \mathcal{O}_{\overline{X}} \longrightarrow \mathcal{O}_{\overline{X}}(D_i) \longrightarrow \mathcal{O}_{D_i}(D_i) \longrightarrow 0.$$

□

Corollary 2.4.23. *For a partition α of j we find:*

$$\begin{aligned} c^\alpha(\Omega^1_{\overline{X}}) &= \prod_\ell \left(\sum_{i=0}^{\alpha_\ell} c_i(\Omega^1_{\overline{X}}(\log)) \Delta_{\alpha_\ell - i} \right) \\ &= \sum_{\beta,\gamma} d_{\alpha,\beta,\gamma} c^\beta(\Omega^1_{\overline{X}}(\log)) \Delta^\gamma, \end{aligned}$$

where the $d_{\alpha,\beta,\gamma}$ depend only on α, β, γ and not on X.

Corollary 2.4.24. *We have that:*

$$E_{\overline{X}}(\ell) = \sum_{i=0}^{n'} \ell^i [c_1(\Omega^1_{\overline{X}}(\log))^i] \sum_{|\alpha|=n-i} b_\alpha \left(\sum_{\substack{|\beta|<|\alpha| \\ |\gamma|=|\alpha|-|\beta|}} d_{\alpha,\beta,\gamma} c^\beta(\Omega^1_{\overline{X}}(\log)) \Delta^\gamma \right),$$

where the coefficients b_α and $d_{\alpha,\beta,\gamma}$ depend only on α, β, γ and n and not otherwise on X.

Remark. We have the following remarks about the above:

- All of the intersections in the above formula take place in the boundary, since $|\gamma| > 0$ for every term appearing in the formula.
- There are only finitely many connected components of boundary components and finitely many inequivalent orbits of boundary component.
- Boundary components are of the form:

$$\overline{\Gamma_F \backslash F} \ltimes (\mathbb{Z}^{2m} \backslash \mathbb{C}^m) \ltimes \overline{O(\sigma)}$$

  for the various boundary components F and cones σ.

- Intersections between adjacent F's in $\overline{X}^{BB}$ is understood by the spherical Bruhat-Tits building of G over $\mathbb{Q}$.
- The intersections of two cones in F are either another cone of F or a cone of an adjacent boundary component F' contained in the closure of F.
- The Chern classes generally 'descend well' to adjacent boundary components, see [Tsu80, Lem. 5.1].

In general [Tsu80, Sections 3,4,5] provides guidelines for computing these intersection numbers.

Remark. The above results combine to reduce the issue of computing dimension formulas to the following steps:

1. Computing the Hilbert polynomial $P_{\check{\mathcal{D}}}$. These are known in all the basic cases.
2. Computing the volume $\mathrm{Vol}_{HM}(X)$. This depends on the choice of Γ, the formulas typically involve special values of L-functions.
3. Computing the terms $b_\alpha, d_{\alpha,\beta,\gamma}$. This is a formal, though unpleasant calculation and in high dimensions it is probably best left to computer algebra software.
4. Computing the intersection numbers of all the terms appearing (see the previous remark).

2.4.4 The Orthogonal Case

The following discussion follows closely that of [GHS08, Section 2].

Theorem 2.4.25. *Let $\mathcal{D}$ be the symmetric space for an orthogonal group of signature $(2, n)$, then:*

$$\chi(\mathcal{O}_{\check{\mathcal{D}}}(-n)^\ell) = \chi(\mathcal{O}_{\mathbb{P}^{n+1}}(-n\ell)) - \chi(\mathcal{O}_{\mathbb{P}^{n+1}}(-n\ell - 2)) = \binom{n+1-n\ell}{n} - \binom{n-1-n\ell}{n}.$$

Proof. We have describe $\check{\mathcal{D}}$ as a quartic in $\mathbb{P}^{n+1}$ with canonical bundle $\mathcal{O}_{\check{\mathcal{D}}}(-n)$. The adjunction formula places it into the following exact sequence:

$$0 \to \mathcal{O}_{\mathbb{P}^{n+1}}(-n\ell - 2) \to \mathcal{O}_{\mathbb{P}^{n+1}}(-n\ell) \to \mathcal{O}_{\check{\mathcal{D}}}^{\ell} \to 0.$$

This allows us to compute the Hilbert polynomial of $\mathcal{O}_{\check{\mathcal{D}}}$ from that of $\mathcal{O}_{\mathbb{P}^{n+1}}$. In particular using the fact that $\dim(H^0(\mathcal{O}_{\mathbb{P}^{n+1}}(k))) = \binom{n+1+k}{n}$ allows us to check the result. □

The non-trivial volume forms on a Hermitian symmetric domain $\mathcal{D}$ are induced by the Killing form and the identification of $\mathfrak{p}$ with $\mathcal{T}_{\mathcal{D},x}$, where x is any base point. Up to scaling this form is unique.

For the group $\mathrm{O}_{2,n}$ it is shown in [Hel01, p. 239] that the tangent spaces for $\mathcal{D}$ and $\check{\mathcal{D}}$ are respectively:

$$\begin{pmatrix} 0 & U \\ U^t & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & U \\ -U^t & 0 \end{pmatrix}$$

in the Lie algebra of G. The killing form is $\mathrm{Tr}(M_1 M_2^t)$ which induces the form $2\,\mathrm{Tr}(U_1 U_2^t)$. Fix a lattice L in the underlying quadratic space. In [Sie67] Siegel computed the volume of $\mathrm{O}(L)\backslash\mathcal{D}$ relative to $\mathrm{Tr}(U_1 U_2^t)$ as:

$$2\alpha_\infty(L,L)\,|D(L)|^{(2+n+1)/2}\left(\prod_{k=1}^{2}\pi^{-k/2}\Gamma(k/2)\right)\left(\prod_{k=1}^{n}\pi^{-k/2}\Gamma(k/2)\right),$$

where $\alpha_\infty(L,L)$ is the real Tamagawa volume of $\mathrm{O}(L)$. The computations of [Hua79] when combined with the above yield the formula:

$$\mathrm{Vol}(\check{\mathcal{D}}) = 2\left(\prod_{k=1}^{n+2}\pi^{k/2}\Gamma(k/2)^{-1}\right)\left(\prod_{k=1}^{n}\pi^{-k/2}\Gamma(k/2)\right)\left(\prod_{k=1}^{2}\pi^{-k/2}\Gamma(k/2)\right).$$

Combining these results we find:

Proposition 2.4.26. *The Hirzebruch-Mumford volume for an orthogonal symmetric space is:*

$$\mathrm{Vol}_{HM}(\mathrm{SO}(L)\backslash\mathcal{D}) = \alpha_\infty(L,L)\,|D(L)|^{(2+n+1)/2}\left(\prod_{k=1}^{n+2}\pi^{k/2}\Gamma(-k/2)\right).$$

In order to compute $\alpha_\infty(L,L)$ we use several facts.

Proposition 2.4.27. *For an indefinite lattice of rank at least* 3 *the genus equals the spinor genus.*

This follows from [Kit93, Thm 6.3.2].

Proposition 2.4.28. *The weight of a lattice depends only on its spinor genus.*

This is discussed in [GHS08, p224]. See also [Shi99, Thm 5.10].

Now using the fact that the Tamagawa volume of $\mathrm{SO}_V(\mathbb{Q})\backslash\mathrm{SO}_V(\mathbb{A}) = 2$ we may conclude:

Proposition 2.4.29. *For an indefinite lattice of rank at least* 3 *the following formula holds:*

$$\prod_p \alpha_p(L,L) = \frac{2}{|spn^+(L)|}$$

or equivalently:

$$\alpha_\infty(L,L) = \frac{2}{|spn^+(L)|}\prod_p \alpha_p(L,L)^{-1},$$

where $spn^+(L)$ is the proper spinor genus of L.

Remark. It is known (see [Kit93, Cor 6.3.1]) that $|spn^+(L)|$ is a power of 2. Moreover, by [Kit93, Cor 6.3.2] computing $|spn^+(L)|$ can be reduced to a finite computation.

The local densities $\alpha_p(L,L)$ can also be computed. These computations are explained in Chapter 4. Note that α_p differs from β_p by a factor of $q^{\mathrm{rank}(L)\nu(2)}$.

2.4.5 Non-Neat Level Subgroups

An important aspect of the above discussion was the appearance of the term 'non-singular'. In order to obtain a non-singular variety from a locally symmetric space one is forced to take blowups. This process is not (trivially) well-behaved with respect to the existence or dimension of sections. The above machinery only works directly, without the need for any modifications, when the locally symmetric space is non-singular. Consequently, an important result is that every locally symmetric space has a non-singular finite cover. This result follows from the following:

Theorem 2.4.30. *Suppose* $p \nmid \Phi_\ell(1)$ *and* $\deg(\Phi_\ell) \leq n$ *for all* ℓ, *then* $\Gamma(p) \subset \mathrm{GL}_n(\mathbb{Z})$ *is neat.*

See [Bor69, Prop. 17.4].

Two natural questions now arise:

Question 1. What does it mean to have a modular form on a singular space?

Question 2. How can one compute the dimension of this space from the corresponding dimension of the cover?

Remark. The reason the first question is important is that line bundles may not descend to a desingularization of the quotient. Notice that the desingularization of $\overline{(\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H})}$ is $\mathbb{P}^1$. If the line bundle of modular forms of weight 2 descended, it would by necessity have global sections. Moreover, even if the line bundle does descend, it is not clear that Γ-invariant sections will descend to holomorphic sections.

Notation 2.4.31. Suppose we have a normal subgroup $\Gamma' \subset \Gamma$ with Γ' neat. Denote by $S_k(\Gamma')$ the space of weight k cusp forms on $X(\Gamma')$. Define $S_k(\Gamma) = S_k(\Gamma')^\Gamma$ to be the space of Γ-invariant cusp forms. Define $\tilde{S}_k(\Gamma) \subset S_k(\Gamma)$ to be the subspace of cusp forms which extend to holomorphic forms on a desingularization $\tilde{X}(\Gamma)$ of $X(\Gamma) = \Gamma\backslash X(\Gamma')$.

Proposition 2.4.32. *With the notation as above we can compute:*

$$\dim(S_k(\Gamma)) = \sum_{\gamma\in\Gamma/\Gamma'} \mathrm{tr}(\gamma|S_k(\Gamma')).$$

The proof is a standard argument. A generalization of the Riemann-Roch theorem by Atiyah and Singer [AS68] allows this to be computed.

We first introduce the following notation:

Notation 2.4.33. Suppose $\gamma \in \Gamma$, χ is a character of Γ and $\theta \in \mathbb{C}^\times$. Denote by $X^\gamma = \{x \in X \mid x = \gamma(x)\}$ and by $N_\gamma = N_{X_\gamma}$ the normal bundle of X^γ in X. For a vector bundle $\mathcal{E}$ denote by $\mathcal{E}_\gamma(\theta)$ the θ-eigenspace of γ and by $\mathcal{E}(\chi)$ the χ-isotypic component. Suppose $c_t(\mathcal{E}) = \prod(1 - x_i t)$, then set $U^\theta(\mathcal{E}) = \prod(\frac{1-\theta}{1-\theta e^{x_i}})$ and $\mathrm{ch}(\mathcal{E})(\gamma) = \sum_\chi \chi(\gamma)\,\mathrm{ch}(\mathcal{E}(\chi))$.

Theorem 2.4.34. *Suppose k is sufficiently large so that $H^i(\overline{X}, \Omega_X^N(\log)^{k-1}) = 0$ for $i > 0$ then:*

$$\mathrm{tr}(\gamma|S_k(\Gamma)) = \left\{ \frac{\mathrm{ch}(\Omega_X^N(\log)^{k-1} \otimes \Omega_X^N|X^\gamma)(\gamma) \prod_\theta U^\theta(N_\gamma(\theta))\,\mathrm{td}(X^\gamma)}{\det(1-\gamma|N_\gamma^*)} \right\} [X^\gamma].$$

This is a polynomial in the weight k of degree at most X^γ.

See [Tai82, Sec. 2] and [AS68, Thm. 3.9].

Remark. The contribution of the identity element of Γ in this formula gives us the Riemann-Roch theorem for $S_k(\Gamma)$. To evaluate this formula one needs a complete understanding of the ramification locus of the quotient map.

On the issue of the relation of $S_k(\Gamma)$ to $\tilde{S}_k(\Gamma)$ we have the following result.

Proposition 2.4.35. *Let $\tilde{X}(\Gamma)$ be a non-singular model of $X(\Gamma)$ and let $\tilde{X}(\langle\gamma, \Gamma'\rangle)$ be the non-singular model of $X(\langle\gamma, \Gamma'\rangle)$ which covers it. A Γ'-invariant form extends to $\tilde{X}(\Gamma)$ if and only if it extends to $\tilde{X}(\langle\gamma, \Gamma'\rangle)$ for all $\gamma \in \Gamma$.*

See [Tai82, Prop. 3.1].

Definition 2.4.36. Let γ act on X with a fixed point $x \in X$. Suppose the eigenvalues for the action of γ on $\mathcal{T}_{X,x}$ are $e^{2\pi i \alpha_j}$ for $j = 1, \ldots, n$. We say the singularity at x is γ-**canonical** if $\sum_j \alpha_j - \lfloor \alpha_j \rfloor \geq 1$.

Proposition 2.4.37. *Every invariant form extends to $\tilde{X}(\langle\gamma, \Gamma\rangle)$ if and only if all the singularities are γ^k-canonical for all $\gamma^k \neq \mathrm{Id}$.*

See [Tai82, Prop. 3.2].

Remark. Forms which have sufficiently high orders of vanishing along the ramification divisor will still extend even if the singularities are not canonical.

Theorem 2.4.38. *Let L be a lattice of signature $(2, n)$ with $n \geq 9$ and let $\Gamma \subset \Gamma'$ be as above. There exists a toroidal compactification of $X(\Gamma)$ such that all the singularities are γ-canonical for all $\gamma \in \Gamma'$.*

See [GHS07, Thm 2].

Remark. The results of [GHS07] are slightly more refined. They show that for $n \geq 6$ the only source of non-canonical singularities on the interior are reflections. For $n \geq 7$ the reflections no longer give non-canonical singularities. For the boundary, they show the 0-dimensional cusps never present non-canonical singularities (by a choice of toroidal compactification). They also show that the 1-dimensional cusps may only have non-canonical singularities over the usual points $i, \omega \in \mathbb{H}$ and these points present no problems if $n \geq 9$. Moreover, from their proof one can compute lower bounds on ℓ such that $\Gamma(\ell)$ would only give canonical singularities.

The computations involved in obtaining these results use the structure of singularities that we will discuss in the following section.

2.5 Ramification for Orthogonal Shimura Varieties

The purpose of this section is to describe the nature of the ramification between different levels for the orthogonal group. The only other discussion of this topic with which we are familiar is the work of [GHS07, Sec. 2]. Some of the results here are motivated by their constructions.

Let L be a $\mathbb{Z}$-lattice of signature $(2, n)$. Recall that:

$$\mathcal{D}_L = \mathcal{K}_L = \{[\vec{z}] \in \mathbb{P}(L \otimes_{\mathbb{Z}} \mathbb{C}) \mid q(\vec{z}) = 0,\ b(\vec{z}, \overline{\vec{z}}) > 0\}.$$

Denote by O_L the orthogonal group of L. For Γ a subgroup of $\mathrm{O}_L(\mathbb{Z})$ we set:

$$X_L(\Gamma) := \Gamma \backslash \mathcal{D}_L.$$

When Γ is neat $X_L(\Gamma)$ can be given the structure of a smooth quasi-projective variety. We also wish to think about $X_L(\Gamma)$ when Γ is not neat. It will be a quotient of $X_L(\Gamma')$ for some neat subgroup $\Gamma' \subset \Gamma$ by a finite group of automorphisms. The quotient certainly exists as a stack (though we shall not discuss this further). However, one often expects that one can make sense of it as a scheme, in which case the cover $\pi_\Gamma : X_L(\Gamma') \to X_L(\Gamma)$ will be a ramified covering.

The first thing we shall do is describe the structure of some 'explicit' ramification divisors. We will next explain why this captures all of the ramification.

2.5.1 Generalized Heegner Cycles

We now define a class of cycles on our spaces. This is essentially the same definition as the cycles considered in [Kud04], see also [Kud97a].

Definition 2.5.1. Let $S \subset L$ be a (primitive) sublattice of signature $(2, n')$. Then $S^\perp$ is a (primitive) negative-definite sublattice of L. Define:

$$\mathcal{D}_{L,S} = \{[\vec{z}] \in \mathcal{D}_L \mid b(\vec{z}, \vec{y}) = 0 \text{ for all } \vec{y} \in S^\perp\}.$$

This is a codimension rank $S^\perp$ subspace of $\mathcal{D}_L$, defined by algebraic conditions. Moreover, we see that:

$$\mathcal{D}_S \simeq \mathcal{D}_{L,S} \subset \mathcal{D}_L.$$

Let $\Phi_S = \{S' \mid S' = \gamma S \text{ for some } \gamma \in \Gamma\}$. Define:

$$H_{L,S} = \bigcup_{S' \in \Phi_S} \mathcal{D}_{L,S'}$$

to be the **generalized Heegner cycle** associated to this set of (primitive) embeddings of S into L. Its image in $X_L(\Gamma)$ will be an analytic cycle. A more careful analysis and a precise definition can result in obtaining an algebraic cycle (see [Kud04]).

Remark. In the definitions above we could just as well have taken $S \subset L^\#$, the dual of L, or in fact any lattice in $L \otimes \mathbb{Q}$. However, for our purposes, since

$(S^\perp)^\perp \cap L$ would give a primitive lattice generating the same $\mathcal{D}_{L,S}$, there is no real loss of generality in assuming this for our purposes.

We should remark that if S has corank 1 then $H_{L,S} = H_{\overline{x}_i, q(x_i)}$ is just a usual Heegner divisor (see [Bru02, p. 80]). This justifies our choice of name. It is not our intent to imply that there is (or is not) a relation to the generalized Heegner cycles arising from certain Kuga-Sato varieties (see [BDP10]).

2.5.2 Ramification near $\mathcal{D}_{L,S}$

We introduce the following notation (for any non-degenerate S):

$$\begin{aligned}
\Gamma_S &= \{\gamma \in \Gamma \mid \gamma S \subset S\}, \\
\overline{\Gamma}_S &= \{\gamma \in \mathrm{O}_S \mid \gamma \text{ lifts to } \Gamma\}, \text{ and} \\
\tilde{\Gamma}_S &= \{\gamma \in \Gamma_S \mid \gamma|_{S^\perp} = \mathrm{Id}\}.
\end{aligned}$$

Remark. It would be convenient if $\tilde{\Gamma}_S \simeq \overline{\Gamma}_S$, however, this is hard to guarantee if $L \neq S \oplus S^\perp$.

We return to the setting where $S \subset L$ is a sublattice of signature $(2, n')$, so that $S^\perp$ is a negative-definite lattice. It follows that $\overline{\Gamma}_{S^\perp}$, and hence $\tilde{\Gamma}_{S^\perp}$, are both finite groups. We find that $\tilde{\Gamma}_S \times \tilde{\Gamma}_{S^\perp} \hookrightarrow \mathrm{O}_L$, while $\overline{\Gamma}_S \times \overline{\Gamma}_{S^\perp}$ may not. We have the following maps:

$$\begin{array}{ccc}
X_S(\tilde{\Gamma}_S) & \hookrightarrow & (\tilde{\Gamma}_S \times \tilde{\Gamma}_{S^\perp}) \backslash \mathcal{D}_L \\
\downarrow & & \downarrow \\
X_S(\overline{\Gamma}_S) & \longrightarrow & X_L(\Gamma).
\end{array}$$

Remark. If we want the bottom map to be injective we would need that for each $\sigma \in O_L$ with $x, \sigma(x) \in \mathcal{D}_{L,S^\perp}$ then there exists $\tau \in O_S$ with $\tau(x) = \sigma(x)$.

We wish to explain the local ramification near $D_{L,S}$. Fix e_1 and e_2 isotropic vectors spanning a hyperplane in $S \otimes K$, where K is a totally real quadratic extension of $\mathbb{Q}$. Note that we cannot always take e_1 and e_2 in S. We may then choose to express the spaces $\mathcal{D}_S$ and $\mathcal{D}_L$ as tube domains relative to the same pair e_1, e_2. In particular we may write:

$$\mathcal{D}_L = \{\vec{u} \in \mathcal{U}_L = \langle e_1, e_2 \rangle^\perp \subset L \otimes \mathbb{C} \mid q(\Im(\vec{u})) > 0\}$$

with $\mathcal{D}_{L,S}$ in $\mathcal{D}_L$ being precisely:

$$\mathcal{D}_{L,S} = \{\vec{u} \in \mathcal{U}_S = \langle e_1, e_2, S^\perp \rangle^\perp \subset L \otimes \mathbb{C} \mid q(\Im(\vec{u})) > 0\}.$$

Thus we see that in a neighbourhood of $\mathcal{D}_{L,S}$ in $\mathcal{D}_L$ we can express

$$\mathcal{D}_L = \mathcal{D}_{L,S} \oplus (S^\perp \otimes \mathbb{C}).$$

Then $\tilde{\Gamma}_{S^\perp}$ acts on the complementary space $S^\perp \otimes \mathbb{C}$. We see that the cycle $\mathcal{D}_{L,S}$ is the generic ramification locus for this action. That is, $\mathcal{D}_{L,S}$ is maximal among cycles fixed by this action (with respect to inclusion among cycles).

Remark. We remark that for some points of $\mathcal{D}_{L,S}$ the group $\Gamma_{S^\perp} = \Gamma_S$ may also cause ramification in the quotient. This ramification will not in general be generic, and it will typically restrict to some sub-cycle of $\mathcal{D}_{L,S}$.

Indeed, a group element g fixes $\tau \in \mathcal{D}_{L,S}$ if and only if τ is an eigenspace of g. Thus g can only fix all of $\mathcal{D}_{L,S}$ if S is an eigenspace. This would imply that τ acts as -1 on S. Such an element acts trivially on $\mathcal{D}_S$ as this is a projective space. The effect of the quotient by g is the same as by $-g \in \mathrm{O}_{S^\perp}$.

2.5.3 Generalized Special Cycles

We will now introduce another type of cycle on the spaces $X = \Gamma \backslash \mathcal{D}_L$ which play a role in ramification. We will call these **generalized special cycles** because of their relationship to special points (see Section 2.6). Some of the constructions we shall perform will become more natural with the material in Chapter 3.

Let $F/\mathbb{Q}$ be a CM-field and consider the CM-algebra:

$$E = F^d = F^{(1)} \times \cdots \times F^{(n)}.$$

Denote complex conjugation for both F and E by σ . View E as an F-algebra under the diagonal embedding of F into E. Label the embeddings $\mathrm{Hom}(F,\mathbb{C})$ as $\{\rho_1,\overline{\rho_1},\dots\rho_m,\overline{\rho_m}\}$. Pick $\lambda=(\lambda^{(1)},\dots,\lambda^{(n)})\in(E^\sigma)^\times$ such that $\rho_1(\lambda^{(1)})\in\mathbb{R}^+$ but $\rho_j(\lambda^{(i)})\in\mathbb{R}^-$ for all other combinations of i,j. We now consider the rational quadratic space $(V,q_{E,\sigma,\lambda})$ given by $V=E$ and

$$q_{E,\sigma,\lambda}(x)=\tfrac{1}{2}\,\mathrm{Tr}_{E/\mathbb{Q}}(\lambda x\sigma(x)).$$

Notice that the signature of the quadratic form is of the shape $(2,\ell)$. We define also the F-quadratic space $(V',q'_{E,\sigma,\lambda})$ given by $V'=E$ and

$$q'_{E,\sigma,\lambda}(x)=\tfrac{1}{2}\,\mathrm{Tr}_{E/F}(\lambda x\sigma(x)).$$

Notice that $q_{E,\sigma,\lambda}(x)=\mathrm{Tr}_{F/\mathbb{Q}}(q'_{E,\sigma,\lambda}(x))$. We have the tori $T_{E,\sigma}$ and $T_{F,\sigma}$ defined by:

$$T_{E,\sigma}(R)=\{x\in(E\otimes_{\mathbb{Q}}R)^\times\mid x\sigma(x)=1\},$$
$$T_{F,\sigma}(R)=\{x\in(F\otimes_{\mathbb{Q}}R)^\times\mid x\sigma(x)=1\},$$

as well as maps:

$$T_{F,\sigma}\overset{\Delta}{\hookrightarrow}T_{E,\sigma}\hookrightarrow\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{O}_{q'_{E,\sigma,\lambda}})\hookrightarrow\mathrm{O}_{q_{E,\sigma,\lambda}},$$

where the first map Δ is the diagonal embedding. Now suppose further that: $q=q_{E,\sigma,\lambda}\oplus q^\perp$ and consider the inclusion:

$$\mathrm{O}_{q_{E,\sigma,\lambda}}\hookrightarrow\mathrm{O}_q\,.$$

Definition 2.5.2. The **generalized special cycle** associated to the inclusions $T_{F,\sigma}\hookrightarrow\overset{\phi}{\cdots}\hookrightarrow\mathrm{O}_q$ as above is:

$$\mathcal{D}_\phi=\{[\vec{z}]\in\kappa_q^+\mid g\vec{z}=\rho_0(g)\vec{z}\text{ for all }g\in T_{F,\sigma}(\mathbb{R})\}.$$

For any lattice L in the quadratic space of q this gives us a cycle in $\mathcal{D}_L$. Set $\Phi = \{\gamma^{-1}\phi\gamma \mid \gamma \in \Gamma\}$ and define:

$$H_\phi = \bigcup_{\phi \in \Phi} \mathcal{D}_\phi.$$

The image of H_ϕ in $X = \Gamma\backslash\mathcal{D}_L$ is a cycle on X of the form:

$$\Gamma'\backslash\mathcal{D}_\phi = \Gamma'\backslash \operatorname{Res}_{F/\mathbb{Q}}(\mathrm{O}_{q'_{E,\sigma,\lambda}})(\mathbb{R})/K_{E,\sigma,\lambda},$$

where $\Gamma' = \Gamma \cap \operatorname{Res}_{F/\mathbb{Q}}(\mathrm{O}_{q'_{E,\sigma,\lambda}})(\mathbb{Z})$ and $K_{E,\sigma,\lambda}$ is a maximal compact subgroup of $\operatorname{Res}_{F/\mathbb{Q}}(\mathrm{O}_{q'_{E,\sigma,\lambda}})(\mathbb{R})$. Note that:

$$\operatorname{Res}_{F/\mathbb{Q}}(\mathrm{O}_{q'_{E,\sigma,\lambda}})(\mathbb{R}) \simeq \mathrm{O}_{2,m-2}(\mathbb{R}) \times \mathrm{O}_m(\mathbb{R})^{d-1}.$$

Remark. If $d = 1$ then the special cycle will be a special point.

2.5.4 Ramification Near $\mathcal{D}_\phi$

Notation 2.5.3. Denote the group of N^{th} roots of unity by μ_N and a choice of generator by ζ_N.

The group μ_N has a unique irreducible rational representation ψ_N. The representation ψ_N is precisely the $\varphi(N)$-dimensional representation of μ_N acting on the rational vector space $\mathbb{Q}(\zeta_N)$ by multiplication.

For each $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ the generator ζ_N acts on:

$$x_a = \sum_{b \in \mathbb{Z}/N\mathbb{Z}} \zeta_N^{-b} \otimes \zeta_N^{a^{-1}b} \in \mathbb{Q}(\zeta_N) \otimes \psi_N$$

by multiplication by ζ_N^a. We shall denote this (a)-isotypic eigenspace by $\psi_N(a) \subset \mathbb{Q}(\zeta_N) \otimes \psi_N$.

Conversely, we recover the rational subspace $\mathbb{Q}\zeta_N^b$ as being spanned by:

$$\sum_\gamma \gamma(\zeta_N^b)\gamma(x_a),$$

where the sum is over $\gamma \in \operatorname{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. The vectors ζ_N^a for $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ form a rational basis for ψ_N.

Now consider the special case of the previous section where $F = \mathbb{Q}(\zeta_N)$ and $E = \mathbb{Q}(\zeta_N)^n$. Assume that $q = q_{E,\sigma,\lambda}$. Moreover, assume that the integral structure on $E = F^d$ is of the form $L = \oplus L_i$, where the L_i are fractional ideals of $F^{(i)}$. This requirement is equivalent to saying the integral structure is such that via $\mu_N \subset T_F \subset \mathrm{O}_q$ we find $\mu_N \subset \mathrm{O}_q(\mathbb{Z})$.

Proposition 2.5.4. *The cycle $\mathcal{D}_\phi$ is the ramification divisor for μ_N under this action. Moreover, locally near D_ϕ we have that:*

$$\mathcal{D}_L = \mathcal{D}_\phi \times \prod_{a \in (\mathbb{Z}/N\mathbb{Z})^\times \setminus \{1\}} \mathbb{C}^r(a-1),$$

where the action of μ_N on $\mathbb{C}^r(a)$ is via χ^a.

Proof. We identify the tangent space near $\tau \in D_\phi$ with:

$$\mathcal{T}_{\mathcal{D}_L,\tau} = \tau^\perp/\tau = \oplus_a (L \otimes \mathbb{C})(a)/\tau.$$

Without loss of generality (or rather by choice of ζ_N) we may suppose τ is in the ζ_N-eigenspace. The above then becomes:

$$\tau^\perp/\tau = \mathcal{T}_{\mathcal{D}_\phi}/\tau \bigoplus_{a \neq 1} ((L \otimes \mathbb{C})(a)/\tau).$$

We see that the action of μ_N on $(L \otimes \mathbb{C})(a)/\tau$ is by ζ_N^{a-1}, where the -1 comes from the action on τ. We thus see that in a neighbourhood of τ around $\mathcal{D}_\phi$ the group μ_N acts non-trivially, whereas it clearly acts trivially on $\mathcal{D}_\phi$. □

Remark. As with the previous case, points $\tau \in \mathcal{D}_\phi$ may have other sources of ramification.

2.5.5 Ramification at τ

We will now explain why the situations described above are in fact the only source of ramification. Fix $\tau \in \mathcal{D}_L$. We define a lattice $S \subset L$ by setting:

$$S = (\{\Re(\tau), \Im(\tau)\}^\perp)^\perp.$$

Note that the lattice $S^\perp$ is a potentially 0-dimensional negative-definite lattice. We observe that $\tau \in \mathbb{C} \otimes S$. We wish to consider the stabilizer of $\tau \in \mathcal{D}_L$. This is precisely:

$$\Gamma_\tau = \{\gamma \in \Gamma \mid \text{there exists } \lambda_\gamma \in \mathbb{C}^\times \text{ with } \gamma(\tau) = \lambda_\gamma \tau\}.$$

We immediately obtain a homomorphism $\chi_\tau : \Gamma_\tau \to \mathbb{C}^\times$ given by $\chi_\tau(\gamma) = \lambda_\gamma$.

We have the following key results from [GHS07, Sec. 2.1].

Proposition 2.5.5. *With the above notation we see the following:*

- *There is an inclusion* $\Gamma_\tau \subset \Gamma_S$.
- *The kernel* $\ker(\chi_\tau)$ *equals* $\tilde{\Gamma}_{S^\perp}$.
- *The image of* $\Gamma_\tau/\tilde{\Gamma}_{S^\perp}$ *is a cyclic subgroup of* $\overline{\Gamma}_S$.

Proof. The first point follows immediately from the definition of S and Γ_S.

To see the second point, notice that the inclusion $\tilde{\Gamma}_{S^\perp} \subset \ker(\chi_\tau)$ is apparent from the discussion of Section 2.5.2. Now for the reverse inclusion, if $g \in \ker(\chi_\tau)$ and $x \in S$ we see:

$$(\tau, x) = (g\tau, gx) = (\tau, gx).$$

This implies that:

$$(\tau, x - gx) = (\overline{\tau}, x - gx) = 0,$$

and thus, $x - gx \in S^\perp$. However, $S^\perp$ is negative-definite and thus:

$$S \cap S^\perp = (S^\perp)^\perp \cap S^\perp = 0.$$

For the final point notice that:

$$\Gamma_\tau/\tilde{\Gamma}_{S^\perp} \simeq \chi_\tau(\Gamma_\tau) = \mu_{r_\tau} \subset \mathbb{C}^*.$$

Thus the natural map:

$$\Gamma_S \to \overline{\Gamma}_S$$

takes $\Gamma_\tau/\tilde{\Gamma}_{S^\perp}$ to a cyclic subgroup of $\overline{\Gamma}_S$. □

It follows from the proposition that the group $\Gamma_\tau/\tilde{\Gamma}_{S^\perp}$ gives an action of μ_{r_τ} on S.

Proposition 2.5.6. *There are no trivial eigenvectors for the action of μ_{r_τ} on S.*

Proof. Suppose $\vec{x}$ is a nontrivial eigenvector and that $g \in \mu_{r_\tau}$ is a nontrival element. Then we write:

$$(\tau, x) = (g\tau, gx) = \chi_\tau(g)(\tau, x).$$

Likewise since $\overline{\tau}$ is also an eigenvector we find:

$$(\overline{\tau}, x) = (g\overline{\tau}, gx) = \overline{\chi_\tau(g)}(\overline{\tau}, x).$$

Therefore, $x \in S^\perp \cap S = \{0\}$. □

It follows from this proposition that $S = \phi_{r_\tau}^d$ as a representation of μ_{r_τ}.

Proposition 2.5.7. *We can decompose $S = \phi_{r_\tau}^d$ in such a way that q is non-degenerate on each factor and this is an orthogonal decomposition with respect to q.*

Proof. First we observe that we can proceed by induction provided there exists at least one non-degenerate factor. Indeed, if $q|_{\phi_{r_\tau}}$ is non-degenerate it follows that μ_N stabilizes $(\phi_{r_\tau})^\perp$. We may thus proceed inductively on d.

Next we observe that the restriction of q is non-degenerate if and only if it is non-trivial. This follows from two key facts:

1. $\mathrm{Gal}(\mathbb{Q}(\zeta_{r_\tau})/\mathbb{Q})$ acts transitively on eigenspaces, and
2. $b(x_a, x_b) = 0$ if $a \neq b^{-1}$.

It follows that if $\varphi(r_\tau) > 2$, then $q|_{\phi_{r_\tau}}$ is non-degenerate since there are no isotropic spaces of size larger than 2.

For the case of $\varphi(r_\tau) = 2$ it is not possible to have $d = 1$. It follows that there exists a pair of ϕ_{r_τ} such that the restriction of q to $\phi_{r_\tau}^{(1)} \oplus \phi_{r_\tau}^{(2)}$ is nontrivial. If q restricts trivially to each factor, set $y_i^{(1)} = x_i^{(1)} + x_i^{(2)}$ and $y_i^{(2)} = x_i^{(1)} - x_i^{(2)}$. The restriction of q is then nontrivial on $\mathrm{span}(y_i^{(j)}) \simeq \phi_{r_\tau}$. This completes the argument. □

Proposition 2.5.8. *If $\chi_\tau(\Gamma_\tau) \not\subset \{\pm 1\}$ then τ is on a special cycle $\mathcal{D}_\phi$ of $\mathcal{D}_S$, where $F = \mathbb{Q}(\chi(\Gamma_\tau))$. Hence, τ is on a generalized special cycle of $\mathcal{D}_L$.*

Proof. Because the $\mathbb{Q}$-span of $\phi_{r_\tau}(\mu_{r_\tau}) \subset \mathrm{End}(\phi_{r_\tau})$ is equal to $\mathbb{Q}(\zeta_{r_\tau})$ we may extend the action of μ_{r_τ} to one of T_F on each factor. This implies by way of the results of Chapter 3 that we are in the setting of the previous section. In particular, there exists a unique factor which is not negative-definite, and for it there exists a unique $\mathbb{R}$-factor which is positive-definite. □

Claim. *If $\chi_\tau(\Gamma_\tau) = \{\pm 1\}$ then the image of Γ_τ acting on $\mathcal{D}_{L,S}$ acts trivially on all of $\mathcal{D}_{L,S}$.*

Proof. This follows since the entire space is the (-1)-eigenspace. □

Remark. From Propositions 2.5.5 and 2.5.8 it follows immediately that the ramification of $\mathcal{D}_L$ consists entirely of the ramification along $\mathcal{D}_{L,S}$ coming from $\tilde{\Gamma}_{S^\perp}$, and the ramification along $\mathcal{D}_\phi \subset \mathcal{D}_{L,S}$ coming from the action of μ_N on $\mathcal{D}_\phi$.

Note though that if $\tilde{\Gamma}_{S^\perp} \neq \overline{\Gamma}_S$ then the quotient action by μ_N does not act trivially on the $S^\perp \otimes \mathbb{C}$ component of the tangent space to $\mathcal{D}_{L,S}$. This phenomenon can only arise if $L \neq S \oplus S^\perp$.

2.6 Explicit Class Field theory (and Canonical Models)

2.6.1 Shimura Varieties and Hermitian Symmetric Spaces

There is an important relation between Shimura varieties (or at least their points over $\mathbb{C}$) and Hermitian symmetric spaces. More details of this relation are found in the notes of Milne [Mil05] or the work of Deligne [Del71]. The following section illustrates this connection.

Notation 2.6.1. We shall denote by $\mathbb{S} = \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)$ and $\mathbb{S}^1 \subset \mathbb{S}$ the subtorus consisting of the norm 1 elements. Concretely this means:

$$\mathbb{S}(R) \simeq \{\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \mid a, b \in R\} \text{ and } \mathbb{S}^1(R) \simeq \{\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \mid a, b \in R,\ a^2 + b^2 = 1\}.$$

For a reductive group G denote its centre by $Z(G)$ and let $G^{\mathrm{ad}} = G/Z(G)$ be the associated semi-simple group.

Definition 2.6.2. A **connected Shimura datum** is (G, X), a semi-simple algebraic group G defined over $\mathbb{Q}$ and a $G^{\mathrm{ad}}(\mathbb{R})^+$ conjugacy class of maps $\rho : \mathbb{S}^1_{\mathbb{R}} \to G^{\mathrm{ad}}_{\mathbb{R}}$ satisfying the following axioms:

1. The only eigenvalues that appear in the representation of $\mathbb{S}^1$ on $\mathrm{Lie}(G^{\mathrm{ad}})_{\mathbb{C}}$ induced by ρ are $a + bi, a - bi$ and 1.
2. Conjugation by $\rho\left(\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\right)$ is a Cartan involution of G^{ad}.
3. G^{ad} has no $\mathbb{Q}$-simple factors G_i such that $G_i(\mathbb{R})$ is compact.

A **Shimura datum** is (G, X), a reductive algebraic group G defined over $\mathbb{Q}$ and a $G(\mathbb{R})$ conjugacy class of maps $\rho : \mathbb{S}_{\mathbb{R}} \to G_{\mathbb{R}}$ satisfying the same axioms.

As per the introduction on Hermitian symmetric spaces (Section 2.2) such a conjugacy class is equivalent to a Hermitian symmetric space. One must be careful about the normalizations of h versus ρ to obtain the above conditions.

Definition 2.6.3. We shall denote the finite adéles of $\mathbb{Q}$ by $\mathbb{A}^f$.

Let (G, X) be a connected Shimura datum and K be the maximal compact subgroup associated to the Cartan involution coming from $\rho \in X$. The **connected Shimura variety** associated to (G, X) is the inverse system:

$$M_{\mathbb{C}}(G, \rho)(\mathbb{C}) = \lim_{\substack{\leftarrow \\ \Gamma}} \Gamma \backslash G^{\mathrm{ad}}(\mathbb{R})/K = \lim_{\substack{\leftarrow \\ K^f}} G^{\mathrm{ad}}(\mathbb{Q}) \backslash G^{\mathrm{ad}}(\mathbb{A})/K \times K^f,$$

where the Γ run over all 'congruence' subgroups of $G(\mathbb{Q})$ and the K^f run over compact open subgroups of $G(\mathbb{A}^f)$.

For (G, X) a Shimura datum the **Shimura variety** associated to (G, X) is:

$$M_{\mathbb{C}}(G, \rho)(\mathbb{C}) = \lim_{\substack{\leftarrow \\ K^f}} G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K^f,$$

where K^f run over compact open subgroups of $G(\mathbb{A}^f)$.

Given (G_1, X_1) and (G_2, X_2) together with a map $f : G_1 \to G_2$ such that $f(X_1) \subset X_2$, one obtains a morphism of Shimura varieties.

Remark. What we have just defined is the 'complex points' of the Shimura variety. The Shimura variety should be viewed as the associated complex scheme, or inverse system of complex schemes associated to this system. Such schemes exist by the theorem of Baily-Borel (see [BB66]).

The adèlic description makes it clear that there exists an action of the finite adéles on a Shimura variety.

2.6.2 Shimura Reciprocity

In order to explain the context of our results concerning special fields we must first introduce the notions of special points and Shimura reciprocity. We give here a very terse description of the ideas at work. We will follow fairly closely the format of [Del71] where you may find a more thorough exposition.

Definition 2.6.4. Let $\tau : E \to \mathbb{C}$ be a number field with a complex embedding and let $M_{\mathbb{C}}(G, \rho)$ the complex model of the Shimura variety associated to G. A **model** over E of $M_{\mathbb{C}}(G, \rho)$ consists of:

1. a scheme $M_E(G, \rho)$ over E, endowed with a continuous action of $G(\mathbb{A}^f)$, and
2. an isomorphism $M_E(G, \rho) \otimes_{E,\tau} \mathbb{C} \simeq M_{\mathbb{C}}(G, \rho)$ compatible with the action of $G(\mathbb{A}^f)$.

To give a scheme M over E together with a continuous action of $G(\mathbb{A}^f)$ amounts to giving:

1. a scheme ${}_K M$ over E for every open compact subgroup K of $G(\mathbb{A}^f)$, and

2. a homomorphism $J_{L,K}(x) : {}_KM \to {}_LM$ for every pair K and L of compact open subgroups of $G(\mathbb{A}^f)$ and for each $x \in G(\mathbb{A}^f)$ with $xKx^{-1} \subset L$. These homomorphisms must satisfy:
   (a) $J_{M,L}(y)J_{L,K}(x) = J_{M,K}(yx)$.
   (b) $J_{K,K}(x) = \mathrm{Id}$ if $x \in K$.
   (c) For K a normal subgroup of L, the map $J_{K,K}$ defines an action of L/K on ${}_KM$, and moreover, $J_{L,K}(e)$ defines $(L/K)\backslash {}_KM \to {}_LM$.

Let F be a finite extension of E, together with a complex embedding extending that of E. If $M_E(G,\rho)$ is a model of $M_{\mathbb{C}}(G,\rho)$ over E, we denote by $M_F(G,\rho) = M_E(G,\rho) \otimes_E F$ the model of $M_{\mathbb{C}}(G,\rho)$ over F.

Given a model $M_E(G,\rho)$ there is an action of $\mathrm{Gal}(\overline{E}/E)$ on $M_{\overline{E}}(G,\rho)$, and thus on the profinite system:

$$\pi_0(M_{\overline{E}}(G,\rho)) = \lim_{\leftarrow} \pi_0({}_KM_{\overline{E}}(G,\rho)) \xrightarrow{\sim} \pi_0(M_{\mathbb{C}}(G,\rho)).$$

Likewise the group $G(\mathbb{A}^f)$ acts on $\pi_0(M_{\overline{E}}(G,\rho))$. The action factors through:

$$\pi(G) := \pi_0(G(\mathbb{A})/G(\mathbb{Q}))$$

and again through its quotient $\pi(G)/\pi_0(K_\infty)$. This makes $\pi_0(M_{\overline{E}}(G,\rho))$ into a principal homogeneous space under the commutative group $\pi(G)/\pi_0(K_\infty)$ (see [Del71, 3.4]). As these two actions commute this induces a map:

$$\lambda_M : \mathrm{Gal}(\overline{E}/E) \to \pi(G)/\pi_0(K_\infty).$$

For a number field E, class field theory identifies the largest abelian quotient of $\overline{E}/E$ with the group $\pi_0(T_E(\mathbb{A})/T_E(\mathbb{Q}))$ and the above map can be interpreted as:

$$\lambda_M : \mathrm{Gal}(\overline{E}/E)^{ab} = \pi_0(T_E(\mathbb{A})/T_E(\mathbb{Q})) \to \pi(G)/\pi_0(K_\infty).$$

We shall call this morphism the **reciprocity map**.

Remark. It would be a very desirable property of models that morphisms should descend to them.

Given a pair of Shimura data (G_1, ρ_1) and (G_2, ρ_2) together with models $M_{E_1}(G_1, \rho_1)$ and $M_{E_2}(G_2, \rho_2)$ over E_1 and E_2, respectively. Suppose there is a morphism $f : (G_1, \rho_1) \to (G_2, \rho_2)$ that descends to the models:

$$f_{E_1} : M_{E_1}(G_1, \rho_1) \to M_{E_2}(G_2, \rho_2).$$

The immediate implication is that $E_2 \subset E_1$. It also follows immediately that the Galois action on $M_{E_2}(G_2, \rho_2)$ must induce reciprocity on $M_{E_1}(G_1, \rho_1)$.

Example. The simplest example of a Shimura datum comes from taking the group $G = T$ a rational torus such that $T(\mathbb{R})$ is compact. In this case the varieties ${}_K M_{\mathbb{C}}(G, \rho)$ are finite sets. Thus to give a model over any field E which splits T is equivalent to giving a Galois action on this set.

Definition 2.6.5. The **canonical model** for the Shimura variety of a rational torus T_E is the unique model for which the reciprocity morphism is the reciprocity morphism of class field theory. There exists a minimal field $E(T, \rho)$ over which this model can be defined. It is often called the **reflex field** or **special field** of the point. We shall say that a field E is a **special field** for a Shimura variety if it is the special field for a special point on that variety.

Definition 2.6.6. A point $h \in M_{\mathbb{C}}(G, \rho)$ is called a **special point** if h is in the image of some $M_E(T, \rho')$.

Definition 2.6.7. For a Shimura variety $M_{\mathbb{C}}(G, \rho)$ a model $M_E(G, \rho)$ over E is said to be **weakly canonical** if for every special point h that is associated to $M_{\mathbb{C}}(T, \rho')$ the inclusion from the canonical model $M_{E(T,\rho')}(T, \rho')$ is defined over the composite field $E(T, \rho')E$.

The model is said to be **canonical** if the field E is the field of definition of an associated Hodge filtration (see [Del71, 3.13]).

Theorem 2.6.8. *Given any Shimura variety a canonical model exists and is unique.*

For many types of Shimura varieties this theorem follows from an explicit construction for a canonical model for the Siegel spaces (see [Del79, Sec. 2.3]). More generally see [Mil83].

2.6.3 Special Fields for the Orthogonal Group

From the concrete descriptions of the structure of the Hermitian symmetric spaces associated to orthogonal groups (see Section 2.2) and the structure of tori in orthogonal groups we shall describe later (see Chapter 3), we easily obtain the following characterization:

Proposition 2.6.9. *A CM-field L with totally real subfield K is a special field for the Shimura variety associated to O_q if there exists a CM-algebra E containing L as a direct factor, ie. $E = E' \oplus L$, for which the associated algebraic torus $T_{E,\sigma}$ embeds into O_q in such a way that the trivial eigenspace of $T_{L,\sigma} \subset T_{E,\sigma}$ is negative-definite.*

Remark. It is not immediately clear to what extent the condition "the trivial eigenspace of $T_{L,\sigma}$ is negative-definite", which does not appear in the general conditions for embedding tori, places any new restrictions. This condition might appear to present an obstruction to the local-global principle for the embedding of algebras. As such a remark is in order on the obstruction to the local-global principal (for a more detailed discussion see [PR10] and [BF13]). The source of the local-global conditions is precisely the requirement (see proof of Corollary 3.5.4):

We can divide the Hasse-Witt conditions between the factors in such a way that each factor can control the ones it is given and each factor is given an even number.

This is not an obstruction if:

For each pair i, j there exists a non-split quaternion algebra A which is split *by $E_i^{\phi_i}$ and $E_j^{\phi_j}$ for all CM-types ϕ_i of E_i and ϕ_j of E_j.*

or equivalently:

For each pair i, j there exists p a prime of $\mathbb{Q}$ and $\mathfrak{p}_i, \mathfrak{p}_j | p$ primes of E_i, E_j such that both $\mathfrak{p}_i, \mathfrak{p}_j$ do not split respectively over E_i^σ, E_j^σ.

For each factor E_i of E the Chebotarov density theorem tells us that the density of primes of $\mathbb{Q}$ that have a factor in E_i^σ that is inert in E_i should be at least $1/[E_i : \mathbb{Q}]$. If E_i were Galois, this ratio can be more explicitly computed as:

$$\left|\{\gamma \in \mathrm{Gal}(E_i/\mathbb{Q}) \mid \sigma = \alpha^{-1}\gamma^r\alpha \text{ for some } \alpha, r\}\right| / \left|\mathrm{Gal}(E_i/\mathbb{Q})\right|.$$

The formula is looking for elements where a power of Frobenius is a conjugate of σ. If C_σ is the largest cyclic 2-group in $\mathrm{Gal}(E_i/\mathbb{Q})$ containing σ and Γ_2 is a Sylow 2-subgroup, then this ratio is at least $\frac{|C_\sigma|-1}{|\Gamma_2|}$. It follows that if the E_i are chosen at random then we expect infinitely many primes to prevent any local-global obstructions. Moreover, given an extension E_1 the conditions one needs to impose on E_2 to make $E_1 \oplus E_2$ not satisfy the local-global principle places many restrictions on E_2. It is not at all apparent that such an E_2 can even exist. Nonetheless, examples do exist where the local-global conditions will fail when E_1 is degree 4 and E_2 is degree 2 (see [PR10, Ex. 7.5]).

Claim. *Let $E = \overline{E_1E_2}$ be the normal closure of the composite field. If there exists $\sigma_E \in \mathrm{Gal}(E/k)$ such that $\sigma_E|_{E_i} = \sigma$ for $i = 1, 2$ then $E_1 \oplus E_2$ satisfies the local-global principle.*

For a more precise statement about CM-algebras see [BF13, Cor 4.1.1]. The key point here is that when $\mathrm{Frob}_p = \sigma_E$ it must also restrict to both $\sigma_E|_{E_i}$, and consequently, the associated primes over p in each factor are inert.

Theorem 2.6.10. *Suppose (V, q) is a quadratic space over $\mathbb{Q}$ of signature $(2, \ell)$ with ℓ even. Suppose that (E, σ) is a CM-field with complex conjugation σ and that $[E : \mathbb{Q}] = 2 + \ell$. Then $T_{E,\sigma} \hookrightarrow \mathrm{O}_q$ if and only if:*

1. *E^ϕ splits the even Clifford algebra C_q^0 for all CM-types ϕ of E, and*

2. $D(q) = (-1)^{(2+\ell)/2}\delta_{E/\mathbb{Q}}$.

If this occurs then E is a special field.

See Theorem 3.1.2.

Theorem 2.6.11. *Suppose (V, q) is a quadratic space over $\mathbb{Q}$ of signature $(2, \ell)$ with ℓ odd. Suppose that (E, σ) is a CM-field with complex conjugation σ and that $[E : \mathbb{Q}] = 1 + \ell$. Then $T_{E,\sigma} \hookrightarrow \mathrm{O}_q$ if and only if:*

1. E^ϕ *splits the even Clifford algebra* C_q^0 *for all CM-types* ϕ *of* E.

If this occurs then E is a special field.

See Theorem 3.1.2.

Theorem 2.6.12. *Suppose (V, q) is a quadratic space over $\mathbb{Q}$ of signature $(2, \ell)$ with ℓ even. Suppose that (E, σ) is a CM-field with complex conjugation σ and that $[E : \mathbb{Q}] = \ell$. Set $d = (-1)^{\ell/2}D(q)\delta_{E/\mathbb{Q}}$. Then $T_{E,\sigma} \hookrightarrow \mathrm{O}_q$ if and only if:*

1. E^ϕ *splits* $\mathbb{Q}(\sqrt{d}) \otimes_{\mathbb{Q}} \mathrm{C}_q^0$ *for all CM-types* ϕ *of* E.

The field E can always be made a special field.

Proof. It is apparent that the condition to have E embed into O_q is that $T_{E\oplus\mathbb{Q}(\sqrt{d}),\sigma} \hookrightarrow \mathrm{O}_q$. From this the only conditions that remain then are the splitting conditions and the local-global conditions.

The local-global conditions here are automatic because complex conjugation on each factor is induced by an element of the Galois group of the composite field. Note that E is not always a special field but it is for certain embeddings $T_{E,\sigma} \hookrightarrow \mathrm{O}_q$. □

Theorem 2.6.13. *Suppose (V, q) is a quadratic space over $\mathbb{Q}$ of signature $(2, \ell)$. Suppose that (E, σ) is a CM-field with complex conjugation σ and that $[E : \mathbb{Q}] < \ell$. Then $T_{E,\sigma} \hookrightarrow \mathrm{O}_q$ in such a way that E is the special field for the corresponding special point.*

Proof. Picking $\lambda \in E^\sigma$ with precisely 1 positive embedding we claim that we may write:

$$q \simeq q_{E,\sigma,\lambda} \oplus q'.$$

Indeed, such a space q' would have dimension at least 3. Quadratic forms of dimension 3 are universal for discriminants, Hasse invariants and signatures. That is the form:

$$Dqx_1^2 + Hx_2^2 + -qHx_3^2$$

has discriminant $-D$, and Hasse invariant $(D,-1)(q,DH)$. We can thus easily satisfy any imposed discriminant, Hasse invariant and signature conditions by picking H, q, D appropriately and noting that the sign of D must be compatible with the signature conditions that we are imposing. □

Example. The special fields for Shimura curves attached to quaternion algebras over $\mathbb{Q}$ are precisely the quadratic CM-fields which split the quaternion algebra. In this case the quadratic form is the one coming from the reduced norm restricted to the trace 0 elements.

The special fields for Hilbert modular surfaces are either degree 2 or 4. The degree 4 CM-fields are precisely those which satisfy the discriminant condition. In this case we use the quadratic form:

$$x_1^2 - x_2^2 + x_3^2 - Dx_4^2.$$

The even Clifford algebra is trivial, and hence there is no splitting condition. To investigate degree 2 extensions notice that the form is isomorphic to:

$$x_1^2 + D_1x_2^2 - D_1x_3^2 - Dx_4^2.$$

Hench, any quadratic extension $\mathbb{Q}(\sqrt{D_1})$ can be made a special field.

CHAPTER 3
Characterization of Special Points of Orthogonal Symmetric Spaces

The main content of this chapter has been published in [Fio12].

It is available at http://dx.doi.org/10.1016/j.jalgebra.2012.08.030.

The version here contains some minor corrections and changes.

3.1 Introduction

Given an algebraic group G defined over $\mathbb{Q}$ and its associated symmetric space $G(\mathbb{R})/K$, where K is a maximal compact subgroup, one is interested in the special points (see [Del71, 3.15]). They correspond to those algebraic tori $T \subset G$ which are maximal, defined over $\mathbb{Q}$ and for which $T(\mathbb{R})$ is compact. To such a torus T one can associate a field F which is the special field for the corresponding point. This special field appears as part of an étale algebra E which is naturally associated to the torus. We wish to answer the following:

Question. Given a quadratic form q with its corresponding orthogonal group O_q, what are the conditions on an étale algebra E such that E is associated to a maximal torus T of O_q?

This problem is taken up, to some extent, by Shimura in [Shi80]. Some work on the problem also appears in my masters thesis [Fio09] as well as several other papers. This work is in fact complementary to my masters thesis where an abstract classification in terms of group cohomology is given. The relationship between those results and these will be the subject of future work (see Chapter 5 for further details). The most useful description for our current purposes is the work of Brusamarello, Chuard-Koulmann and Morales [BCKM03], from which one can extract various necessary and sufficient conditions on the algebra E. In this paper we rephrase the conditions which can be derived from [BCKM03].

The primary goal of this work is thus to prove the following:

Theorem 3.1.1. *Let (V, q) be a quadratic space over a number field k of dimension $2n$ or $2n+1$ and discriminant $D(q)$, and let (E, σ) be a degree $2n$ field extension E of k of discriminant $\delta_{E/k}$ together with an involution σ. Then O_q contains a torus of type (E, σ) if and only if the following three conditions are satisfied:*

1. *E^ϕ splits the even Clifford algebra C_q^0 for all σ-types ϕ of E.*
2. *If $\dim(V)$ is even then $\delta_{E/k} = (-1)^n D(q)$.*
3. *Let ν be a real infinite place of k and let s be the number of homomorphisms from E to $\mathbb{C}$ over ν for which σ corresponds to complex conjugation. The signature of q is of the form $(n - \frac{s}{2} + 2i, n + \frac{s}{2} - 2i)_\nu$ if the dimension is even and either $(n - \frac{s}{2} + 2i + 1, n + \frac{s}{2} - 2i)_\nu$ or $(n - \frac{s}{2} + 2i, n + \frac{s}{2} - 2i + 1)_\nu$ if $\nu((-1)^n D(q)\delta_{E/k})$ is respectively positive or negative when the dimension is odd, where $0 \leq i \leq \frac{s}{2}$.*

Moreover, for any E satisfying condition (2) we have that $\sqrt{D(q)} \in E^\phi$ for every σ-type ϕ of E.

The notion of a σ-type will be introduced in Definition 3.2.2.

We remark that the conditions in the theorem above are independent of the choice of similarity class representative for the quadratic form that defines O_q. We also note that one can replace the first condition of Theorem 3.1.1 by the condition that for all primes p of k where the even Clifford algebra is not split, there exists a prime $\mathfrak{p}|p$ of E^σ such that $\mathfrak{p}$ does not split in E. The equivalence of these conditions is the content of Lemma 3.5.9 and comes up in the proof of the main theorem.

We would also like to point out that the theorem above, which holds for fields with involutions, does not extend to arbitrary étale algebras with involution. It follows from our proof that the conditions in the theorem are sufficient to ensure that there exist local embeddings for all of the places of k.

Thus, the only obstacle to generalizing to étale algebras is the existence of a local-global principle. We would like to thank Prof. Eva Bayer, for pointing out the recent work of Prasad and Rapinchuk [PR10] on this problem. In their paper they provide both a counterexample to the local-global principle for étale algebras as well as giving a sufficient condition for when a local-global principle still holds. We also refer the reader to the forthcoming work of Eva Bayer [BF13] which gives a complete description of the obstructions to the local-global principle.

The original motivation for this work came from the problem of determining which CM-fields could be associated to the special points of a given a orthogonal group. The following corollary answers this question.

Corollary 3.1.2. *Suppose in the theorem that $k = \mathbb{Q}$, the signature of q is $(2, \ell)$ and (E, σ) is a CM-field with complex conjugation σ. Then O_q contains a torus of type (E, σ) if and only if:*

1. *For each prime p of $\mathbb{Q}$ with local Witt invariant $W(q)_p = -1$ there exists a prime $\mathfrak{p}|p$ of E^σ that does not split in E.*
2. *If ℓ is even, then $D(q) = (-1)^{(2+\ell)/2}\delta_{E/\mathbb{Q}}$. (No further conditions if ℓ is odd.)*

Corollary 3.1.3. *Suppose that $k = \mathbb{Q}$ and the signature of q is $(2, \ell)$. Let F be a totally real field. Then there exists a CM-field E with $E^\sigma = F$, such that the orthogonal group O_q contains a torus of type (E, σ) if and only if:*

1. *No condition if ℓ odd.*
2. *If ℓ is even, then (up to squares) $D(q) = N_{F/k}(\delta)$ for an element $\delta \in F$ which satisfies the condition that for all primes p of k with $W(q)_p = -1$ there is at least one prime $\mathfrak{p}|p$ of F such that δ is not a square in $F_\mathfrak{p}$.*

As a final application, we have the following which recovers classical results concerning the classification of CM-points, and answers the more recently raised question of classifying almost totally real cycles on the Hilbert modular surfaces associated to real quadratic fields (see [DL03]).

Corollary 3.1.4. *Let $d \in \mathbb{Q}$ be a squarefree positive integer. Consider the quadratic form:*

$$q_d = x_1^2 - x_2^2 + x_3^3 - dx_4^2.$$

This implies $\mathrm{Spin}_{q_d}(\mathbb{R}) \simeq \mathrm{SL}_2(\mathbb{R})^2$ *is associated to the Hilbert modular surface for $\mathbb{Q}(\sqrt{d})$. Let (E, σ) be an algebra of dimension 4 with involution σ. Then* O_q *has a torus of type (E, σ) if and only if the σ-reflex fields of E all contain $\mathbb{Q}(\sqrt{d})$. In particular, the algebras associated to tori in* Spin_{q_d} *all contain $\mathbb{Q}(\sqrt{d})$.*

3.2 Preliminaries

We begin by recalling a few of the basic notions relevant to the statement of the theorem.

For this section let k be a field of characteristic 0, fix an algebraic closure $\overline{k}$ and let $\Gamma = \mathrm{Gal}(\overline{k}/k)$ be the absolute Galois group.

3.2.1 Étale Algebras

By an **étale algebra** E over k of dimension n we mean a product of finite (separable) field extensions E_i/k where the dimension of E as a k-module is n. The **discriminant** $\delta(E/k)$ or $\delta_{E/k}$ is the product of the field discriminants $\delta_{E_i/k}$. We have that $E \otimes_k \overline{k} \simeq \times_\rho \overline{k} e_\rho$, where the e_ρ are orthogonal idempotents indexed by $\rho \in \mathrm{Hom}_{k-alg}(E, \overline{k})$. The isomorphism is given by the map $x \otimes \alpha \mapsto \sum_\rho \alpha\rho(x)e_\rho$. The Galois group Γ acts on the collection $\{e_\rho\}$ by ${}^\tau e_\rho = e_{\tau\circ\rho}$. This action, together with the natural action on coefficients, corresponds to having Γ act on $E \otimes_k \overline{k}$ via the second factor so that $\left(E \otimes_k \overline{k}\right)^\Gamma \simeq E$. Thus, the descent data needed to fully specify the k-isomorphism class of an n-dimensional étale algebra is the Galois action on the collection $\{e_\rho\}$. For a more detailed discussion of the theory of Galois descent, in particular how it applies to this setting see [KMRT98, Ch. 18]. The key result is:

Proposition 3.2.1. *There exists a bijective correspondence between isomorphism classes of étale algebras over k of dimension n and isomorphism classes of Γ-sets of size n. The correspondences being $E \mapsto \mathrm{Hom}_{k-alg}(E, \overline{k})$ and $\Omega \mapsto \left(\times_{\rho\in\Omega}\overline{k}e_\rho\right)^\Gamma$.*

We will often use this result to construct étale algebras by specifying a Γ-set.

By an **étale algebra with involution** (E, σ) over k we shall mean an étale algebra E over k together with $\sigma \in \mathrm{Aut}_{k-alg}(E)$ of exact order 2. We will denote by $E^\sigma = \{x \in E | \sigma(x) = x\}$ the fixed étale subalgebra of σ. The action of σ on E induces an action on idempotents given by $\sigma : e_\rho \mapsto e_{\rho\circ\sigma}$. We see immediately that this action commutes with the Galois action. Now, consider the disjoint collection of sets $\mathrm{Hom}_{k-alg}(E, \overline{k}) = \sqcup\{\rho, \rho\circ\sigma\}$. Since the actions of σ and Γ on $\mathrm{Hom}_{k-alg}(E, \overline{k})$ commute we find that Γ acts on the collection of sets $\{\rho, \rho\circ\sigma\}$. We can thus consider the étale algebra whose idempotents come with this action. It is the subalgebra E^σ of E under the inclusion map $e_{\{\rho,\rho\circ\sigma\}} \mapsto e_\rho + e_{\rho\circ\sigma}$.

Convention. *For the remainder of this paper we restrict our attention to the case where* $\dim_k(E^\sigma) = \left\lceil \frac{\dim_k(E)}{2} \right\rceil$. *For the most part we shall also assume that* $\dim_k(E)$ *is even. Unless it is otherwise specified, all algebras with involution satisfy these additional properties.*

We will now introduce the notions of σ-types and σ-reflex algebras. These generalize the notion of CM-types and CM-reflex algebras which are important in the theory of complex multiplication and have been extensively studied. We shall only mention the notions which will be of use to us. For a more detailed exposition of CM-types and CM-reflex fields see either [Lan83, 1.2 and 1.5] or [Mil06, 1.1, pp.12-19].

Definition 3.2.2. Let (E, σ) be an algebra with involution. A subset $\phi \subset \mathrm{Hom}_{k-alg}(E, \overline{k})$ is said to be a **σ-type** of E if $\phi \sqcup \phi\sigma = \mathrm{Hom}_{k-alg}(E, \overline{k})$. Denote the set of σ-types:

$$\Phi = \{\phi \subset \mathrm{Hom}_{k-alg}(E, \overline{k}) | \phi \sqcup \phi\sigma = \mathrm{Hom}_{k-alg}(E, \overline{k})\}.$$

Then both Γ and σ act on Φ and these actions commute. For a σ-type $\phi \in \Phi$ denote its orbit in Φ under Γ by $\Gamma\phi \subset \Phi$ and denote the stabilizer by $\Gamma_\phi = \{\gamma \in \Gamma | \gamma\phi = \phi\}$.

We define the **σ-reflex algebra** of ϕ to be (E^ϕ, σ), where E^ϕ is the étale algebra whose idempotents are indexed by $\Gamma\phi \cup \Gamma\phi\sigma$ with the induced action of Γ and σ.

We define the **complete σ-reflex algebra** to be (E^Φ, σ), which is the étale algebra whose idempotents are indexed by Φ with the natural action of Γ and σ.

Proposition 3.2.3 (Alternate definition of reflex field)**.** *Let ϕ be a σ-type of E and define $\widetilde{E^\phi} = \overline{k}^{\Gamma_\phi}$. If $\Gamma\phi = \Gamma\phi\sigma$ then E^ϕ is a field and $E^\phi \simeq \widetilde{E^\phi}$. Otherwise, if $\Gamma\phi \neq \Gamma\phi\sigma$ then $E^\phi = \widetilde{E^\phi} \times \widetilde{E^\phi}$.*

Proof. We claim that $\widetilde{E^\phi}$ naturally has idempotents corresponding to $\Gamma\phi$. Indeed, the idempotents of $\widetilde{E^\phi} = \overline{k}^{\Gamma_\phi}$ correspond to $\mathrm{Hom}_k(\overline{k}^{\Gamma_\phi}, \overline{k})$, which is naturally identified with Γ/Γ_ϕ as Γ-sets. The map sends $\gamma\Gamma_\phi$ to $\gamma \circ \mathrm{Id}$ where $\mathrm{Id} : \overline{k}^{\Gamma_\phi} \to \overline{k}$ is the identity inclusion. Likewise we can identify Γ/Γ_ϕ and $\Gamma\phi$ as Γ-sets via the map $\gamma\Gamma_\phi \mapsto \gamma\phi$. By the correspondence between Γ-sets and étale algebras we conclude $\widetilde{E^\phi}$ is isomorphic to the étale algebra whose idempotents are $\Gamma\phi$. If $\Gamma\phi = \Gamma\phi\sigma$ this gives us the result. Otherwise, E^ϕ has idempotents $\Gamma\phi \sqcup \Gamma\phi\sigma$. As the action of Γ is from the left on $\Gamma\phi\sigma$ it follows that as Γ-sets $\Gamma\phi\sigma$ is isomorphic to $\Gamma\phi$. Thus we conclude $E^\phi = \widetilde{E^\phi} \times \widetilde{E^\phi}$. □

Definition 3.2.4. Let (E, σ) be an étale algebra with involution over k and let ϕ be a σ-type of E. There is a natural map $N_\phi : E \to E^\phi$ which is defined by:

$$N_\phi\left(\sum_\rho a_\rho e_\rho\right) = \sum_{\phi_i \in (\Gamma\phi \cup \Gamma\phi\sigma)} \left(\prod_{\rho\in\phi_i} a_\rho\right) e_{\phi_i}.$$

This map is called the σ-**reflex norm** of the σ-type ϕ.

We want to show that this map, which a priori maps $E \otimes_k \overline{k}$ to $E^\phi \otimes_k \overline{k}$, actually maps E to $E^\phi = (E^\phi \otimes_k \overline{k})^\Gamma$. Since $E = (E \otimes_k \overline{k})^\Gamma$ we have that for $\gamma \in \Gamma$ and $\sum_\rho a_\rho e_\rho \in E$ the formula:

$$\sum_\rho a_\rho e_\rho = \gamma\left(\sum_\rho a_\rho e_\rho\right) = \sum_\rho \gamma(a_\rho) e_{\gamma\circ\rho}$$

implies that $\gamma(a_\rho) = a_{\gamma\circ\rho}$. Using this we check that:

$$\gamma\left(\prod_{\rho\in\phi_i} a_\rho\right) = \prod_{\rho\in\phi_i} \gamma(a_\rho) = \prod_{\rho\in\phi_i} a_{\gamma\circ\rho} = \prod_{\rho\in\gamma(\phi_i)} a_\rho.$$

Finally we may check that:

$$\begin{aligned}\gamma\left(N_\phi\left(\sum_\rho a_\rho e_\rho\right)\right) &= \sum_{\phi_i\in(\Gamma\phi\cup\Gamma\phi\sigma)} \gamma\left(\prod_{\rho\in\phi_i} a_\rho\right) e_{\gamma\phi_i} \\ &= \sum_{\phi_i\in(\Gamma\phi\cup\Gamma\phi\sigma)} \left(\prod_{\rho\in\gamma(\phi_i)} a_\rho\right) e_{\gamma\phi_i} \\ &= N_\phi\left(\sum_\rho a_\rho e_\rho\right).\end{aligned}$$

Hence we conclude that $N_\phi\left(\sum_\rho a_\rho e_\rho\right) \in (E^\phi \otimes_k \overline{k})^\Gamma = E^\phi$.

Proposition 3.2.5 (Computing σ-reflex algebras)**.** *We summarize some results which allow for the computation of σ-reflex algebras.*

1. *Let E be a field with σ an involution of E and let ϕ be a σ-type of E. Then $E^\phi = \widetilde{E^\phi}$ as above.*
2. *Let F be an étale algebra and let $(E, \sigma) = (F \times F, \sigma)$, where σ interchanges the factors F. Then there are a number of different σ-types of E:*

(a) *Let* $\phi = \mathrm{Hom}(F, \overline{k}) \subset \mathrm{Hom}(F \times F, \overline{k})$ *correspond to maps on the first factor. Then* $E^\phi = k \times k$ *where* σ *acts by interchanging factors.*

(b) *Fix one element* $\rho \in \mathrm{Hom}(F, \overline{k})$ *and set* $\phi = (\mathrm{Hom}(F, \overline{k}) \setminus \{\rho\}) \cup \{\rho \circ \sigma\}$*. Then* $E^\phi = \rho(F) \times \rho(F)$ *where* σ *acts by interchanging factors.*

(c) *More generally one any choice of* $S \subset \mathrm{Hom}(F, \overline{k})$ *one can take* $\phi = \big(\mathrm{Hom}(F, \overline{k}) \setminus S\big) \cup S\sigma$*. Then* $E^\phi = L \times L$ *where* σ *acts by interchanging factors and where* $L = \widetilde{E^\phi} \subseteq \underset{\rho \in S}{\cup} \mathrm{im}(\rho)$*.*

3. *Let* (E_1, σ_1) *and* (E_2, σ_2) *be algebras with involutions. A* σ*-type for* $(E, \sigma) = (E_1 \times E_2, \sigma_1 \times \sigma_2)$ *is of the form* $\phi = \phi_1 \sqcup \phi_2$*, where the* ϕ_i *are* σ_i*-types for* E_i*. Then* $\widetilde{E^\phi} \simeq \widetilde{E_1^{\phi_1}}\widetilde{E_2^{\phi_2}}$ *and so the factors of* E^ϕ *are the composite of those of the* $E_i^{\phi_i}$*.*

Proof. In each case the proof amounts to a direct application of Proposition 3.2.3 together with a computation of Γ_ϕ. For case (1), where E is a field, Proposition 3.2.3 is the complete result. For case (2) where $E = F \times F$ and the factors are interchanged by σ, we note that the orbits of Γ on $\mathrm{Hom}_{k-alg}(E, \overline{k})$ can be decomposed into those factoring through the first F factor and those factoring through the second. Thus Γ_ϕ is just $\{\gamma \in \Gamma \mid \gamma S = S\}$ where $S \subset \mathrm{Hom}(F, \overline{k})$ is the set describing ϕ as in each of the subcases of (2). It is then clear that Γ_ϕ contains $\cap_{\rho \in S} \mathrm{Gal}(\overline{k}/\mathrm{im}(\rho))$. From this one concludes the result in the special cases of $S = \varnothing$ or $S = \{\rho\}$. In case (3) where $E = E_1 \times E_2$, it is clear that $\Gamma_\phi = \Gamma_{\phi_1} \cap \Gamma_{\phi_2}$ which implies the result. □

Corollary 3.2.6. *Write* $(E, \sigma) = \times_i (E_i, \sigma_i)$ *as a direct product where each* $E_i^{\sigma_i}$ *is a field. Then* E^Φ *is a product of even degree field extensions if and only if* E_i *is a field for at least one* i*.*

Proof. If every factor E_i is of the form $E_i^\sigma \times E_i^\sigma$ with σ_i interchanging factors then $E = F \times F$ for $F \simeq \times_i E_i^\sigma$ with σ interchanging factors. Then by the proposition above there exists ϕ with $E^\phi = k \times k$ and thus one of the direct factors of E^Φ is k.

Conversely, by the computations above every factor of E^ϕ is formed as a composite extension of $\widetilde{E_i^{\phi_i}}$. If there exists a factor E_i which is a field then for all ϕ_i the field $\widetilde{E_i^{\phi_i}}$ is even degree. It follows that every factor of E^Φ contains an even degree subextension of the form $\widetilde{E_i^{\phi_i}}$ and so E^Φ is a product of even degree field extensions. □

Proposition 3.2.7 (Localization of Reflex Algebras)**.** *Suppose k is a number field, p be a prime of k (finite or infinite) and let k_p be the completion of k at p. By the localization of (E, σ) and (E^ϕ, σ) at p we mean the algebras $(E_p = E \otimes_k k_p, \sigma_p)$ and $((E^\phi)_p = E^\phi \otimes_k k_p, \sigma_p)$. Let $G = \mathrm{Gal}(\overline{k_p}/k_p)\backslash\Gamma/\Gamma_\phi$, then:*

$$(E^\phi)_p = \bigtimes_{\overline{g} \in G} (E_p)^{(g\phi)_p},$$

where g is any representative of the coset $\overline{g}$. In particular, $(E^\Phi)_p = (E_p)^{\Phi_p}$.

Proof. The idempotents of E_p and $(E^\phi)_p$ are in natural bijection with those of E and E^ϕ, respectively. That is, by fixing a single map $\overline{k} \hookrightarrow \overline{k_p}$ we obtain a Galois equivariant bijection $\mathrm{Hom}_{k-alg}(E, \overline{k}) \simeq \mathrm{Hom}_{k_p-alg}(E_p, \overline{k_p})$ with respect to the associated inclusion $\Gamma_p = \mathrm{Gal}(\overline{k_p}/k_p) \hookrightarrow \mathrm{Gal}(\overline{k}/k)$. This naturally induces a bijection between the set of σ-types for (E, σ) and σ_p-types for (E_p, σ_p). However, because Γ_p is only a subgroup of Γ, the Galois orbit of ϕ_p in Φ_p under Γ_p may be strictly smaller than the Galois orbit of ϕ in Φ under Γ. Hence, it may happen that $(E_p)^{\phi_p} \neq (E^\phi)_p$. In order to capture all of the orbits recall $G = \Gamma_p\backslash\Gamma/\Gamma_\phi$ so that:

$$\Gamma\phi = \bigsqcup_{\overline{g} \in G} \Gamma_p(g\phi),$$

where g is any representative of the coset $\overline{g}$. It follows that:

$$(E^\phi)_p = \bigtimes_{\overline{g} \in G} (E_p)^{(g\phi)_p}.$$

$\square$

3.2.2 Algebraic Tori

We now recall some basic properties of algebraic tori in linear algebraic groups.

Definition 3.2.8. A k-algebraic group is an **algebraic torus** T if it satisfies any of the following equivalent properties (see [Bor91, 8.4 and 8.5] for a proof of the equivalence):

1. T is connected and diagonalizable over $\overline{k}$.
2. T is connected, abelian and all its elements are semisimple.
3. $\overline{k}[T]$ is spanned by $X^*(T) = \mathrm{Hom}_{\overline{k}}(T, \mathbb{G}_m)$.
4. $T_{\overline{k}} \simeq \mathbb{G}_m^n$ for some n.

Given any k-rational representation of T into GL_m there exists a collection $\Omega \subset X^*(T)$ of characters that appear once the representation is diagonalized over $\overline{k}$. We may consider the map:

$$T_{\overline{k}} \to \prod_{\chi\in\Omega} \mathbb{G}_m \qquad t \mapsto (\chi(t))_{\chi\in\Omega}$$

where the natural Galois action of Γ on T is by permuting the χ as per the action of Γ on $X^*(T)$. The descent data needed to recover the isomorphism class of a k-torus of rank n from its $\overline{k}$-isomorphism with $\mathbb{G}_m^n$ is the specification of the Galois action on $X^*(T) \simeq \mathbb{Z}^n$. See [PR94, 2.2.4] for a discussion of Galois descent as it relates to the classification of tori. The key result is:

Proposition 3.2.9. *There exists a contravariant equivalence of categories between k-isomorphism classes of algebraic tori of rank n and $\mathbb{Z}[\Gamma]$-modules which as $\mathbb{Z}$-modules are torsion free and of rank n. The equivalence takes $T \mapsto X^*(T)$.*

Specifying a Galois action on $X^*(T)$ is equivalent to specifying the Galois action on any Galois stable spanning set $\Omega \subset X^*(T)$, in particular those spanning sets arising from faithful representations. Moreover, for a fixed reductive group G of rank n and for any two $\overline{k}$-conjugate tori $T_1, T_2 \subset G$, the sets $\Omega_{T_1}, \Omega_{T_2}$ can be identified (non-canonically). In particular, to classify the k-isomorphism classes of maximal tori contained in G, it suffices to consider a single such spanning set $\Omega \subset \mathbb{Z}^n$. Then any k-torus in G gives a Galois action on Ω which in turn gives rise to a representation $\Gamma \to \mathrm{GL}_n(\mathbb{Z})$. One may then study the tori knowing only that they arise from a Γ-set Ω which spans $\mathbb{Z}^n$. One should note that the condition $T \subset G$ may impose further conditions on which Γ-actions on Ω are possible.

Proposition 3.2.10. *Let Ω be a finite Γ-invariant set of generators of $X^*(T)$. Let $E = E_\Omega$ be the étale algebra whose idempotents are the Γ-set Ω. Consider the torus $T_E := \mathrm{Res}_{E/k}(\mathbb{G}_m)$, that is, the torus such that for any k-algebra R we have $T_E(R) = (E \otimes R)^*$. Then $T \hookrightarrow T_E$.*

Proof. First we note that $X^*(T_E) = \mathbb{Z}^\Omega$. We thus obtain a natural $\mathbb{Z}$-linear map from $X^*(T_E) \to X^*(T)$ by taking Ω, the basis of $X^*(T_E)$, to Ω as a spanning set of $X^*(T)$. This map is surjective and Γ-equivariant thus inducing a surjective map $k[T_E] \to k[T]$ which corresponds to an injective map $T \hookrightarrow T_E$. $\square$

Definition 3.2.11. If E is an étale algebra over k we say a k-torus S is of **type** E if $S \hookrightarrow T_E$ and E contains no proper subalgebras with this property.

Note that any embedding of $S \hookrightarrow T_E$ (where S is of type E) arises as above. To see this consider the representation of S arising from the regular representation of T_E on E. Note also that the Galois closure of the composition of fields which comprise E is a minimal splitting field for the torus S.

Example. Let $L \subset E$ be étale algebras over k and consider $\chi \in \mathrm{Hom}_k(T_E, T_L)$ corresponding to $\chi = N_{E/L}$, then $\mathrm{Ker}(\chi)^0 \subset T_E$ is a torus of type E.

Definition 3.2.12. Let (E, σ) be an étale algebra with involution over k and put $\chi = N_{E/E^\sigma}$. Then we define:

$$T_{E,\sigma} = \mathrm{Ker}(\chi)^0 = \{t \in T_E | t\sigma(t) = 1\}.$$

We remark that under the natural action of T_E on E as a k-vector space, $T_{E,\sigma}$ preserves the bilinear forms defined by:

$$B_{E,\sigma,\lambda}(x, y) = \mathrm{Tr}_{E/k}(\lambda x \sigma(y)),$$

where $\lambda \in E^\sigma$. Moreover, $T_{E,\sigma}$ is a maximal torus in the orthogonal group attached to this bilinear form.

In the case where E is of dimension $2n+1$ but E^σ has dimension n, we find that $E = E' \times k$, where σ acts trivially on the k summand. The only difference with the even case is that one must then take the connected component of the identity to ensure the resulting group is connected.

Proposition 3.2.13. *Let q be a quadratic form over k and let O_q be the associated orthogonal group. Let $T \subset \mathrm{O}_q$ be a maximal k-torus. Then there exists an étale algebra with involution (E, σ) over k such that $T = T_{E,\sigma}$. Moreover, suppose $T_{E,\sigma} \subset \mathrm{O}_q$ is a maximal torus. Then $q(x) = q_{E,\lambda}(x) = \frac{1}{2}\mathrm{Tr}_{E/k}(\lambda x \sigma(x))$ for some choice of $\lambda \in (E^\sigma)^*$.*

Proof. We shall give a sketch of the construction that all tori are of this form, for details see [BCKM03, Prop. 3.3]. As in the discussion relating descent data of tori to étale algebras we observe that for any $T \subset \mathrm{O}_q$ the set of characters Ω_T which appear in the representation is of the form:

$$\Omega_T = \{\chi_1, \ldots, \chi_n, \chi_1^{-1}, \ldots, \chi_n^{-1}\}$$

(including also the trivial character with multiplicity one if $\dim(q)$ is odd) with the χ_i forming a basis of $X^*(T)$. One checks easily that on the étale algebra E which has idempotents indexed by Ω_T one can construct an involution σ

by interchanging χ_i and χ_i^{-1} for each i. It is straightforward to check that $T \cong T_{E,\sigma}$, and σ restricts to the adjoint involution with respect to q.

The statement concerning the structure of quadratic forms preserved by such tori is the content of any of [Shi80, Prop. 5.4],[BCKM03, Prop. 3.9] and [Fio09, Thm. 4.4.1]. We present the argument of [BCKM03]. By interpreting the quadratic space as a rank one E-module, we may consider the adjoint maps for the two quadratic forms (that is, q and $q_{E,1}$), both of which are preserved by T, as being isomorphisms from E to its linear dual. Hence, composing one with the inverse of the other, $\alpha = \mathrm{ad}(q_{E,1})^{-1} \circ \mathrm{ad}(q) : E \to E$ gives an E-automorphism of E which must correspond to multiplication by a unit λ. We may then conclude that $q = q_{E,\lambda}$. □

3.2.3 Clifford Algebras

Definition 3.2.14. Let (V, q) be a quadratic space over k. We define the associated **Clifford algebra** to be:

$$\mathrm{C}_q = \bigoplus_{i \geq 0} V^{\otimes i} / \langle x \otimes x - q(x) \rangle.$$

The involution $v \mapsto -v$ on V induces an involution of C_q. We define the even and odd parts of the Clifford algebra to be respectively the $+1$ and -1 eigenspaces for this involution and denote them C_q^0 and C_q^1.

The structure of the Clifford algebra as a graded algebra is well known; in particular we have:

Theorem 3.2.15. *If $m = \dim(V)$ is odd then:*

1. $Z(\mathrm{C}_q) \simeq k(\sqrt{d})$, *where* $d = (-1)^{(m-1)/2} D(q)$ *and* $D(q)$ *is the discriminant of* q,
2. C_q^0 *is a central simple algebra over* k *and* $\mathrm{C}_q \simeq \mathrm{C}_q^0 \hat{\otimes} Z(\mathrm{C}_q)$ *(where* $\hat{\otimes}$ *is the graded tensor product), and*
3. C_q *is a central simple algebra over* $Z(\mathrm{C}_q)$ *(if the centre is not a field we mean* $\mathrm{C}_q \simeq \mathrm{C}_q^0 \times \mathrm{C}_q^0$*).*

If $m = \dim(V)$ is even then:

1. C_q *is a central simple algebra over* k*,*
2. $Z(\mathrm{C}_q^0) = k(\sqrt{d})$*, where* $d = (-1)^{m/2}D(q)$ *and* $D(q)$ *is the discriminant of* q*, and*
3. *if* $\mathrm{C}_q \simeq \mathrm{M}_t(A)$ *(where* A *is a division algebra) then* $\mathrm{C}_q^0 \simeq \mathrm{M}_{t/2}(A \otimes Z(\mathrm{C}_q^0))$*.*

Proof. The above theorem is essentially the content of [Lam05, V.2.4-5]. The final statement in the even case is not explicitly stated in [Lam05] but follows from the proof of [Lam05, IV.3.8]. □

Definition 3.2.16. Let (V, q) be a non-degenerate quadratic space over k of dimension m with an orthogonal basis $\{e_i\}$, where we write $q(e_i) = a_i$. We then define the following invariants:

- The **discriminant** $D(q) = \prod_i a_i$ viewed as an element of $k^*/(k^*)^2$.
- The **Hasse invariant** $H(q) = \prod_{i<j}(a_i, a_j)$, where (a_i, a_j) is the Hilbert symbol (see [Ser73, Ch. III] and [Ser79, Ch. XIV]), viewed as an element of $\mathrm{Br}(k) = H^2(\Gamma, \pm 1)$.
- The **Witt invariant** $W(q) = \begin{cases} [\mathrm{C}_q^0], & m = 1 \mod 2, \\ [\mathrm{C}_q], & m = 0 \mod 2 \end{cases}$, where $[B]$ denotes the Brauer class of B, viewed as an element of $\mathrm{Br}(k) = H^2(\Gamma, \pm 1)$.
- The **signature** $(r_\rho, s_\rho)_\rho$ at each real infinite place ρ of k.
- The **orthogonal discriminant** $D^{\mathrm{orth}}(q) = \delta(Z(\mathrm{C}_q^0)/k)$ viewed as an element of $k^*/(k^*)^2$.
- The **orthogonal Witt invariant** $W^{\mathrm{orth}}(q) = [\mathrm{C}_q^0]$ viewed as an element of $\mathrm{Br}(Z(\mathrm{C}_q^0))$.

Remark. The first four invariants are properly invariants of q, indeed when k is a number field they entirely determine q. The latter three are invariants of the orthogonal group associated to q. That is, O_q determines q only up to similarity (rescaling by k^*). Likewise, the signature, orthogonal discriminant and orthogonal Witt invariant determine q up to similarity.

The last two invariants are not standard.

Proposition 3.2.17. *Let* $m = \dim(V)$. *We have the following relations among the above invariants:*

1. $D(q) = \begin{cases} (-1)^{(m-1)/2}\delta(Z(\mathrm{C}_q)), & m = 1 \mod 2, \\ (-1)^{m/2}\ \delta(Z(\mathrm{C}_q^0)), & m = 0 \mod 2, \end{cases}$
2. $H(q) = W(q) \cdot (-1, D(q))^{(m-1)(m-2)/2} \cdot (-1,-1)^{(m+1)m(m-1)(m-2)/8}$, *where the product is in the Brauer group,*
3. $W^{orth}(q) = [W(q) \otimes Z(\mathrm{C}_q^0)]$.

These properties are the content of [Lam05, V.2.5, V.3.20 and V.2.4-5], respectively.

Theorem 3.2.18. *Let* (E, σ) *be an étale algebra with involution over* k *such that* $T_{E,\sigma} \hookrightarrow \mathrm{O}_q$ *as a maximal subtorus. Then* E^Φ *embeds into* C_q^0 *as a maximal étale algebra stable under the canonical involution of* C_q. *Moreover, the canonical involution restricts to* σ *on* E^Φ.

Proof. We claim that it is sufficient to consider the case of $\dim(V)$ even. Indeed, if $\dim(V)$ is odd then we can decompose $V = V' \oplus \mathrm{span}_k(\vec{v})$ where $T_{E,\sigma}$ acts trivially on $\vec{v}$. With $q' = q|_{V'}$ and $T_{E,\sigma} \hookrightarrow \mathrm{O}_{q'}$ and using that $\mathrm{C}_{q'} \hookrightarrow \mathrm{C}_q$ we obtain the result.

We may identify the space V with E. Thus $V \otimes_k \overline{k}$ is identified with $E \otimes_k \overline{k}$. Suppose under the isomorphism of V with E we have that $q(x) = \frac{1}{2}\mathrm{Tr}_{E/k}(\lambda x \sigma(x))$. We use $\{e_\rho\}_{\rho \in \mathrm{Hom}_{k-alg}(E,\overline{k})}$ as the generators for the Clifford algebra after base change to $\overline{k}$. We note that we recover both C_q^0 and V as the Galois invariants of $\mathrm{C}_q^0 \otimes_k \overline{k}$ and $V \otimes_k \overline{k}$, respectively. Moreover, as the inclusion $V \hookrightarrow \mathrm{C}_q$ is k-rational, the Galois actions on the $\{e_\rho\}$ viewed as elements of $V \otimes_k \overline{k}$ or as elements of $\mathrm{C}_q \otimes_k \overline{k}$ is the same.

For each $\rho \in \mathrm{Hom}_{k-alg}(E, \overline{k})$ set $\delta_\rho = \frac{1}{\rho(\lambda)} e_\rho \otimes e_{\rho\circ\sigma} \in \mathrm{C}_q^0$. These elements satisfy the following properties:

1. The action of σ on δ_ρ agrees with the canonical involution of C_q,

2. $\delta_\rho^2 = \delta_\rho$,

3. $\delta_\rho \sigma(\delta_\rho) = 0$ and $\delta_\rho + \sigma(\delta_\rho) = 1$,

4. the δ_ρ all commute, and

5. the Galois action on $\{\delta_\rho\}$ is the same as that on $\{e_\rho\}$.

Now for each σ-type $\phi \in \Phi$ of E set $\delta_\phi = \prod_{\rho \in \phi} \delta_\rho$. These elements then satisfy the following properties:

1. $\delta_\phi^2 = \delta_\phi$,

2. $\delta_{\phi_1}\delta_{\phi_2} = 0$ for $\phi_1 \neq \phi_2$,

3. $\sum_\phi \delta_\phi = \prod_\rho (\delta_\rho + \delta_{\rho\circ\sigma}) = 1$, and

4. the Galois action on $\{\delta_\phi\}_{\phi\in\Phi}$ is the same as that on $\{\phi\}_{\phi\in\Phi}$.

Thus the δ_ϕ are Galois stable orthogonal idempotents and hence by taking Galois invariants give an étale subalgebra of C_q^0. As the Galois action on idempotents matches that of E^Φ, this gives an embedding of E^Φ into C_q^0. Moreover, this algebra is preserved by the canonical involution of C_q, and the involution restricts to σ on it.

The algebra is maximal as an étale subalgebra for dimension reasons. □

Remark. We have the map $\varphi : E \to \mathrm{C}_q^0$ given by:

$$\varphi\left(\sum_\rho x_\rho e_\rho\right) = \sum_{\phi\in\Phi}\left(\prod_{\rho\in\phi} x_\rho\right)\delta_\phi = \prod_{\rho\in\phi'}(x_\rho\delta_\rho + x_{\rho\circ\sigma}\delta_{\rho\circ\sigma})$$

where ϕ' is any σ-reflex type of E. It is a multiplicative map (it is the reflex norm followed by the inclusion). Moreover, the image of $T_{E,\sigma}$ lies in the spin group, with φ being a section of the natural covering map $\theta : \mathrm{Spin}_q \to \mathrm{O}_q$. Indeed, we have $\theta(\varphi(\sum_\rho x_\rho e_\rho))(1_E) = \sum_\rho x_\rho x_{\rho\circ\sigma}^{-1} e_\rho$. Note that $T_{E,\sigma}$ consists of those elements where $x_\rho = x_{\rho\circ\sigma}^{-1}$, and hence $\theta \circ \phi = x^2$ on $T_{E,\sigma}$.

3.3 Computing Invariants

In this section we will compute the invariants of the forms $\mathrm{Tr}_{E/k}(\lambda x \sigma(x))$.

Recall that for L/F a finite extension of fields and $\mathcal{O}$ an order of L, the discriminant $\delta_{\mathcal{O}/\mathcal{O}_F}$ of $\mathcal{O}$ is that of the F-quadratic form $Q(x) = \mathrm{Tr}_{L/F}(x^2)$ on $\mathcal{O}$.

Lemma 3.3.1. *Let F be a number field or a p-adic field and let $L = F(z)$ be an algebraic extension of degree m with $f_z(X) \in \mathcal{O}_F[X]$ the minimal (monic) polynomial of z. Let $\delta_{L/F}(z)$ be the discriminant of the order $\mathcal{O}_F[z] \subset L$. Let $\lambda \in L^*$ and consider the quadratic form $Q(x) = \mathrm{Tr}_{L/F}(\lambda x^2)$. Then:*

$$\begin{aligned} D(Q) &= N_{L/F}(\lambda)\delta_{\mathcal{O}_F[z]/\mathcal{O}_F}(z) \\ &= N_{L/F}(\lambda)\left(\prod_{i<j}(\rho_i(z) - \rho_j(z))\right)^2 \\ &= N_{L/F}(\lambda)(-1)^{m(m-1)/2}N_{L/F}(f_z'(z)), \end{aligned}$$

where ρ_i are the m embeddings $L \hookrightarrow \overline{F}$.

Proof. These are well-known equalities. To compute $\det\left(\mathrm{Tr}_{L/F}(\lambda z^\ell z^j)\right)_{\ell j}$ factor the matrix as:

$$\left(\mathrm{Tr}_{L/F}(\lambda z^\ell z^j)\right)_{\ell j} = \left(\rho_i(\lambda z^\ell)\right)_{\ell i} \cdot \left(\rho_i(z^j)\right)_{ij} = \mathrm{diag}(\rho_i(\lambda)) \cdot \left(\rho_i(z)^\ell\right)_{\ell i} \cdot \left(\rho_i(z)^j\right)_{ij}.$$

By applying the Vandermonde determinant formula and a comparing the result to $N_{L/F}(f_z'(z))$ yields the result. □

Lemma 3.3.2. *Let L/F be an extension of either number fields or local fields. The corestriction (or transfer map) $\mathrm{Cor}_{L/F} : \mathrm{Br}(L)[2] \to \mathrm{Br}(F)[2]$ satisfies:*

$$\mathrm{Cor}_{L/F}((a, b)_L) = (a, N_{L/F}(b))_F$$

for all $a \in F^*, b \in L^*$.

This is [Ser79, Ex. XIV.3.4].

The second part of the following result is the main theorem of the paper of Brusamarello–Chuard-Koulmann–Morales and will be important in the sequel.

Theorem 3.3.3. *Let (E,σ) be an étale algebra with involution over k of dimension $2n$ and let $\lambda \in E^{\sigma *}$. Then the invariants of $q_{E,\lambda}(x) = \frac{1}{2}\operatorname{Tr}_{E/k}(\lambda x \sigma(x))$ are:*

1. $D(q_{E,\lambda}) = (-1)^n \delta_{E/k}$,
2. $H(q_{E,\lambda}) = H(q_{E,1}) \cdot \operatorname{Cor}_{E^\sigma/k}(\lambda, \delta_{E/E^\sigma})$,
3. $W(q_{E,\lambda}) = W(q_{E,1}) \cdot \operatorname{Cor}_{E^\sigma/k}(\lambda, \delta_{E/E^\sigma})$.

Proof. The first statement is well known, though we include a proof for the convenience of the reader. By writing $E = E^\sigma(\sqrt{d}) := E^\sigma[y]/(y^2 - d)$ we may write $x \in E$ as $x = s + t\sqrt{d}$. Then we observe that $q_{E,\lambda}(x) = \operatorname{Tr}_{E^\sigma/k}(\lambda s^2) + \operatorname{Tr}_{E^\sigma/k}(-\lambda d t^2)$. Set $Q_\lambda(s) = \operatorname{Tr}_{E^\sigma/k}(\lambda s^2)$ and $Q_{-\lambda d}(t) = \operatorname{Tr}_{E^\sigma/k}(-\lambda d t^2)$ so that $q_{E,\lambda} \simeq Q_\lambda \oplus Q_{-d\lambda}$. We thus have $D(q_{E,\lambda}) = D(Q_\lambda)D(Q_{-\lambda d})$. By Lemma 3.3.1 this gives:

$$
\begin{aligned}
D(q_{E,\lambda}) &= N_{E^\sigma/k}(\lambda) \cdot \delta_{E^\sigma/k} \cdot N_{E^\sigma/k}(-\lambda d) \cdot \delta_{E^\sigma/k} \\
&= N_{E^\sigma/k}(-d) = (-1)^n N_{E^\sigma/k}(d) \pmod{(k^*)^2}.
\end{aligned}
$$

By observing that $\delta_{E/k} = N_{E^\sigma/k}(\delta_{E/E^\sigma})\delta^2_{E^\sigma/k}$ (see [Ser79, Prop. III.4.8]) and that $\delta_{E^\sigma(\sqrt{d})/E^\sigma} = d \pmod{(k^*)^2}$ we conclude the result.

The second statement is the content of [BCKM03, Thm. 4.3]. The final statement follows from the first two statements by using Proposition 3.2.17. The proposition states that the Hasse and Witt invariants differ by a constant depending only on the discriminant. As $D(q_{E,\lambda}) = D(q_{E,1})$ the second and third statement are thus equivalent. □

The above theorem, together with some easy special cases, is largely sufficient for the proof of our main result (see the proof of Lemma 3.5.5 for how it comes into play). However, we would like to give more precise formulas for the Hasse and Witt invariants that can be directly computed from the data describing the fields. This has the advantage of giving the information we need in the special cases, as well as being of interest in its own right. The first step is a lemma which is useful for explicitly calculating traces.

Lemma 3.3.4 (Euler)**.** *Let $L = F(z)$ be a finite separable extension of F of degree m with $f_z(x) \in \mathcal{O}_F[x]$ the minimal (monic) polynomial of z. We then have:*

$$\mathrm{Tr}_{L/F}\left(\frac{z^\ell}{f_z'(z)}\right) = \begin{cases} 1, & \ell = m-1 \\ 0, & 0 \le \ell < m-1. \end{cases}$$

This is [Ser79, III.6, Lem. 2].

The next step is to show that the fields in which we are interested are always primitively generated in a simple way.

Proposition 3.3.5. *Let F/k be any finite separable extension of infinite fields of characteristic not 2, and let E/F be a quadratic extension. Then there exists $\alpha \in E$ such that $E = k(\alpha)$ and $F = k(\alpha^2)$.*

Proof. Suppose $E = F(\sqrt{\beta})$ with $\beta \in F$ and $F = k(\gamma)$. We claim it suffices to show that there exists an $\ell \in k$ such that $F = k((\ell+\gamma)^2\beta)$. Indeed, if $F = k((\ell+\gamma)^2\beta)$ then $F \subset k((\ell+\gamma)\sqrt{\beta})$ and so $\gamma \in k((\ell+\gamma)\sqrt{\beta})$. Hence $\sqrt{\beta} \in k((\ell+\gamma)\sqrt{\beta})$ and thus $F(\sqrt{\beta}) = k((\ell+\gamma)\sqrt{\beta})$. Consequently, taking $\alpha = (\ell+\gamma)\sqrt{\beta}$ gives the result.

Now let $\ell_1, \ell_2, \ell_3 \in k$ be distinct values such that $k((\ell_i+\gamma)^2\beta)$ are all the same field, say L. Since all these values are in the same field, so are their linear combinations. We compute that:

$$\frac{(\ell_1+\gamma)^2\beta}{(\ell_2-\ell_1)(\ell_3-\ell_1)} + \frac{(\ell_2+\gamma)^2\beta}{(\ell_1-\ell_2)(\ell_3-\ell_2)} + \frac{(\ell_3+\gamma)^2\beta}{(\ell_1-\ell_3)(\ell_2-\ell_3)} = \beta.$$

This shows that $\beta \in L$. We then observe that:

$$\frac{1}{(\ell_2-\ell_1)}\left((\ell_2+\gamma)^2 - (\ell_1+\gamma)^2\right) - \ell_2 - \ell_1 = 2\gamma.$$

This proves that $\gamma \in L$, and hence $L = F = k((\ell_1+\gamma)^2\beta)$. □

The following lemma combines the above two results to show that for a particular choice of $\lambda \in E^\sigma$ the invariants of $q_{E,\lambda}$ can be computed explicitly.

Lemma 3.3.6. *Let F/k be an extension of number fields of degree m. Suppose $F = k(z)$. Let $E = F(\sqrt{z}) = k(\sqrt{z})$ and σ be the non-trivial element of $\mathrm{Gal}(E/F)$. Let f_z be the minimal (monic) polynomial for z over k. View E as a $2m$-dimensional k-vector space equipped with the quadratic form $Q(x + y\sqrt{z}) = q_{E,-f_z'(z)^{-1}}(x + \sqrt{z}y)$. Then:*

1. $H(Q) = (-1,-1)_k^{m(m-1)/2} \cdot (N_{F/k}(z), -1)_k^{m-1}$, *and*
2. $W(Q) = 1$.

Proof. Let $\widetilde{E} = F(\sqrt{-z}) = k(\sqrt{-z})$ and notice that $f_{\sqrt{-z}}(X) = f(-X^2)$ is the minimal polynomials of $\sqrt{-z}$. Hence $f'_{\sqrt{-z}}(X) = -2Xf_z'(-X^2)$, in particular $f'_{\sqrt{-z}}(\sqrt{-z}) = -2\sqrt{-z}f_z'(z)$. Therefore under the identification of $F \times F$, using its natural basis, with $\widetilde{E}$ under the basis $1, \sqrt{-z}$ and writing $w = x + y\sqrt{-z}$ we compute:

$$\begin{aligned} q_{E,-f_z'(z)^{-1}}(x + \sqrt{z}y) &= \mathrm{Tr}_{F/k}\left(\frac{-1}{f_z'(z)}(x^2 - zy^2)\right) \\ &= \mathrm{Tr}_{\tilde{E}/k}\left(\frac{-1}{2f_z'(z)}w^2\right) \\ &= \mathrm{Tr}_{\tilde{E}/k}\left(\frac{\sqrt{-z}}{f'_{\sqrt{-z}}(\sqrt{-z})}w^2\right). \end{aligned}$$

Now, by Lemma 3.3.4, for any extension $k(\alpha)/k$ of degree n, the matrix for the quadratic form

$$\widetilde{Q}(x) = \mathrm{Tr}_{k(\alpha)/k}\left(\frac{\alpha}{f_\alpha'(\alpha)}x^2\right)$$

in the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ has the shape:

$$\begin{pmatrix} 0 & & \cdots & & 1 & a_1 \\ & & & 1 & a_1 & a_2 \\ \vdots & & \iddots & & & \\ & 1 & & \iddots & & \vdots \\ 1 & a_1 & & & & \\ a_1 & a_2 & & \cdots & & a_n \end{pmatrix},$$

for some values $a_i \in k$. Note that the form is non-degenerate on the span of $\{1, \alpha, \ldots, \alpha^{n-2}\}$ and let β be a generator for the orthogonal complement. Then $\{1, \alpha, \ldots, \alpha^{n-2}, \beta\}$ is a basis and the matrix for $\widetilde{Q}$ with respect to it is:

$$A = \begin{pmatrix} 0 & & \cdots & & 1 & 0 \\ & & & 1 & a_1 & 0 \\ \vdots & & \iddots & & & \\ & 1 & & \iddots & & \vdots \\ 1 & a_1 & & & & \\ 0 & 0 & & \cdots & & Y \end{pmatrix},$$

for some $Y \in k$.

Lemma 3.3.7. *The matrices:*

$$\begin{pmatrix} 0 & & \cdots & & 1 & \\ & & & 1 & a_1 & \\ \vdots & & \iddots & & & \\ & 1 & & & \vdots & \\ 1 & a_1 & & \cdots & a_n & \end{pmatrix} \quad \textit{and} \quad \begin{pmatrix} 0 & & \cdots & & 1 \\ & & & 1 & 0 \\ \vdots & & \iddots & & \\ & 1 & & & \vdots \\ 1 & 0 & & \cdots & 0 \end{pmatrix}$$

represent the same quadratic form. In particular, denoting by $\langle y_1, \ldots, y_n \rangle$ the diagonal form with diagonals y_i, the quadratic form associated to either matrix *is isomorphic to one of:*

$$\langle 1, -1 \rangle^{\frac{n-1}{2}} \oplus \langle 1 \rangle \quad \text{or} \quad \langle 1, -1 \rangle^{\frac{n}{2}}$$

depending on the parity of n.

Proof. This is a simple inductive argument using the similarity-transform defined by:

$$\begin{pmatrix} 1 & 0 & \cdots & & 0 \\ -a_1 & 1 & & & \\ -a_2 & 0 & \ddots & & \vdots \\ \vdots & & & & \\ -a_{n-1} & & & & \\ -\frac{1}{2}a_n & 0 & & \cdots & 1 \end{pmatrix}.$$

□

It follows from the lemma that $\widetilde{Q}$ is isomorphic to one of:

$$\langle 1, -1 \rangle^{\frac{n-2}{2}} \oplus \langle 1, Y \rangle \quad \text{or} \quad \langle 1, -1 \rangle^{\frac{n-1}{2}} \oplus \langle Y \rangle.$$

Next, by Lemma 3.3.1 we know that the discriminant of $\widetilde{Q}$ is:

$$N_{k(\alpha)/k}(\alpha) N_{k(\alpha)/k}(f'_\alpha(\alpha)^{-1}) \delta_{k(\alpha)/k} = N_{k(\alpha)/k}(\alpha)(-1)^{n(n-1)/2}.$$

We conclude that $Y = N_{k(\alpha)/k}(\alpha)(-1)^{n-1}$ up to squares. In particular, in the case $\alpha = \sqrt{-z}$, we can immediately see that the Hasse invariant of the quadratic form is:

$$\begin{aligned} H(Q) &= (-1,-1)_k^{m(m-1)/2} \cdot (N_{k(\sqrt{-z})/k}(\sqrt{-z}), -1)_k^{m-1} \\ &= (-1,-1)_k^{m(m-1)/2} \cdot (N_{k(z)/k}(z), -1)_k^{m-1}. \end{aligned}$$

Moreover, since the quadratic form has discriminant $(-1)^m N_{k(z)/k}(z)$ we compute using Proposition 3.2.17 that the Witt invariant is:

$$\begin{aligned} W(Q) = & \ ((-1)^m N_{k(z)/k}(z), -1)_k^{m-1} \cdot (-1,-1)_k^{m(m-1)/2} \cdot \\ & \qquad\qquad\qquad (-1,-1)_k^{m(m-1)/2} \cdot (N_{k(z)/k}(z), -1)_k^{m-1} \\ = & \ 1. \end{aligned}$$

□

Combining the above two results, we may now give a general formula for the Hasse and Witt invariants for the forms $q_{E,\lambda}$.

Theorem 3.3.8. *Let $F = k(z)$ be an extension of degree m, let $E = k(\sqrt{z})$, and let $\lambda \in F$. Consider the quadratic form $q_{E,\lambda}(x) = \frac{1}{2}\operatorname{Tr}_{E/k}(\lambda N_{E/F}(x))$. Then:*

1. $H(q_{E,\lambda}) = \operatorname{Cor}_{F/k}((-\lambda f_z'(z), z)_F) \cdot (N_{k(z)/k}(z), -1)_k^{m-1} \cdot (-1,-1)_k^{m(m-1)/2}$, *and*
2. $W(q_{E,\lambda}) = \operatorname{Cor}_{F/k}((-\lambda f_z'(z), z)_F)$.

Proof. From Theorem 3.3.3 we have the following two equations:

$$H(q_{E,\lambda}) = H(q_{E,1}) \cdot \operatorname{Cor}_{F/k}((\lambda, z)_F), \text{ and}$$
$$H(q_{E,-f_z'(z)^{-1}}) = H(q_{E,1}) \cdot \operatorname{Cor}_{F/k}((-f_z'(z), z)_F).$$

Solving for $H(q_{E,1})$ and substituting the results of Lemma 3.3.6 yields:

$$\begin{aligned} H(q_{E,\lambda}) &= H(q_{E,-f_z'(z)^{-1}}) \cdot \operatorname{Cor}_{F/k}(\lambda f_z'(z)) \\ &= (-1,-1)_k^{m(m-1)/2} \cdot (N_{F/k}(z), -1)_k^{m-1} \cdot \operatorname{Cor}_{F/k}((-\lambda f_z'(z), z)_F). \end{aligned}$$

The Witt invariant computation follows similarly. □

3.4 Local Invariant Computations for $\operatorname{Tr}(\lambda x^2)$

The above gives us a global cohomological description of the invariants of the quadratic forms in which we are interested. However, the quadratic forms

$\mathrm{Tr}(\lambda x^2)$, which were studied extensively by Serre (see [Ser84]) and others, are not in general covered by the previous section. Moreover, we have further interest in a detailed local description of these forms as this has applications to computing local densities and discriminant groups. Similar calculations can be found in the work of Epkenhans (see [Epk89, Lem. 1]). The current section gives a description of these quadratic forms in terms of basic combinatorial data regarding the ramification structure of the field extensions involved.

Lemma 3.4.1. *Let F/k be an unramified extension of non-Archimedean local fields of degree f, with residue characteristic different from 2. Let π_k be a uniformizer of k. Let Q_F be any quadratic form on a vector space V over F of dimension n. View V as a k-vector space via restriction of scalars. The form $Q_k(x) = \mathrm{Tr}_{F/k}(Q_F(x))$ on V has invariants:*

$$D(Q_k) = N_{F/k}(D(Q_F))\delta_{F/k}^n, \text{ and}$$
$$H(Q_k) = H(Q_F)\left[(\pi_k, N_{F/k}(D(Q_F)))_k(\pi_k, \delta_{F/k})_k(\pi_k, -1)_k^{f(f-1)/2}\right]^{\nu_{\pi_F}(D(Q_F))}.$$

(By abuse of notation we identify the 2-torsion in the Brauer groups of F and k via the natural isomorphism.)

Proof. It suffices to check the formula for a member of each isomorphism class of quadratic space over V. If $n \geq 3$ by checking the Hasse invariants and discriminants one finds that every isomorphism class of non-degenerate quadratic space over V is represented by one of:

$$\langle 1\rangle^{n-3} \oplus \langle b, \pi_k, ab\pi_k\rangle \quad \text{or} \quad \langle 1\rangle^{n-2} \oplus \langle b, ab\pi_k\rangle,$$

for some $a, b \in \mathcal{O}_F^*$. We refer to these as the first and second cases. In either case by decomposing the form into the diagonal pieces with trivial and non-trivial valuations we may write:

$$\mathrm{Tr}_{F/k}(Q_F) \cong M_1 \oplus \pi_k M_2.$$

In the first case, M_1 has discriminant $\delta_{F/k}^{n-2} N_{F/k}(b)$ and dimension $f \cdot (n-2)$, whereas M_2 has discriminant $N_{F/k}(ab)$ and dimension $2f$. One then computes in the first case that:

$$\begin{aligned} H(Q_k) &= (\pi_k, -1)_k^f \cdot (N(ab), \pi_k)_k \\ &= (\pi_k, -1)_F \cdot (ab, \pi_k)_F \\ &= H(Q_F). \end{aligned}$$

In the second case, M_1 has discriminant $\delta_{F/k}^{n-1} N_{F/k}(b)$ and M_2 has discriminant $\delta_{F/k} N_{F/k}(ab)$. Thus we have:

$$\begin{aligned} H(Q_k) &= (\pi_k, N_{F/k}(b))_k \cdot (\pi_k, N_{F/k}(a))_k^{f-1} \cdot (\pi_k, \delta_{F/k})_k^{fn-1} \cdot (\pi_k, -1)_k^{f(f-1)/2} \\ &= (\pi_k, N_{F/k}(a))_k^{f-1} \cdot (\pi_k, \delta_{F/k})_k \cdot (\pi_k, -1)_k^{f(f-1)/2} \\ &= H(Q_F) \left[(\pi_k, N_{F/k}(D(Q_F)))_k \cdot (\pi_k, \delta_{F/k})_k \cdot (\pi_k, -1)_k^{f(f-1)/2} \right]. \end{aligned}$$

Here we have used the fact that $\delta_{F/k}^f$ is a square in k for an unramified extension.

For the cases $n = 1, 2$ we must check that similar formulas hold for: $\langle b\pi_k, ab\pi_k \rangle, \langle 1, a \rangle, \langle a \rangle, \langle a\pi_k \rangle$. We omit these calculations. □

The results on the structure of trace forms for ramified extensions will rely on the following lemma.

Lemma 3.4.2. *Let L/F be a totally ramified extension of local fields. Let $z = \pi_L$ be a uniformizer of $\mathcal{O}_L$ and $f_z(x)$ be the minimal (monic) polynomial of z. Then f_z is an Eisenstein polynomial and the collection $1, z, z^2, \ldots, z^{m-1}$ is an $\mathcal{O}_F$-basis of $\mathcal{O}_L$ and $N_{L/F}(z)$ is a uniformizer of F.*

See [Ser79, Prop. I.6.18] for a proof.

Before proceeding with the next two lemmas we will introduce some notation. Let L/F be a totally ramified extension of local fields of degree m. Let π_L be a uniformizer of L and set $\pi_F = N_{L/F}(\pi_L)$ to be a uniformizer of

F. Let $f = f_{\pi_L}$ be the minimal monic polynomial of π_L over F. Suppose $u \in \mathcal{O}_L^*$, $v \in \mathcal{O}_F^*$, $0 \leq \ell \leq m$, $k \in \mathbb{Z}$ and set $\lambda = \frac{\pi_F^k}{uv^2\pi_L^\ell f'(\pi_L)}$. We remark that if the residue characteristic is not 2, then for any given $\lambda \in L^*$ there exists corresponding u, v, ℓ, k. Now denote by $Q(x)$ the F-quadratic form on L given by $Q(x) = \mathrm{Tr}_{L/F}(\lambda x^2)$ and consider $M_1 = \mathrm{span}\{uvz^\ell, \ldots, uvz^{m-1}\}$ and $M_2 = \mathrm{span}\{v, \ldots, vz^{\ell-1}\}$ as quadratic subspaces of L.

Lemma 3.4.3. *With the notation as above, we have the following properties of Q, M_1, M_2:*

1. *The discriminant of Q is $D(Q) = (-1)^{m(m-1)/2}u^{-m}\pi_F^{mk-\ell}$.*
2. *The decomposition $L = M_1 \oplus M_2$ is orthogonal with respect to Q.*
3. *The discriminants of $\frac{1}{\pi_F^k}Q|_{M_1}$ and $\frac{1}{\pi_F^{k-1}}Q|_{M_2}$ are respectively:*

$$D(\frac{1}{\pi_F^k}Q|_{M_1}) = (-1)^{(m-\ell)(m-\ell-1)/2}u^{m-\ell} \text{ and}$$
$$D(\frac{1}{\pi_F^{k-1}}Q|_{M_2}) = (-1)^{\ell(\ell+1)/2-m\ell}u^{-\ell}.$$

   Hence these forms are unimodular.

4. *The Hasse invariant is:*

$$H(Q) = (\pi_F, u)^{(m-\ell)\ell} \cdot (\pi_F, -1)^{k(m^2(m-1)/2+\ell^2(1-m))-\ell(m-\ell)(m-\ell-1)/2}.$$

Proof. The formula for the discriminant of Q is Lemma 3.3.1. The orthogonal decomposition is an elementary calculation which follows from Lemma 3.3.4 and Lemma 3.4.2.

Next, noticing that $u \in F$ we can use Lemma 3.3.4 to compute that the matrix representations of $\frac{1}{\pi_F^k}Q|_{M_1}$ and $\frac{1}{\pi_F^{k-1}}Q|_{M_2}$. We see that they are respectively:

$$u\begin{pmatrix} 0 & & \cdots & & 0 & 1 \\ & & & 0 & 1 & * \\ \vdots & & \iddots & & * & \\ & 0 & & \iddots & & \vdots \\ 0 & 1 & * & & & \\ 1 & * & & \cdots & & * \end{pmatrix} \quad \text{and} \quad \frac{1}{u}\begin{pmatrix} * & & \cdots & & * & a \\ & & & & a & 0 \\ \vdots & & \iddots & & & \\ & & & \iddots & & \vdots \\ * & a & 0 & & & \\ a & 0 & & \cdots & & 0 \end{pmatrix},$$

where $a = \frac{\pi_F}{f(0)} = (-1)^m$. One can explicitly calculate the $*$ terms from the coefficients of f, but what is of particular importance is that in both cases one finds that $a_{ij} = a_{lk}$ whenever $i + j = l + k$. As a consequence of this using Lemma 3.3.7 we can explicitly find a change of basis matrix so that the result is of form:

$$u\begin{pmatrix} 0 & & \cdots & & 0 & 1 \\ & & & 0 & 1 & 0 \\ \vdots & & \iddots & & 0 & \\ & 0 & & \iddots & & \vdots \\ 0 & 1 & 0 & & & \\ 1 & 0 & & \cdots & & 0 \end{pmatrix} \quad \text{and} \quad \frac{1}{u}\begin{pmatrix} X & 0 & \cdots & & & 0 \\ 0 & & & & 0 & 1 \\ \vdots & & \iddots & & 1 & 0 \\ & & & \iddots & & \vdots \\ & 0 & 1 & & & \\ 0 & 1 & 0 & \cdots & & 0 \end{pmatrix}.$$

The determinants of the matrices are then:

$$(-1)^{(m-\ell)(m-\ell-1)/2}u^{m-\ell} \text{ and } (-1)^{(\ell-1)(\ell-2)/2}u^{-\ell}X,$$

respectively. Thus knowing $D(Q)$ we have that up to squares X is:

$$X = (-1)^{(\ell-1)(\ell-2)/2+\ell(\ell+1)/2-m\ell}u^{-\ell-m-\ell+m} = (-1)^{m\ell+1}.$$

The computation of the discriminants of the M_i and then the Hasse invariant of Q are direct calculations. $\square$

Remark. If the residue characteristic is not 2 the above gives us a method to calculate the invariants of forms $\mathrm{Tr}_{L/F}(\lambda x^2)$ for an arbitrary λ.

We now restrict ourselves to the case that the residue characteristic is not 2. In addition to the above notation, suppose that E/L is a quadratic extension with involution σ. Fix w a non-square element of $\mathcal{O}_F^*$. Writing $x = x_1 + x_2\sqrt{\delta_{E/E^\sigma}}$ consider the quadratic form on E

$$q_{E/F,\lambda}(x) = \tfrac{1}{2}\,\mathrm{Tr}_{E/F}(\lambda x\sigma(x)) \simeq \mathrm{Tr}_{E^\sigma/F}(\lambda x_1^2) - \mathrm{Tr}_{E^\sigma/F}(\lambda\delta_{E/E^\sigma}x_2^2).$$

Then set $\lambda' = \lambda\delta_{E/E^\sigma}$, $k' = k$ and choose u', v', ℓ' so that $\lambda' = \frac{\pi_F^k}{u'v'^2\pi_L^{\ell'}f'(\pi_L)}$. Let Q', M_i' be defined similarly to Q, M_i using λ' instead of λ so that $q_{E/F,\lambda}(x) = Q(x_1) - Q'(x_2)$. Now define $N_i = M_i \oplus -M_i'$ and $\widetilde{N_1} = \frac{1}{\pi_F^k}N_1$ and $\widetilde{N_2} = \frac{1}{\pi_F^{k-1}}N_2$ their unimodular rescalings.

Lemma 3.4.4. *With the notation as above we have the following:*

1. *If $\delta_{E/E^\sigma} = w$ then $\ell' = \ell$ and $u' = wu$. Then:*

$$D(\widetilde{N_1}) = (-1)^{\ell-m}w^{\ell-m} \text{ and } D(\widetilde{N_2}) = (-1)^{-\ell}w^{-\ell}.$$

It follows that:

$$D(q_{E/F,\lambda}(x)) = (-1)^m w^m \pi_F^{2(mk-\ell)}, \text{ and}$$
$$H(q_{E/F,\lambda}(x)) = (\pi_F, w)^{km-\ell}.$$

2. *If $\delta_{E/E^\sigma} = \pi_{E^\sigma}$ then $\ell' = \ell - 1$ and $u' = u$. Then:*

$$D(\widetilde{N_1}) = (-1)u \text{ and } D(\widetilde{N_2}) = (-1)^{m+1}u.$$

It follows that:

$$D(q_{E/F,\lambda}(x)) = (-1)^m \pi_F^{2(mk-\ell)+1}, \text{ and}$$
$$H(q_{E/F,\lambda}(x)) = (\pi_F, u)\cdot(\pi_F, -1)^{k(\ell-m-1)+m+\ell(\ell+1)/2}.$$

3. *If $\delta_{E/E^\sigma} = w\pi_{E^\sigma}$ then $\ell' = \ell - 1$ and $u' = wu$. Then:*

$$D(\widetilde{N_1}) = (-1)uw^{\ell-m+1} \text{ and } D(\widetilde{N_2}) = (-1)^{m-1}uw^{1-\ell}.$$

It follows that:

$$D(q_{E/F,\lambda}(x)) = (-1)^m w^m \pi_F^{2(mk-\ell)+1}, \text{ and}$$
$$H(q_{E/F,\lambda}(x)) = (\pi_F, u) \cdot (\pi_F, w)^{(m\ell-m-\ell^2-1)} \cdot (\pi_F, -1)^{k(\ell-m-1)+m+\ell(\ell+1)/2}.$$

4. *If E^σ/F is still an extension of fields but $E = E^\sigma \times E^\sigma$, $\delta_{E/E^\sigma} = 1$, then $\ell' = \ell$ and $u' = u$. Then:*

$$D(\widetilde{N_1}) = (-1)^{\ell-m} \text{ and } D(\widetilde{N_2}) = (-1)^{-\ell}.$$

It follows that:

$$D(q_{E/F,\lambda}(x)) = (-1)^m \pi_F^{2(mk-\ell)}, \text{ and}$$
$$H(q_{E/F,\lambda}(x)) = 1.$$

Proof. The proof is a direct, although tedious, calculation based on Lemma 3.4.3. □

Remark. By combining the results above for totally ramified extensions with those of Lemma 3.4.1 one obtains results for arbitrary extensions.

In the formulas above the parameter m is determined by the ramification degree of E^σ. The parameters k and ℓ are controlled together by both the higher ramification degrees of E^σ and the valuation of λ. Finally the square class of u is controlled by the square class of λ.

The following two lemmas are direct computations.

Lemma 3.4.5. *Let F/k be an extension of local fields of residue characteristic 2. Then when viewed as a quadratic form on $F \times F$ the Witt invariant of $\mathrm{Tr}_{F/k}(x^2 - y^2)$ is 1.*

Lemma 3.4.6. *Let $F = \mathbb{R}$ or $F = \mathbb{C}$, then as a quadratic form on $F \times F$ the Witt invariants of $\mathrm{Tr}_{F/\mathbb{R}}(x^2 + y^2)$ and $\mathrm{Tr}_{F/\mathbb{R}}(x^2 - y^2)$ are 1, and the Witt invariant of $\mathrm{Tr}_{F/\mathbb{R}}(-x^2 - y^2)$ is -1.*

3.5 The Main Results

We recall the main result:

Theorem 3.5.1. *Let* O_q *be an orthogonal group over a number field* k *defined by a quadratic form* q *of dimension* $2n$ *or* $2n+1$, *and let* (E,σ) *be a field extension of* k *with an involution and of dimension* $2n$. *Then* O_q *contains a torus of type* (E,σ) *if and only if the following three conditions are satisfied:*

1. E^ϕ *splits the even Clifford algebra* $W^{orth}(q)$ *for all* σ*-types* ϕ *of* E.
2. *If* $\dim(q)$ *is even then* $\delta_{E/k} = (-1)^n D(q)$.
3. *Let* ν *be a real infinite place of* k *and let* s *be the number of homomorphisms from* E *to* $\mathbb{C}$ *over* ν *for which* σ *corresponds to complex conjugation. The signature of* q *is of the form* $(n - \frac{s}{2} + 2i, n + \frac{s}{2} - 2i)_\nu$ *if the dimension is even and either* $(n - \frac{s}{2} + 2i + 1, n + \frac{s}{2} - 2i)_\nu$ *or* $(n - \frac{s}{2} + 2i, n + \frac{s}{2} - 2i + 1)_\nu$ *if* $\nu((-1)^n D(q)\delta_{E/k})$ *is respectively positive or negative when the dimension is odd, where* $0 \leq i \leq \frac{s}{2}$.

Moreover, for any E *satisfying condition (2) we have that* $\sqrt{D(q)} \in E^\phi$ *for every* σ*-type* ϕ *of* E.

By Proposition 3.2.13 the entire theorem is reduced to showing that the conditions are equivalent to the existence of $\lambda \in (E^\sigma)^*$ such that the quadratic form $q_{E,\lambda} = \frac{1}{2}\operatorname{Tr}_{E/k}(\lambda x \sigma(x))$ has the same invariants as q. We now proceed with a series of lemmas which will conclude with the result.

Lemma 3.5.2. *Let* (E,σ) *be an étale algebra over* k *with involution and let* $\lambda \in E^\sigma$. *For a real infinite place* ν *of* k *the quadratic form* $q_{E,\lambda} = \frac{1}{2}\operatorname{Tr}_{E/k}(\lambda x\sigma(x))$ *has signature* $(n + \frac{r}{2} - \frac{s}{2}, n - \frac{r}{2} + \frac{s}{2})_\nu$ *where* s *(respectively* r*) is the number of real embeddings* $\rho \in \mathrm{Hom}_{k-alg}(E^\sigma, \mathbb{R})$ *of* E^σ *which are ramified in* E *with* $\rho(\lambda) > 0$ *(respectively* $\rho(\lambda) < 0$*).*

Proof. This is an immediate check. ☐

Lemma 3.5.3. *Let F be a number field, let $e_\nu = \pm 1$ be a collection of numbers indexed by the places of F, and let $\delta \in F$. Then there exist $\lambda \in F$ with $(\lambda, \delta)_\nu = e_\nu$ if and only if the following three conditions are satisfied:*

1. *All but finitely many e_ν are 1.*
2. *An even number of the e_ν are -1.*
3. *For each ν there exists $\lambda_\nu \in F_\nu$ with $(\lambda_\nu, \delta)_{F_\nu} = e_\nu$.*

Proof. This is well known. For the result over $\mathbb{Q}$ see [Ser73, Thm. 2.2.4], for the result over an algebraic number field see [O'M00, 71:19a].

□

Corollary 3.5.4. *Let (E, σ) be an extension of a number field k of degree $2n$ together with an involution. For each place ν of k let $e_\nu \in \{\pm 1\}$, and for each infinite place let $(s_\nu, r_\nu)_\nu$ be such that $s_\nu, r_\nu \in \mathbb{N}$ and $s_\nu + r_\nu = 2n$. Then there exists $\lambda \in E^\sigma$ with $q_{E,\lambda}$ having signatures $(s_\nu, r_\nu)_\nu$ and Hasse invariants e_ν if and only if the following three conditions are satisfied:*

1. *All but finitely many e_ν are 1.*
2. *An even number of the e_ν are -1.*
3. *For each ν there exists $\lambda_\nu \in E_\nu^\sigma$ such that $H(q_{E_\nu,\lambda_\nu}) = e_\nu$ and moreover, the signature of q_{E_ν,λ_ν} is $(s_\nu, r_\nu)_\nu$ if ν is an infinite place of k.*

Proof. Supposing there exists a λ, then conditions (1), (2) and (3) are immediate.

Let us prove the converse. For $\mu \in (E^\sigma)^*$ denote by $Q_{E/E^\sigma,\mu}(x) = \frac{1}{2}\operatorname{Tr}_{E/E^\sigma}(\mu x \sigma(x))$ the E^σ-quadratic form on E. First we recall Theorem 3.3.3 tells us that:

$$H(q_{E,\mu})_\nu = H(q_{E,1})_\nu \prod_{u|\nu} H(Q_{E/E^\sigma,\mu})_u,$$

where the u run over places of E^σ over ν. Now for each place u of E^σ define $f_u \in \{\pm 1\}$ as follows:

- If $u|\nu$ is an infinite place, set $f_u = H(Q_{E/E^\sigma,\lambda_\nu})_u$.

- If $u|\nu$ is a finite place and $H(q_{E,1})_\nu e_\nu = 1$, set $f_u = 1$.
- If $u|\nu$ is a finite place and $H(q_{E,1})_\nu e_\nu = -1$, set $f_u = H(Q_{E/E^\sigma,\lambda_\nu})_u$.

We now notice that for each place ν of k we have:

$$\prod_{u|\nu} f_\mu = \prod_{u|\nu} H(Q_{E_\nu/E_\nu^\sigma,\lambda_\nu})_u = H(q_{E,1})_\nu H(q_{E_\nu,\lambda_\nu}) = H(q_{E,1})_\nu e_\nu$$

and moreover, that only finitely many $f_u \neq 1$. It follows that $\prod_u f_u = \prod_\nu H(q_{E,1})_\nu e_\nu = 1$. Finally we have that if $f_u \neq 1$ then $f_u = H(Q_{E/E^\sigma,\lambda_\nu})_\mu = (\lambda_\nu, \delta_{E/E^\sigma})_u$. The values f_u thus satisfy the conditions of Lemma 3.5.3 and we conclude that there exists $\lambda \in E^\sigma$ with $(\lambda, \delta_{E/E^\sigma})_u = f_u$. By the choices of the f_u we find:

$$H(q_{E,\lambda})_\nu = H(q_{E,1})_\nu \prod_{u|\nu} H(Q_{E_\nu/E_\nu^\sigma,\lambda})_u = H(q_{E,1})_\nu \prod_{u|\nu} f_u = e_\nu.$$

Finally, by Lemma 3.5.2 the signature of $q_{E,\lambda}$ at a real infinite place ν is given by:

$$\left(\tfrac{1}{2} \sum_{u|\nu} m_u (H(Q_{E_\nu/E_\nu^\sigma,\lambda})_u + 1), \tfrac{1}{2} \sum_{u|\nu} m_u (H(Q_{E_\nu/E_\nu^\sigma,-\lambda})_u + 1) \right),$$

where $m_u = 1$ if $E_u = \mathbb{R} \times \mathbb{R}$ and $m_u = 2$ if $E_u = \mathbb{C}$. Since $H(Q_{E_\nu/E_\nu^\sigma,\lambda})_u = H(Q_{E_\nu/E_\nu^\sigma,\lambda_\nu})_u$ for all u it follows that the signature of $q_{E,\lambda}$ at ν is the same as that of q_{E_ν,λ_ν}, which is to say it is precisely $(s_\nu, r_\nu)_\nu$. □

Lemma 3.5.5. *Let (E, σ) be an étale algebra with involution. Let $E_\mathfrak{p} = \times_i E_{\mathfrak{p}i}$ be a decomposition into a product of fields. Then there exists values $\lambda_+, \lambda_- \in E^\sigma$ such that the $\mathfrak{p}$-adic part of the Hasse invariant for $\frac{1}{2}\operatorname{Tr}_{E/k}(\lambda_\pm x\sigma(x))$ is respectively $+1$,-1 if and only if the involution σ restricts to an automorphism of $E_{\mathfrak{p}i}$ for one of the constituent fields $E_{\mathfrak{p}i}$ of the étale algebra $E_\mathfrak{p}$. Moreover, if $W(q_{E,\lambda})_\mathfrak{p}$ is independent of λ then $W(q_{E,\lambda})_\mathfrak{p} = 1$ for all λ.*

Proof. From Theorem 3.3.3 recall that we have:

$$W(q_{E,\lambda}) = C_E \cdot \mathrm{Cor}_{E^\sigma/k}((\lambda, \delta_{E/E^\sigma})_{E^\sigma}),$$

for some constant C_E which does not depend on λ. Thus, both $\lambda_\pm$ exist if and only if $\mathrm{Cor}_{E^\sigma_\mathfrak{p}/k_\mathfrak{p}}((\lambda, \delta_{E_\mathfrak{p}/E^\sigma_\mathfrak{p}})_{E^\sigma_\mathfrak{p}})$ is not constant as a function of λ. Writing $E^\sigma_\mathfrak{p} = \times_j E^\sigma_{\mathfrak{p}j}$ let ρ_j be the projection of $E^\sigma_\mathfrak{p}$ onto the jth factor. Using the fact that the cohomology and the corestriction maps factor as products we have:

$$\mathrm{Cor}_{E^\sigma_\mathfrak{p}/k_\mathfrak{p}}((\lambda, \delta_{E_\mathfrak{p}/E^\sigma_\mathfrak{p}})_{E^\sigma_\mathfrak{p}}) = \prod_j \mathrm{Cor}_{E^\sigma_{\mathfrak{p}j}/k_\mathfrak{p}}((\rho_j(\lambda), \rho_j(\delta_{E_\mathfrak{p}/E^\sigma_\mathfrak{p}}))_{E^\sigma_{\mathfrak{p}j}}).$$

We thus conclude that both $\lambda_\pm$ exist if and only if for at least one j the function $\mathrm{Cor}_{E^\sigma_{\mathfrak{p}j}/k_\mathfrak{p}}((\rho_j(\lambda), \rho_j(\delta_{E_\mathfrak{p}/E^\sigma_\mathfrak{p}}))_{E^\sigma_{\mathfrak{p}j}})$ is not constant with respect to λ. The corestriction map being injective for local fields, this is equivalent to $(\lambda_j, \rho_j(\delta_{E_\mathfrak{p}/E^\sigma_\mathfrak{p}}))_{E^\sigma_{\mathfrak{p}j}}$ being non-constant. This last assertion is the same as saying that $\rho_j(\delta_{E_\mathfrak{p}/E^\sigma_\mathfrak{p}})$ is a non-square or that σ acts as the non-trivial field automorphism on the factor $E_{\mathfrak{p}i}$ of $E_\mathfrak{p}$ that is over $E^\sigma_{\mathfrak{p}j}$.

For the second part, we need to show that whenever $W(q_{E,\lambda})_\mathfrak{p}$ is independent of λ then $W(q_{E,\lambda})_\mathfrak{p} = 1$. Indeed if $W(q_{E,\lambda})_\mathfrak{p}$ does not depend on λ, then by the first part of the lemma $E_\mathfrak{p}/E^\sigma_\mathfrak{p}$ has no factors which are field extensions. Thus the element z appearing in the formula in Theorem 3.3.8 is a square and this implies $W(q_{E,\lambda})_\mathfrak{p} = \mathrm{Cor}_{E^\sigma_\mathfrak{p}/k_\mathfrak{p}}((-\lambda f'_z(z), z)_{E^\sigma_\mathfrak{p}}) = 1$. □

Corollary 3.5.6. *Let E/k be an extension of number fields. Let q be a quadratic form of dimension $2n$. Then O_q has a torus of type (E, σ) if and only if the following three conditions are satisfied:*

1. *For all primes $\mathfrak{p}$ of k where none of the factors of $E_\mathfrak{p}$ are proper field extensions of factors of $E^\sigma_\mathfrak{p}$, we have $W(q)_\mathfrak{p} = 1$.*
2. *We have $(-1)^n \delta_{E/k} = D(q)$ (equivalently $(-1)^n \delta_{E_\mathfrak{p}/k_\mathfrak{p}} = D(q_\mathfrak{p})$ for all $\mathfrak{p}$).*
3. *The signature conditions of Theorem 3.5.1.*

Proof. By Proposition 3.2.13 we have that O_q has a torus of type (E, σ) if and only if there exists $\lambda \in (E^\sigma)^*$ such that the quadratic form $q_{E,\lambda} = \frac{1}{2}\operatorname{Tr}_{E/k}(\lambda x \sigma(x))$ has the same invariants as q. Thus we must show that the existence of such a λ is equivalent to the conditions of the corollary.

For each place ν of k set $e_\nu = H(q)_\nu$ and for each infinite places set $(s_\nu, r_\nu)_\nu$ to be the signature of q. Then the $e_\nu, (s_\nu, r_\nu)_\nu$ satisfy (1) and (2) of Corollary 3.5.4 as they arise from the quadratic form q. We thus have by Corollary 3.5.4 that the question of existence is local.

We now check that conditions (1), (2) and (3) are equivalent to the local conditions on the existence of λ_ν for all places ν of k. For a finite place ν of k a λ_ν exists with $q_{E_\nu,\lambda_\nu} \simeq q$ if and only if a λ_ν exists with both $D(q_{E_\nu,\lambda_\nu}) = D(q)$ and $H(q_{E_\nu,\lambda_\nu}) = H(q)_\nu$. Theorem 3.3.3 tells us that (2) (at ν) is equivalent to the discriminant condition and Lemma 3.5.5 tells us that (1) (at ν) is equivalent to the Hasse invariant condition. For an infinite place ν we have by Lemma 3.5.2 that the existence of a λ_ν is equivalent to (3) at ν. Note that for infinite places (3) implies (1) and (2). We have thus shown that the existence of a global λ is equivalent to (1), (2) and (3) for all ν, which completes the result. □

Corollary 3.5.7. *Let E/k be an extension of number fields. Let q be a quadratic form of dimension $2n+1$. Then O_q has a torus of type (E,σ) if and only if the following two conditions are satisfied:*

1. *For all primes $\mathfrak{p}$ of k where none of the factors of $E_\mathfrak{p}$ are proper field extensions of factors of $E^\sigma_\mathfrak{p}$, we have $W(q)_\mathfrak{p} = 1$.*
2. *The signature conditions of Theorem 3.5.1.*

Proof. We proceed as in the previous corollary, except we now have the added flexibility of choosing what the orthogonal complement of the sub-quadratic space $q_{E,\lambda}$ looks like. In particular, O_q has a torus of type (E,σ) if and only if $q \simeq q_{E,\lambda} \oplus \langle a \rangle$ for some $\lambda \in (E^\sigma)^*$. In order for q and $q_{E,\lambda} \oplus \langle a \rangle$ to have equal discriminants it is necessary that $a = (-1)^n D(q)/\delta_{E/k}$. As this can always be done there is no discriminant condition in this case. Again as above, by Corollary 3.5.4 the question of the existence of λ is local.

We must find the local condition on Witt invariants. Knowing the discriminants of $q_{E,\lambda}$ and $\langle a \rangle$ we see that $H(q_{E,\lambda} \oplus \langle a \rangle)_{\mathfrak{p}}$ depends on λ if and only if $H(q_{E,\lambda})_{\mathfrak{p}}$ does. Hence this also holds for the Witt invariants. Furthermore, the obstructions to changing Witt invariants arise at the same places as in Corollary 3.5.6. Now, we compute that $W(q)_{\mathfrak{p}} = W(-aq_{E,\lambda})_{\mathfrak{p}} = W((-1)^{n+1} D(q)\delta_{E/k} q_{E,\lambda})_{\mathfrak{p}}$ (see [Lam05, V.2.9]). Next, by Theorem 3.3.8 we know that if the Witt invariant of $q_{E,\lambda}$ is independent of λ then $W(q_{E,\lambda})_{\mathfrak{p}} = 1$ independently of λ, and consequently independently of rescaling. In particular it follows that $W(q)_{\mathfrak{p}} = W((-1)^{n+1} D(q)\delta_{E/k} q_{E,\lambda})_{\mathfrak{p}} = 1$. This gives us the condition on Witt invariants (1).

Finally, the signature conditions (2) are precisely those of Lemma 3.5.2 together with the sign contribution that is dictated by the $\langle a \rangle$ piece at each ν. □

Remark. The condition "$E_{\mathfrak{p}}$ contains no field extensions of factors of $E^{\sigma}_{\mathfrak{p}}$," can be rephrased as "for all constituent fields E_i of E and all the primes $\mathfrak{p}_i$ above $\mathfrak{p}$ in E_i^{σ}, there exists at least one $\mathfrak{p}_i$ which does not split in E_i."

This condition thus says that for some computable collection of primes which divide the discriminant of the quaternion algebra, none are totally split between E^{σ} and E. We point out that there is no condition on the behaviour of these primes between k and E^{σ}. We also point out that primes which divide the discriminant of E to odd degree ramify for at least one place, and so automatically satisfy this condition.

Lemma 3.5.8. *Let (E, σ) be an étale algebra with involution. Then every reflex algebra of (E, σ) contains an element y such that $y^2 = \delta_{E/k}$.*

Proof. Suppose $E = E^\sigma(\sqrt{x})$ with x chosen so that $\delta_{E/E^\sigma} = x$. Then we have $\delta_{E/k} = (-1)^n N(x)$. Let ϕ be a σ-type of E. Then let:

$$y = \prod_{\rho \in \phi} \rho(\sqrt{x}) \in E^\phi,$$

and moreover, we see that $\sigma(y) = (-1)^n y$ and $y\sigma(y) = N(x) = (-1)^n \delta_{E/k}$. The result follows. □

Lemma 3.5.9. *Let (E, σ) be an étale algebra over k with involution, and let A be a quaternion algebra over k. Then E^ϕ splits A for all σ-types ϕ of E if and only if we have $[A_\mathfrak{p}] = 1$ for every place $\mathfrak{p}$ where $E_\mathfrak{p}$ contains no factors which are quadratic extensions of factors of $E_\mathfrak{p}^\sigma$.*

Proof. We first state some facts concerning the splitting of quaternion algebras. A quaternion algebra is split by an étale algebra E if it is split by each factor. A quaternion algebra is split by a field L if it is split locally everywhere, that is, for each prime $\mathfrak{p}_L$ in L. A local field L splits a nonsplit quaternion algebra if and only if L contains a quadratic subextension.

Thus, every reflex algebra E^ϕ splits a quaternion algebra A if and only if E^Φ does. This happens if and only if $E_\mathfrak{p}^\Phi$ splits A for every prime $\mathfrak{p}$ of k. Consequently E^Φ splits a quaternion algebra A if and only if for each $\mathfrak{p}$ we have that $A_\mathfrak{p}$ nonsplit implies $(E_\mathfrak{p})^\phi$ has even degree for all ϕ.

It follows from Corollary 3.2.6 that $(E_\mathfrak{p})^\phi$ has even degree for all ϕ if and only if at least one factor of $E_\mathfrak{p}/E_\mathfrak{p}^\sigma$ is a field extension. Thus, the only condition for E^Φ to split A is that if $A_\mathfrak{p}$ is not already split, then $E_\mathfrak{p}/E_\mathfrak{p}^\sigma$ must contain a field extension. □

Proof of Theorem 3.5.1. What remains to show is that the conditions of Corollaries 3.5.6 and 3.5.7 in the even and odd cases, respectively, are equivalent to those of Theorem 3.5.1. We see immediately that the conditions on signatures and discriminants are the same and that the additional data about discriminants in the even case is provided by Lemma 3.5.8. What remains to show is that the Witt invariant conditions agree.

Lemma 3.5.9 tells us precisely that the condition of the corollaries (for all primes $\mathfrak{p}$ of k where none of the factors of $E_{\mathfrak{p}}$ are proper field extensions of factors of $E^{\sigma}_{\mathfrak{p}}$, we have $W(q)_{\mathfrak{p}} = 1$) is equivalent to the statement that all the σ-reflex fields of E split $W(q)$. Thus we want to show that we can replace $W(q)$ by $W^{\mathrm{orth}}(q)$ in the condition of the previous sentence. In the odd dimensional case there is nothing to show as these are equal. For the even case, since $W^{\mathrm{orth}}(q) = W(q) \otimes_k Z(\mathrm{C}^0_q)$ and $Z(\mathrm{C}^0_q) \subset E^{\phi}$ it follows that:

$$W^{\mathrm{orth}}(q) \otimes_k E^{\phi} = W(q) \otimes_k Z(\mathrm{C}^0_q) \otimes_k E^{\phi} = (W(q) \otimes_k E^{\phi}) \oplus (W(q) \otimes_k E^{\phi}).$$

It follows that E^{ϕ} splits $W(q)$ if and only if it splits $W^{\mathrm{orth}}(q)$. This gives us the equivalence of the final condition of the theorem with those of the corollaries and thus completes the proof. □

3.6 Applications

One of the primary motivations for this work is to understand the possible special fields associated to the special points on Shimura varieties of orthogonal type (see [Del71]). We now give some applications in this direction.

Corollary 3.6.1. *Suppose in Theorem 3.5.1 that $k = \mathbb{Q}$, the signature of q is $(2, \ell)$ and (E, σ) is a CM-field with complex conjugation σ. Then O_q contains a torus of type (E, σ) if and only if:*

1. *For each prime p of $\mathbb{Q}$ with local Witt invariant $W(q)_p = -1$ there exists a prime $\mathfrak{p}|p$ of E^{σ} that does not split in E.*
2. *If ℓ is even, then $D(q) = (-1)^{(2+\ell)/2}\delta_{E/\mathbb{Q}}$. (No further conditions if ℓ is odd.)*

Proof. We have put ourselves in a situation in which the signature condition is automatic. We thus must check only the remaining conditions. The discriminant condition remains the same, and the Witt invariant condition is precisely that of Corollary 3.5.6. □

Corollary 3.6.2. *Suppose that $k = \mathbb{Q}$ and the signature of q is $(2, \ell)$. Let F be a totally real field. Then there exists a CM-field E with $E^\sigma = F$, and the orthogonal group O_q containing a torus of type (E, σ) if and only if:*

1. *No condition if ℓ odd.*
2. *If ℓ is even, then (up to squares) $D(q) = N_{F/k}(\delta)$ for an element $\delta \in F$ which satisfies the condition that for all primes p of k with $W(q)_p = -1$ there is at least one prime $\mathfrak{p}|p$ of F such that δ is not a square in $F_\mathfrak{p}$.*

Proof. In this case we are now looking for any CM-field extension.

The norm condition in the even dimension is precisely the condition required so that we have a quadratic extension of the desired discriminant and the desired primes are not totally split. To eliminate entirely the Witt invariant conditions in the odd case we note that we can simply force these to be ramified in the quadratic extension. □

Remark. In order to satisfy the condition that the primes where $W(q)_p = -1$ will not split in the quadratic extension for δ one is looking to modify δ by an element of square norm which is not a square modulo some prime $\mathfrak{p}$ over p. Elements of square norm tend to be contained in quadratic subextensions. Let $L \subset F$ be a degree 2 subextension. We claim that L contains an element which is not a square in $\mathcal{O}_{F\mathfrak{p}}$. Indeed, if $\mathfrak{p}$ is ramified or inert over L one may take any representative of a nonsquare in $\mathcal{O}_L/(\mathfrak{p} \cap \mathcal{O}_L)$. If $\mathfrak{p}$ is split take any representative of a uniformizer of $\mathcal{O}_{L(\mathfrak{p}\cap\mathcal{O}_L)}$.

Corollary 3.6.3. *Let $d \in \mathbb{Q}$ be a squarefree positive integer. Consider the quadratic form:*

$$q_d = x_1^2 - x_2^2 + x_3^3 - dx_4^2.$$

This implies $\mathrm{Spin}_{q_d}(\mathbb{R}) \simeq \mathrm{SL}_2(\mathbb{R})^2$ is associated to the Hilbert modular space for $\mathbb{Q}(\sqrt{d})$. Let (E, σ) be a field of dimension 4 with involution σ. Then O_q has a torus of type (E, σ) if and only if the σ-reflex fields of E all contain $\mathbb{Q}(\sqrt{d})$.

Proof. Firstly, a computation using Proposition 3.2.17 together with the fact that $H(q_d) = (-1, -d)$ shows $W(q_d) = 1$. Thus all the σ-reflex fields E^ϕ automatically split the even Clifford algebra. Since Theorem 3.5.1 already states that if O_q has a torus of type (E, σ) then $\sqrt{d} \in E^\phi$ for all ϕ. It thus remains only to show, that under the present conditions, $\sqrt{d} \in E^\phi$ for all ϕ implies both the discriminant and signature conditions of Theorem 3.5.1 hold. To this end, we introduce some further notation.

Let $m \in \mathbb{Q}$ be such that $E^\sigma = \mathbb{Q}(\sqrt{m})$, let τ be the non-trivial automorphism of E^σ and let $\delta = a + b\sqrt{m} \in E^\sigma$ be such that $E = E^\sigma(\sqrt{\delta})$. Let N be the normal closure of E over $\mathbb{Q}$, then one checks that $N = \mathbb{Q}(\sqrt{m}, \sqrt{\delta\tau(\delta)}, \sqrt{\delta})$ has degree 4 or 8 over $\mathbb{Q}$. Set $M = \mathbb{Q}(\sqrt{\delta\tau(\delta)}, \sqrt{\delta} + \sqrt{\tau(\delta)}) \subseteq N$. Notice that σ extends to N and that on its restriction to M we have $M^\sigma = \mathbb{Q}(\sqrt{\delta\tau(\delta)})$.

We now must divide the argument into two cases depending on $\mathrm{Gal}(N/\mathbb{Q})$. In the first case suppose $\mathrm{Gal}(N/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^2$. Then we may assume $\delta \in \mathbb{Q}$ and so the two σ-reflex fields of E are $M = \mathbb{Q}(\sqrt{\delta})$ and $\mathbb{Q}(\sqrt{m\delta})$ with their intersection being $\mathbb{Q}$. It follows that $\sqrt{d} \in E^\phi$ for all ϕ implies d is a square. Moreover, as E is biquadratic, $\delta_{E/\mathbb{Q}}$ is a square and E is either CM or totally real. Thus $\sqrt{d} \in E^\phi$ for all ϕ is equivalent to $d = \delta_{E/\mathbb{Q}}$ mod squares. (Notice that the case of d a square is technically excluded from the statement of the corollary.)

Now in the second case suppose $\mathrm{Gal}(N/\mathbb{Q}) \neq (\mathbb{Z}/2\mathbb{Z})^2$. Then $\mathrm{Gal}(N/\mathbb{Q})$ is either $\mathbb{Z}/4\mathbb{Z}$ or D_8. In either case a check shows that M is (up to isomorphism) the unique σ-reflex field for E and M^σ is the only quadratic subextension of M. Moreover, the discriminant of E is $\delta_{E/\mathbb{Q}} = \delta\tau(\delta)$ and $M^\sigma = \mathbb{Q}(\sqrt{\delta\tau(\delta)})$ hence $\sqrt{d} \in E^\phi$ for all ϕ is equivalent to $d = \delta\tau(\delta) = \delta_{E/\mathbb{Q}}$ mod squares. Finally, since $b^2m = (a^2 - \delta\tau(\delta))$ it follows that $\delta = a + \sqrt{a^2 - \delta\tau(\delta)}$. Thus using that $\delta\tau(\delta) = r^2 d > 0$ we find that E is either totally complex or totally real.

We have thus shown that in all cases, $\sqrt{d} \in E^\phi$ for all ϕ implies that $d = \delta_{E/\mathbb{Q}}$ and that E is either totally complex or totally real. One now observes that E being totally complex or totally real implies the signature condition and this concludes the proof. □

Remark. It follows that the tori in Spin_q are all associated to algebras which are two dimensional over $\mathbb{Q}(\sqrt{d})$. This is well known for the tori associated to CM-points, but we have shown the analogous fact also holds for those associated to so-called almost totally real cycles (for the definition see the discussion following [DL03, Prop. 2.4]). It is worth noting that these E can never be ATR extensions, that is extensions with only one complex place. It is the reflex fields of these E which may be ATR extensions.

CHAPTER 4
Representation Densities for Hermitian Lattices

4.1 Introduction

The issue of computing local densities goes back decades to when they were first introduced by Siegel [Sie35]. These types of computations have many applications beyond those originally envisioned (see for example [GK93, Kud97b, SP04, GHS08, GV12] among others) and formulas for them have been worked out to cover many cases (see for example [Pal65, Wat76, Kit93, Shi99, Kat99, SH00, Yan04]).

The primary application we have in mind in the present work is for computing the arithmetic volumes of the orthogonal groups that arise from Hermitian lattices. These lattices arise in the study of special points on orthogonal Shimura varieties and these arithmetic volumes relate, by way of the Hirzebruch-proportionality principle and the Riemann-Roch theorem (see [Mum77, GHS08]), to the dimensions of spaces of modular forms on the associated Shimura varieties.

Another important application is their use, by way of the Siegel mass formula, as part of a stopping condition when enumerating the genus of a lattice. This has important applications in the theory of algebraic automorphic forms on orthogonal groups (see [Gro99] and [GV12]). The sections of this paper are organized as follows:

(4.2) We introduce the general theory of lattices so far as it is needed in the sequel.

(4.3) We discuss specifically lattices over p-adic rings.

(4.4) We introduce representation densities and develop formulas for computing them.

(4.5) We obtain results about the structure of lattices under transfer.

(4.6) We develop formulas for the representation densities of Hermitian lattices in terms of the invariants of the fields involved.

(4.7) We discuss the concrete example of $\mathbb{Q}(\mu_p)$.

Almost none of the introductory content (Sections 2 and 3) is new, however we present it in the format we intend to use in the sequel. Many results on representation densities are known:

- The work of Pall, Watson and the book of Kitaoka, [Pal65, Wat76, Kit93], give formulas for $\beta_{\mathfrak{p}}(L, L)$ over $\mathbb{Z}_p$ for arbitrary L and p.
- Katsuraga [Kat99] computes $\beta_{\mathfrak{p}}(L, M)$ over $\mathbb{Z}_2$.
- Shimura [Shi99] computes formulas for $\beta_{\mathfrak{p}}(L, L)$ when L is maximal, over $\mathcal{O}_{\mathfrak{p}}$ any finite extension of $\mathbb{Z}_p$.
- Hironaka-Sato [SH00] computes $\beta_{\mathfrak{p}}(L, M)$ over $\mathbb{Z}_p$ when $p \neq 2$.

However, formulas for all cases do not yet exist. Our results (Section 4) cover the case of computing $\beta_{\mathfrak{p}}(L, L)$ where L is unimodular over any finite extension of $\mathbb{Z}_p$ (including especially $p = 2$). This is the content of Theorems 4.4.11 and 4.4.18. We also give clean reduction formulas to compute $\beta_{\mathfrak{p}}(L, L)$ for arbitrary L in terms of the collection of all of its Jordan decompositions. This is the content of Theorem 4.4.28.

By a **Hermitian form** we mean a quadratic form of the shape:

$$q_{E,\lambda}(x) = \mathrm{Tr}_{E/k}(\lambda x \sigma(x)),$$

where E is an étale k-algebra with involution σ and λ is a unit of E^σ, the subalgebra of elements fixed by σ. By a **Hermitian lattice** we mean a fractional ideal Λ of $\mathcal{O}_E$ in E. In order to study the representation density problem specifically for Hermitian lattices we must first obtain structure theorems for lattices that arise from transfer. That is, we compute properties of the Jordan decomposition for lattices whose quadratic forms arise as $\mathrm{Tr}_{R_2/R_1}(q_{R_2})$. This is the content of Section 5. Having done this, we can convert the usual formulas for representation densities, which are expressed in terms of combinatorial data about Jordan decompositions, to formulas that express the density in terms of properties of the fields involved. This is done in Section 6.

4.2 General Notions of Lattices

In this section we introduce the general theory of lattices. Many good references exist which treat this topic in a varying degree of generality. See for example [Kit93] and [O'M00]. We shall initially work quite generally, adding more structure as it is required. We shall eventually be most interested in the theory of lattices over $\mathcal{O}_k$, the maximal order in a number field k. Note that these are not always PIDs, however, their localizations always are.

Definition 4.2.1. Let R be an integral domain and K be its field of fractions. By a **lattice** Λ over R we mean a projective R-module of finite rank, together with a symmetric R-bilinear pairing:

$$b_\Lambda : \Lambda \times \Lambda \to K,$$

which induces a duality $\mathrm{Hom}_R(\Lambda, K) = \Lambda \otimes_R K$. We shall sometimes denote $b_\Lambda(x, y) = (x, y)$ when the pairing b_Λ is understood. A lattice is said to be **integral** if $(x, y) \in R$, **even** if $(x, x) \in 2R$ and **unimodular** if the pairing induces an isomorphism $\mathrm{Hom}_R(\Lambda, R) = \Lambda$, or more generally **$\mathfrak{a}$-modular** if the pairing induces an isomorphism $\mathrm{Hom}_R(\Lambda, R) = \mathfrak{a}^{-1}\Lambda$ (for $\mathfrak{a}$ a projective R-module of rank 1, that is, an invertible fractional ideal of R). Notice that $\mathfrak{a}$-modular is equivalent to having $\mathrm{Hom}_R(\Lambda, \mathfrak{a}) = \Lambda$ by noting that:

$$\mathrm{Hom}_R(\Lambda, \mathfrak{a}) = \mathfrak{a} \otimes_R \mathrm{Hom}_R(\Lambda, R) = \mathfrak{a} \otimes \mathfrak{a}^{-1}\Lambda = \Lambda.$$

We will refer to a lattice as **modular** if there exists some $\mathfrak{a}$ for which it is $\mathfrak{a}$-modular. Note that not all lattices are modular.

We shall sometimes denote the bilinear form as $b_\Lambda(\cdot,\cdot)$ when we need to specify the underlying lattice.

Remark. We are explicitly requiring that all lattices be non-degenerate with respect to the bilinear form b_Λ. If the pairing on the 'lattice' might not induce an isomorphism the 'lattice' shall be referred to as a module or submodule.

We will at times consider symmetric bilinear forms on an R-module M valued in another R-module M', that is,

$$(\cdot,\cdot) : M \times M \to M'.$$

We may even consider such pairings when R is not an integral domain. These do not fit into our definition of lattices though many notions remain valid. The most common examples of this would be either taking $M' = R/I$, for any ideal I of R, or reducing all of R, M, M' by I.

We will also need the following notion in order to deal with certain complexities in characteristic 2.

Definition 4.2.2. Let R be a ring and let M' be an R-module. We define a **quadratic module** M over R (or more precisely an **M'-valued quadratic module**) to be a module M over R together with a function $q : M \to M'$ satisfying $q(\lambda x) = \lambda^2 q(x)$ for all $x \in M$ and $\lambda \in R$ and such that

$$B_M(x,y) := q(x+y) - q(x) - q(y)$$

is a bilinear pairing. For a quadratic module M we define:

$$M^\perp := \{x \in M \mid B_M(x,y) = 0 \ \text{ for all } y \in M\} \text{ and}$$
$$\mathrm{Rad}(M) := \{x \in M^\perp \mid q(x) = 0\}.$$

A quadratic module is said to be **regular** or **non-degenerate** if $M^\perp = \emptyset$.

Remark. In the above, one typically takes $M' = R$ or $M' = K$, the total ring of fractions or $M' = R/I$.

Notation 4.2.3. Given a lattice Λ, by q_Λ or simply q we shall always mean:

$$q_\Lambda(x) = b_\Lambda(x, x).$$

To a lattice we may also associate another bilinear pairing:

$$B_\Lambda(x, y) := q_\Lambda(x + y) - q_\Lambda(x) - q_\Lambda(y).$$

Note well that $B_\Lambda(x, y) = 2b_\Lambda(x, y)$ and that $q_\Lambda(x) = b_\Lambda(x, x)$ as these conventions vary by author. Notice also that in characteristic 2 one may not recover b_Λ from q_Λ as this would involve dividing by 2 whereas if $2 \in K^\times$ then non-degenerate quadratic modules and lattices are equivalent.

Remark. For both lattices and quadratic modules $L \oplus M$ shall always mean an orthogonal direct sum.

This level of generality is too much for many of our purposes. Having the following additional constraints gives major simplifications to the theory:

1. If Λ is free we may express $(\cdot, \cdot)$ by a matrix.
2. If R is a principal ideal domain, the theory of modules simplifies. In particular, every lattice is free. We may often replace R by its (completed) localizations to attain this.
3. The theory is simpler if the characteristic of R is not 2.

Note that some of the results which follow are true without some (or all) of the above constraints, however, for simplicity of presentation we may sometimes assume them. Note that these assumptions hold when we work over $\mathbb{Z}, \mathbb{Q}, \mathbb{Z}_p$ for all $p, \mathbb{F}_p$ where $p \neq 2$, or the many finite ring extensions of these. These assumptions may fail for Dedekind domains; however as our study of these is done almost entirely with their localizations this will not be an issue. We will occasionally still need to work in characteristic 2 and it will be apparent when this is happening.

Definition 4.2.4. Assume that Λ is free and let $X = \{x_1, \ldots, x_n\}$ be a basis for Λ. We write:

$$A = A_X = ((x_i, x_j))_{i,j}$$

for the matrix corresponding to this lattice and choice of basis.

Definition 4.2.5. Given a lattice Λ we define the **dual** lattice to be:

$$\Lambda^{\#} = \{x \in \Lambda \otimes K \mid (x, y) \in R \text{ for all } y \in \Lambda\}$$

together with the induced pairing.

Definition 4.2.6. A submodule $L \subset \Lambda$ is said to be **primitive** if $KL \cap \Lambda = L$.

A collection of elements $\{x_1, \ldots, x_m\}$ is said to be **primitive** in Λ if the collection can be extended to a basis for Λ.

Proposition 4.2.7. *Suppose R is a PID, then a collection $\{x_1, \ldots, x_m\}$ is primitive if and only if $\langle x_1, \ldots, x_m \rangle_R \subset \Lambda$ is primitive.*

Proof. The forward direction is clear. For the converse we set:

$$L = \langle x_1, \ldots, x_m \rangle_R$$

and consider the exact sequence:

$$1 \to L \to \Lambda \to \Lambda/L \to 1.$$

Since L is primitive, Λ/L is torsion free, hence free. We may thus split the sequence and write:

$$\Lambda = L \oplus (\Lambda/L).$$

A choice of basis for Λ/L gives us the desired extension of the basis for L. □

Definition 4.2.8. A submodule $L \subset \Lambda$ is said to be **isotropic** if $(\cdot, \cdot)\,|_L = 0$. It is said to be **anisotropic** if it has no isotropic submodules. A projective submodule is said to be **pseudo-hyperbolic** if it has an isotropic submodule of half its rank. A projective submodule is said to be **hyperbolic** if it is generated by two isotropic submodules.

Definition 4.2.9. Lattices Λ have the following invariants:

- For Λ projective, the **rank** r_Λ of Λ as an R module.
- For Λ integral, the **discriminant group** $D_\Lambda = \Lambda^\#/\Lambda$ together with the induced pairing mapping into K/R.
- For Λ free, the **discriminant** $\delta_\Lambda = \det(A_X) \in K/(R^\times)^2$ for a choice of basis X.

  If Λ is not free we have at our disposal the discriminant $D(q)$ of $\Lambda \otimes K$ which is an element of $K/(K^\times)^2$, and the **discriminant ideal** which is the R ideal generated by $\det(A_X)$ running over all maximal linearly independent subsets X of Λ. Alternatively, for a projective module over a Dedekind domain, one may take the discriminant ideal to be the product of the local discriminant ideals.
- For Λ integral, the **level** or **stuffe** of Λ is N_Λ, the annihilator ideal of D_Λ. More precisely:

  $$N_\Lambda = \{\lambda \in R \mid \lambda x \in \Lambda \text{ for all } x \in \Lambda^\#\}.$$

  Over a PID this is the 'minimal' N such that NA_X^{-1} is integral.
- Supposing $\Lambda \otimes K$ is isomorphic to the diagonal form $(a_i)_i$ and denoting the Hilbert symbol by $(\cdot,\cdot)_K$, the **Hasse invariant** is

  $$H(\Lambda) = H(q) = \prod_{i<j} (a_i, a_j)_K \in H^2(K, \{\pm 1\}).$$

  (see [Ser73, Ch. III] and [Ser79, Ch. XIV]).
- The **Witt invariant**, $W(\Lambda) = W(q)$ is the class in $H^2(K, \{\pm 1\})$ of either the Clifford algebra or the even Clifford algebra of Λ when the parity of r_Λ is, respectively, even or odd.

- For each embedding $R \hookrightarrow \mathbb{R}$ we have an associated **signature** (the dimension of any maximal isotropic $\mathbb{R}$-submodule of $\Lambda \otimes_R \mathbb{R}$.)
- The **norm ideal** $\mathfrak{N}_\Lambda$ is the R-ideal generated by $\{(x, x) \mid x \in \Lambda\}$.
- The **scale ideal** $\mathfrak{S}_\Lambda$ is the R-ideal generated by $\{(x, y) \mid x, y \in \Lambda\}$. Note that $\mathfrak{N}_\Lambda \subset \mathfrak{S}_\Lambda$ and $2\mathfrak{S}_\Lambda \subset \mathfrak{N}_\Lambda$.
- The **norm group** $\mathfrak{n}_\Lambda$ is the group: $\{(x, x) \mid x \in \Lambda\} + 2\mathfrak{S}_\Lambda$, it is an additive subgroup of K.
- If R is Noetherian consider $\mathfrak{m}_\Lambda \subset \mathfrak{n}_\Lambda$ the largest R-ideal contained in $\mathfrak{n}_\Lambda$. Then for π an ideal of R, define the **π-weight ideal** to be the ideal $\mathfrak{w}_{\Lambda,\pi} = \pi\mathfrak{m}_\Lambda + 2\mathfrak{S}_\Lambda$. When we are working over a local ring we shall denote this by $\mathfrak{w}_\Lambda$ as π is understood to be the unique maximal ideal.

Remark. It is clear that the above are all invariants as they are defined naturally. The extent to which these determine a lattice depends largely on the setting. They are typically insufficient to characterize a lattice in the context in which we are working.

Proposition 4.2.10. *If $X = \{x_1, \ldots, x_n\}$ is a basis for Λ then $X^\# = A_X^{-1}X = \{x_1^\#, \ldots, x_n^\#\}$ is a basis for $\Lambda^\#$ with $b_\Lambda(x_i, x_j^\#) = \delta_{ij}$ and $A_{X^\#} = A_X^{-1}$.*

This is a straight forward check.

Proposition 4.2.11. *If $L \subset \Lambda$ is isotropic then $L' = K \cdot L \cap \Lambda$ is isotropic and primitive.*

This is clear.

Proposition 4.2.12. *Suppose R is a PID. If $L \subset \Lambda$ is pseudo-hyperbolic, then $(-1)^{\mathrm{rank}(L)/2}\delta_L$ is a square.*

If $L \subset \Lambda$ is isotropic, then there exists $L \subset L' \subset \Lambda$ with L' pseudo-hyperbolic and primitive (L' need not be an orthogonal direct factor of Λ). Moreover, $\delta_{L'}|\delta_\Lambda$.

Proof. Suppose $L \subset \Lambda$ is isotropic and without loss of generality primitive. We wish to find a basis for Λ with respect to which the matrix for the bilinear form is of the shape:

$$\left(\begin{smallmatrix} 0 & A & 0 \\ A^t & X & Y \\ 0 & Y^t & Z \end{smallmatrix}\right).$$

To do this, first select an arbitrary basis $\{\tilde{y_1}, \ldots, \tilde{y_\ell}\}$ for L and an extension $\{\tilde{y_1}, \ldots, \tilde{y_\ell}, \tilde{z_1}, \ldots \tilde{z_m}\}$ to a basis for Λ. Next, perform an invariant factor decomposition (see [Jac85, Thm. 3.8]) of the matrix:

$$\left(b_\lambda\left(\tilde{y_i}, \tilde{z_j}\right)\right)_{ij}.$$

This corresponds to an elementary change of basis of both the span of $\{\tilde{y_1}, \ldots, \tilde{y_\ell}\}$ and the span of $\{\tilde{z_1}, \ldots, \tilde{z_m}\}$. The new bases $\{y_1, \ldots, y_\ell\}$ and $\{z_1, \ldots, z_m\}$ combine to provide one in which the bilinear form has the desired shape.

We now take L' as the span of $\{y_1, \ldots, y_\ell, z_1, \ldots, z_\ell\}$. The assertion about discriminants is now a consequence of elementary fact that the determinant of the block matrix $\left(\begin{smallmatrix} 0 & A & 0 \\ A^t & X & Y \\ 0 & Y^t & Z \end{smallmatrix}\right)$ is $(-1)^n \det(A)^2 \det(Z)$, where A is n by n. □

Remark. The above proof gives us slightly more information about what assumptions can be made about the shape of the matrix for the bilinear form.

In some circumstances one may be able to obtain even more refined structure theorems. We have for example the following claim:

Proposition 4.2.13. *Over $\mathbb{Z}$ there exist two isomorphism classes of integral pseudo-hyperbolic lattices of dimension $2n$ with square free discriminants. Letting H be the hyperbolic quadratic module whose matrix is given by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and H' be the pseudo-hyperbolic quadratic module whose matrix is given by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, then the isomorphism classes are precisely H^n and $H^{n-1} \oplus H'$.*

This is a straight forward check.

Proposition 4.2.14. *Every unimodular sublattice $L \subset \Lambda$ of an integral lattice is an orthogonal direct summand. More generally, if $\mathfrak{S}_\Lambda = \mathfrak{a}$ then every $\mathfrak{a}$-modular sublattice $L \subset \Lambda$ is an orthogonal direct summand.*

Proof. We first give a concrete proof assuming R is a PID. In this case the second statement reduces to the first by rescaling the form. We remark that L is primitive.

Let $X = \{x_1, \ldots, x_l\}$ be a basis of L, and $Y = \{x_1, \ldots, x_l, y_1, \ldots, y_k\}$ be an extension of X to a basis for Λ. Write $A_Y = \begin{pmatrix} A_X & V \\ V^t & U \end{pmatrix}$. Since $A_X^{-1}V$ is a matrix with entries in R we may use the change of basis matrix:

$$\begin{pmatrix} \mathrm{Id}_\ell & -A_X^{-1}V \\ 0 & \mathrm{Id}_k \end{pmatrix}.$$

This corresponds to a basis $\{x_1, \ldots, x_l, \tilde{y_1}, \ldots, \tilde{y_k}\}$ and we find $\Lambda = L \perp \langle \tilde{y_1}, \ldots, \tilde{y_k} \rangle$.

Working more generally, that is without assuming the lattice is free, given any $z \in \Lambda$ the assumption that $\mathfrak{S}_\Lambda = \mathfrak{a}$ implies $b_\Lambda(z, \cdot) \in \mathrm{Hom}_R(\Lambda, \mathfrak{a})$. It then follows that $b_\Lambda(z, \cdot)|_L \in \mathrm{Hom}_R(L, \mathfrak{a})$. Now, by the $\mathfrak{a}$-modularity of L we have $\mathrm{Hom}_R(L, \mathfrak{a}) \simeq L$ and thus $b_\Lambda(z, \cdot)|_L \in \mathrm{Hom}_R(L, \mathfrak{a}) \simeq L$. We may therefore conclude that there exists $x \in L$ with $b_\Lambda(z - x, \cdot)|_L = 0$. It follows that $z - x \in L^\perp$ and hence $z = x + (z - x)$ is a decomposition of Λ into $L \oplus L^\perp$. $\square$

4.3 Lattices over p-adic Rings

Here we enter into the improved setting of having R a (complete) local ring whose maximal ideal is principal, generated by π. More specifically we intend to work with a p-**adic ring**, by which we mean the maximal order of a p-adic field (a finite extension of $\mathbb{Q}_p$). We shall denote by $\nu = \nu_\pi$ the π-adic valuation.

In this context we have the following important result to recall:

Theorem 4.3.1. *A quadratic module over a p-adic field K is entirely determined by its rank, its discriminant and its Hasse invariant.*

See [O'M00, Thm 63:20].

Notation 4.3.2. For $a, b \in R$, with $ab \neq 1$, we shall denote by $L_{a,b}$ the binary lattice whose bilinear form has matrix $\left(\begin{smallmatrix} a & 1 \\ 1 & b \end{smallmatrix}\right)$.

For $0 \neq c \in R$ we shall denote by U_c the unary lattice whose bilinear form has matrix (c).

For a lattice L and an element $r \in R$ we shall denote by rL the lattice whose underlying module is L but whose bilinear form is r times that of L, that is, $b_{rL} = rb_L$.

Lemma 4.3.3.

1. *$L_{a,b} = U_{c_1} \oplus U_{c_2}$ if and only if one of a, b or 2 is in $R^\times$.*
2. *The discriminant of $L_{a,b}$ is $-(1-ab)$.*
3. *The Hasse invariant of $L_{a,b}$ is $(a, 1-ab)_\mathfrak{p} = (b, 1-ab)_\mathfrak{p}$.*
4. *Let M be any integral lattice, suppose $\beta = b_M(x,x)$ for some $x \in M$ and $u \in R^\times$, if $L_{a+u^{-1}\beta,b}$ is unimodular then:*

$$uL_{a,b} \oplus M = uL_{a+u^{-1}\beta,b} \oplus M'$$

for some lattice M'. In the case $b = 0$ then $uL_{a+u^{-1}\beta,b}$ is unimodular and moreover $M' \simeq M$.

Proof. For the first point, in the forward direction use the fact that every unimodular sublattice is a direct summand, together with the determinant of the matrix. For the other direction, use the fact that if none of a,b or 2 is a unit, then $\mathfrak{N}_{L_{a,b}} \neq R$ and is unimodular whereas if $U_{c_1} \oplus U_{c_2}$ is unimodular then $\mathfrak{N}_{U_{c_1} \oplus U_{c_2}} = R$.

The second point is a direct calculation. For the third, notice that over K we have the change of basis:

$$\begin{pmatrix} 1 & 0 \\ -a^{-1} & 1 \end{pmatrix} \begin{pmatrix} a & 1 \\ 1 & b \end{pmatrix} \begin{pmatrix} 1 & -a^{-1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & b - a^{-1} \end{pmatrix}.$$

Thus the Hasse invariant is $(a, b - a^{-1})_\mathfrak{p} = (a, 1 - ab)_\mathfrak{p}$ (using that $(a, -a)_\mathfrak{p} = 1$).

The argument for the forth point is [O'M00, 93:12]. If x, y is the basis for $uL_{a,b}$ and $z \in M$ satisfies $b_M(z,z) = \beta$, then the lattice spanned by $x + z, y$ is isomorphic to $uL_{a+u^{-1}\beta,b}$, and as it is unimodular we have by Proposition 4.2.14 that it is a direct factor of $uL_{a,b} \oplus M$. For the special case of $b = 0$, consider $\phi : M \to uL_{a+u^{-1}\beta,b} \oplus M'$ given by $\phi(u) = u - (u,z)y$. One checks easily that this is an isometry, and that the image of M is in M'. The existence of an inverse map $\phi'(u) = u + (u,z)y$ mapping M' to M implies ϕ is an isometry between M and M'. □

Lemma 4.3.4. *Every lattice Λ over a p-adic ring R can be expressed as:*

$$\Lambda = L \oplus \Lambda',$$

where L has rank 1 or 2. Moreover, L can be taken to be $\mathfrak{a}$-modular for some $\mathfrak{a}$. Note that neither L nor Λ' are unique.

Proof. Pick either $x \in \Lambda$ such that $q_\Lambda(x)R = \mathfrak{S}_\Lambda$ or x, y in Λ such that $(x,y)\,R = \mathfrak{S}_\Lambda$. This is possible since as we are working over a discrete valuation ring, and $\mathfrak{S}_\Lambda$ has generators $\{b_\Lambda(x_i, y_i)\}$, the principle of domination tells us that there exists a single pair (x_i, y_i) with $b_\Lambda(x_i, y_i)R = \mathfrak{S}_\Lambda$. If for such a pair $q_\Lambda(x_i)R = \mathfrak{S}_\Lambda$ work only with x_i, otherwise, work with the pair (x_i, y_i).

In the first case, the lattice spanned by x is an $\mathfrak{S}_\Lambda$-modular direct factor. In the second case, the lattice spanned by x, y is an $\mathfrak{S}_\Lambda$-modular direct factor. Here we are using that in the respective cases the matrix is of the form:

$$(\pi^r) \qquad \text{or} \qquad \begin{pmatrix} a\pi^{r+1} & \pi^r \\ \pi^r & b\pi^r \end{pmatrix},$$

where $\mathfrak{S}_\Lambda = \pi^r R$ and $a, b \in R$ and that these matrices give π^r-modular lattices. The sublattice then splits as a direct factor by Proposition 4.2.14. □

Theorem 4.3.5 (Existence of Jordan Decompositions)**.** *Every lattice Λ over a p-adic ring R can be expressed as:*

$$\Lambda \simeq \oplus_i L_i,$$

where the L_i are $\mathfrak{a}_i$-modular, with the $\mathfrak{a}_i$ distinct. Such a decomposition is called a ***Jordan Decomposition****. Note that such decompositions are not in general unique, but see Theorem 4.3.14.*

Proof. This follows immediately by induction from the lemma above, and by grouping the factors which have the same modularity. □

Example. As an example, the above results and some straight forward computations allow one to check that every lattice over $\mathbb{Z}_2$ is a direct sum of lattices of the form $2^k U_c$ and $2^k L_{a,b}$ for $k \in \mathbb{Z}$, $c \in \mathbb{Z}_2^\times$ and $a, b \in \{2, 4, 6, 8\}$. See Theorem 4.3.12 for a more thorough classification.

It should be remarked that in spite of the following "Witt type theorem," a decomposition $\Lambda = L_1 \oplus K_1 = L_2 \oplus K_2$ with $L_1 \simeq L_2$ does not imply $K_1 \simeq K_2$.

Theorem 4.3.6 (Knesser)**.** *Let R be a local ring with unique maximal ideal $\mathfrak{p}$. Let $L_1, L_2 \subset \Lambda$ be submodules of Λ and $F \subset \Lambda$ be a subset satisfying:*

1. *$\frac{1}{2} q_\Lambda(F)$ and $b_\Lambda(F, \Lambda)$ are both subsets of R,*
2. *$\mathrm{Hom}(L_1, R), \mathrm{Hom}(L_2, R) \subset \{b_\Lambda(x, \cdot) \mid x \in F\}$, where $b_\Lambda(x, \cdot)$ is viewed as a map from Λ to R, and*
3. *$\sigma : L_1 \to L_2$ an isometry such that $\sigma(x) - x \in F$ for all $x \in L_1$.*

Then σ can be extended to an isometry of Λ which acts trivially on $F^\perp$. Moreover, if F contains an element z such that:

1. *$q_\Lambda(z) \in 2R^\times$ and,*
2. *if the residue field is $\mathbb{F}_2$, then also $(F, z) \subset \mathfrak{p}$,*

then σ is induced by products of reflections in elements of F.

Proof. See [Kit93, Thm 1.2.2].

We may reduce to the case where we have the 'moreover' assumption as follows: adjoin a hyperplane H, spanned by x, y, to Λ and $R(x+y) \subset H$ to F, Rx to both L_1 and L_2 and extend σ by setting $\sigma(x) = x$. As $(x+y)^{\perp}$ would include $x - y$, the isometry which the theorem guarantees exists must be trivial on both x and $x - y$ and hence y and thus on H. Hence σ has a restriction to the original Λ , though no longer coming from reflections in F.

Now we suppose we satisfy the 'moreover' assumptions. First we claim that for all $\ell \in L_1$ there exists $f \in F$ such that $\frac{1}{2}q(f), (f, \ell), (f, \sigma(\ell)) \in R^{\times}$. Indeed, let z_1 be the element from the moreover statement, z_2 be such that $(\ell, z_2) \in R^{\times}$ and z_3 be such that $(\sigma(\ell), z_3) \in R^{\times}$, and if $|R/\pi| \neq 2$ suppose $a^2 \not\equiv 1 \pmod{\pi}$ then one of:

$$(\sigma(\ell)-\ell), z_1, z_2, z_3, z_1+z_2, z_1+z_3, z_2+z_3, z_1+z_2+z_3, az_1+z_2, az_1+z_3, az_1+z_2+z_3$$

satisfies the condition. One uses the fact that if a does not exist we have $(x, F) \subset \pi$.

For an element $y \in \Lambda$ with $\frac{1}{2}q(y) \in R^{\times}$ define the reflection in y as $\tau_y(\ell) = \ell - 2(y, \ell)q(y)^{-1}r$.

We proceed by induction on the rank of L_1. Suppose the rank of L_1 is 1 and that it is generated by ℓ. There are two cases. If we may take $f = \sigma(\ell) - \ell$ to be the element above, then we find:

$$\tau_f(\ell) = \sigma(\ell).$$

Otherwise, let f be the element from above and set $g = \sigma(\ell) - \tau_f(\ell)$. One then computes that $\frac{1}{2}q(g) \in R^{\times}$ and

$$\tau_g(\tau_f(\ell)) = \sigma(\ell).$$

This completes the rank 1 case.

Suppose L has rank r. Let $\ell \in L_1$ be a primitive element, and suppose f is the element guaranteed to exist as above. Set $L_1' = \{y \in L_1 \mid (y, f) = 0\}$. Since $(f, \ell) \in R^\times$ then L_1' is primitive of rank $r-1$. By induction there exists τ generated by reflections in F such that $\tau|_{L_1'} = \sigma|_{L_1'}$. Now, taking instead $\tau^{-1}\sigma$ for σ, $F \cap L_1'^{\perp}$ for F and $L_1 = R\ell$, we find that we again satisfy the conditions of the theorem. Hence there exists τ' with $\tau'(\ell) = \tau^{-1}\sigma(\ell)$. Since $L' \subset F^\perp$ we have $\tau'|_{L_1'} = \mathrm{Id}$. It follows that $\tau \circ \tau'|_{L_1} = \sigma$. □

Corollary 4.3.7. *Suppose R is a p-adic ring. Let M_1, M_2 be integral R lattices and $N_1 = N_2$ unimodular lattices with $\mathfrak{N}_{N_1} \subset (2)$. Then $N_1 \oplus M_1 \simeq N_2 \oplus M_2$ implies that $M_1 \simeq M_2$.*

Proof. Identify $\Lambda := N_1 \oplus M_1$ with $N_2 \oplus M_2$ via any isomorphism. In the notation of the above theorem, take $L_1 = N_1$, $L_2 = N_2$, and $F = \Lambda$. The map which identifies N_1 and N_2 thus extends to an isometry of Λ which necessarily maps $M_1 = N_1^\perp$ to $N_2^\perp = M_2$. □

Lemma 4.3.8. *For $p \neq 2$ every unimodular lattice Λ over a p-adic ring R with rank at least 3 has a hyperbolic sublattice.*

Proof. Using Hensel's lemma and the existence of an isotropic vector mod π we conclude there exists an isotropic vector in Λ. By Propositions 4.2.12 and 4.2.14 and the unimodularity of Λ we conclude that Λ has a pseudo-hyperbolic direct factor. An easy calculation shows that since 2 is invertible all unimodular pseudo-hyperbolic lattices are hyperbolic. □

Corollary 4.3.9. *For $p \neq 2$ and a p-adic ring R, the isomorphism classes of unimodular lattices Λ over R are classified by their rank and discriminant.*

Proof. By induction, we may show $\Lambda = H^n \oplus L$, where L is unimodular and has rank 0,1 or 2. It then suffices to observe that the discriminant classifies binary and unary unimodular forms when $p \neq 2$. □

Lemma 4.3.10. *Suppose $p = 2$, then the isomorphism classes of unimodular lattices Λ over R are determined by their rank, discriminant, Hasse invariant and norm groups.*

Proof. See [O'M00, 93:16].

We assume that L and K have the same rank, discriminant, Hasse invariant and norm groups. By Corollary 4.3.7 we may replace L and K by $L \oplus H$ and $K \oplus H$, respectively, so that we may also assume that $q_L(L) = q_K(K) = \mathfrak{n}_L$. We will show that:

$$L \oplus H^{\operatorname{rank} L} = L \oplus -L \oplus L = K \oplus -L \oplus L = K \oplus H^{\operatorname{rank} L}$$

and hence hyperbolic cancellation (Corollary 4.3.7) on $H^{\operatorname{rank} L}$ will allow us to conclude $K = L$. Indeed, both $K \oplus -L$ (respectively, $L \oplus -L$) is pseudo-hyperbolic. Now using that $q(K \oplus -L) \subset q(L)$ (respectively, $q(L \oplus -L) \subset q(L)$ and $q(L \oplus -L) \subset q(K)$) we may change the bases for $K \oplus -L \oplus L$, by Lemma 4.3.3 (4), so that $K \oplus -L \oplus L = H^{\operatorname{rank} L} \oplus L$. In the respective cases the same argument shows $L \oplus -L \oplus L = H^{\operatorname{rank} L} \oplus L$ and $K \oplus -L \oplus L = H^{\operatorname{rank} L} \oplus K$. This concludes the result. □

Lemma 4.3.11. *For a lattice L over a 2-adic ring letting $a\pi^t$ be an element of minimal valuation in $\mathfrak{n}_L$ we find: $\mathfrak{n}_L = a\pi^t R^2 + \mathfrak{w}_L$.*

Proof. See [O'M00, 93:3].

Certainly we have $a\pi^t R^2 \subset \mathfrak{n}_L$, and by definition $\mathfrak{w}_L \subset \mathfrak{n}_L$, hence:

$$a\pi^t R^2 + \mathfrak{w}_L \subset \mathfrak{n}_L.$$

Conversely, any element $z \in \mathfrak{n}_L$ of valuation at least t has an expression of the form:

$$z = a\pi^t x^2 + a\pi^{t+1} y^2 \pmod{2\pi^t}.$$

Since $a\pi^t x^2, 2\pi^t \in \mathfrak{n}_L$ we have $a\pi^{t+1} y^2 \in \mathfrak{n}_L$.

We claim $\pi^{t+1}y^2z \in \mathfrak{n}_L$ for all $z \in R$. Indeed, write $\pi^{t+1}y^2z = a\pi^t u^2 + a\pi^{t+1}y^2v^2 \pmod{2\pi^t}$ with $u, v \in R$. By the subgroup structure of $\mathfrak{n}_L$ we find $\pi^{t+1}y^2z \in \mathfrak{n}_L$.

We now claim $a\pi^t y^2 z \in \mathfrak{n}_L$ for all z. By solving the equation:

$$a\pi^t y^2 z = a\pi^t v^2 \pmod{\pi^{t+1}}$$

we see that as $a\pi^t v^2 \in \mathfrak{n}_L$ by the subgroup structure of $\mathfrak{n}_L$ we find $\pi^t y^2 z \in \mathfrak{n}_L$. It follows that $\pi^t y^2 \subset \mathfrak{m}_L$. Therefore $\pi^{t+1}y^2z \in \mathfrak{w}_L$. This concludes the result. $\square$

Theorem 4.3.12. *Let L be a unimodular lattice over a 2-adic ring R with uniformizer π. Fix $\alpha \in R^\times$ such that $\delta_L = -(1+\alpha\pi^r)$ modulo $(R^\times)^2$, such that furthermore either r is odd or $r = \nu(4)$. Fix also $a \in R^\times$ such that $a\pi^t \in q_L(L)$ is an element of minimal valuation represented by L. Then $\mathfrak{w}_L = (\pi^s)$, where $r-t \geq s \geq t$ and $s+t$ is odd or $s = \nu(2)$. Let $\rho \in R/\pi R$ be such that $x^2+x+\rho$ is irreducible mod π.*

Then L is isomorphic to precisely one of:

1. $H^n \oplus \begin{pmatrix} \pi^s & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} a\pi^t & 1 \\ 1 & -a^{-1}\alpha\pi^{r-t} \end{pmatrix}$,
2. $H^n \oplus \begin{pmatrix} \pi^s & 1 \\ 1 & 4\rho\pi^{-s} \end{pmatrix} \oplus \begin{pmatrix} a\pi^t & 1 \\ 1 & -a^{-1}(\alpha - 4\rho)\pi^{r-t} \end{pmatrix}$,
3. $H^n \oplus \begin{pmatrix} \pi^s & 1 \\ 1 & 0 \end{pmatrix} \oplus (-\delta_L)$,
4. $H^n \oplus \begin{pmatrix} \pi^s & 1 \\ 1 & 4\rho\pi^{-s} \end{pmatrix} \oplus (-(1-4\rho)\delta_L)$,
5. $\begin{pmatrix} a\pi^t & 1 \\ 1 & -a^{-1}\alpha\pi^{r-t} \end{pmatrix}$ *or*
6. $(-(1-\alpha\pi^r))$.

Proof. This is a consequence of Lemma 4.3.10. One only needs to observe that these examples cover all possible combinations of ranks, discriminants, Hasse invariants and norm groups. Lemma 4.3.11 allows one to check we have all of the possible norm groups. The observation that $(1+4\rho, \pi)_{\mathfrak{p}} = -1$ allows one to check we have all possible Hasse invariants. □

Corollary 4.3.13. *Every unimodular lattice Λ over a 2-adic ring R with rank at least 5 has a hyperbolic sublattice.*

It should be emphasized before stating the following result that Jordan decompositions over 2-adic rings are not typically unique.

Theorem 4.3.14 (Uniqueness of Jordan Decompositions)**.** *Let $\Lambda = \bigoplus_{i=1}^{r_1} L_i = \bigoplus_{j=1}^{r_2} K_j$ be two Jordan decomposition of a lattice over a p-adic ring with L_i being $\mathfrak{a}_i$-modular and K_j being $\mathfrak{b}_j$-modular, $\mathfrak{a}_{i_1}|\mathfrak{a}_{i_2}$ for $i_1 < i_2$, and $\mathfrak{b}_{j_1}|\mathfrak{b}_{j_2}$ for $j_1 < j_2$. Then:*

1. $r_1 = r_2$,
2. $\mathfrak{a}_i = \mathfrak{b}_i$,
3. $\operatorname{rank} L_i = \operatorname{rank} K_i$,
4. $\mathfrak{N}_{L_i} = \mathfrak{a}_i$ *if and only if* $\mathfrak{N}_{K_i} = \mathfrak{a}_i$*, and*
5. *if* $p \neq 2$ *then* $L_i \simeq K_i$.

Proof. See [O'M00, 91:9].

Let $a \in R$. Consider $\Lambda^{(a)} = \{x \in \Lambda \mid (x, \Lambda) \subset (a)\} = a\Lambda^{\#} \cap \Lambda$. Observe that forming $^{(a)}$ commutes with orthogonal direct sums, and that for a modular lattice $L^{(a)} = L$ if and only if L is a-modular. Otherwise $L^{(a)} \subset \pi L$.

It follows that the sublattices L_i and K_j which are the (π^r)-modular in the Jordan decomposition are characterized modulo π^{r+1} by the reduction modulo π of $\frac{1}{\pi^r}(L^{(\pi^r)})$. In particular, the rank, discriminant, and whether or not the diagonal contains a unit modulo π are determined. This completes the proof. □

4.4 Local Densities

We now move from general theory to a more particular problem, that is, we now focus our attention on what are called interchangeably representation densities, local densities or arithmetic volumes. Throughout this section we shall continue to assume that R is a p-adic ring, with maximal ideal $\mathfrak{p}$. We shall denote by π a uniformizer and $q = |R/\mathfrak{p}R|$ the size of the residue field, which is finite by assumption. We shall fix an additive Haar measure on R, normalized so that the volume of R is 1. In this context we continue to have that all lattices are free.

4.4.1 Notion of Local Densities

Fundamentally the notion of representation density has to do with assigning a volume to sets of the form:

$$\mathrm{Isom}(\Lambda_1, \Lambda_2) = \{\phi \in \mathrm{Hom}_R(\Lambda_1, \Lambda_2) \mid b_{\Lambda_2}(\phi(x), \phi(y)) = b_{\Lambda_1}(x, y)\},$$

the isometric embeddings from Λ_1 to Λ_2. Such sets are typically infinite, so simply counting elements is insufficient.

This problem can be approached both locally and globally and there are a number of different ways to formulate the notion. The various definitions are typically, up to constants, equivalent. We take the following definition of local density; for some the α definition is more natural.

Definition 4.4.1. Let L and M be lattices over a p-adic ring R, with bilinear forms b_L, b_M. Consider the map $\mathcal{F}_{b_L} : \mathrm{Hom}_R(M, L) \to \mathrm{Sym}^2(M^\vee)$ which takes the maps from M to L to the space of symmetric bilinear forms on M given by $(\mathcal{F}_{b_L}(\phi))(x, y) = b_L(\phi(x), \phi(y))$. Some references define the **local density** at R to be:

$$\alpha_R(b_M, b_L) = \alpha_R(M, L) = \tfrac{1}{2} \lim_{U \to b_M} \frac{\int_{\mathcal{F}_{b_L}^{-1}(U)} dX}{\int_U dT}.$$

Here $dX = \prod_{ij} dx_{ij}$ and $dT = \prod_{i \le j} dt_{ij}$ are the standard measures when viewing the spaces as matrix spaces with respect to some chosen basis. The limit is being taken over the directed family of open subset U of $\mathrm{Sym}^2(M^\vee)$ containing b_M. By [Han05, Lemma 2.2] this does not depend on the choice of integral basis.

We define the local density to be:

$$\beta_R(M,L) = (q^{-\operatorname{rank}(M)v_\pi(2)})\alpha_R(M,L).$$

When $R = \mathcal{O}_\mathfrak{p}$ one often denotes the local densities by $\beta_\mathfrak{p}$ rather than β_R.

The above definition may seem quite unwieldy and difficult to compute. The following proposition gives a more concrete interpretation of these values.

Proposition 4.4.2. *Let R be a p-adic ring with residue field $\mathbb{F}_q$ and uniformizer π. Let M and N be two quadratic modules over R of ranks m and n, respectively. Fix $h \in \mathbb{Z}$ sufficiently large so that $\pi^{h-1}q_M(M^\#) \in (2)$ and $\pi^{h-1}q_N(N) \in (2)$, and let $r, r' \in \mathbb{Z}$ be such that $r, r' - \nu(2) \geq h$. Denote $\xi_r = (q^r)^{m(m+1)/2-mn}$ then define $B_R(M,N,r)$ to be:*

$$\xi_r \cdot |\{\phi \in \mathrm{Hom}_R(M, N/\pi^r N) \mid b_N(\phi(x),\phi(x)) = b_M(x,x) \pmod{2\pi^r}\}|$$

and define $A_R(M,N,r')$ to be:

$$\xi_{r'} \cdot \left|\{\phi \in \mathrm{Hom}_R(M, N/\pi^{r'} N) \mid b_N(\phi(x),\phi(y)) = b_M(x,y) \pmod{\pi^{r'}}\}\right|.$$

These values are independent respectively of r and r'. Moreover,

$$\beta_R(M,N) = B_R(M,N,r) \text{ and } \alpha_R(M,N) = A_R(M,N,r').$$

Proof. These results are a combination of [Han05, Lemma 3.2] and [Kit93, Lemmas 5.6.1 and 5.6.5].

We first claim that our choice h is such that the isomorphism class of M is determined by the reduction modulo r' of the bilinear form. To this end, it suffices to show that this holds for any expression of $M = \oplus L_i$, where the L_i are binary and unary modular lattices. Notice that if there exists a unary factor $(a\pi^t)$ (with $\nu(a) = 0$) then by definition $r' \geq 2\nu(2) + t + 1$. Hence, for unary lattices we can determine a modulo 4π, and hence we can determine the isomorphism class. Next, notice that if there exists a binary factor $\pi^t \left(\begin{smallmatrix} a\pi^s & 1 \\ 1 & b\pi^u \end{smallmatrix}\right)$ (with $\nu(a), \nu(b) = 0$, and $s, u \geq 1$) then now by definition $r' \geq 2\nu(2) - \min(s, u) + t + 1$ and hence we can determine the discriminant of $\left(\begin{smallmatrix} a\pi^s & 1 \\ 1 & b\pi^u \end{smallmatrix}\right)$ modulo 4π, the Hasse invariant and the norm group, and hence the isomorphism class.

We now show that $A_R(M, N, r')$ is independent of r'. Let $b_{M,i}$ be a set of bilinear forms on M whose reductions modulo $\pi^{r'+1}$ forms a complete set of representatives of bilinear forms modulo $\pi^{r'+1}$ (up to equality) whose reduction modulo $\pi^{r'}$ equals b_M. There are precisely $q^{m(m+1)/2}$ such $b_{M,i}$. Let M_i denote the lattice M with quadratic form $b_{M,i}$.

We claim $A_R(M_i, N, r' + 1)$ is independent of i. It suffices to show that $\mathrm{GL}(M/\pi^{r'+1}M)$ acts transitively on the $b_{M,i}$, or equivalently that M_i and M are isomorphic as lattices. This follows since the isomorphism class of M is determined by its reduction modulo $\pi^{r'}$. The value $A_R(M_i, N, r' + 1)$ is therefore independent of i. It follows from the fact that the map:

$$\sqcup_i \{\phi \in \mathrm{Hom}_R(M_i, N/\pi^{r'+1}N) \mid b_N(\phi(x), \phi(y)) = b_{M_i}(x, y) \pmod{\pi^{r'+1}}\}$$

$$\downarrow$$

$$\{\phi \in \mathrm{Hom}_R(M, N/\pi^{r'}N) \mid b_N(\phi(x), \phi(y)) = b_M(x, y) \pmod{\pi^{r'}}\}$$

is q^{mn} to 1 we may now conclude that $A_R(M, N, r') = A_R(M, N, r' + 1)$ and is thus independent of r'.

A similar argument covers the case of $B_R(M, N, r)$.

Next, we cover the claim that $\alpha_R(M, N) = A_R(M, N, r')$. For the integral definition one may take for U those sets of the form $b_M + \pi^{r'}\,\mathrm{Sym}^2(M^\vee)$ as these form a fundamental neighbourhood system. For such U the collection $\mathcal{F}_{b_L}^{-1}(U)$ becomes precisely the maps which reduce modulo $\pi^{r'}$ to those contributing in the definition of $A_R(M,N,r')$. The volume of U is then $q^{r'mn}$ whereas the volume of $\mathcal{F}_{b_L}^{-1}(U)$ is precisely $A_R(M,N,r')q^{r'm(m+1)/2}$. From this we conclude the result.

The difference between the definition of $A_R(M,N,r')$ and $B_R(M,N,r')$ is entirely captured in a slight change in flexibility on the diagonal. This leads to a difference of a factor of $q^{-\operatorname{rank}(M)v_\pi(2)}$ between the two terms. This allows us to conclude that $\beta_R(M,N) = B_R(M,N,r)$. Notice in particular that an element of the set defining $B_R(M,N,r)$ determines an element of the set defining $A_R(M,N,r-\nu(2))$ and that this mapping is $q^{\operatorname{rank}(M)v_\pi(2)}$ to 1. □

Remark. It can be useful to think of the local density as counting the number of elements of $\operatorname{Isom}(M,N)$, or of it as being the probability that a linear map is in $\operatorname{Isom}(M,N)$ (even though it is not literally either of those things, it is a rescaling of these numbers when one thinks of L/π^r for large r).

Proposition 4.4.3. *Suppose that $L = L_1 \oplus L_2$ and the following hypothesis is satisfied:*

$$L_1 \oplus L_2 \simeq M_1 \oplus M_2 \text{ and } L_1 \simeq M_1 \text{ implies } L_2 \simeq M_2.$$

Then for any lattice L_3 we have the following formula:

$$\beta_R(L_1 \oplus L_3, L) = \beta_R(L_1, L)\beta_R(L_3, L_2).$$

Proof. This follows immediately from the description in terms of counting isometries and book-keeping the rescaling constants. □

Remark. This type of 'cancellation law' does not hold in general, nonetheless, one can use cases where it does hold (see for example Corollary 4.3.7) as a way to inductively prove formulas for representation densities.

4.4.2 Computing Local Densities

Computing local densities is in general considered to be highly technical. The resulting formulas become quite complicated in the general case. In spite of this, in this section we will compute the local densities $\beta_{\mathfrak{p}}(L, L)$ for an arbitrary lattice over an arbitrary p-adic ring. The combinatorics behind actually carrying out the computation in any given case will require detailed understanding of the isomorphism class of the given lattice. In particular one needs to be able to compute the set of all possible Jordan decompositions. We will thus not present complete formulas for this in the most general cases. Instead, we give a reduction formula in terms of these combinatorics and formulas for all the terms that can appear.

The general structure of this section is as follows:

1. Reduce the problem for (π^t)-modular lattices to unimodular lattices. See in particular Proposition 4.4.4.
2. Reduce the problem for unimodular lattices to the special case of certain lattices of rank at most 4, see Theorem 4.4.11.
3. Compute the representation density for these special cases. This is done in a series of lemmas culminating in Theorem 4.4.18.
4. Reduce the general problem for an arbitrary lattice to the combinatorial problem of understanding all the Jordan decompositions together with the problem for modular lattices. See Theorem 4.4.28.

♦ Rescaling

Our first step is an elementary lemma which allows us to compute the local density of rescaled lattices.

Proposition 4.4.4. *Let R be a p-adic ring with field of fractions K. Let M and L be lattices over R and $c \in K^\times$. The following formula holds:*

$$\beta_R(M, L) = |c|_\pi^{m(m+1)/2}\, \beta_R(cM, cL),$$

where $m = \operatorname{rank}(M)$.

Proof. This is an elementary computation, see [Han05, Lemma 3.1]. □

As a consequence of the above proposition, it is possible to compute $\beta_R(L, L)$ in the case of $\mathfrak{a}$-modular lattices simply by treating the case of unimodular lattices.

Remark. There is no reasonable formula for $\beta_R(cM, L)$ or $\beta_R(M, cL)$ in terms of $\beta_R(M, L)$ unless we make further assumptions. In particular some of these could be 0 while the others are not.

⧫ Unimodular Lattices

We now discuss the problem of computing the local density $\beta_R(L, L)$ for a unimodular lattice.

Lemma 4.4.5. *Suppose L is any unimodular lattice and $L(e)$ is any even unimodular lattice. The following formula holds:*

$$\beta_R(L(e) \oplus L, L(e) \oplus L) = \beta_R(L(e), L(e) \oplus L) \cdot \beta_R(L, L).$$

Proof. This follows immediately from Corollary 4.3.7 and Proposition 4.4.3. □

Lemma 4.4.6. *Suppose L is a unimodular lattice and $L(e)$ is any even unimodular lattice of rank $2n$. Set $\Lambda = L \oplus L(e)$ then define:*

$$L^{(2)} := \{x \in L \mid (x, x) \in 2R\} \text{ and } \Lambda^{(2)} := \{x \in \Lambda \mid (x, x) \in 2R\}.$$

Then $L^{(2)}$ and $\Lambda^{(2)}$ are lattices, $\Lambda^{(2)} = L(e) \oplus L^{(2)}$, and:

$$\beta_R(L(e), \Lambda) = [L : L^{(2)}]^{-2n} \beta_R(L(e), \Lambda^{(2)}).$$

Proof. Denote by $\xi_r = (q^r)^{n-2n^2-2n\ell}$. Now pick r sufficiently large so that $\pi^r L \subset L^{(2)}$. It follows that $\beta_R(L(e), \Lambda)$ is given by:

$$\xi_r \cdot \left|\{\phi \in \mathrm{Hom}_R(L(e), \Lambda/\pi^r\Lambda) \mid q(x) = q(\phi(x)) \pmod{2\pi^r}\}\right|,$$

and $\beta_R(L(e), \Lambda^{(2)})$ is given by:

$$\xi_r \cdot \left|\{\phi \in \mathrm{Hom}_R(L(e), \Lambda^{(2)}/\pi^r(\Lambda^{(2)})) \mid q(x) = q(\phi(x)) \pmod{2\pi^r}\}\right|.$$

Then because $L(e)$ is even, it is clear that $\beta_R(L(e), \Lambda)$ can be computed as:

$$\xi_r \cdot \left|\{\phi \in \mathrm{Hom}_R(L(e), \Lambda^{(2)}/\pi^r\Lambda) \mid q(x) = q(\phi(x)) \pmod{2\pi^r}\}\right|.$$

For each element $\phi \in \mathrm{Hom}_R(L(e), \Lambda^{(2)}/\pi^r\Lambda)$, there are precisely $[L : L^{(2)}]^{2n}$ many extensions of ϕ to a map in $\mathrm{Hom}_R(L(e), \Lambda^{(2)}/\pi^r\Lambda^{(2)})$, all of which automatically satisfy $q(x) = q(\phi(x)) \pmod{2\pi^r}$ as that condition was already well-defined. Comparing formulas completes the proof. □

Lemma 4.4.7. *Suppose L is a unimodular lattice of rank ℓ and $L(e)$ is any even unimodular lattice of rank $2n$. Define Λ, $L^{(2)}$ and $\Lambda^{(2)}$ as above. Consider the vector spaces $V_1 = L(e)/\pi L(e)$ and $V_2 = \Lambda^{(2)}/\pi\Lambda^{(2)}$ together with the quadratic form $\tilde{Q}_i(x) = \frac{1}{2}(x, x) \pmod{\pi}$ for their respective pairings valued in $R/\pi R$. Then the local density $\beta_R(L(e), \Lambda^{(2)})$ is:*

$$q^{n-2n^2-2n\ell}\left|\{\sigma : V_1 \to V_2 \mid \tilde{Q}_1(x) = \tilde{Q}_2(\sigma(x)) \text{ for all } x\}\right|.$$

Proof. Firstly we observe by Proposition 4.4.2 that $\beta_R(L(e), \Lambda^{(2)})$ is:

$$q^{n-2n^2-2n\ell}\left|\{\sigma : L(e) \to \Lambda^{(2)}/\pi\Lambda^{(2)} \mid q(x) = q(\sigma(x)) \pmod{2\pi}\}\right|.$$

Secondly, we observe that:

$$\left|\{\sigma : L(e) \to \Lambda^{(2)}/\pi\Lambda^{(2)} \mid q(x) = q(\sigma(x)) \pmod{2\pi}\}\right| = \left|\{\sigma : V_1 \to V_2 \mid \tilde{Q}_1(x) = \tilde{Q}_2(\sigma(x))\}\right|.$$

The result then follows immediately. □

Remark. The space V_2 may not be a regular quadratic module.

Definition 4.4.8. For a regular quadratic module V of dimension $2n$ we define:

$$\chi(V) = \begin{cases} 1 & V \simeq H^n \text{ and } n > 0 \\ -1 & \text{otherwise.} \end{cases}$$

Lemma 4.4.9. *Every quadratic module W over a field of characteristic 2 decomposes as:*

$$W_0 \oplus W' \oplus \mathrm{Rad}(W)$$

with W_0 a maximal regular sublattice and $W^\perp = W' \oplus \mathrm{Rad}(W)$. Note that the isomorphism class of W_0 is unique if and only if $W^\perp = \mathrm{Rad}(W)$.

See [Kit93, Thm 1.2.1 and Ex. 1.2.2].

Lemma 4.4.10. *Suppose V is a (non-trivial) regular quadratic module represented by W, that is, for which there exists at least one isometry from V into W. Write $W = W_0 \oplus W^\perp$ as in Lemma 4.4.9 and set $v = \dim(V)$ and $w = \dim(W_0)$. The number of isometries from V into W is:*

$$q^{v\dim(W) - v(v+1)/2} \left(\prod_{e=(w-v)/2+1}^{w/2-1} (1 - q^{-2e}) \right) (1 - \chi(W_0) q^{-w/2}) \xi,$$

where ξ is given by:

$$\xi = \begin{cases} 1 + \chi(V \oplus -W_0) q^{(v-w)/2} & W^\perp = \mathrm{Rad}(W) \\ 1 + \chi(W_0) q^{-w/2} & W^\perp \neq \mathrm{Rad}(W). \end{cases}$$

See [Kit93, Prop 1.3.3].

Remark. Notice that the above formula, which appears to depend on a choice of W_0 in W, does so only when $W^\perp = \mathrm{Rad}(W)$.

Theorem 4.4.11. *Consider a unimodular lattice Λ. Then Λ has a decomposition $\Lambda = L(e) \oplus L$, where $L(e)$ is a maximal even dimensional even unimodular sublattice of Λ and L has rank at most 4. Let $\ell = \mathrm{rank}(L)$ and*

$2n = \mathrm{rank}(L(e))$. *Then:*

$$\beta_R(\Lambda, \Lambda) = [L : L^{(2)}]^{-2n} \xi \beta_R(L, L) \prod_{e=1}^{n} (1 - q^{-2e}),$$

where:

$$\xi = \begin{cases} 2(1 + \chi(L(e)) q^{-n})^{-1} & L(e) \text{ non-trivial and independent of choices} \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Such a decomposition exists by Theorem 4.3.12. Lemma 4.4.5 gives us the formula:

$$\beta_R(L(e) \oplus L, L(e) \oplus L) = \beta_R(L(e), L(e) \oplus L) \cdot \beta_R(L, L).$$

Lemma 4.4.6 allows us to evaluate:

$$\beta_R(L(e), L(e) \oplus L) = [L : L^{(2)}]^{-2n} \beta_R(L(e), L(e) \oplus L^{(2)}).$$

Lemma 4.4.7 then reduces the computation of $\beta_R(L(e), L(e) \oplus L^{(2)})$ to a computation over the residue field. Finally, Lemma 4.4.10 gives the precise formula for this computation. Combining the results allows us to conclude the theorem. □

Remark. If $L(e)$ is as above, then one has $\chi(L(e)) = (\pi, (-1)^{n/2} D(L(e)))_{\mathfrak{p}}$.

Corollary 4.4.12. *Suppose $p \neq 2$ and maintain the notation of Theorem 4.4.11, then:*

$$\beta_R(\Lambda, \Lambda) = 2 \prod_{e=1}^{n} (1 - q^{-2e}) \begin{cases} (1 + \chi(L(e)) q^{-n})^{-1} & \ell = 0 \\ 1 & \ell = 1. \end{cases}$$

Proof. When $p \neq 2$ all lattices are even and hence we have that L is either 0 or 1-dimensional. The result now follows immediately from the theorem and the observation that for a 1-dimensional lattice the representation density is 2. □

♦ **Unimodular Lattices of Rank at Most 4**

We are now left only to consider the case where the residue characteristic is 2. Theorem 4.4.11 reduces this case to that of computing $\beta_R(L,L)$ and of understanding $L^{(2)}$, in the case of L unimodular of rank at most 4 with no even unimodular factors. Such low rank unimodular lattices with no even unimodular factors are precisely those appearing as L in Theorem 4.4.11. We first discuss the problems of understanding $L^{(2)}$.

Proposition 4.4.13. *Consider L a unimodular lattice of rank at most 4 over a 2-adic ring with no nontrivial even unimodular factors. Denote by $W = L^{(2)}/\pi L^{(2)}$ with the induced form $\tilde{Q}(x) = \frac{1}{2}(x,x) \pmod{\pi}$. Then we have the following cases:*

- *Case $n = 4$. Write $L = \begin{pmatrix} a\pi^t & 1 \\ 1 & c\pi^{r-t} \end{pmatrix} \oplus \begin{pmatrix} \pi^s & 1 \\ 1 & 4b\pi^{-s} \end{pmatrix}$ with $t < s < r-t$, $t+s$ is odd, and either r odd or $r = \nu(4)$. Then $\mathrm{Rad}(W) \neq W^\perp$. Moreover,*

$$\log_q([L : L^{(2)}]) = \nu(2) - (s+t-1)/2.$$

- *Case $n = 3$. Write $L = \begin{pmatrix} \pi^s & 1 \\ 1 & b\pi^{\nu(4)-s} \end{pmatrix} \oplus (d)$ with $\nu(2) > s > 0$ and s odd. Then $\mathrm{Rad}(W) \neq W^\perp$. Moreover,*

$$\log_q([L : L^{(2)}]) = \nu(2) - (s-1)/2.$$

- *Case $n = 2$, Write L with matrix $\begin{pmatrix} a\pi^t & 1 \\ 1 & c\pi^{r-t} \end{pmatrix}$ with either $r > t$ odd or $r = \nu(4)$. Then $\mathrm{Rad}(W) = W^\perp$ unless $r - t \leq \nu(2)$ or $\nu(2) - t$ is even. Moreover,*

$$\log_q([L : L^{(2)}]) = \begin{cases} \left\lceil \frac{\nu(2)-t}{2} \right\rceil & r - t \geq \nu(2), \\ \nu(2) - (r-1)/2 & \textit{otherwise.} \end{cases}$$

- *Case $n = 1$ Then $\mathrm{Rad}(W) = W^\perp$ unless $\nu(2)$ is even. Moreover,*

$$\log_q([L : L^{(2)}]) = \left\lceil \frac{\nu(2)}{2} \right\rceil.$$

Proof. In each case we will denote the basis with respect to which the matrix is given by $\{\vec{x}_1, \ldots, \vec{x}_n\}$.

The argument shall use the following observation. If $x, y \in L$ are such that $\nu_\pi(q(x))$ is odd and $\nu_\pi(q(y))$ is even, then since:

$$q(\eta x + \theta y) = \eta^2 q(x) + \theta^2 q(y) \pmod 2,$$

the only way to have $\nu_\pi(q(\eta x + \theta y)) \geq \nu_\pi(2)$ is to have both $2\nu_\pi(\eta) + \nu_\pi(q(x)) \geq \nu_\pi(2)$ and $2\nu_\pi(\theta) + \nu_\pi(q(y)) \geq \nu_\pi(2)$.

The observation allows us to easily compute bases for the following three cases. In the case of $n = 1$ it is clear that a basis for $L^{(2)}$ is:

$$\{\pi^{\lceil \nu_\pi(2)/2 \rceil} \vec{x}_1\}.$$

In the case of $n = 2$ a basis for $L^{(2)}$ is:

$$\{\pi^{\lceil (\nu_\pi(2)-t)/2 \rceil} \vec{x}_1, \pi^{\max(0, \lceil (\nu_\pi(2)-(r-t))/2 \rceil)} \vec{x}_2\}.$$

In the case of $n = 3$ a basis for $L^{(2)}$ is:

$$\{\pi^{\lceil (\nu_\pi(2)-s)/2 \rceil} \vec{x}_1, \vec{x}_2, \pi^{\lceil \nu_\pi(2)/2 \rceil} \vec{x}_3\}.$$

For the case of $n = 4$, we can eliminate some of the conditions by using that $t, s \leq r - t$. We do this by fixing η and θ so that:

$$\eta^2 a \pi^t + \theta^2 \pi^s = c \pi^{r-t} \pmod 2.$$

Now a basis for $L^{(2)}$ is:

$$\{\pi^{\lceil (\nu_\pi(2)-t)/2 \rceil} \vec{x}_1, \eta \vec{x}_1 + \vec{x}_2 + \theta \vec{x}_3, \pi^{\lceil (\nu_\pi(2)-s)/2 \rceil} \vec{x}_3, \vec{x}_4\}.$$

It is now an easy calculation to determine $[L : L^{(2)}]$. Moreover, it is apparent that $W^\perp = W$ and thus $\text{Rad}(W) = W^\perp$ if and only if $\tilde{Q}$ is trivial. This is easily checked on the bases we have given. □

We now discuss the problem of computing $\beta_R(L, L)$ for unimodular lattices L of rank at most 4 with no even unimodular factors. The general strategy is as follows:

1. Describe a constructive process for enumerating and counting all choices of basis that give a bilinear form that 'looks like' the original.
2. Show that the number of ways of obtaining each possible form that 'looks like' the original is the same.
3. Count the number of possible forms that 'look like' the original.
4. Obtain the result.

The above is made more precise in the following proofs.

Lemma 4.4.14. *Suppose L is a unimodular lattice of rank 1. Then:*

$$\beta_R(L, L) = 2.$$

This case is a simple check.

Lemma 4.4.15. *Suppose L is the unimodular lattice of rank 2 over a 2-adic ring represented by $\begin{pmatrix} a\pi^t & 1 \\ 1 & c\pi^{r-t} \end{pmatrix}$ with $a, c \in R^\times$, $2t < r$ and either $r < \nu(4)$ odd or $r = \nu(4)$. Then:*

$$\beta_R(L, L) = \begin{cases} 4q^{(r-1)/2-\nu(2)} & r - t \leq \nu(2) \\ 2q^{-\lceil(\nu(2)-t)/2\rceil} & \nu(2) < r - t. \end{cases}$$

Proof. By Proposition 4.4.2 we need to count the elements in the set:

$$\Phi = \{\phi : L \to L/\pi^{\nu(2)-t+1}L \mid q_L(\phi(x)) = q_L(x) \pmod{\pi^{\nu(4)-t+1}}\}.$$

Consider the following sets:

$$X = \{\vec{x} \in L/\pi^{\nu(2)-t+1}L \mid q_L(\vec{x}) = a\pi^t \pmod{\pi^{\nu(4)-t+1}}\},$$

$$Y_{\vec{x}} = \{\vec{y} \in L/\pi^{\nu(2)-t+1}L \mid (\vec{x},\vec{y}) = 1 \pmod{\pi^{\nu(2)-t+1}}, \nu(q(\vec{y})) = r-t\}, \text{ and}$$

$$\tilde{Y} = \{q_L(\vec{y}) \pmod{\pi^{\nu(4)-t+1}} \mid \vec{y} \in Y_{\vec{x}}|,\ \vec{x} \in X\}.$$

We claim that $|Y_{\vec{x}}|$ is independent of the choice of $\vec{x} \in X$. Indeed, letting $\vec{x}_0$ and $\vec{y}_0$ be the original basis it is clear that:

$$Y_{\vec{x}} = \{(\vec{x}, (\vec{x},\vec{y'})^{-1}\vec{y'}) \mid \vec{y'} = (x\pi^{\lceil (r-2t)/2\rceil}\vec{x}_0 + \vec{y}_0)\},$$

where x runs over elements of $R/\pi^{\nu(2)-t+1-\lceil (r-2t)/2\rceil}R$. If follows that:

$$|Y_{\vec{x}}| = q^{\nu(2)+1-\lceil r/2\rceil}.$$

We next compute $\left|\tilde{Y}\right|$. The values of $q_L(\vec{y})$ that can appear are precisely those such that:

$$1 - aq_L(\vec{y})\pi^t = 1 - ac\pi^r \pmod{(R^\times)^2}$$

as these are the values that give isomorphic quadratic forms. This is precisely the same as the number of elements modulo $\pi^{\nu(4)+1}$ that are squares, and congruent to 1 modulo π^r. We thus have:

$$\left|\tilde{Y}\right| = \tfrac{1}{2}q^{\nu(2)+1-\lceil r/2\rceil}.$$

We now compute $|X|$. We are counting solutions for $x, y \pmod{\pi^{\nu(2)-t+1}}$ of:

$$a\pi^t x^2 + 2xy + c\pi^{r-t}y^2 = a\pi^t \pmod{\pi^{\nu(4)-t+1}}.$$

We make the substitution $x = 1 + x$ and this becomes:

$$a\pi^t x^2 + 2a\pi^t x + 2y + 2xy + c\pi^{r-t}y^2 = 0 \pmod{\pi^{\nu(4)-t+1}}.$$

By inspecting the valuations of monomials that result from such a switch (of $x = x + 1$), in particular the parity of their valuations, it is apparent that we have:

$$x = 0 \pmod{\pi^{\max(\nu(2)-(r-1)/2, \lceil(\nu(2)-t)/2\rceil)}} \text{ and}$$
$$y = 0 \pmod{\pi^{\max(\nu(2)+t-r, \nu(2)+t)}},$$

where the first terms are maximal if and only if $\nu(2) \geq r - t$. If we perform the substitutions:

$$x = \pi^{\max(\nu(2)-(r-1)/2, \lceil(\nu(2)-t)/2\rceil)}x' \text{ and } y = \pi^{\max(\nu(2)+t-r, 0)}y'$$

the equation becomes:

$$a\pi^{\nu(2)+\delta}x^2 + 2y + 2\pi P(x, y) = 0 \qquad r - t > \nu(2), \text{ or}$$
$$2y + 2cy^2 + 2\pi P(x, y) = 0 \qquad r - t \leq \nu(2)$$

for some polynomial P and $\delta \in \{0, 1\}$. (Notice the only way we could have had both an x^2 and y^2 term was if $r - t = t = \nu(2)$ but we have excluded that case from consideration). We observe that by dividing by 2 we may solve for y in terms of x. As the equation is non-singular, we may use Hensel's lemma to find solutions and the total number of solutions is equal to the number of solutions modulo π. There are precisely 2 solutions modulo π if $\nu(2) \geq r - t$ and 1 solution otherwise. We thus find:

$$|X| = \begin{cases} 2q^{(r-t-t-1)/2+1} & \nu(2) \geq r - t \\ q^{\lfloor(\nu(2)-t)/2\rfloor+1} & \text{otherwise.} \end{cases}$$

The set Φ corresponds precisely to the fibre of

$$\{(\vec{x}, \vec{y}) \mid \vec{x} \in X, \vec{y} \in Y_{\vec{x}}\}$$

over $c\pi^{r-t} \in \tilde{Y}$. The automorphism group of $L/\pi^{\nu(2)-t+1}L$ acts simply transitively on this fibre. However, noting that the original choice of $c\pi^{r-t}$ is arbitrary, the automorphism group acts simply transitively on each fibre of:

$$\{(\vec{x}, \vec{y}) \mid \vec{x} \in X, \vec{y} \in Y_{\vec{x}}\}$$

over $\tilde{Y}$.

It thus follows that:

$$|\Phi| = \frac{|X|\,|Y_{\vec{x}}|}{\left|\tilde{Y}\right|}.$$

Thus we find:

$$|\Phi| = \begin{cases} 4q^{(r-t-t-1)/2+1} & r-t \leq \nu(2) \\ 2q^{\lfloor(\nu(2)-t)/2\rfloor+1} & \nu(2) < r-t. \end{cases}$$

Combining terms completes the result. □

Lemma 4.4.16. *Suppose $L = L_{\pi^t, b\pi^{\nu(4)-t}} \oplus U_{-d}$ is a unimodular lattice of rank 3 over a 2-adic ring with $t < \nu(2)$ odd and $b, d \in R^\times$, then:*

$$\beta_R(L, L) = 4q^{(1-t)/2}.$$

Proof. By Proposition 4.4.2 we need to count elements in the set:

$$\Phi = \{\phi : L \to L/\pi^{\nu(2)+1}L \mid q_L(\phi(x)) = q_L(x) \pmod{\pi^{\nu(4)+1}}\}.$$

As in the previous lemma consider the following sets:

$$X = \{\vec{x} \in L/\pi^{\nu(4)+1}L \mid q_L(\vec{x}) = \pi^t \pmod{\pi^{\nu(4)+1}}\},$$

$$Y_{\vec{x}} = \{\vec{y} \in L/\pi^{\nu(2)+1}L \mid (\vec{x}, \vec{y}) = 1 \pmod{\pi^{\nu(2)+1}}, \nu(q_L(\vec{y})) = \nu(4)\},$$

$$\tilde{Y} = \{q_L(\vec{y}) \pmod{\pi^{\nu(4)+1}} \mid \vec{y} \in Y_{\vec{x}},\ \vec{x} \in X\},$$

$$Z_{\vec{x},\vec{y}} = \{\vec{z} \in \langle \vec{x}, \vec{y}\rangle^\perp/\pi^{\nu(2)+1} \mid q_L(\vec{z}) = -d \pmod{\pi^{\nu(4)+1}}\}.$$

We claim that $|Y_{\vec{x}}|$ is independent of $\vec{x} \in X$. Indeed, letting $\vec{x}_0, \vec{y}_0, \vec{z}_0$ be the original basis it is clear for parity reasons that:

$$Y_{\vec{x}} = \{(\vec{x}, (\vec{x}, \vec{y'})\vec{y'}) \mid \vec{y'} = x\pi^{\nu(2)-t}\vec{x}_0 + \vec{y}_0 + z\pi^{\nu(2)-(t-1)/2}\vec{z}_0\},$$

where $x \in R/\pi^{t+1}R$ and $z \in R/\pi^{(t-1)/2+1}R$. We thus find:

$$|Y_{\vec{x}}| = q^{t+(t-1)/2+2}.$$

Next we compute $\left|\tilde{Y}\right| = \frac{1}{2}q$. The argument is identical to the previous lemma, except we note that the discriminant of this block is well-defined modulo squares because it controls the Hasse invariant of the form.

Now $|Z_{\vec{x},\vec{y}}| = 2$ independently of $\vec{x}, \vec{y}$. This follows as the orthogonal complement is isomorphic to U_{-d} by necessity, (again because the Hasse invariant controls the discriminant).

We now compute $|X|$. We are counting solutions for $x, y, z \pmod{\pi^{\nu(2)+1}}$ of:

$$\pi^t x^2 + 2xy + \pi^{\nu(4)-t}y^2 + cz^2 = \pi^t \pmod{\pi^{\nu(4)+1}}.$$

It is clear that we may replace z by $\pi^{\lceil \nu(2)/2 \rceil}z$ and get:

$$x^2 + \pi^{\nu(2)-t}xy + b\pi^{\nu(4)-2t}y^2 + c\pi^{\nu(2)+2\lceil \nu(2)/2\rceil - t}z^2 = 1 \pmod{\pi^{\nu(4)-t+1}}.$$

We now replace x by $1 + \pi^{\lceil (\nu(2)-t)/2 \rceil}x$ and the expression modulo $\pi^{\nu(4)-t+1}$ becomes:

$$2\pi^{\lceil (\nu(2)-t)/2\rceil}x + \pi^{2\lceil (\nu(2)-t)/2\rceil}x^2 + \pi^{\nu(2)-t}y +$$
$$\pi^{\lceil 3(\nu(2)-t)/2\rceil}xy + b\pi^{\nu(4)-2t}y^2 + c\pi^{2\lceil \nu(2)/2\rceil - t}z^2 = 0.$$

This reduces to:

$$2\pi^{\delta}x + \pi^{\delta}x^2 + y + \pi^{\delta+\nu(2)-t}xy + b\pi^{\nu(2)-t}y^2 + c\pi^{1-\delta}z^2 = 0 \pmod{\pi^{\nu(2)+1}},$$

where $\delta = \begin{cases} 0 & \nu(2) \text{ odd} \\ 1 & \text{otherwise.} \end{cases}$
As in the previous case, this equation is non-singular in y, hence, for all values of z, x we may find a unique solution for y. It follows that:

$$|X| = q^{\lfloor \nu(2)/2 \rfloor + \lfloor (\nu(2)-t)/2 \rfloor - t + 2} = q^{\nu(2)-(t+1)/2-t+2}.$$

As in the previous lemma it follows that:

$$|\Phi| = 2q^{t+(t-1)/2+1} \, |X| \, |Y_{\vec{x}}| \, |Z_{\vec{x},\vec{y}}| \left| \tilde{Y} \right|^{-1}.$$

We may thus conclude that $|\Phi| = 4q^{3\nu(2)-3t-(t-1)/2+3}$. Combining terms completes the result. □

Lemma 4.4.17. *Suppose $L = L_{\pi^s, b\pi^{\nu(4)-s}} \oplus L_{a\pi^t, c\pi^{r-t}}$ is a unimodular lattice of dimension 4 over a 2-adic ring with $t < s < \nu(2)$, $a, b, c \in R^\times$, $s - t$ odd, and $r < \nu(4)$ odd or $r = \nu(4)$. In this situation:*

$$\beta_R(L, L) = 4q^{-3\nu(2)+2t-2-(r-t-s)/2} \begin{cases} q^{(r-t-t-1)/2+1} & r - t \le \nu(2) \\ q^{\lfloor (\nu(2)-t)/2 \rfloor + 1} & \nu(2) \le r - t \end{cases}$$

Proof. We make the following definitions:

$$\Phi = \{g \in \mathrm{GL}(L/\pi^{\nu(4)-t+1}L) \mid g^t A g = \left(\begin{smallmatrix} \pi^s & 1 \\ 1 & b\pi^{\nu(4)-s} \end{smallmatrix}\right) \oplus \left(\begin{smallmatrix} a\pi^t & 1 \\ 1 & c\pi^{r-t} \end{smallmatrix}\right)\},$$

$$X = \{\vec{x} \in L/\pi^{\nu(2)-t+1}L \mid q_L(x) = \pi^s \pmod{\nu(4) - t + 1}\},$$

$$Y_{\vec{x}} = \{\vec{y} \in L/\pi^{\nu(2)-t+1}L \mid (\vec{x}, \vec{y}) = 1 \pmod{\pi^{\nu(2)-t+1}}, \nu(q_L(\vec{y})) \ge \nu(4) - s\},$$

$$\tilde{Y} = \{q_L(\vec{y}) \in R/\pi^{\nu(4)-t+1}R \mid \vec{y} \in Y_{\vec{x}},\ \vec{x} \in X\},$$

$$Z_{\vec{x},\vec{y}} = \{(\vec{z}, \vec{w}) \in \langle \vec{x}, \vec{y} \rangle^\perp / \pi^{\nu(2)-t+1} \mid (\vec{z}, \vec{w}) = 1 \pmod{\pi^{\nu(2)-t+1}}, \nu(q_L(\vec{z})) = t\},$$

$$\tilde{Z}_{\vec{x},\vec{y}} = \{(q_L(\vec{z}), q_L(\vec{w})) \in (R/\pi^{\nu(4)-t+1}R)^2 \mid (\vec{z}, \vec{w}) \in Z_{\vec{x},\vec{y}}\}$$

$$\hat{Z}_{\tilde{y}} = \{\Lambda \text{ a lattice modulo } \pi^{\nu(4)-t+1} \text{ up to isomorphism} \mid L_{\pi^s, \tilde{y}} \oplus \Lambda \simeq L\}.$$

In the above we are taking $\tilde{y} \in \tilde{Y}$.

Our first claim is that $|Y_{\vec{x}}| = q^{\nu(2)-3t+3+s+(s+t-1))/2}$ and that this is independent of $\vec{x} \in X$. Indeed, we can compute its value as follows:

$$Y_{\vec{x}} = \{(\vec{x}, \vec{y'})^{-1}\vec{y'} \mid \nu(q_L(\vec{y'})) = \nu(4) - s\}.$$

Thus its size is the number of solutions to:

$$\pi^s x^2 + 2x + a\pi^t z^2 + 2zw + c\pi^{r-t} w^2 = 0 \pmod{\pi^{\nu(4)-s}},$$

where x, z, w are taken in $R/\pi^{\nu(2)-t+1}R$. In the event that $r - t > \nu(4) - s$ then for parity reasons we must have:

$$x = 0 \pmod{\pi^{\nu(2)-s}} \text{ and } z = 0 \pmod{\pi^{\nu(2)-(s+t-1)/2}}.$$

One finds then that there are no further conditions and thus counting solutions we find:

$$|Y_{\vec{x}}| = q^{\nu(2)-3t+3+s+(s+t-1)/2}.$$

Otherwise we suppose $r - t \leq \nu(4) - s$. Next we may choose η, ϵ such that:

$$\eta^2 c + \epsilon^2 a\pi = 1.$$

For parity reasons we again find:

$$x = 0 \pmod{\pi^{(r-t-s)/2}} \text{ and } z = 0 \pmod{\pi^{(r+1)/2-t}}.$$

We may thus substitute:

$$x = \pi^{(r-t-s)/2}x' \text{ and } w = \eta x' + w' \text{ and } z = \pi^{(r+1)/2-t}(\epsilon x' + z).$$

The whole expression modulo $\pi^{\nu(4)-s}$ then becomes:

$$2\pi^{(r-t-s)/2}x + \pi^{r-t+1}z^2 + \pi^{r-t}w^2 + \pi^{\nu(2)+(r-t-s)/2+1}P(x, w, z) = 0$$

for some polynomial P. It is now apparent that:

$$z = 0 \pmod{\pi^{\lceil(\nu(2)-(3r-3t-s)/2-1)/2\rceil}} \text{ and } w = 0 \pmod{\pi^{\lceil(\nu(2)-(3r-3t-s)/2)/2\rceil}}$$

and that x is determined modulo $\pi^{\nu(2)-s-(r-t-s)/2}$ by the other parameters. One finds then that there are no further conditions and thus counting solutions we find:

$$|Y_{\vec{x}}| = q^{\nu(2)-3t+3+s+(s+t-1))/2}.$$

Next we compute $\left|\tilde{Y}\right|$. Indeed, so long as there exist values $\alpha, \gamma \in R^{\times}$ such that:

$$L \simeq L_{\pi^s, \beta\pi^{\nu(4)-s}} \oplus L_{\alpha\pi^t, \gamma\pi^{r-t}}$$

then $\beta \in \tilde{Y}$. The two conditions:

$$\mathfrak{n}_L = \alpha R^2 + \pi^s, \text{ and}$$
$$H(L) = (\alpha, \delta_L)(\pi^t, \delta_L)(\pi^{s+t}, 1 - \beta\pi^{\nu(4)})$$

can be solved for all β if $r - t \leq \nu(4) - s$. If however, $r - t > \nu(4) - s$ then, since (α, δ_L) cannot depend on α, only half of the potential values for β will work. The other condition:

$$\delta_L = (1 - \alpha\gamma\pi^r)(1 - \beta\pi^{\nu(4)}) \pmod{R^2}$$

can always be solved by γ. It follows that:

$$\left|\tilde{Y}\right| = q^{s-t+1} \begin{cases} \frac{1}{2} & r - t > \nu(4) - s \\ 1 & \text{otherwise.} \end{cases}$$

We now claim that $\left|\tilde{Z}_{\vec{x},\vec{y}}\right|$ is independent of $\vec{x} \in X$ and $\vec{y} \in Y_{\vec{x}}$. Indeed there are three conditions for $(\alpha, \gamma) \in \tilde{Z}_{\vec{x},\vec{y}}$. The first condition is:

$$H(L) = (\alpha, \delta_L)(\pi^t, \delta_L)(\pi^{s+t}, 1 - q_L(\vec{y})\pi^{\nu(4)}).$$

This condition cannot be unsatisfiable. Hence, it is either imposing a condition (independently of $\vec{y}$), or is not imposing a condition (independently of $\vec{y}$). The second condition is:

$$\mathfrak{n}_L = \alpha R^2 + \pi^s.$$

This condition is independent of $\vec{y}$. The final condition is:

$$\delta_L = (1 - \alpha\gamma\pi^r)(1 - q_L(\vec{y})\pi^{\nu(4)}) \pmod{R^2}.$$

For each α satisfying the first two conditions we are imposing a condition on the variable γ. The number of values for γ satisfying the condition is independent of $\vec{y}$.

Now, we claim that $|Z_{\vec{x},\vec{y}}|$ is independent of $\vec{x} \in X$ and $\vec{y} \in Y_{\vec{x}}$. Indeed, the value of $|Z_{\vec{x},\vec{y}}|$ is precisely $\left|\mathrm{Aut}(\langle \vec{x}, \vec{y}\rangle^{\perp}/\pi^{\nu(4)-t+1})\right| \left|\tilde{Z}_{\vec{x},\vec{y}}\right|$. Our computations in Lemma 4.4.15 show this depends only on t and r. Explicitly, the value is:

$$\left|\mathrm{Aut}(\langle \vec{x}, \vec{y}\rangle^{\perp}/\pi^{\nu(4)-t+1})\right| = \begin{cases} 4q^{(r-t-t-1)/2+1} & r - t \leq \nu(2) \\ 2q^{\lfloor(\nu(2)-t)/2\rfloor+1} & \nu(2) < r - t. \end{cases}$$

Next, we claim that $\left|\hat{Z}_{\tilde{y}}\right|$ is independent of $\tilde{y} \in \tilde{Y}$. Equivalence classes of lattices $\overline{\Lambda} \in \hat{Z}_{\tilde{y}}$ have representatives of the form $L_{\alpha,\gamma}$ where $(\alpha, \gamma) \in \tilde{Z}_{\vec{x},\vec{y}}$ for some $\vec{x} \in X$, $\vec{y} \in Y_{\vec{x}}$. We may thus represent $\overline{\Lambda}$ by $\overline{(\alpha, \gamma)}$. Now, as the Hasse invariant and discriminant of $\Lambda \in \hat{Z}_{\tilde{y}}$ are determined by $\tilde{y}$ and L, the only freedom to modify Λ is picking its norm generator. In terms of $\overline{(\alpha, \gamma)}$ this amount to fixing the square class of α module π^{r-2t}. The first constraint on the square class of α is that it must give the norm generator of L module π^s. This determines the square class of α modulo π^{s-t}. This leaves us with precisely:

$$q^{(r-t-s)/2}$$

many options for such square classes. The only other constraint on α is that it must give the correct Hasse invariant. As above, the Hasse invariant depends on α through (α, δ_L). Thus, it follows that:

$$\left|\hat{Z}_{\tilde{y}}\right| = q^{(r-t-s)/2} \begin{cases} \frac{1}{2} & r - t \leq \nu(4) - s \\ 1 & \text{otherwise.} \end{cases}$$

We now compute $|X|$. We are solving for $x, y, z, w \in R/\pi^{\nu(2)-t+1}R$ in the following equation modulo $\pi^{\nu(4)-t+1}$:

$$\pi^s x^2 + 2xy + b\pi^{\nu(4)-s}y^2 + a\pi^t z^2 + 2zw + c\pi^{r-t}w^2 = \pi^s.$$

Pick η, ϵ such that $\eta^2 + \pi a \epsilon^2 = c \pmod{\pi^{\nu(2)}}$. We may then make the following substitutions:

$$x = 1 + \eta\pi^{\lceil (r-t-s)/2 \rceil} w + x \text{ and } z = \epsilon\pi^{\lceil (r+1)/2 \rceil - t} w + z.$$

The equation then becomes:

$$\pi^s x^2 + 2y + a\pi^t z^2 + 2zw + \pi^{\nu(2)+1} P(x, y, z, w) = 0$$

for some polynomial P. For parity reasons we now see that:

$$x = 0 \pmod{\pi^{\lceil (\nu(2)-s)/2 \rceil}} \text{ and } z = 0 \pmod{\pi^{\lceil (\nu(2)-t)/2 \rceil}}.$$

This equation is now solvable in y, and determines y modulo $\pi^{\nu(2)-t+1}$. Counting solutions, we find that there are:

$$|X| = q^{\nu(4)-3t+3+(s+t-1)/2)}.$$

We now observe that:

$$|\Phi| = |X| \, |Y_{\vec{x}}| \, |Z_{\vec{x},\vec{y}}| \left|\tilde{Y}\right|^{-1} \left|\tilde{Z}_{\vec{x},\vec{y}}\right|^{-1} \left|\hat{Z}_{\tilde{y}}\right|^{-1}.$$

To see this, consider the map:

$$\{(\vec{x},\vec{y},\vec{z},\vec{w}) \mid \vec{x}\in X,\ \vec{y}\in Y_{\vec{x}},\ (\vec{z},\vec{w})\in Z_{\vec{x},\vec{y}}\} \to (R/\pi^{v(4)-t+1}R)^3$$

given by $(\vec{x},\vec{y},\vec{z},\vec{w}) \mapsto (q_L(\vec{y}), q_L(\vec{z}), q_L(\vec{w}))$ and observe that $|\Phi|$ is precisely the size of each fibre. We thus must show that the size of the image is:

$$\left|\tilde{Y}\right| \left|\tilde{Z}_{\vec{x},\vec{y}}\right| \left|\hat{Z}_{\tilde{y}}\right|.$$

The image of this map is precisely:

$$\{(\tilde{y},\tilde{z},\tilde{w}) \mid \tilde{y}\in\tilde{Y},\ \overline{(\tilde{z},\tilde{w})}\in\hat{Z}_{\tilde{y}}.\}$$

This set is naturally fibred over:

$$\{(\tilde{y},\overline{(\alpha,\gamma)}) \mid \tilde{y}\in\tilde{Y},\ \overline{(\alpha,\gamma)}\in\hat{Z}_{\tilde{y}}\}.$$

Moreover, the size of the fibre over $(\tilde{y},\overline{(\alpha,\gamma)})$ is precisely $\left|\tilde{Z}_{\vec{x},\vec{y}}\right|$ where $\vec{x}\in X$ and $\vec{y}\in Y_{\vec{x}}$ are any vectors such that $(\alpha,\gamma)\in\tilde{Z}_{\vec{x},\vec{y}}$. From this the claim about $|\Phi|$ follows immediately.

We, therefore, have that:

$$\left|\mathrm{Aut}(L/\pi^{\nu(4)-t+1}L)\right| = 4q^{3\nu(2)-4t+4-(r-t-s)/2}\begin{cases} q^{(r-t-t-1)/2+1} & r-t\le\nu(2)\\ q^{\lfloor(\nu(2)-t)/2\rfloor+1} & \nu(2)\le r-t\end{cases}$$

Combining terms gives the desired result. □

The above lemmas cover the final few cases we needed to completely solve the problem of computing local densities for unimodular lattices over 2-adic rings. By combining the results we get the following theorem:

Theorem 4.4.18. *Consider a unimodular lattice L of rank at most 4 over a 2-adic ring R with no even unimodular factors. Let π be a uniformizer of R and $q=|R/\pi R|$. Recall that $L^{(2)}=\{x\in L\mid (x,x)\in 2R\}$. Denote by W the* *quadratic module* $L^{(2)}/\pi L^{(2)}$ *with the induced form* $\tilde{Q}(x) = \frac{1}{2}(x,x) \pmod{\pi}$. *Then:*

- *Case* $n = 4$. *Write* $L = \begin{pmatrix} a\pi^t & 1 \\ 1 & c\pi^{r-t} \end{pmatrix} \oplus \begin{pmatrix} \pi^s & 1 \\ 1 & 4b\pi^{-s} \end{pmatrix}$ *with* $t < s < r - t$, $t + s$ *is odd, and either* r *odd or* $r = \nu(4)$.

  Then $\mathrm{Rad}(W) \neq W^{\perp}$. *Moreover,* $[L : L^{(2)}] = q^{\nu(2)-(s+t-1)/2}$ *and the local density is:*

$$\beta_R(L,L) = 4q^{-3\nu(2)+2t-2-(r-t-s)/2} \begin{cases} q^{(r-t-t-1)/2+1} & r - t \le \nu(2) \\ q^{\lfloor(\nu(2)-t)/2\rfloor+1} & \nu(2) \le r - t \end{cases}$$

- *Case* $n = 3$. *Write* $L = \begin{pmatrix} \pi^s & 1 \\ 1 & b\pi^{\nu(4)-s} \end{pmatrix} \oplus (d)$ *with* $\nu(2) > s > 0$ *and* s *odd.*

  Then $\mathrm{Rad}(W) \neq W^{\perp}$. *Moreover,* $[L : L^{(2)}] = q^{\nu(2)-(s-1)/2}$ *and the local density is:*

$$\beta_R(L,L) = 4q^{(1-t)/2}.$$

- *Case* $n = 2$. *Write* L *with matrix* $\begin{pmatrix} a\pi^t & 1 \\ 1 & c\pi^{r-t} \end{pmatrix}$ *with either* $r > t$ *odd or* $r = \nu(4)$.

  Then $\mathrm{Rad}(W) = W^{\perp}$ *unless* $r - t \le \nu(2)$ *or* $\nu(2) - t$ *is even.*

  Moreover, $[L : L^{(2)}] = \begin{cases} q^{\left\lceil \frac{\nu(2)-t}{2} \right\rceil} & r - t \ge \nu(2) \\ q^{\nu(2)-(r-1)/2} & \textit{otherwise} \end{cases}$ *and the local density is:*

$$\beta_R(L,L) = \begin{cases} 4q^{(r-1)/2-\nu(2)} & r - t \le \nu(2) \\ 2q^{-\lceil(\nu(2)-t)/2\rceil} & \nu(2) < r - t. \end{cases}$$

- *Case* $n = 1$. *Then* $\mathrm{Rad}(W) = W^{\perp}$ *unless* $\nu(2)$ *is even.*

  Moreover, $[L : L^{(2)}] = q^{\left\lceil \frac{\nu(2)}{2} \right\rceil}$ *and the local density is:*

$$\beta_R(L,L) = 2.$$

♦ The Case of $\mathbb{Z}_p$

Of course things are much simpler over $\mathbb{Z}_p$, or any p-adic ring except for 2-adic rings which are ramified over $\mathbb{Z}_2$. In such cases there are in fact only a small number of possibilities for unimodular lattices L with no even unimodular factors. In this context one can recover the results in Kitaoka's book which give formulas for the local densities of unimodular lattices over $\mathbb{Z}_p$.

Theorem 4.4.19. *Let L be a unimodular $\mathbb{Z}_p$-lattice. Let $L(e)$ be any maximal unimodular (even dimensional) even sublattice of L. We then have a decomposition $L = L(e) \oplus L(o)$. Let $n = \mathrm{rank}(L)$ and $n(e) = \mathrm{rank}(L(e))$ and set:*

$$t = \begin{cases} 0 & L \text{ is even} \\ n-2 & L \text{ is odd,} \end{cases}$$

$$E = \begin{cases} (1+\chi(L(e))p^{-n(e)/2}) & \chi(L(e)) \text{ is independent of choice of } L(e), \\ 1 & \text{otherwise;} \end{cases} \quad \text{and}$$

$$P = \prod_{j=1}^{\left\lfloor \frac{n_i(e)}{2} \right\rfloor} (1-p^{-2j}).$$

Note that for $p = 2$ the isomorphism class of lattice $L(e)$, and hence $\chi(L(e))$, depends on a choice if and only if $\mathrm{rank}(L(o)) = 2$ and the discriminant satisfies $\delta_{L(o)} = 1 \pmod 4$, whereas for $p \neq 2$ one has $L(e)$ depends on a choice if and only if the rank of L is odd.

Then the local density is:

$$\beta_p(L, L) = 2p^{-t} P E^{-1}.$$

Proof. This is the effect of carrying out the computations of [Kit93, Thm 5.6.3] for a single unimodular Jordan block. Notice that we have renormalized E and that this is accounted for by t.

We now compare to our results. For the case $p \neq 2$ we are comparing to Corollary 4.4.12 and it suffices to observe the equivalence between the condition $\chi(L(e))$ is independent of choice of $L(e)$ and the statement that the rank of L is odd. Indeed, any quadratic form in 3 variables over $\mathbb{Z}_p$ with $p \neq 2$ represents both a hyperplane, and a two dimensional unimodular lattice which is not a hyperplane. Hence when the rank of L is odd, when picking $L(e)$ we may make either of these choices so that $L(e)$ depends on choice. When the rank L is even $L = L(e)$ and there is no choice.

For the case $p = 2$ we must apply Theorem 4.4.11 and Theorem 4.4.18. Theorem 4.4.11 gives us the formula:

$$\beta_p(L, L) = [L : L^{(2)}]^{-n(e)} \xi \beta_R(L(o), L(o)) \prod_{e=1}^{n} (1 - q^{-2e}),$$

where:

$$\xi = \begin{cases} 2(1 + \chi(L(e))q^{-n})^{-1} & L(e) \text{ non-trivial and independent of choices} \\ 1 & \textit{otherwise.} \end{cases}$$

The first thing to observe is that over $\mathbb{Z}_2$ the classification of unimodular lattices (Theorem 4.3.12) implies that $L(o)$ has rank 0, 1 or 2. In the case of rank 0 the result is immediate as $L = L^{(2)}$ and there are no choices. In the case of rank 1 Theorem 4.4.18 gives us that $[L : L^{(2)}] = 2$, $\beta_R(L(o), L(o)) = 2$ and $\chi(L(e))$ is always independent of choices. The factors then combine to give the desired formula.

Finally , in the case of rank 2, we first observe that in Theorem 4.4.18 the constant r is 1 if $\delta_q = 1 \pmod 4$ and 2 otherwise whereas the constant t must be 0. Consequently the theorem gives us that $[L : L^{(2)}] = 2$,

$$\beta_R(L(o), L(o)) = \begin{cases} 2 & \delta_q = 1 \pmod 4 \\ 1 & \delta_q = 3 \pmod 4. \end{cases}$$

and finally $\chi(L(e))$ is independent of choices unless $\delta_q = 1 \pmod 4$. It is now an easy check to compare the resulting formulas. □

Corollary 4.4.20. *The local density of a unimodular lattice for a non-dyadic p-adic ring is determined entirely by its rank and discriminant mod π.*

The local density of a unimodular lattice for a dyadic p-adic ring is determined entirely by its rank, discriminant mod 4, Hasse invariant and norm group.

Proof. Over $\mathbb{Z}_p$ this is apparent from the formulas above, though the result holds more generally. Indeed, for the non-dyadic case this information determines the lattice. In the dyadic case, this follows by inspection of the computation we performed.

Concretely over $\mathbb{Z}_2$ one can compute that $\chi = 0$ when $n - n(e) = 2$ and $D = (-1)^{n(e)/2} \pmod 4$ otherwise χ is given by:

$$\chi = \begin{cases} (-1,-1)^{n(e)(n(e)-2)/8} H & n = n(e) \\ ((-1)^{n(e)/2}, (-1)^{n(e)/2} D)(-1,-1)^{n(e)(n(e)-2)/8} H & \text{otherwise.} \end{cases}$$

This is based on the observation that in the first case the isomorphism class is not well defined, and in the latter two cases the Hasse invariant of the odd part is trivial, hence we can easily compute the Hasse invariant of $L(e)$. Noting that $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$ have different Hasse invariants allows us to distinguish them in this way. □

♦ General Lattices - Jordan Decompositions

Computing local densities is equivalent to computing $|\mathrm{Aut}(L/\pi^r L)|$ which can be done indirectly by computing the probability that a randomly chosen element of $\mathrm{GL}(L/\pi^r L)$ preserves the quadratic form on L. Once one is working in the realm of probabilities, it is natural to use conditional probabilities that are easier to compute to arrive at a solution. This is the approach we shall take.

We shall use the following notation.

Notation 4.4.21. Let R be a p-adic ring, with uniformizer π and $|R/\pi| = q$. Suppose L is a lattice over R.

By a Jordan decomposition I of L we mean a decomposition:

$$L = \oplus L_i^I,$$

where the L_i^I are unimodular and ordered by valuations of their scale ideals. Two Jordan decompositions, I and J, are considered isomorphic if $L_i^I \simeq L_i^J$ for all i. We will denote by JD_L the set of all Jordan decompositions of L up to isomorphism.

We fix r sufficiently large so that the isomorphism classes of all of the L_i^J are determined by their reductions modulo π^r.

We shall say a matrix A which represents the quadratic form on L is in the **Jordan form** $I \in JD_L$ (modulo π^r) if A has a block diagonal decomposition $\oplus A_i$, where the A_i represent modular lattices in ascending order and A_i represents L_i^I for some choice of basis for each i.

Lemma 4.4.22. *Let A be any matrix representation for L. Then the probability that for $g \in \mathrm{GL}(L/\pi^r L)$ the matrix $g^t A g$ is in Jordan form (modulo π^r) is:*

$$P_{JD,r} = |\mathrm{GL}(L/\pi^r L)|^{-1} \left(\prod_i \left| \mathrm{GL}(L_i^I/\pi^r L_i^I) \right| \right) q^w,$$

where $w = \sum_i (2r - i) n_i \sum_{j>i} n_j$.

Proof. The proof is an inductive exercise in book keeping. We first count the number of ways of finding a minimal modular block. In order to pick a set of vectors which will span a minimally modular block one needs to select a $\mathrm{GL}(L_i^I/\pi^r L_i^I)$ combination of the vectors that were in the original minimally modular block. One can then give an arbitrary contribution from the vectors which were complementary to the minimal modular block. This arbitrary choice contributes a factor of $q^{rn_i \sum_{j>i} n_j}$.

We then must proceed inductively on the space which is orthogonally complementary. The degree of freedom in picking an orthogonally complementary space (modulo π^r) is precisely $q^{(r-i)n_i \sum_{j>i} n_j}$.

Taking products of number of choices at each inductive steps gives us the result. □

Definition 4.4.23. Let $I \in JD_L$. Suppose that $g \in \mathrm{GL}(L/\pi^r L)$ is chosen at random. Suppose $g^t A g$ is in Jordan form (modulo π^r). Denote the conditional probability probability that the Jordan form J of $g^t A g$ is equal to I as Jordan decompositions (modulo π^r) as given that $g^t A g$ is in Jordan form (modulo π^r) as:

$$P_{I=J,r}.$$

Lemma 4.4.24. *Let A be any matrix representation for L. Let $I \in JD_L$. Fix a matrix A_I representing the Jordan form I. Suppose that for a random $g \in \mathrm{GL}(L/\pi^r L)$ the matrix $g^t A g$ is in Jordan form $J \in JD_L$ (modulo π^r). Moreover, suppose $I = J$ as Jordan decompositions. Then the conditional probability that $g^t A g = A_I \mod \pi^r$ is:*

$$P_{eq,I,r} = \prod_i \frac{\left|\mathrm{Aut}(L_i^I/\pi^r L_i^I)\right|}{\left|\mathrm{GL}(L_i^I/\pi^r L_i^I)\right|}.$$

Proof. The set of possible values of $g^t A g$ is acted upon by $\prod_i \mathrm{GL}(L_i^I/\pi^r L_i^I)$ with the size of the stabilizer being $\left|\prod_i \mathrm{Aut}(L_i^I/L_i^I \pi^r)\right|$. In particular, then the probability that we get any given representative is $\prod_i \frac{\left|\mathrm{Aut}(L_i^I/L_i^I \pi^r)\right|}{\left|\mathrm{GL}(L_i^I/\pi^r L_i^I)\right|}$. □

Lemma 4.4.25. *Let A be any matrix representation for L. Let $I \in JD_L$. Fix a matrix A_I representing the Jordan form I. The absolute probability that an* *element $g \in \mathrm{GL}(L/\pi^r L)$ gives $g^t A g = A_I \mod \pi^r$ is:*

$$P_{Aut,L,r} = P_{JD,r} P_{I=J,r} P_{eq,I,r}.$$

Proof. This is a trivial statement in conditional probabilities. □

Remark. Notice that $P_{\mathrm{Aut},L,r}$ and $P_{JD,r}$ are independent of the choice of I while $P_{I=J,r}$ and $P_{\mathrm{eq},I,r}$ depend on the choice.

Lemma 4.4.26. *With all the notation as above, we have the formula:*

$$P_{Aut,L,r} = P_{JD,r} \left(\sum_{I \in JD_L} P_{eq,I,r}^{-1} \right)^{-1}.$$

Proof. By observing that $P_{\mathrm{eq},I,r} \neq 0$ for all I we may write:

$$P_{\mathrm{Aut},L,r} P_{\mathrm{eq},I,r}^{-1} = P_{JD,r} P_{I=J,r}.$$

By summing over $I \in JD$ we obtain:

$$P_{\mathrm{Aut},L,r} \sum_{I \in JD} P_{\mathrm{eq},I,r}^{-1} = P_{JD,r} \sum_{I \in JD} P_{I=J,r}.$$

Since $\sum_{I \in JD} P_{I=J,r} = 1$ we obtain the result. □

Lemma 4.4.27. *Suppose L is a lattice of rank ℓ then:*

$$\beta_R(L,L) = q^{\ell v_\pi(2) + r\ell(1-\ell)/2} \left| \mathrm{GL}(L/\pi^r L) \right| P_{Aut,L,r}.$$

Proof. This is immediate from Proposition 4.4.2 and the definition of the probability. □

Combining the above lemmas we arrive at the following very general theorem.

Theorem 4.4.28. *With the notation as above we have:*

$$\beta_R(L,L) = q^w \left(\sum_{I \in JD} \prod_i \beta_R(L_i^I, L_i^I)^{-1} \right)^{-1} = q^{\tilde{w}} \left(\sum_{I \in JD} \prod_i \beta_R(\tilde{L}_i^I, \tilde{L}_i^I)^{-1} \right)^{-1},$$

where $\tilde{L}_i^I$ *is the unimodular rescaling of* L_i^I *and* $w, \tilde{w}$ *are given by:*

$$w = \sum_i i n_i (\sum_{j>i} n_j) \text{ and}$$
$$\tilde{w} = w + \sum_i (n_i(n_i+1)/2).$$

Proof. This is a direct calculation. The only tricky part is the book-keeping on the exponents of q. □

Remark. In order to use this theorem to derive specific formulas for a given lattice one must understand the set JD_L. For a non-dyadic ring there is a unique Jordan decomposition. The problem is thus fully solved in this case.

For the dyadic case it is worth remembering that most of the factors involved in the formula of local density for a unimodular lattice do not depend on the isomorphism class. Hence there are many terms which can be factored out of the sum. Moreover, whenever there is dependence on the isomorphism class through $\chi(L_i(e))$ it is typically symmetric and cancels out. Both of these phenomenon can be seen in the structure of the formulas over $\mathbb{Z}_2$ in the next theorem.

We now state the formulas from Kitaoka's book for $\mathbb{Z}_p$ explicitly as they will be of use.

Theorem 4.4.29 (Kitaoka)**.** *Let* L *be a* $\mathbb{Z}_p$*-lattice. Let* $L = \oplus_i L_i$*, where the* L_i *are non-trivial* p^{a_i}*-modular lattices with distinct* a_i*. Let* $L_i(e)$ *be any maximal even dimensional unimodular even sublattice such that we may write*

$L_i = L_i(e) \oplus L_i(o)$. *Define the following values:*

$$n_i = \operatorname{rank}(L_i),$$
$$n_i(e) = \operatorname{rank}(L_i(e)),$$
$$s = \left|\{i \mid n_i \neq 0\}\right|,$$
$$w = \sum_i a_i n_i \left((n_i+1)/2 + \sum_{a_j > a_i} n_j \right),$$

and set

$$\chi(i) = \begin{cases} 0 & n_i = 0 \\ 0 & p \neq 2 \text{ and } n_i \text{ odd} \\ 0 & p = 2 \text{ and one of } a_i - 1, a_i + 1 \text{ blocks is odd} \\ 0 & p = 2, L_i \text{ odd }, n_i \text{ even and } D(L_i) \neq (-1)^{n_i/2} \pmod 4 \\ \chi(L_i(e)) & \text{otherwise.} \end{cases}$$

For $p \neq 2$ *set* $t = 0$ *and* $u = 0$, *if* $p = 2$ *set:*

$$t = \sum_i \begin{cases} 0 & L_i = 0 \text{ and } a_i - 1, a_i + 1 \text{ blocks are even} \\ -1 & L_i = 0, \text{ one of } a_i - 1, a_i + 1 \text{ blocks is odd} \\ 0 & L_i \neq 0 \text{ is even} \\ 0 & L_i \text{ is odd } a_i + 1 \text{ block is even} \\ 1 & L_i \text{ is odd } a_i + 1 \text{ block is odd,} \end{cases}$$

and

$$u = \sum_i \begin{cases} n_i & L_i \text{ is odd} \\ 0 & \text{otherwise.} \end{cases}$$

Finally set:

$$E_i = 1 + \chi(i) p^{-n_i(e)/2} \quad \text{and} \quad P(m) = \prod_{j=1}^{m} (1 - p^{-2j}).$$

Then we have the following formula for the local density:

$$\beta_p(L, L) = 2^{s-t} p^{w-u} \prod_i P\left(\left\lfloor \tfrac{n_i(e)}{2} \right\rfloor\right) E_i^{-1}.$$

Proof. This is only a slight modification of [Kit93, Thm 5.6.3], we have adjusted the definition of E, introduced the value u and modified t accordingly. □

Remark. The proof of Kitaoka is not in the spirit of the probabilistic argument we gave above. We will not fully derive this result from our previous result; we will, however, explain why the formula is in the shape one should expect.

The first thing to notice is that the only way to have multiple Jordan decompositions is to have Jordan blocks which are odd. This explains why conditions on the presence of odd Jordan blocks appear in the theorem.

The next thing to notice is that having a different isomorphism class for one Jordan block does not change which formulas can appear for other Jordan blocks, even though it may change which precise isomorphism classes can occur. The effect of this is that the sum over Jordan decompositions can be factored as a product of sums over the formulas that appear for each Jordan block. The observation that $(1+q^{-e})+(1-q^{-e}) = 2$ then accounts for some of the factors of 2 which appear in the formulas. The conditions in the definition of t account mostly for these extra powers of 2, as well as the number of Jordan decompositions. The parameter u accounts mostly for $[L_i : L_i^{(2)}]^{-n_i}$.

The following corollaries are useful for computing explicitly local densities in special cases. They eliminate the need to explicitly find all the invariants of the Jordan blocks.

Corollary 4.4.30. *Suppose $p \neq 2$ and L_p is a $\mathbb{Z}_p$-lattice with exactly 2 Jordan blocks which are p^j, p^{j+1} modular and of dimension n_j, n_{j+1}, respectively. Then the Local density of L_p is determined entirely by the ranks of the blocks, and the discriminant D and Hasse invariant H of L_p.*

In particular the local density is:

$$4q^{j(n_j+n_{j+1})(n_j+n_{j+1}+1)/2+n_{j+1}(n_{j+1}+1)/2}\prod_{i=1}^{\lfloor n_j/2\rfloor}(1-q^{-2i})\prod_{i=1}^{\lfloor n_{j+1}/2\rfloor}(1-q^{-2i})\xi,$$

where:

$$\xi=\begin{cases}(1+\chi(j)q^{n_j/2})^{-1}(1+\chi(j+1)q^{n_{j+1}/2})^{-1} & n_j, n_{j+1} \textit{ even}\\ (1+\chi(j)q^{n_j/2})^{-1} & n_j \textit{ even and } n_{j+1} \textit{ odd}\\ (1+\chi(j+1)q^{n_{j+1}/2})^{-1} & n_j \textit{ odd and } n_{j+1} \textit{ even}\\ 1 & \textit{otherwise.}\end{cases}$$

One can compute $\chi(i)$ *as:*

$$\chi(i)=\begin{cases}0 & n_i \textit{ odd}\\ (p,-1)_p^{(i+1)(n_j+n_{j+1})/2}(p,D)_p^{i+1}H & \textit{both blocks even}\\ (p,-1)_p^{(i+1)(n_j+n_{j+1}-1)/2}H & \textit{otherwise.}\end{cases}$$

Proof. One only needs to check that the computations for $\chi(i)$ are accurate, otherwise this is simply evaluating the Theorem 4.4.29 in this case. Checking χ is simply a matter of computing the Hasse invariant for a diagonal form and its rescaling by p. Then by observing the dependence on the discriminant of each block in the various cases we may conclude the result. □

Corollary 4.4.31. *Suppose* $p = 2$ *and* L_p *is a* $\mathbb{Z}_p$*-lattice with exactly* 2 *Jordan blocks which are* p^j, p^{j+1} *modular and of dimension* n_j, n_{j+1}*, respectively. Then the Local density of* L_p *is determined entirely by the ranks and parities of the blocks and the discriminant and Hasse invariants of* L_p*. Note that a method for computing the local densities is made explicit in the proof.*

Proof. We shall denote by D and H the discriminant and Hasse invariant of L_p and by D_i and H_i the discriminant and Hasse invariants of the ith modular block. We shall, as necessary, compute these in order to make implicit use of

Corollary 4.4.20. Set:

$$w = j(n_j + n_{j+1})(n_j + n_j + 1)/2 + n_{j+1}(n_{j+1} + 1)/2.$$

There are 4 cases to consider depending on the parities of the blocks.

1. Both the p^j and p^{j+1} blocks are odd.

   There are at least 4 and potentially more Jordan decompositions. Importantly, each 'formula' appears equally often so that the sums resolve cleanly and are independent of the isomorphism classes of blocks.

   One can check that Kitaoka's formula (Theorem 4.4.29) is independent of the isomorphism class of the blocks and depends only on dimension. In particular the local density is:

$$2^{w+n+5} \prod_{i=1}^{n_j(e)/2} (1 - p^{-2i}) \prod_{i=1}^{n_{j+1}(e)/2} (1 - p^{-2i}).$$

2. The p^j block is odd and the p^{j+1} block is even.

   In this case there are 2 Jordan decompositions. The formula for exactly one of the two blocks changes, cancelling its contribution. We only need to know the contribution of the other block.

   Without loss of generality the p^{j+1} block is hyperbolic. Thus the p^{j+1} block has determinant $(-1)^{n_{j+1}/2}$ and Hasse invariant $(-1,-1)^{\ell(\ell+2)/8}$. We can thus determine both the determinant and Hasse invariant of the p^j block. The determinant is $(-1)^{n_{j+1}/2}D$ and the Hasse invariant is:

$$(-1,-1)^{n_{j+1}(n_{j+1}+2)/8+n_{j+1}/2}(-1,D)^{n_{j+1}/2}.$$

   Consequently, Corollary 4.4.20 tells us that $\chi(j) = 0$ if $n_j - n_j(e) = 2$ and $D = (-1)^{(n_j(e)+n_{j+1})/2} \pmod 4$, and that otherwise $\chi(j)$ is give by:

$$(2,D)_2^{j(n_j+n_{j+1}-1)}(-1,-1)^{(n_{j+1}+n_j(e))(n_{j+1}+n_j(e)+2)/8}(D,-1)_2^{(n_{j+1}+n_j(e))/2}H.$$

Therefore, the local density can be explicitly computed as:

$$2^{w+n_j+3}(1+\chi(j)p^{n_j(e)/2})^{-1}\prod_{i=1}^{n_j(e)/2}(1-p^{-2i})\prod_{i=1}^{n_{j+1}(e)/2}(1-p^{-2i}).$$

3. The p^j block is even and the p^{j+1} block is odd.

   In this case there are 2 Jordan decompositions. The formula for exactly one of the two blocks changes cancelling its contribution. We only need to know the contribution of the other block.

   Without loss of generality the p^j block is hyperbolic. Thus this block has determinant $(-1)^\ell$ and Hasse invariant $(-1)^{\ell/2}$. We can thus determine both the determinant and Hasse invariant of the p^{j+1} block. Consequently, Corollary 4.4.20 tells us that $\chi(j+1)=0$ if $n_{j+1}-n_{j+1}(e)=2$ and $D=(-1)^{(n_{j+1}(e)+n_j)/2} \pmod 4$, otherwise $\chi(j+1)$ is:

$$(2,D)^{(j+1)(n_j+n_{j+1}-1)}(-1,-1)^{(n_j+n_{j+1}(e))(n_j+n_{j+1}(e)+2)/8}(D,-1)_2^{(n_j+n_{j+1}(e))/2}H.$$

   Therefore, the local density can be explicitly computed as:

$$2^{w+n_{j+1}+3}(1+\chi(j+1)p^{n_{j+1}(e)/2})^{-1}\prod_{i=1}^{n_j(e)/2}(1-p^{-2i})\prod_{i=1}^{n_{j+1}(e)/2}(1-p^{-2i}).$$

4. Both the p^j and p^{j+1} blocks are even.

   In this case there is a unique Jordan decomposition and the discriminants of the unimodular blocks are $(-1)^{n_j/2}$ mod 4. As $\chi(i)=(2,D_i)_2$, the goal is to solve for $(2,D_i)_2$. We have that:

$$1=(D_j,D_{j+1}),\ \text{and}\ H_i=(2,D_i)(-1,-1)^{n_i(n_i+2)/8}.$$

   It follows that:

$$\begin{aligned}H&=H_jH_{j+1}(D_j,D_{j+1})_2(2,D_j)_2^{j+1}(2,D_{j+1})_2^j\\&=(-1,-1)_2^{n(n+2)/8}(2,D_j)_2^{j+1}(2,D_{j+1})_2^j.\end{aligned}$$

Thus we may solve:

$$\chi(i) = (-1,-1)_2^{n(n+2)/8}(2,D)_2^i H.$$

Therefore the local density can be explicitly computed as:

$$2^{w+2}(1+\chi(j)p^{n_j(e)/2})^{-1}(1+\chi(j+1)p^{n_{j+1}(e)/2})^{-1}\prod_{i=1}^{n_j(e)/2}(1-p^{-2i})\prod_{i=1}^{n_{j+1}(e)/2}(1-p^{-2i}).$$

□

4.5 Transfer of Lattices

Let $R_1 \subset R_2$ be a finite extension of rings. Given a quadratic module (L_{R_2}, q_{R_2}) over R_2, one can construct a quadratic module (L_{R_1}, q_{R_1}) over R_1 by viewing L_{R_2} as a module over R_1 and taking $q_{R_1}(x) = \mathrm{Tr}_{R_2/R_1}(q_{R_2}(x))$. We shall refer to this as **transfer**.

The purpose of this section is to study properties of this process over p-adic rings. We are particularly interested in the transfer of Hermitian lattices, that is, quadratic forms of the form:

$$q_{R_2}(x) = \tfrac{1}{2}\,\mathrm{Tr}_{R_3/R_2}(\lambda x\sigma(x)) = \lambda x\sigma(x),$$

where $x \in R_3$ a quadratic extension of R_2, σ the nontrivial automorphism of R_3/R_2, and λ is a unit in the fraction field of R_2. The subsection of this section are organized as follows:

(4.5.1) We give some basic results about trace forms for local fields.

(4.5.2) We compute invariants for the forms q_{R_1}.

(4.5.3) We describe Jordan decompositions when $p \neq 2$ for both unary and binary forms.

(4.5.4) We describe Jordan decompositions when $p = 2$ for both unary and binary forms.

In the following section we shall use these results to compute local densities for Hermitian lattices over $\mathbb{Q}$.

4.5.1 Trace Forms for Local Fields

The next few lemmas are important for various computations.

Lemma 4.5.1 (Euler)**.** *Let $L = F(z)$ be a finite separable extension of F of degree m with $f_z(x) \in \mathcal{O}_F[x]$ the minimal (monic) polynomial of z. We then have:*

$$\operatorname{Tr}_{L/F}\left(\frac{z^\ell}{f_z'(z)}\right) = \begin{cases} 1 & \ell = m-1 \\ 0 & 0 \leq \ell < m-1. \end{cases}$$

See [Ser79, III.6 Lemma 2].

Lemma 4.5.2. *Let L/F be a totally ramified extension of local fields of degree m. Let $z = \pi_L$ be a uniformizer of $\mathcal{O}_L$ and $f_z(x)$ be the minimal (monic) polynomial of z. Then f_z is an Eisenstein polynomial and the collection $1, z, z^2, \ldots, z^{m-1}$ is an $\mathcal{O}_F$-basis of $\mathcal{O}_L$ and $N_{L/F}(z)$ is a uniformizer of F.*

See [Ser79, Prop I.6.18].

Lemma 4.5.3. *Let L/F be a totally ramified extension of local fields of degree m. Let $z = \pi_L$ be a uniformizer of $\mathcal{O}_L$ and $f_z(x)$ be the minimal (monic) polynomial of z. Then for $0 \leq \ell \leq m-1$ and k any integer, we have:*

$$\nu_F\left(\operatorname{Tr}_{L/F}\left(\frac{z^{km+\ell}}{f_z'(z)}\right)\right) \geq k.$$

Moreover, this is an equality if $\ell = m-1$.

Proof. As $\pi_F = N_{L/F}(z)$ is a uniformizer of F we write $z^m = u\pi_F$. We see that:

$$\operatorname{Tr}_{L/F}\left(\frac{z^{km+\ell}}{f_z'(z)}\right) = \pi_F^k \operatorname{Tr}_{L/F}\left(\frac{u^k z^\ell}{f_z'(z)}\right).$$

As $u^k z^\ell \in \mathcal{O}_L$ write:

$$u^k z^\ell = \sum_{i=0}^{m-1} a_i z^i,$$

with $a_i \in \mathcal{O}_F$. Then:

$$\operatorname{Tr}_{L/F}\left(\frac{u^k z^\ell}{f_z'(z)}\right) = a_{m-1} \in \mathcal{O}_F.$$

The result follows immediately.

To show we have an equality if $\ell = m-1$ write:

$$u^k = \sum_{i=0}^{m-1} a_i z^i.$$

Then we compute that:

$$\mathrm{Tr}_{L/F}\left(\frac{u^k z^\ell}{f_z'(z)}\right) = \sum_{i=0}^{m-1} a_i \,\mathrm{Tr}_{L/F}\left(\frac{z^{m-1+i}}{f_z'(z)}\right) = a_0 \pmod{\pi_F}.$$

As $v_L(u) = 0$ it follows that $v_F(a_0) = 0$, which concludes the result. $\square$

Example. We have the following special cases of the above. Write the minimal monic polynomial f_z of z as $f_z(X) = \sum_i a_i X^i$. Then:

$$\mathrm{Tr}_{L/F}\left(\frac{z^\ell}{f_z'(z)}\right) = \begin{cases} -a_{m-1} & \ell = m \\ a_{m-1}^2 - a_{m-2} & \ell = m+1 \\ 1/a_0 & \ell = -1 \\ a_1/a_0^2 & \ell = -2. \end{cases}$$

The results for other powers can also be computed directly from the coefficients.

4.5.2 Invariants of q_{R_1}

The most basic of questions is to understand the standard invariants of the quadratic modules which result from transfer.

The following Lemma is immediate.

Lemma 4.5.4. *Transfer commutes with orthogonal direct sums.*

⧫ Discriminants and Hasse Invariants

Proposition 4.5.5 (Discriminants). *Let R_2/R_1 be an extension of p-adic rings or orders in number fields. Suppose L is an R_2-lattice (and hence also an R_1-lattice) which is free over R_2 with quadratic form q_{R_2}. Suppose that R_2 is free over R_1. Consider the form $q_{R_1}(y) = \mathrm{Tr}_{R_2/R_1}(q_{R_2}(y))$ as a quadratic form on*

L viewed as an R_1-lattice. Then:

$$\delta_{q_{R_1}} = N_{R_2/R_1}(\delta_{q_{R_2}})\delta^n_{R_2/R_1},$$

where δ_{R_2/R_1} is the usual discriminant relative to the trace form.

Proof. If q_{R_1} is diagonalizable then by multiplicitivity of determinants and norms we may reduce the problem to studying the unary case. In this setting we have the usual argument (see Lemma 3.3.1). The argument works integrally. Note that in the argument cited one can use $\{z_\ell\}$, any basis for the ring of integers, and this basis need not be a power basis $\{z^\ell\}$.

More generally we need to work with lattices which may not be diagonalizable. Consider $L' \subset L$ a free diagonalizable lattice in the same quadratic module. There exists a basis for L and a matrix $M = \mathrm{diag}(a_1, \ldots, a_n)U$, where $a_i \in R_2^\times$ and U is an upper triangular unipotent matrix with respect to which $L' = ML$. The discriminant of L' differs from that of L by $\prod_i^n a_i^2$.

Fix a basis for R_2 over R_1. For $x \in R_2$ let (x) denote the matrix for x acting on R_2 as an R_1-module in this basis.

Passing to R_1 the matrix which realizes L' as a submodule can be taken to have a block decomposition $M' = \mathrm{diag}((a_1), \ldots, (a_n))U'$, where U' is the matrix whose blocks are (U_{ij}). The determinant of $(a_i) = N_{R_2/R_1}(a_i)$, and hence the determinant of this change of basis becomes the norm of the original change of basis. We thus relate $\delta_{L,q_{R_1}}$, $\delta_{L,q_{R_2}}$, $\delta_{L',q_{R_2}}$ and $\delta_{L',q_{R_1}}$ by

$$\begin{aligned} \delta_{L,q_{R_1}} &= N_{R_2/R_1}\left(\prod_i a_i\right)\delta_{L',q_{R_1}} \\ &= N_{R_2/R_1}\left(\prod_i a_i\right)N_{R_2/R_1}\left(D\delta_{L',q_{R_2}}\right) \\ &= N_{R_2/R_1}\left(D\delta_{L,q_{R_2}}\right). \end{aligned}$$

The formula thus holds for L. □

Theorem 4.5.6 (Hasse Invariants). *Let R_2/R_1 be an extension of p-adic rings. Let L be an R_2-lattice of rank n with quadratic form q_{R_2}. Denote by $Q_{R_2/R_1,\lambda}(x) = \mathrm{Tr}_{R_2/R_1}(\lambda x^2)$ and by $d = N_{R_2/R_1}(D(q_{R_2}))$. We will consider the form $q_{R_1} = \mathrm{Tr}_{R_2/R_1}(q_{R_2})$. Continue to denote $(\cdot,\cdot)_{R_1}$ the Hilbert symbol. We have the following results:*

1. *The form q_{R_1} has Hasse invariant:*

$$H_{R_1}(q_{R_1}) = H_{R_1}(Q_{R_2/R_1,1})^{n+1} H_{R_1}(Q_{R_2/R_1,D(q_{R_2})})(\delta_{R_2/R_1}, d)_{R_1}^{n+1} H_{R_2}(q_{R_2}).$$

   We view these all as being in the same cohomology group $H^2(K_1, \pm 1)$ by identifying the different groups with $\{\pm 1\}$ or equivalently via corestriction, which is injective for local fields.

2. *If $p \neq 2$ and the extension R_2/R_1 is unramified, then:*

$$H_{R_1}(q_{R_1}) = H_{R_2}(q_{R_2})(\pi_{R_1}, (-1)^{n(n-1)/2}\delta_{R_2/R_1} d)_{R_1}^{v_{R_2}(D(q_{R_2}))}.$$

3. *Consider the case $p \neq 2$, $u \in R_1^\times$ and R_2/R_1 is totally ramified. Let $\lambda = \frac{\pi_{R_2}^k}{uf'(\pi_{R_2})\pi_{R_2}^\ell}$, where f is the minimal polynomial of π_{R_2}. The form $Q_{R_2/R_1,\lambda}$ has Hasse invariant:*

$$H_{R_1}(Q_{R_2/R_1,\lambda}) = (\pi_{R_1}, u)_{R_1}^{n(n-\ell)} (\pi_{R_1}, -1)_{R_1}^{k(n^2(n-1)/2+\ell^2(1-n))-\ell(n-\ell)(n-\ell-1)/2}.$$

4. *Suppose $p = 2$ and the extension is Galois. The form $Q(x) = \mathrm{Tr}_{R_2/R_1}(x^2)$ has Hasse invariant:*

$$H_{R_1}(Q) = \begin{cases} (-1,-1)^{(n^2-1)/8} & n = 1 \pmod 2 \\ (\delta_{R_2/R_1}, (-1)^{(n+2)/4})_{R_1} & n = 2 \pmod 4 \\ 1 & n = 0 \pmod 4 \text{ and } -1 \in R_2^2 \\ (-1,-1)_{R_1}(2, \delta_{R_2/R_1})_{R_1} & n = 4 \pmod 8, -1 \in N_{R_2/R_1}(R_2) \\ -(-1,-1)_{R_1}(2, \delta_{R_2/R_1})_{R_1} & n = 4 \pmod 8, -1 \notin N_{R_2/R_1}(R_2) \\ (2, \delta_{R_2/R_1})_{R_1} & \text{otherwise.} \end{cases}$$

The first and fourth statements are [Epk89, Lemma 1 and Theorem 1], respectively; the second and third are Lemmas 3.4.1 and 3.4.3 , respectively.

Remark. The above theorem fails to provide a complete description of how to compute Hasse invariants for certain dyadic fields. This is remedied for binary forms of the following special type.

Theorem 4.5.7. *Suppose R_3 is a p-adic ring with an involution σ. Let $z \in R_2 = R_3^\sigma$ be such that $\sqrt{z}$ generates $R_3[\frac{1}{p}]$ as a $R_1[\frac{1}{p}]$-algebra (note that by Proposition 3.3.5 such a z exists). View R_3 as a binary R_2-lattice with quadratic form:*

$$q_{R_2}(x + y\sqrt{z}) = \lambda((x + y\sqrt{z})\sigma(x + y\sqrt{z})) = \lambda x^2 - z\lambda y^2$$

so that $D(q_{R_2}) = -z$ and $H(q_{R_2}) = (\lambda, z)$. Let f be the minimal monic polynomial for z over R_1 and $m = [R_2 : R_1]$. Then:

$$H(q_{R_1}) = \mathrm{Cor}_{R_2/R_1}((z, -\lambda f_z'(z))_{R_2}) \cdot (N_{R_2/R_1}(z), -1)_{R_1}^{m-1} \cdot (-1, -1)_{R_1}^{m(m-1)/2}.$$

See Theorem 3.3.8.

⧫ Modularity

Proposition 4.5.8. *Suppose that R_2/R_1 is an unramified extension of p-adic rings and that L is a π^r-modular lattice with quadratic form q_{R_2}. Then L is also π^r-modular as an R_1-lattice. Moreover, the valuation of the norm ideal $\mathfrak{N}_L$ and scale ideal $\mathfrak{S}_L$ are unchanged. In particular, Jordan decompositions are taken to Jordan decompositions.*

Proof. It is clear that we have:

$$\mathfrak{N}_{L/R_1} = \mathrm{Tr}_{R_2/R_1}(\mathfrak{N}_{L/R_2}) \text{ and } \mathfrak{S}_{L/R_1} = \mathrm{Tr}_{R_2/R_1}(\mathfrak{S}_{L/R_2}).$$

Indeed, picking an element $x \in L$, where $\nu(q_{R_2}(x))$ is minimal write $q_{R_2}(x) = u\pi^t$ with π a uniformizer of R_1 and u a unit. Then $q_{R_1}(ax) = \pi^t \mathrm{Tr}_{R_2/R_1}(ua^2)$. For $p \neq 2$ the unimodularity $\mathrm{Tr}_{R_2/R_1}(ua^2)$ implies that there exists $a \in R_2$ for which this is a unit. For $p = 2$ notice that $a \mapsto \mathrm{Tr}_{R_2/R_1}(ua^2)$ is surjective on the residue field. The claim for $\mathfrak{N}_{L/R_1}$ follows immediately, the proof for $\mathfrak{S}_{L/R_1}$ is similar.

The question of π^r modularity now follows from the observation that L is π^r-modular if and only if $\mathfrak{S}_L = (\pi^r)$ and $\mathfrak{S}_{L^\#} = (pi^{-r})$. $\square$

With the above result in hand, we shall for the time being restrict to the case of totally ramified extensions. We introduce some notation before proceeding.

Let R_2/R_1 be a totally ramified extension of p-adic rings of degree m. Let π_{R_2} be a uniformizer of R_2 and set $\pi_{R_1} = N_{R_2/R_1}(\pi_{R_2})$ to be a uniformizer of R_1. Let $f(X) = f_{\pi_{R_2}}(X)$ be the minimal monic polynomial of π_{R_2} over R_1. Suppose $u_1 \in R_1^\times$, $u_2 \in R_2^\times$, $v \in R_2^\times$, $0 \leq \ell \leq m$, $k \in \mathbb{Z}$, set $u = u_1 u_2$ and set:

$$\lambda = \frac{\pi_{R_1}^k}{u_1 u_2 v^2 \pi_{R_2}^\ell f'(\pi_{R_2})}.$$

We remark that if the residue characteristic is not 2, then for any given λ in the fraction field of R_2 there exists (non-unique) corresponding values for u_1, v, ℓ, k with $u_2 = 1$. Now denote by $q_{R_2}(x)$ the R_2-quadratic form on R_2 given by λx^2, and by $q_{R_1}(x)$ the R_1-quadratic form on R_2 given by $q_{R_1}(x) = \mathrm{Tr}_{R_2/R_1}(\lambda x^2)$. Consider:

$$M_1 = \mathrm{span}\{v, \ldots, v\pi_{R_2}^{\ell-1}\} \text{ and } M_2 = \mathrm{span}\{uv\pi_{R_2}^\ell, \ldots, uv\pi_{R_2}^{m-1}\}$$

as quadratic submodules of R_2. These submodules will play important roles in the construction of Jordan decompositions.

4.5.3 Transfer Over Non-Dyadic p-adic Rings

The case of $p \neq 2$ is simpler for both unary and Hermitian forms. We thus present the results for this case separately. We assume in this section that the constant u_2, as introduced above, is 1. The important feature we will show is that in both the unary and binary cases we know that there are at most two

Jordan blocks and that their modularity differs by a power of π_{R_1}. We may thus completely recover the invariants of the blocks as in Corollary 4.4.30.

Theorem 4.5.9. *Suppose R_2/R_1 is a totally ramified extension of p-adic fields for $p \neq 2$. Let λ, q_{R_1}, M_1 and M_2 be as above. Then $R_2 = M_1 \oplus M_2$ is a Jordan decomposition with M_1 and M_2 being, respectively, $\pi_{R_1}^{k-1}$ and $\pi_{R_1}^{k}$ modular. Moreover, the discriminants of $\frac{1}{\pi_{R_1}^{k-1}} q_{R_1}|_{M_1}$ and $\frac{1}{\pi_{R_1}^{k}} q_{R_1}|_{M_2}$ are, respectively:*

$$D\left(\frac{1}{\pi_{R_1}^{k-1}} q_{R_1}|_{M_1}\right) = (-1)^{\ell(\ell+1))/2 - m\ell} u^{-\ell} \text{ and}$$
$$D\left(\frac{1}{\pi_{R_1}^{k}} q_{R_1}|_{M_2}\right) = (-1)^{(m-\ell)(m-\ell-1)/2} u^{m-\ell}.$$

See Lemma 3.4.3.

In addition to the above notation, suppose that R_3/R_2 is a quadratic extension with involution σ. Fix w a non-square element of $R_1^{\times}$. Writing $x = x_1 + x_2\sqrt{\delta_{R_3/R_2}}$ consider the quadratic form on R_3 given by:

$$q_{R_3/R_1}(x) = \tfrac{1}{2}\operatorname{Tr}_{R_3/R_1}(\lambda x \sigma(x)) \simeq \operatorname{Tr}_{R_2/R_1}(\lambda x_1^2) - \operatorname{Tr}_{R_2/R_1}(\lambda \delta_{R_3/R_2} x_2^2).$$

Then set $\lambda' = \lambda\delta_{R_3/R_2}$, $k' = k$, $u_2' = 1$ and choose u_1', v', ℓ' so that $\lambda' = \frac{\pi_{R_1}^{k}}{u'v'^2\pi_{R_2}^{\ell'} f'(\pi_{R_2})}$. Let q_{R_1}', M_i' be defined similarly to q_{R_1}, M_i using λ' instead of λ so that $q_{R_3/R_1}(x) = q_{R_1}(x_1) - q_{R_1}'(x_2)$. Now define $N_i = M_i \oplus -M_i'$ and $\widetilde{N_1} = \frac{1}{\pi_{R_1}^{k-1}} N_1$ and $\widetilde{N_2} = \frac{1}{\pi_{R_1}^{k}} N_2$ their unimodular rescalings.

Theorem 4.5.10. *The orthogonal decomposition $R_3 = N_1 \oplus N_2$ is a Jordan decomposition for R_3 with the form q_{R_3/R_1}. The sublattices N_1 and N_2 are, respectively, $\pi_{R_1}^{k-1}$ and $\pi_{R_1}^{k}$-modular. Moreover:*

1. *If $\delta_{E/R_2} = w$ then $D(\widetilde{N_1}) = (-1)^{-\ell} w^{-\ell}$ and $D(\widetilde{N_2}) = (-1)^{\ell-m} w^{\ell-m}$.*
2. *If $\delta_{E/R_2} = \pi_{R_2}$ then $D(\widetilde{N_1}) = (-1)^{m+1} u$ and $D(\widetilde{N_2}) = -u$.*
3. *If $\delta_{E/R_2} = w\pi_{R_2}$ then $D(\widetilde{N_1}) = (-1)^{m-1} u w^{1-\ell}$ and $D(\widetilde{N_2}) = -u w^{\ell-m+1}$.*
4. *If $\delta_{E/R_2} = 1$, then $D(\widetilde{N_1}) = (-1)^{-\ell}$ and $D(\widetilde{N_2}) = (-1)^{\ell-m}$.*

See Lemma 3.4.4.

4.5.4 Transfer Over Dyadic Rings

The case of $p = 2$ is more complex for a variety of reasons, the failure of diagonalizability being the most prominent. The goal of this section is to attain results on Jordan decompositions similar to those of the previous section keeping track of the additional information about norm ideals. In order to account for non-diagonalizability, we must consider both unary and binary lattices.

As before we set $\lambda = \frac{\pi_{R_1}^k}{u_1 u_2 v^2 f'(\pi_{R_2})\pi_{R_2}^\ell}$ with $u_1 \in R_1^\times$, $u_2, v \in R_2^\times$, $0 \leq \ell \leq m$, $k \in \mathbb{Z}$ and let $f(X)$ be the minimal monic polynomial of π_{R_2}. Consider:

$$M_1 = \operatorname{span}\{v, \dots, v\pi_{R_2}^{\ell-1}\} \text{ and } M_2 = \operatorname{span}\{uv\pi_{R_2}^{\ell}, \dots, uv\pi_{R_2}^{m-1}\},$$

as quadratic submodules of R_2. Note that we may no longer assume that $u_2 = 1$.

Proposition 4.5.11 (Unary Forms)**.** *Let $q_{R_2}(x) = \lambda x^2$ and set:*

$$q_{R_1} = \operatorname{Tr}_{R_2/R_1}(q_{R_2}).$$

Then $R_2 = M_1 \oplus M_2$ is a Jordan decomposition with M_1 and M_2 being, respectively, $\pi_{R_1}^{k-1}$ and $\pi_{R_1}^k$-modular. They differ in modularity by a multiple of π_{R_1}, hence their discriminants may depend on the choice of Jordan decomposition. Set $\widetilde{M_1} = \frac{1}{\pi_{R_1}^{k-1}} M_1$ and $\widetilde{M_2} = \frac{1}{\pi_{R_1}^{k}} M_2$. We can in general only say if $\mathfrak{N}_{\widetilde{M_i}}$ is R_1. We have the following cases:

- *$\mathfrak{N}_{\widetilde{M_1}} \subset (\pi_{R_1})$ if ℓ is even and $u_2 \cong \frac{\pi_{R_1}}{\pi_{R_2}^m} \pmod{R_2^2 \pi_{R_2}^\ell}$. Otherwise $\mathfrak{N}_{\widetilde{M_1}} = R_1$.*
- *$\mathfrak{N}_{\widetilde{M_2}} \subset (\pi_{R_1})$ if $m - \ell$ is even and $u_2 \cong 1 \pmod{R^2 \pi_{R_2}^{m-\ell}}$. Otherwise $\mathfrak{N}_{\widetilde{M_2}} = R_1$.*

Proof. One easily checks by Lemma 4.5.1 that $M_1 \perp M_2$.

Moreover, the matrix for M_1 is of the form $(a_{ij})_{i,j}$, where the a_{ij} satisfy:

1. $a_{i_1 j_1} = a_{i_2 j_2}$ whenever $i_1 + j_1 = i_2 + j_2$.

2. $v_{R_1}(a_{i,\ell-i}) = k-1$.
3. $v_{R_1}(a_{i,j}) > k-1$ whenever $i+j>\ell$.
4. If ℓ is even and $u_2 \cong \frac{\pi_{R_2}^m}{\pi_{R_1}} \pmod{R_2^2\pi_{R_2}^\ell}$, then $v_{R_1}(a_{ii}) > k-1$ for all i.

   Otherwise there exists i with $\nu(a_{ii}) = k-1$.

The first statement is immediate, the second and third follow from Lemma 4.5.3. The last statement is seen as follows. Firstly, the statement depends only on the square class of u_2. This is true even though modifying u_2 changes the basis as the conclusion about the norm groups we are making is independent of choice of Jordan decomposition. We may thus choose to write:

$$u_2 = 1 + c_1\pi_{R_2} + c_3\pi_{R_2}^3 + \cdots \pmod{\pi_{R_2}^\ell}$$

with $c_i \in R_1$. Now by taking $x = \pi_{R_2}^{(\ell-i)/2}$ and setting $\mathrm{Tr}_{R_2/R_1}(\lambda x^2) = 0 \pmod{\pi_{R_1}^k}$ we can solve for $c_i \mod \pi_{R_1}$ in terms of c_j with $j<i$ (the equations involve the coefficients of f but these are constant). Explicitly we are solving:

$$c_i = \pi_{R_1}(\mathrm{Tr}_{R_2/R_1}(\pi^{-1-i}) + \sum_{j<i} c_j \,\mathrm{Tr}_{R_2/R_1}(\pi^{j-i-1})) \pmod{\pi_{R_1}}.$$

Lemma 4.5.3 tells us that the right hand side makes sense. As this is solvable we conclude that up to squares there is a unique value of u_2 modulo $\pi_{R_2}^\ell$ which makes all values of the quadratic form be contained in $\pi_{R_1}R_1$. Observing that $u_2 = \pi_{R_2}/\pi_{R_1}^m$ does this allows us to conclude the result.

The matrix for M_2 is of the form $(b_{ij})_{i,j}$, where the b_{ij} satisfy:

1. $b_{i_1j_1} = b_{i_2j_2}$ whenever $i_1+j_1 = i_2+j_2$.
2. $v_{R_1}(b_{i,m-\ell-i}) = k$.
3. $v_{R_1}(b_{i,j}) > k$ whenever $i+j > m-\ell$.
4. If $m-\ell$ is even and $u_2 \cong \frac{\pi_{R_2}^m}{\pi_{R_1}} \pmod{R^2\pi_{R_2}^{m-\ell}}$, then $v_{R_1}(b_{ii}) > k$ for all i.

   Otherwise there exists i with $v_{R_1}(b_{ii}) = k$.

The arguments are identical to those for M_1 except that 1 is the necessary congruence. $\square$

Taking λ as above, we will now consider binary forms. Since we are not interested in those that decompose as direct sums of unary forms we consider L over R_2 of the form:

$$\lambda \begin{pmatrix} u_3\pi^a & 1 \\ 1 & u_4\pi^{a+b} \end{pmatrix} = \frac{\pi_{R_1}^k}{u_1u_2v^2} \begin{pmatrix} \frac{u_3}{f'(\pi_{R_2})\pi_{R_2}^{\ell-a}} & \frac{1}{f'(\pi_{R_2})\pi_{R_2}^{\ell}} \\ \frac{1}{f'(\pi_{R_2})\pi_{R_2}^{\ell}} & \frac{u_4}{f'(\pi_{R_2})\pi_{R_2}^{\ell-a-b}} \end{pmatrix}$$

with $a > 0$ and $b \geq 0$.

We use the basis:

$$\{v, \ldots v\pi_{R_2}^{\ell-1}\}e_1 \cup \{vu\pi_{R_2}^{\ell}, \ldots, vu\pi_{R_2}^{m-1}\}e_1,$$
$$\{v, \ldots v\pi_{R_2}^{\ell-1}\}e_2 \cup \{vu\pi_{R_2}^{\ell}, \ldots, vu\pi_{R_2}^{m-1}\}e_2,$$

where e_1, e_2 denote respectively the first and second coordinates of L.

Define the following quadratic submodules with the given basis:

$$M_1 = \{v, \ldots v\pi_{R_2}^{\ell-1}\}e_1, \quad M_1' = \{v, \ldots, v\pi_{R_2}^{\ell-1}\}e_2,$$
$$M_2 = \{vu\pi_{R_2}^{\ell}, \ldots, vu\pi_{R_2}^{m-1}\}e_1, \quad M_2' = \{vu\pi_{R_2}^{\ell}, \ldots, vu\pi_{R_2}^{m-1}\}e_1.$$

Also define $N_1 = M_1 + M_1'$ and $N_2 = M_2 + M_2'$. Note these are not orthogonal decompositions. We are considering the span of both in the ambient space. Moreover, N_1 and N_2 also need not be orthogonal complements.

Proposition 4.5.12 (Binary Forms)**.** *Let $a > 0$,$b \geq 0$, $u_3 \in R_1^\times$ and $u_4 \in R_2^\times$. Let q_{R_2} be the form associated to the matrix $\lambda \begin{pmatrix} u_1\pi^a & 1 \\ 1 & u_2\pi^{a+b} \end{pmatrix}$. Then the form:*

$$q_{R_1} = \mathrm{Tr}_{R_2/R_1}(q_{R_2})$$

has 2 Jordan blocks, N_1 and N_2 of modularities $\pi_{R_1}^{k-1}$ and $\pi_{R_1}^k$, respectively. They differ in modularity by a multiple of π_{R_1}. We can only in general determine if the norm ideals are R_1.

- *$\mathfrak{N}_{\widetilde{N_1}} \subset (\pi_{R_1})$ if and only if $\max(\ell - a, 0)$ and $\max(\ell - a - b, 0)$ are even, and $u_2u_3 \cong \pi_{R_1}/\pi_{R_2}^m \pmod{\pi_{R_2}^{\ell-a}}$ and $u_2u_4 \cong \pi_{R_1}/\pi_{R_2}^m \pmod{R_1^2\pi_{R_2}^{\ell-a-b}}$*

- $\mathfrak{N}_{\widetilde{N_2}} \subset (\pi_{R_1})$ *if and only if* $\max(m-\ell-a,0)$ *and* $\max(m-\ell-a-b,0)$ *are even, and* $u_2u_3 \cong 1 \pmod{\pi_{R_2}^{m-\ell-a}}$ *and* $u_2u_4 \cong 1 \pmod{R_1^2\pi_{R_2}^{m-\ell-a-b}}$.

Proof. Viewing the underlying space under the basis M_1, M_1', M_2, M_2' as above the matrix for q_{R_1} is of the form:

$$\begin{pmatrix} A & B & D^t & 0 \\ B & C & 0 & E^t \\ D & 0 & F & G \\ 0 & E & G & H \end{pmatrix}.$$

The blocks (that is the submatrices $A, \dots, H$) have the following properties:

1. A, B, C are ℓ by ℓ matrices and, F, G, H are $m-\ell$ by $m-\ell$ matrices.
2. For all the blocks we have $*_{i_1j_1} = *_{i_2j_2}$ whenever $i_1+j_1 = i_2+j_2$. In particular, the square blocks are symmetric.
3. $\nu(*_{ij}) \geq k-1$ for all blocks and all i,j. Furthermore,

$$\nu(A_{ij}) > k-1 \text{ for } i+j > \ell-a,$$

$$\nu(B_{ij}) > k-1 \text{ for } i+j > \ell,$$

$$\nu(B_{ij}) = k-1 \text{ for } i+j = \ell,$$

$$\nu(C_{ij}) > k-1 \text{ for } i+j > \ell-a-b,$$

$$\nu(D_{ij}), \nu(E_{ij}) > k-1 \text{ for all } i,j,$$

$$\nu(F_{ij}) > k \text{ for } i+j > m-\ell-a,$$

$$\nu(G_{ij}) > k \text{ for } i+j > m-\ell,$$

$$\nu(G_{ij}) = k \text{ for } i+j = m-\ell, \text{ and}$$

$$\nu(H_{ij}) > k \text{ for } i+j > m-\ell-a-b.$$

4. The discriminant of $\frac{1}{\pi_{R_1}^{k-1}}\left(\begin{smallmatrix} A & B \\ B & C\end{smallmatrix}\right)$ and the discriminant of $\frac{1}{\pi_{R_1}^{k-1}}\left(\begin{smallmatrix} F & G \\ G & H\end{smallmatrix}\right)$ are units mod π_{R_1}.

5. There are changes of basis which realize both N_1 and N_2 as Jordan blocks (though not simultaneously).

   Hence the questions of whether the norm ideals of the rescaled Jordan blocks are contained in R_1 are determined by $\frac{1}{\pi_{R_1}^{k-1}} \left(\begin{smallmatrix} A & B \\ B & C \end{smallmatrix} \right)$ and $\frac{1}{\pi_{R_1}^{k}} \left(\begin{smallmatrix} F & G \\ G & H \end{smallmatrix} \right)$.

6. The lattice N_1 is odd unless $\max(\ell - a, 0)$ and $\max(\ell - a - b, 0)$ are even, and $u_2 u_3 \cong \pi_{R_1}/\pi_{R_2}^m \pmod{\pi^{\ell-a}}$ and $u_2 u_4 \cong \pi_{R_1}/\pi_{R_2}^m \pmod{R_1^2 \pi^{\ell-a-b}}$

7. The lattice N_2 is odd unless $\max(m - \ell - a, 0)$ and $\max(m - \ell - a - b, 0)$ are even, and $u_2 u_3 \cong 1 \pmod{\pi^{m-\ell-a}}$ and $u_2 u_4 \cong 1 \pmod{R_1^2 \pi^{m-\ell-a-b}}$.

Points (1) and (2) are direct checks. Point (3) uses Lemma 4.5.3. Point (4) is elementary yet tedious to check. First observe that since modulo π_{R_1} the matrix $\frac{1}{\pi_{R_1}^{k-1}} \left(\begin{smallmatrix} A & B \\ B & C \end{smallmatrix} \right)$ is of the form:

$$\left(\begin{smallmatrix} * & * & u \\ * & X & 0 \\ u & 0 & 0 \end{smallmatrix} \right),$$

where X is a $2\ell - 2$ by $2\ell - 2$ block, it has determinant $-u^2 \det(X)$. We may iterate this procedure on X until X is of the form:

$$\begin{pmatrix} \tilde{A} & \tilde{B} \\ \tilde{B} & \tilde{C} \end{pmatrix}$$

with $\tilde{A}, \tilde{B}, \tilde{C}$ being $\ell - a - b$ by $\ell - a - b$ blocks. We may iterate until X has additional non-zero entries on the bottom row and rightmost column. Now use the fact that:

$$\det \left(\begin{smallmatrix} \tilde{A} & \tilde{B} \\ \tilde{B} & \tilde{C} \end{smallmatrix} \right) = \det(\tilde{C}) \det(\tilde{A} - \tilde{B}\tilde{C}^{-1}\tilde{B}),$$

combined with the observation that:

$$\tilde{A} - (\tilde{B}\tilde{C}^{-1}\tilde{B})_{ij} \in \begin{cases} \pi_{R_1} R_1 & i + j > \ell - a - b \\ R_1^* & i + j = \ell - a - b \end{cases}$$

to conclude the result. We may perform an analogous argument for $\left(\begin{smallmatrix} F & G \\ G & H \end{smallmatrix} \right)$.

For point (5) notice that the change of bases needed are, respectively:

$$\begin{pmatrix} \mathrm{Id} & -\left(\begin{smallmatrix} A & B \\ B & C \end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix} D^t & 0 \\ 0 & E^t \end{smallmatrix}\right) \\ 0 & \mathrm{Id} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \mathrm{Id} & 0 \\ -\left(\begin{smallmatrix} F & G \\ G & H \end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix} D & 0 \\ 0 & E \end{smallmatrix}\right) & \mathrm{Id} \end{pmatrix}.$$

The matrices $\left(\begin{smallmatrix} D & 0 \\ 0 & E \end{smallmatrix}\right)\left(\begin{smallmatrix} A & B \\ B & C \end{smallmatrix}\right)^{-1}$ and $\left(\begin{smallmatrix} D & 0 \\ 0 & E \end{smallmatrix}\right)\left(\begin{smallmatrix} F & G \\ G & H \end{smallmatrix}\right)^{-1}$ are integral by points (3) and (4). One sees that orthogonal complements of N_2 and N_1 are preserved, respectively, modulo $\pi_{R_1}^{k-1}$ and $\pi_{R_1}^{k}$. Hence they are modular and we indeed have a Jordan decomposition.

The arguments for (6) and (7) are analogous to that of the previous lemma. Indeed, one has norm ideal R_1 if and only if the diagonal contains a unit. Hence the problem reduces to considering the blocks on the diagonal, and we are reduced to the situation of the previous lemma, (except that we have now two different subblocks to check for each Jordan decomposition). □

Remark. Note that though N_1 and N_2 are Jordan blocks for some Jordan decompositions, it is not necessarily true that the space for q_{R_1} is isomorphic to $N_1 \oplus N_2$ as N_1 and N_2 may not be Jordan blocks in the same decomposition.

We now move to the special case of forms which arise from Hermitian forms. We quickly review the possible quadratic extensions R_3/R_2 of a 2-adic ring. On the level of their fields of fractions they are of the form $K(\sqrt{z})$. We therefore look at the various cases for z.

- $z = u\pi_{R_2}$ for $u \in R_2^*$.

  Then the extension is ramified, has uniformizer $\sqrt{u\pi_{R_2}}$, $\delta_{R_3/R_2} = 4u\pi_{R_2}$, and the ring of integers has integral basis: $1, \sqrt{u\pi_{R_2}}$.

  In this basis the Hermitian form $q_{R_2} = \frac{1}{2}\operatorname{Tr}_{R_3/R_2}(\lambda x\sigma(x))$ has matrix:

$$\lambda \begin{pmatrix} 1 & 0 \\ 0 & -u\pi_{R_2} \end{pmatrix}.$$

  In this case $k = \left\lceil \frac{v_{R_2}(2\lambda f'(\pi_{R_2}))+1}{2m} \right\rceil$ and $\ell = -(v_{R_2}(\lambda f'(\pi_{R_2})) - mk)$.

- $z = 1 + a\pi_{R_2}^{2r+1}$ for $0 \leq r < v_{\pi_{R_2}}(2)$ and $a \in R^\times$.

  Then the extension is ramified, has uniformizer $\frac{1+\sqrt{1+a\pi_{R_2}^{2r+1}}}{\pi_{R_2}^r}$, $\delta_{R_3/R_2} = \frac{4}{\pi_{R_2}^{2r}}(1+a\pi_{R_2}^{2r+1})$, and the ring of integers has integral basis: $1, \frac{1+\sqrt{1+a\pi_{R_2}^{2r+1}}}{\pi_{R_2}^r}$.

  In this basis the Hermitian form $q_{R_2} = \frac{1}{2}\operatorname{Tr}_{R_2(R_3/R_2}(\lambda x\sigma(x))$ has matrix:

$$\lambda\frac{1}{\pi_{R_2}^r}\begin{pmatrix} \pi_{R_2}^r & 1 \\ 1 & -a\pi_{R_2}^{r+1} \end{pmatrix}.$$

  In this case $k = \left\lceil \frac{v_{R_2}(\lambda f'(\pi_{R_2}))-r}{m} \right\rceil$ and $\ell = -(v_{R_2}(\lambda f'(\pi_{R_2})) - r - mk)$.

- $z = 1 + b\pi^{2r}$ for $r = v_{\pi_{R_2}}(2)$ and $x^2 + \frac{2}{\pi_{R_2}^r}x - b$ irreducible mod π_{R_2} .

  Then the extension is unramified, has uniformizer π_{R_2}, $\delta_{R_3/R_2} = (1 + b\pi^{2r})$, and the ring of integers has integral basis $1, \frac{1+\sqrt{1+b\pi_{R_2}^{2r}}}{\pi_{R_2}^r}$.

  In this basis the Hermitian form $q_{R_2} = \frac{1}{2}\operatorname{Tr}_{R_3/R_2}(\lambda x\sigma(x))$ has matrix:

$$\lambda\frac{1}{\pi_{R_2}^r}\begin{pmatrix} \pi_{R_2}^r & 1 \\ 1 & -b\pi_{R_2}^{r} \end{pmatrix}.$$

  In this case $k = \left\lceil \frac{v_{R_2}(\lambda f'(\pi_{R_2}))-r}{m} \right\rceil$ and $\ell = -(v_{R_2}(\lambda f'(\pi_{R_2})) - r - mk)$.

We already have from the above that the quadratic forms which result from these cases will have 2 Jordan blocks. We thus proceed to summarize the results we can conclude about these cases.

Proposition 4.5.13. *Let R_3 is the maximal order of $R_2(\sqrt{z})$, R_2 and R_1 being as above. Let $\lambda = \frac{\pi_{R_1}^k}{u_1u_2v^2f'(\pi_{R_2})\pi_{R_2}^\ell}$ with $u_1 \in R_1^\times$, $u_2, v \in R_2^\times$, $0 \leq \ell \leq m$, $k \in \mathbb{Z}$ and let $f(X)$ be the minimal monic polynomial of π_{R_2}. consider the Hermitian form $q_{R_2}(x) = \frac{1}{2}\operatorname{Tr}_{R_3/R_2}(\lambda x\sigma(x))$, and $q_{R_1}(x) = \operatorname{Tr}_{R_2/R_1}(q_{R_2}(x))$. The form q_{R_1} has two Jordan blocks N_1 and N_2, they are $\pi_{R_1}^{k-1}$ and $\pi_{R_2}^k$- modular, respectively. Moreover, we have:*

1. *If $z = a\pi_{R_2}$ then the blocks are of dimension $2\ell - 1$ and $2(m-\ell)+1$, respectively. Both blocks are always odd (ie $\mathfrak{N} = R_1$).*

2. *If* $z = (1 + a\pi_{R_2}^{2r+1})$ *then the blocks are of dimension* 2ℓ *and* $2(m-\ell)$*, respectively. The block* N_1 *is odd if* $r < \ell$ *whereas* N_2 *is odd if* $r < m - \ell$*.*
3. *If* $z = (1 + b\pi^{2r})$ *then the blocks are of dimension* 2ℓ *and* $2(m-\ell)$*, respectively. Neither block is ever odd.*

Proof. The result follows immediately from the above discussion and Proposition 4.5.12. □

Remark. As in Proposition 4.5.12 we do not give an explicit Jordan decomposition, we only prove one exists with the given properties. The blocks N_1 and N_2 that Proposition 4.5.12 gives us in this case are again both Jordan blocks in some decomposition, but not necessarily in the same decomposition.

4.6 Computing Local Densities For Hermitian Forms over $\mathbb{Q}$

The problem of computing the main terms in the dimension formulas for spaces of modular forms on orthogonal Shimura varieties is reduced by Theorem 2.4.20 to the computation of $\mathrm{Vol}_{HM}(\mathrm{SO}(L)\backslash\mathcal{D})$. Proposition 2.4.26 reduces this to computing $\alpha_\infty(L, L)$. By Proposition 2.4.29 and the remark following, the main computational issue is computing $\alpha_p(L, L)$, or equivalently $\beta_p(L, L)$. We now have all the tools in hand to carry out the task of computing the local densities for Hermitian lattices over $\mathbb{Q}$. This is what we shall do in this section.

The idea is as follows: given the ring of integers $\mathcal{O}$ of some étale algebra E over $\mathbb{Q}$, we wish to understand the local densities for the form $\frac{1}{2}\operatorname{Tr}_{E/\mathbb{Q}}(\lambda x\sigma(x))$, where $\lambda \in E^\times$. For each prime p of $\mathbb{Q}$ we may write $E_p = \oplus_{\mathfrak{p}|p} E_{\mathfrak{p}}$, where the sum is over maximal ideals $\mathfrak{p}$ for the maximal order of E^σ. The first step is thus to understand the Jordan decompositions of the forms $q_{\mathfrak{p}} = \frac{1}{2}\operatorname{Tr} E_{\mathfrak{p}}/\mathbb{Q}_p(\lambda_{\mathfrak{p}} x\sigma_{\mathfrak{p}}(x))$. Having done this we may then understand the Jordan decomposition of the orthogonal direct sum $q_p = \oplus_{\mathfrak{p}} q_{\mathfrak{p}}$ with sufficient precision to compute the local density from the formulas we have. In particular we need strictly more information to compute results for E_p than for $E_\mathfrak{p}$ as the latter only has 2 Jordan blocks and so can be handled more simply.

Before we proceed we point out that this does not actually require that we understand all the invariants of all of the blocks of all of the $q_\mathfrak{p}$. Indeed the formulas for Jordan decompositions do not always depend on all the details of the isomorphism class.

Fix $\mathfrak{p}|p$ a maximal ideal dividing p in the maximal order of E^σ. Set R_3 be the maximal order of $E_\mathfrak{p}$, R_2 the maximal order of $E_\mathfrak{p}^\sigma$ and $R_1 = \mathbb{Z}_p$. Let $e_\mathfrak{p}$ and $f_\mathfrak{p}$ be, respectively, the ramification and inertial degrees of R_2 over R_1. Let $n_\mathfrak{p} = 2m_\mathfrak{p} = [R_3 : R_1]$. We shall denote by $\mathcal{D}_{R_i/R_j}$ the different ideal of R_i over R_j.

We now proceed to define a variety of constants which allow us to describe the Jordan blocks. We have:

$$\delta_\mathfrak{p} = (-1)^{[R_2:R_1]} N_{R_2/R_1}(\tfrac{1}{4}\lambda^2 \mathcal{D}^2_{R_2/R_1} \delta_{R_3/R_2}).$$

This is the discriminant of the quadratic form (see Proposition 4.5.5.) Set:

$$H_\mathfrak{p} = \mathrm{Cor}_{R_2/R_1}((z, -\lambda f_z'(z))_{R_2})(N_{R_2/R_1}(z), -1)_{R_1}^{m_\mathfrak{p}-1}(-1,-1)_{R_1}^{m_\mathfrak{p}(m_\mathfrak{p}-1)/2},$$

where $\sqrt{z}$ primitively generates the fraction field of R_3 over that of R_1. This is the Hasse invariant (see Theorem 4.5.7.)

Set $k_\mathfrak{p} = \left\lceil \frac{v_{R_1}(\delta_\mathfrak{p})}{n_\mathfrak{p}} \right\rceil$. The $k_\mathfrak{p}$ and $k_\mathfrak{p} - 1$ blocks are those which may be non-trivial. The value of $k_\mathfrak{p}$ is clear by considering the discriminant. Set:

$$n_{\mathfrak{p},i} = \begin{cases} n_\mathfrak{p} - v_{R_1}(\delta_\mathfrak{p}) \pmod{n_\mathfrak{p}}^* & i = k-1 \\ v_{R_1}(\delta_\mathfrak{p}) \pmod{n_\mathfrak{p}}^* & i = k \\ 0 & \text{otherwise.} \end{cases}$$

Note that we mean that $n_{\mathfrak{p},i}$ is a value between 0 and $n_\mathfrak{p}$. Moreover, for the $i = k_\mathfrak{p}$ case use $n_\mathfrak{p}$ as the representative for 0, for the $i = k_\mathfrak{p} - 1$ case use 0 (so that if there is only one non-trivial block it is the $k_\mathfrak{p}$ modular block). This represents the dimension of the ith modular block. Again, the computation is clear in consideration of the discriminant.

Set $\ell_\mathfrak{p} = v_{R_2}(\lambda) + v_{R_2}(\mathcal{D}_{R_2/R_1}) + v_{R_2}(\delta_{R_3/R_2})/2 \pmod{e_\mathfrak{p}}$ (a representative between 0 and $e_\mathfrak{p}$). Then define:

$$\chi_{\mathfrak{p},i}(o) = \begin{cases} 0 & p = 2,\ i = k_\mathfrak{p} - 1, k_\mathfrak{p} \text{ and } v_{R_2}(\delta_{R_3/R_2}) \text{ is odd} \\ 0 & p = 2,\ i = k_\mathfrak{p} - 1 \text{ and } \ell_\mathfrak{p} < v_{R_2}(\delta_{R_3/R_2})/2 \\ 0 & p = 2,\ i = k_\mathfrak{p} \text{ and } e_\mathfrak{p} - \ell_\mathfrak{p} < v_{R_2}(\delta_{R_3/R_2})/2 \\ 1 & \text{otherwise.} \end{cases}$$

This value is 1 if $\mathfrak{N}_i \subset 2\mathfrak{S}_i$, and 0 otherwise. This follows immediately from the criterion for evenness of the previous section.

Set $n_{\mathfrak{p},i}(e) = 2\left\lfloor \frac{n_{\mathfrak{p},i} - 1 + \chi_{\mathfrak{p},i}(o)}{2} \right\rfloor$. This represents the dimension of the maximal even dimensional unimodular sublattice with $\mathfrak{N} \subset (2)$. Then:

$$\chi_{\mathfrak{p},i}(e) = \begin{cases} (p,-1)^{(i+1)m_\mathfrak{p}}(\delta_\mathfrak{p}, p)^{i+1}(p,-1)^{n_{\mathfrak{p},i}/2} H_\mathfrak{p} & n_{\mathfrak{p},i} \neq 0 \text{ even}, p \neq 2 \\ (p,-1)^{i m_\mathfrak{p}}(\delta_\mathfrak{p}, p)^{i}(p,-1)^{(n_\mathfrak{p}+2)/2} H_\mathfrak{p} & n_{\mathfrak{p},i} \neq 0 \text{ odd}, p \neq 2 \\ (\delta_\mathfrak{p}, 2)^i(-1,-1)^{(n_\mathfrak{p}^2 - 2n_\mathfrak{p})/8} H_\mathfrak{p} & n_{\mathfrak{p},i}(e) = n_{\mathfrak{p},i} \neq 0, p = 2 \\ 1 & \text{otherwise.} \end{cases}.$$

The above is an intermediate calculation for the discriminant of the ith Jordan block. For $p \neq 2$, it amounts to checking if $(-1)^{n_{\mathfrak{p},i}(e)/2}$ times the discriminant of the block is a square based on the Hasse invariant. For $p = 2$, it computes this when this block is even. The computation assumes the other block is also even, for if it were not we would have the freedom to modify the discriminant of this block.

Let u be a non-square in $R_1^\times$. For $p=2$ set $u=3$. Define:

$$\delta_{\mathfrak{p},i} = \begin{cases} 1 & (\chi_{\mathfrak{p},i}(o)=0 \text{ and } n_{\mathfrak{p},i} \text{ odd}) \text{ or } n_{\mathfrak{p},i}=0 \\ (-1)^{n_\mathfrak{p}-n_{\mathfrak{p},i}/2}\delta_\mathfrak{p} & \chi_{\mathfrak{p},i}(o)=0, n_{\mathfrak{p},i} \text{ even} \\ (-1)^{\lfloor n_{\mathfrak{p},i}/2 \rfloor} u^{(\chi_{\mathfrak{p},i}(e)-1)/2} & \text{otherwise.} \end{cases}$$

This represents a valid discriminant for the ith modular Jordan block. For $p=2$ the value is typically accurate mod 8. If $p=2, n_{\mathfrak{p},i}=1, m_\mathfrak{p}=1$ it is only accurate mod 4 but this case does not impact the following computations. The first two cases compute the discriminant when this block is odd. It does so assuming the complementary block is hyperbolic, since if this block were odd, we would be able to assume the hyperbolicity of the complementary block. We now set:

$$H_{\mathfrak{p},i} = \begin{cases} 1 & p \neq 2 \\ 1 & n_{\mathfrak{p},i}=1 \\ (-1,-1)^{(n_p-n_{p,i})(n_p-n_{p,i}-2)/8}(\delta_{\mathfrak{p},i},-1)^{m_\mathfrak{p}-n_{\mathfrak{p},i}/2}(\delta_\mathfrak{p},2)^i H_\mathfrak{p} & \text{otherwise.} \end{cases}$$

This represents a valid Hasse invariant for the ith modular block. We compute it assuming the complementary block is even. If it is not, then the Hasse invariant of the ith block depends on a choice. Hence the result is still valid. Now we set $\chi_{\mathfrak{p},i}=0$ if n_i is odd or if $p=2$ and either $\chi_{\mathfrak{p},i-1}(o)\chi_{\mathfrak{p},i+1}(o)=0$ or $\chi_{\mathfrak{p},i}(o)=0$ and $\delta_{\mathfrak{p},i}=(-1)^{(n_{\mathfrak{p},i}-1)/2} \pmod 4$ otherwise define $\chi_{\mathfrak{p},i}$ by:

$$\chi_{\mathfrak{p},i} = \begin{cases} ((-1)^{n_{\mathfrak{p},i}/2}\delta_{\mathfrak{p},i},p) & p\neq 2, \\ (-1,-1)^{n_{\mathfrak{p},i}(n_{\mathfrak{p},i}-2)/8}H_{\mathfrak{p},i} & p=2. \end{cases}$$

This value is 0 if the isomorphism class of the maximal even unimodular sublattice is not well-defined. The value is 1 if it is hyperbolic and it is -1 if it is not hyperbolic. The computation is based on those in the proof of Corollary 4.4.20.

We now proceed to introduce the remaining terms which appear in the formulas:

$$t_{\mathfrak{p}} = \sum_i (1-\chi_{\mathfrak{p},i}(o))n_{\mathfrak{p},i} + (1-\chi_{\mathfrak{p},i}(o))(1-\chi_{\mathfrak{p},i+1}(o)) - \sum_i \delta_{n_{\mathfrak{p},i},0}(1-\chi_{\mathfrak{p},i-1}(o)\chi_{\mathfrak{p},i+1}(o)),$$

$$s_{\mathfrak{p}} = \left|\{i \mid n_{\mathfrak{p},i} \neq 0\}\right|,$$

$$w_{\mathfrak{p}} = (k-1)[R_3 : R_1]([R_3 : R_1]+1)/2 + n_k(n_k+1)/2,$$

$$P_{\mathfrak{p},i} = \prod_{j=1}^{\frac{n_{\mathfrak{p},i}(e)}{2}} (1-q^{-2j}),$$

$$E_{\mathfrak{p},i} = (1+\chi_{\mathfrak{p},i}q^{-n_{\mathfrak{p},i}(e)/2})^{-1},$$

$$P_{\mathfrak{p}} = \prod_i P_{\mathfrak{p},i},$$

$$E_{\mathfrak{p}} = \prod_i E_{\mathfrak{p},i}^{-1}.$$

Theorem 4.6.1. *Let $R_1 = \mathbb{Z}_p$ and R_3 be the ring of integers of a p-adic field with involution σ and maximal ideal $\mathfrak{p}$. Suppose $\lambda \in (R_3^\sigma)^\times$. Consider the lattice $L = R_3$ with the bilinear form:*

$$(x,y) = \tfrac{1}{2}\operatorname{Tr}_{R_3/R_1}(\lambda x\sigma(y)).$$

Using all the notation as above, we have:

$$\beta_p(L,L) = 2^{s_{\mathfrak{p}}-t_{\mathfrak{p}}}q^{w_{\mathfrak{p}}}P_{\mathfrak{p}}E_{\mathfrak{p}}.$$

Proof. The result follows immediately from Theorem 4.4.29 and the above computations of the relevant terms. □

We now combine what we know about the quadratic forms $q_{\mathfrak{p}}$ to get sufficient information about the form q_p to compute its local densities. We define the relevant constants in terms of the decomposed ones:

$$n_{p,i} = \sum_{\mathfrak{p}|p} n_{\mathfrak{p},i},$$

$$\delta_{p,i} = \prod_{\mathfrak{p}|p} \delta_{\mathfrak{p},i},$$

$$\chi_{p,i}(o) = \prod_{\mathfrak{p}|p} \chi_{\mathfrak{p},i}(o),$$

$$n_{p,i}(e) = 2\left\lfloor \frac{n_i + 1 - \chi_{p,i}(o)}{2} \right\rfloor, \text{ and}$$

$$H_{p,i} = \prod_{\mathfrak{p}|p} H_{\mathfrak{p},i} \prod_{\mathfrak{p}<\mathfrak{q}} (\delta_{\mathfrak{p},i}, \delta_{\mathfrak{q},i}).$$

The above formulas are all clear. Now we set $\chi_{p,i} = 0$ if n_i is odd or if $p = 2$ and either $\chi_{p,i-1}(o)\chi_{p,i+1}(o) = 0$ or $\chi_{p,i}(o) = 0$ and $\delta_{p,i} = (-1)^{(n_{p,i}-1)/2} \pmod 4$ otherwise define $\chi_{p,i}$ by:

$$\chi_{p,i} = \begin{cases} ((-1)^{n_{p,i}/2}\delta_{p,i}, p) & p \neq 2 \\ (-1,-1)^{n_{p,i}(n_{p,i}-2)/8} H_{p,i} & p = 2. \end{cases}$$

As above, this formula is based on the computations of Corollary 4.4.20. We may now introduce the terms which will appear in the formulas:

$$t_p = \sum_i (1 - \chi_{p,i}(o)) n_{p,i} + (1 - \chi_{p,i}(o))(1 - \chi_{p,i+1}(o)) - \sum_i \delta_{n_{p,i},0}(1 - \chi_{p,i-1}(o)\chi_{p,i+1}(o)),$$

$$s_p = \left|\{i \mid n_{p,i} \neq 0\}\right|,$$

$$w_p = \sum_i i n_{p,i}((n_{p,i}+1)/2 + \sum_{j>i} n_{p,j}),$$

$$P_{p,i} = \prod_{j=1}^{\frac{n_{p,i}(e)}{2}} (1 - q^{-2j}),$$

$$E_{p,i} = (1 + \chi_{p,i} q^{-n_{p,i}(e)/2}).$$

Finally, define:

$$P_p = \prod_i P_{p,i} \quad \text{and} \quad E_p = \prod_i E_{p,i}^{-1}.$$

Theorem 4.6.2. *Let $\mathcal{O}_E$ be the ring of integers of a number field with involution. Using all the notation above the p-adic local density of the form $\frac{1}{2}\operatorname{Tr}_{E/\mathbb{Q}}(\lambda x\sigma(y))$ on $\mathcal{O}_E$ is:*

$$\beta_p(L,L) = 2^{s_p - t_p} q^{w_p} P_p E_p.$$

Proof. Again, the result follows immediately from Theorem 4.4.29 and the above computations of the relevant terms. □

The above formula is complicated. This is largely by virtue of the fact that each $\mathfrak{p}|p$ could contribute to different Jordan blocks, and hence we must independently compute the invariants for each. One can thus in general expect no reasonable cancellation in the above formulas as there are cases where none occurs. The advantage of this formula over those of the previous section is that the formula is expressed entirely in terms of the invariants of the rings involved (and λ) and thus given a ring which one understands, one can compute this formula.

We now present a restricted case, that is, we shall suppose that $\lambda_{\mathfrak{p}}$ has small valuation for all $\mathfrak{p}$ so that $k = 1$ and the final lattice has at most 2 Jordan blocks at each p. In particular assume that $0 \le v_{\mathfrak{p}}(\lambda/2) + v_{\mathfrak{p}}(\delta_{\mathcal{O}_E/\mathcal{O}_{E^\sigma}})/2 + v_{\mathfrak{p}}(\mathcal{D}_{\mathcal{O}_{E^\sigma}/\mathbb{Z}}) \le e_{\mathfrak{p}}$ for all primes $\mathfrak{p}$ of E^σ.

Under these assumptions we have:

- The dimension of the space is $n = 2m = [E : \mathbb{Q}]$.
- The dimensions of the Jordan blocks are:

$$n_{p,0} = n - v_p(N(\lambda/2)^2 \delta_{E/\mathbb{Q}_p}) \quad \text{and} \quad n_{p,1} = v_p(N(\lambda/2)^2 \delta_{E/\mathbb{Q}_p}).$$

- The conditions for the blocks to be odd are:

$\chi_{p,0}(o) = 0$ if and only if either $v_\mathfrak{p}(\delta_{E/E^\sigma})$ odd or $e_\mathfrak{p} > v_\mathfrak{p}(\lambda) + v_\mathfrak{p}(\mathcal{D}_{E^\sigma/\mathbb{Q}})$ for some $\mathfrak{p}$.

$\chi_{p,1}(o) = 0$ if and only if either $v_\mathfrak{p}(\delta_{E/E^\sigma})$ odd or $v_\mathfrak{p}(\delta_{E/E^\sigma}) > 2e_\mathfrak{p} - v_\mathfrak{p}(\lambda) - v_\mathfrak{p}(\mathcal{D}_{E^\sigma/\mathbb{Q}})$ for some $\mathfrak{p}$.

- As before one computes $n_{p,i}(e) = 2\left\lfloor \frac{n_i+1-\chi_{p,i}(o)}{2} \right\rfloor$.
- We have the following formula for $\chi_{p,i}$:

$$\chi_{p,i} = \begin{cases} 0 & n_i = 0 \text{ or } n_i \text{ odd} \\ 0 & p = 2, \chi_{\mathfrak{p},i-1}\chi_{\mathfrak{p},i+1} = 0 \\ 0 & p = 2, \delta_\mathfrak{p} = (-1)^{m-1} \pmod 4 \\ \mathrm{Cor}_{E_p^\sigma/\mathbb{Q}_p}((z, (-1)^m p^{i+1}\lambda f_z'(z))_{E_p^\sigma}) & p \neq 2, n_i \text{ even} \\ \mathrm{Cor}_{E_p^\sigma/\mathbb{Q}_p}((z, (-1)^m 2^i \lambda f_z'(z))_{E_p^\sigma}) & \text{otherwise,} \end{cases}$$

where $\sqrt{z}$ primitively generates the E over $\mathbb{Q}_p$.

Remark. Notice that for all primes which are unramified in E and for which $v_p(N(\lambda)) = 0$ (or for $p = 2$ take $\lambda = 2$) the above formula for $\chi_{p,i}$ reduces to $((-1)^m D, p)$. The lack of symmetry at 2 is a consequence of our normalization of the form. The normalization we have chosen makes the Witt invariant formula cleaner, but breaks the symmetry in this formula.

Now set:

$$t_p = \begin{cases} (1-\chi_{p,0}(o))(n_{p,0}-1) + (1-\chi_{p,1}(o))(n_{p,1}-1) + \\ \qquad (1-\chi_{p,0}(o))(1-\chi_{p,1}(o)) & n_{p,0}n_{p,1} \neq 0 \\ (1-\chi_{p,0}(o))(n_{p,0}-2) + (1-\chi_{p,1}(o))(n_{p,1}-2) & \text{otherwise,} \end{cases}$$

$s_p = |\{i \mid n_{p,i} \neq 0\}|$, and

$w_p = n_{p,1}(n_{p,1}+1)/2.$

Theorem 4.6.3. *Let $E/\mathbb{Q}$ be a finite extension with involution σ, supposing E is primitively generated by $\sqrt{z}$ over $\mathbb{Q}$ with $z \in E^\sigma$. Let $\lambda \in (E^\sigma)^\times$ with:*

$$0 \leq v_\mathfrak{p}(\lambda/2) + v_\mathfrak{p}(\delta_{\mathcal{O}_E/\mathcal{O}_{E^\sigma}})/2 + v_\mathfrak{p}(\delta_{\mathcal{O}_{E^\sigma}/\mathbb{Z}}) \leq e_\mathfrak{p},$$

for all primes $\mathfrak{p}$ of E^σ. Then with notation as above the local density of the form $\frac{1}{2}\operatorname{Tr}_{E/\mathbb{Q}}(\lambda x\sigma(x))$ is:

$$2^{s_p-t_p}q^w \prod_{j=1}^{\frac{n_{p,0}(e)}{2}}(1-q^{-2j}) \prod_{j=1}^{\frac{n_{p,1}(e)}{2}}(1-q^{-2j})(1+\chi_{p,0}q^{-n_{p,0}(e)/2})^{-1}(1+\chi_{p,1}q^{-n_{p,1}(e)/2})^{-1}.$$

Proof. Once again this is an immediate application of Theorem 4.4.29 together with the above computations of the relevant terms. □

4.7 Example of $\mathbb{Q}(\mu_p)$

Fix a prime p of $\mathbb{Z}$. In this section we shall compute the local densities for the form

$$q_{E,\lambda} = \tfrac{1}{2}\operatorname{Tr}_{E/\mathbb{Q}}(\lambda x\sigma(x)),$$

where $E = \mathbb{Q}(\mu_p)$ is the cyclotomic field of pth roots of unity, σ is complex conjugation, and λ is restricted in valuation so that $0 \leq v_\mathfrak{q}(\lambda/2)+v_\mathfrak{q}(\delta_{\mathcal{O}_E/\mathcal{O}_{E^\sigma}})/2+v_\mathfrak{q}(\mathcal{D}_{\mathcal{O}_{E^\sigma}/\mathbb{Z}}) \leq e_\mathfrak{q}$ for all $\mathfrak{q}$.

We shall use the following 'elementary' facts.

- The ring of integers of E is $\mathcal{O}_E = \mathbb{Z}[\zeta_p^a]$ for each $a \in (\mathbb{Z}/p\mathbb{Z})^\times$.
- The ring of integers of $F := E^\sigma$ is:

  $$\mathcal{O}_F = \mathbb{Z}[\zeta_p + \zeta_p^{-1}] = \mathbb{Z}[(\zeta_p - \zeta_p^{-1})^2] = \mathbb{Z}[(\zeta_p^a - \zeta_p^{-a})^2]$$

  for each $a \in (\mathbb{Z}/p\mathbb{Z})^\times$.

  Denote by $z_a = (\zeta_p^a - \zeta_p^{-a})^2$ then z_a is totally negative and $E = \mathbb{Q}(\sqrt{z_a})$.

  Denote by f_z the minimal polynomial of z_a (this does not depend on a).
- There is a unique prime in each of $\mathcal{O}_E$ and $\mathcal{O}_F$ over p. Denote by $\mathfrak{p}$ the prime over p in $\mathcal{O}_F$.

- The discriminant of $E/\mathbb{Q}$ is $\delta_{E/\mathbb{Q}} = (-1)^{(p-1)/2} p^{p-2}$.
- Since $\zeta_p^2 \not\equiv 1 \pmod{\mathfrak{q}}$ for all $\mathfrak{q} \nmid p$ it follows that $\zeta_p^a - \zeta_p^{-a}$ and hence $(\zeta_p^a - \zeta_p^{-a})^2$ is a unit away from 2 and p.
- Since the different ideal is $\mathcal{D}_{F/\mathbb{Q}} = (f_z'(z_a))$ it follows that $f_z'(z_a)$ is a unit at all places away from p.
- The elements $\zeta_p^a - \zeta_p^{-a}$ and $(\zeta_p^a - \zeta_p^{-a})^2$ are uniformizing elements in the respective cases.

  This follows from the observation that the order $\mathbb{Z}[\sqrt{z_a}] = \mathcal{O}_F[\sqrt{z_a}]$ is maximal away from 2.
- The ramification degrees are $e_\ell = \begin{cases} p-1 & \ell = p \\ 1 & \text{otherwise} \end{cases}$.

In the formulas of the previous section we have the following:

- The dimension of the space is $[E : \mathbb{Q}] = p - 1$.
- The dimensions of the Jordan blocks are for $\ell \neq p$ are:

$$n_{\ell,0} = p - 1 - 2\nu_\ell(N_{F/\mathbb{Q}}(\lambda/2)) \text{ and } n_{\ell,1} = 2\nu_\ell(N_{F/\mathbb{Q}}(\lambda/2))$$

  and for $\ell = p$ they are:

$$n_{\ell,0} = 1 - 2\nu_p(N_{F/\mathbb{Q}}(\lambda)) \text{ and } n_{\ell,1} = p - 2 + 2\nu_p(N_{F/\mathbb{Q}}(\lambda)).$$

  Thus we set:

$$w_\ell = n_{\ell,1}(n_{\ell,1}+1)/2 \text{ and}$$
$$s_\ell = \begin{cases} 1 & \ell \neq p, \nu_\ell(N_{F/\mathbb{Q}}(\lambda)) = 0, \pm(p-1)/2 \\ 2 & \text{otherwise.} \end{cases}$$

- The parity of the Jordan blocks at 2 are:

$$\chi_{2,i}(o) = 1$$

so long as the blocks are non-trivial. This is true because the extension is unramified at 2. Consequently, $t_\ell = 0$ for all ℓ.

- The character for the blocks are computed as follows:

$$\chi_{\ell,i} = \begin{cases} 0 & \ell = p \\ \mathrm{Cor}_{E^\sigma/\mathbb{Q}}\left((z_a, (-1)^{(p-1)/2} 2^i \lambda f_z'(z_a))\right)_\ell & \ell = 2 \\ \mathrm{Cor}_{E^\sigma/\mathbb{Q}}\left((z_a, (-1)^{(p-1)/2} \ell^{i+1} \lambda f_z'(z_a))\right)_\ell & \ell \neq 2, p. \end{cases}$$

We are thus interested in computing:

$$\mathrm{Cor}_{F/\mathbb{Q}}\left((z_a, \lambda)\right) \mathrm{Cor}_{F/\mathbb{Q}}\left((z_a, (-1)^{(p-1)/2} f_z'(z_a))\right).$$

For all $\ell \neq 2, p$ we have that z_a and $f_z'(z_a)$ are units and thus:

$$\mathrm{Cor}_{F/\mathbb{Q}}\left((z_a, (-1)^{(p-1)/2} f_z'(z_a))\right)_\ell = 1.$$

For $\ell = 2$ we have that:

$$\mathrm{Cor}_{F/\mathbb{Q}}\left((z_a, (-1)^{(p-1)/2} f_z'(z_a))\right)_2 \cdot (-1)^{(p-1)(p-3)/8}$$

computes the Hasse invariant of the form (for $\lambda = 1$). Since this Hasse invariant is 1 for all places (including infinite) other than p we can conclude that:

$$\begin{aligned} &\mathrm{Cor}_{F/\mathbb{Q}}((z_a,(-1)^{(p-1)/2} f_z'(z_a)))_2 \\ &\qquad = (-1)^{(p-1)(p-3)/8} \mathrm{Cor}_{F/\mathbb{Q}}\left((z_a, (-1)^{(p-1)/2} f_z'(z_a))\right)_p \end{aligned}$$

We are thus reduced to computing $\mathrm{Cor}_{F/\mathbb{Q}}\left((z_a, (-1)^{(p-1)/2} f_z'(z_a)\right)_p$. Observe that:

$$\begin{aligned}
\left(z_a, (-1)^{(p-1)/2} f_z'(z_a)\right)_{\mathfrak{p}} &= \left(z_a, -z_a^{-1}\right)_{\mathfrak{p}}^{(p-3)/2} \left(z_a, (-1)^{(p-1)/2} f_z'(z_a)\right)_{\mathfrak{p}} \\
&= (z_a, -1)_{\mathfrak{p}} \left(z_a, z^{-(p-3)/2} f_z'(z_a)\right)_{\mathfrak{p}} \\
&= (z_a, -1)_{\mathfrak{p}} \prod_{a \neq b \in (\mathbb{Z}/p\mathbb{Z})^\times/\pm 1} \left(z_a, 1 - \tfrac{z_b}{z_a}\right)_{\mathfrak{p}}.
\end{aligned}$$

Now, we may use that z_a is a uniformizer and that:

$$\frac{z_b}{z_a} \cong \frac{a^2}{b^2} \pmod{z_a}.$$

It follows that the terms we wish to evaluate are actually:

$$\left(z_a, 1 - \tfrac{z_b}{z_a}\right)_{\mathfrak{p}} = \left(z_a, 1 - \tfrac{b^2}{a^2}\right)_{\mathfrak{p}} = \left(z_a, 1 - \tfrac{b}{a}\right)_{\mathfrak{p}} \left(z_a, 1 + \tfrac{b}{a}\right)_{\mathfrak{p}}.$$

The resulting expression now becomes:

$$\begin{aligned}
\left(z_a, (-1)^{(p-1)/2} f_z'(z_a)\right)_{\mathfrak{p}} &= (z_a, -1)_{\mathfrak{p}} \prod_{\pm a \neq b \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(z_a, 1 - \tfrac{b}{a}\right)_{\mathfrak{p}} \\
&= (z_a, -2)_{\mathfrak{p}}.
\end{aligned}$$

Applying the Corestriction map we have:

$$\mathrm{Cor}_{F/\mathbb{Q}}\left((z_a, -2)_{\mathfrak{p}}\right) = \left(N_{F/\mathbb{Q}}(z_a), -2\right)_p = \left((-1)^{(p-1)/2} p, -2\right)_p = (p, -2)_p.$$

From this we can conclude that:

$$\mathrm{Cor}_{F/\mathbb{Q}}\left((z_a, (-1)^{(p-1)/2} f_z'(z_a))\right)_2 = (-1)^{(p-1)(p-3)/8} (p, -2)_p = 1.$$

Now, for all $\ell \neq p$ we find:

$$\mathrm{Cor}_{E^\sigma/\mathbb{Q}}\left((z_a, \ell)\right)_\ell = \left(\tfrac{(-1)^{(p-1)/2} p}{\ell}\right) = \left(\tfrac{\ell}{p}\right).$$

Thus we can conclude that:

$$\chi_{\ell,i} = \begin{cases} 0 & \ell = p \\ \mathrm{Cor}_{E^\sigma/\mathbb{Q}}\left((z_a, \lambda)\right)_\ell & \ell = 2, i = 0 \\ \mathrm{Cor}_{E^\sigma/\mathbb{Q}}\left((z_a, \lambda)\right)_\ell \left(\frac{\ell}{p}\right) & \ell = 2, i = 1 \\ \mathrm{Cor}_{E^\sigma/\mathbb{Q}}\left((z_a, \lambda)\right)_\ell & \ell \neq p, i = 1 \\ \mathrm{Cor}_{E^\sigma/\mathbb{Q}}\left((z_a, \lambda)\right)_\ell \left(\frac{\ell}{p}\right) & \ell \neq p, i = 0. \end{cases}$$

⧫ Examples

Combining all of the above we can easily compute the product over all local densities for the following cases:

- Case $\lambda = 2$, the arithmetic volume is:

$$2p^{(p-2)(p-1)/2}(1 - p^{p-1}) \prod_\ell \left(\left(1 + \left(\frac{\ell}{p}\right) \ell^{(p-1)/2}\right) \prod_{i=1}^{(p-1)/2} (1 - \ell^{-2i})^{-1} \right).$$

- Case $\lambda = 2\mu$, where $\mu \in \mathcal{O}_F^\times$ has a unique negative embedding and $(z_a, \mu)_\mathfrak{p} = -1$, the arithmetic volume is:

$$2p^{(p-2)(p-1)/2}(1 - p^{p-1}) \prod_\ell \left(\left(1 + \left(\frac{\ell}{p}\right) \ell^{(p-1)/2}\right) \prod_{i=1}^{(p-1)/2} (1 - \ell^{-2i})^{-1} \right).$$

- Case $\lambda = 2\mu$, where $\mu \in \mathcal{O}_F^\times$ has a unique negative embedding and $(z_a, \mu)_\mathfrak{p} = 1$, the arithmetic volume is:

$$2p^{(p-2)(p-1)/2}(1 - p^{p-1}) \frac{1 - \left(\frac{2}{p}\right) 2^{(p-1)/2}}{1 + \left(\frac{2}{p}\right) 2^{(p-1)/2}} \prod_\ell \left(\left(1 + \left(\frac{\ell}{p}\right) \ell^{(p-1)/2}\right) \prod_{i=1}^{(p-1)/2} (1 - \ell^{-2i})^{-1} \right).$$

- Case $\lambda = 2\mathfrak{q}$, where $(\mathfrak{q})|q \neq p$ is prime and $(q,p)_{\mathfrak{p}} = -1$, set $n_q = \nu_q(N_{F/\mathbb{Q}}(\mathfrak{q}))$ and suppose $(\mathfrak{q}) \neq (q)$ and $\mathfrak{q}$ is totally positive, the arithmetic volume is:

$$2^2 p^{(p-2)(p-1)/2} q^{n_q(n_q-1)/2} \left(1 - q^{n_q}\right) \left(1 + q^{(p-1)/2 - n_q}\right) \prod_{i=1}^{n_q} \left(1 - q^{2i}\right)^{-1}$$
$$\prod_{i=1}^{p-1-n_q} \left(1 - q^{2i}\right)^{-1} \prod_{\ell \neq q} \left(\left(1 + \left(\frac{\ell}{p}\right) \ell^{(p-1)/2}\right) \prod_{i=1}^{(p-1)/2} (1 - \ell^{-2i})^{-1} \right).$$

- Case $\lambda = 2\mathfrak{q}$, where $\mathfrak{q}|q \neq p, 2$ is prime and $(q,p)_{\mathfrak{p}} = 1$, set $n_q = \nu_q(N_{F/\mathbb{Q}}(\mathfrak{q}))$ and suppose $(\mathfrak{q}) \neq (q)$ and $\mathfrak{q}$ is totally positive, the arithmetic volume is:

$$2^2 p^{(p-2)(p-1)/2} q^{n_q(n_q-1)/2} \left(1 + q^{n_q}\right) \left(1 + q^{(p-1)/2 - n_q}\right) \prod_{i=1}^{n_q} \left(1 - q^{2i}\right)^{-1}$$
$$\prod_{i=1}^{p-1-n_q} \left(1 - q^{2i}\right)^{-1} \frac{1 - \left(\frac{2}{p}\right) 2^{(p-1)/2}}{1 + \left(\frac{2}{p}\right) 2^{(p-1)/2}}$$
$$\prod_{\ell \neq q} \left(\left(1 + \left(\frac{\ell}{p}\right) \ell^{(p-1)/2}\right) \prod_{i=1}^{(p-1)/2} (1 - \ell^{-2i})^{-1} \right).$$

Other more complicated combinations can be handled similarly.

CHAPTER 5
Conclusion

The topic of Shimura varieties of orthogonal type provides for many avenues of research. The main results of this thesis resolves only a few. Even these results aren't the end of the road as further questions can still be asked.

In terms of the results of Chapter 3, concerning the characterization of special points (or more accurately algebraic tori) associated to orthogonal groups, the following generalizations remain open:

1. A characterization of the non-maximal tori which do not appear as direct factors. Specifically we can consider embeddings

$$T_{F,\sigma} \hookrightarrow \mathrm{GL}(F^n)$$

   and ask when such a torus preserves a quadratic form on F^n. Or equivalently when does there exist an extension (E, σ) of (F, σ) such that $q \simeq q_{E,\sigma,\lambda}$. This question relates to a characterization of 'generalized special cycles' (see Section 2.5.3).

2. A characterization of the algebraic tori in other reductive groups, including the outer forms of orthogonal groups and Spin groups. For Spin groups, our results shed a fair bit of light on the problem, but in this setting some questions remain open. One may still ask, for example, which algebras are complete reflex algebras? For classical groups arising from involutions one expects many similar phenomena to arise.

3. Even more generally one may ask for a characterization of inclusions of algebraic groups $G \hookrightarrow \mathrm{O}_q$ or more ambitiously $G_1 \hookrightarrow G_2$ or $G_1 \to G_2$. A necessary condition is certainly that for all $T \hookrightarrow G_1$ there exists a map $T \to G_2$. This motivates looking at the case of tori first.

Besides these generalizations, another problem which the present work does not discuss is that of relating the characterization of tori given in Chapter 3 with that given in my masters thesis [Fio09]. The characterization there is in terms of certain cohomology classes in $H^1(\mathrm{Gal}(\overline{k}/k), N_{\mathrm{O}}(T))$ and it would be interesting to relate this to the characterization given here in terms of étale algebras with involution. One expects the correspondence to be quite natural and this is something I intend to look at in a more general context in upcoming work.

As for the results of Chapter 4 a number of natural questions remain open:

4. Obtaining more general formulas for $\beta_{\mathfrak{p}}(L, M)$ for primes $\mathfrak{p}$ over 2. Some of the results of Chapter 4 are easily extended to this context, in particular Theorem 4.4.11. Other results would require performing a significant number of new computations, specifically Theorem 4.4.18. Finally, some of the results may simply not extend in any natural way and thus require entirely new ideas, for example Theorem 4.4.28.
5. Computing more explicitly the contribution of the structure of distinct Jordan decompositions to $\beta_{\mathfrak{p}}(L, L)$. Specifically, over $\mathbb{Q}_2$, the formula simplifies greatly, and one should expect a similar result for other explicit (especially unramified) extensions of $\mathbb{Q}_2$.
6. More refined computation of invariants for transfer of lattices over 2-adic rings. In particular a complete description of the norm group.

A major theme of Chapter 2 is computing dimension formulas. The work here suggests several areas needing more work.

7. An explicit description of a smooth projective toroidal compactification for the $\mathrm{O}(2, n)$ Shimura varieties. In particular a detailed understanding of the cone decomposition for the relevant cone Ω.
8. Computations of the intersection numbers for Chern classes and boundary components relevant for the Riemann-Roch theorem.

9. Explicit formulas for the numbers of cusps of a compactification.
10. More refined results on the vanishing of cohomology.

Another topic of great interest, alluded to in Chapter 2, is that of studying the many types of cycles which appear in orthogonal Shimura varieties. Many of the questions one may ask about these cycles naturally generalize those one asks about special points. In particular, one can ask about the field of definition of a cycle and its irreducible components, and consequently, about the precise role the various cycles may play in explicit class field theory. Moreover, these cycles have an important role in Arakelov theory and an understanding of the relationship between their intersection theory and the special values of L-functions is a topic of great interest.

I hope that the above provides an indication at the breadth of the field which remains to be explored.

Index of Notations

Index of Definitions

REFERENCES

[AMRT10] Avner Ash, David Mumford, Michael Rapoport, and Yung-Sheng Tai, *Smooth compactifications of locally symmetric varieties*, second ed., Cambridge Mathematical Library, Cambridge University Press, Cambridge, 2010, With the collaboration of Peter Scholze.

[AS68] M. F. Atiyah and I. M. Singer, *The index of elliptic operators. III*, Ann. of Math. (2) **87** (1968), 546–604.

[BB66] W. L. Baily, Jr. and A. Borel, *Compactification of arithmetic quotients of bounded symmetric domains*, Ann. of Math. (2) **84** (1966), 442–528.

[BCKM03] Rosali Brusamarello, Pascale Chuard-Koulmann, and Jorge Morales, *Orthogonal groups containing a given maximal torus*, J. Algebra **266** (2003), no. 1, 87–101.

[BDP10] Massimo Bertolini, Henri Darmon, and Kartik Prasanna, *Chow-Heegner points on CM elliptic curves and values of p-adic L-series*, 2010.

[BF13] E. Bayer-Fluckiger, *Embeddings of maximal tori in orthogonal groups*, Ann. Inst. Fourier (Grenoble) (2013), (To Appear).

[BJ06] Armand Borel and Lizhen Ji, *Compactifications of symmetric and locally symmetric spaces*, Mathematics: Theory & Applications, Birkhäuser Boston Inc., Boston, MA, 2006.

[BKY12] Jan Hendrik Bruinier, Stephen S. Kudla, and Tonghai Yang, *Special values of Green functions at big CM points*, Int. Math. Res. Not. IMRN (2012), no. 9, 1917–1967.

[Bor66] Armand Borel, *Introduction to automorphic forms*, Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965), Amer. Math. Soc., Providence, R.I., 1966, pp. 199–210.

[Bor69] ———, *Introduction aux groupes arithmétiques*, Publications de l'Institut de Mathématique de l'Université de Strasbourg, XV. Actualités Scientifiques et Industrielles, No. 1341, Hermann, Paris, 1969.

[Bor91] ———, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991.

[Bor95] Richard E. Borcherds, *Automorphic forms on* $\mathrm{O}_{s+2,2}(\mathbf{R})$ *and infinite products*, Invent. Math. **120** (1995), no. 1, 161–213.

[Bru02] Jan H. Bruinier, *Borcherds products on O(2, l) and Chern classes of Heegner divisors*, Lecture Notes in Mathematics, vol. 1780, Springer-Verlag, Berlin, 2002.

[Bru04] Jan Hendrik Bruinier, *Infinite products in number theory and geometry*, Jahresber. Deutsch. Math.-Verein. **106** (2004), no. 4, 151–184.

[Bru08] ______, *Hilbert modular forms and their applications*, The 1-2-3 of modular forms, Universitext, Springer, Berlin, 2008, pp. 105–179.

[BS58] Armand Borel and Jean-Pierre Serre, *Le théorème de Riemann-Roch*, Bull. Soc. Math. France **86** (1958), 97–136.

[BY06] Jan Hendrik Bruinier and Tonghai Yang, *CM-values of Hilbert modular functions*, Invent. Math. **163** (2006), no. 2, 229–288.

[Del71] Pierre Deligne, *Travaux de Shimura*, Séminaire Bourbaki, 23ème année (1970/71), Exp. No. 389, Springer, Berlin, 1971, pp. 123–165. Lecture Notes in Math., Vol. 244.

[Del79] ______, *Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques*, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, pp. 247–289.

[DL03] Henri Darmon and Adam Logan, *Periods of Hilbert modular forms and rational points on elliptic curves*, Int. Math. Res. Not. (2003), no. 40, 2153–2180.

[DS05] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.

[Epk89] Martin Epkenhans, *Trace forms of normal extensions over local fields*, Linear and Multilinear Algebra **24** (1989), no. 2, 103–116.

[Fio09] Andrew Fiori, *Special points on orthogonal symmetric spaces*, Master's thesis, McGill University, 2009.

[Fio12] ______, *Characterization of special points of orthogonal symmetric spaces*, Journal of Algebra **372** (2012), no. 0, 397 – 419.

[Fre90] Eberhard Freitag, *Hilbert modular forms*, Springer-Verlag, Berlin, 1990.

[Ful84] William Fulton, *Introduction to intersection theory in algebraic geometry*, CBMS Regional Conference Series in Mathematics, vol. 54, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1984.

[Ful98] ______, *Intersection theory*, second ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 2, Springer-Verlag, Berlin, 1998.

[GHS07] V. A. Gritsenko, K. Hulek, and G. K. Sankaran, *The Kodaira dimension of the moduli of $K3$ surfaces*, Invent. Math. **169** (2007), no. 3, 519–567.

[GHS08] V. Gritsenko, K. Hulek, and G. K. Sankaran, *Hirzebruch-Mumford proportionality and locally symmetric varieties of orthogonal type*, Doc. Math. **13** (2008), 1–19.

[GK93] Benedict H. Gross and Kevin Keating, *On the intersection of modular correspondences*, Invent. Math. **112** (1993), no. 2, 225–245.

[Gro99] Benedict H. Gross, *Algebraic modular forms*, Israel J. Math. **113** (1999), 61–93.

[GV12] Matthew Greenberg and John Voight, *Lattice methods for algebraic modular forms on classical groups*, arXiv preprint arXiv:1209.2460 (2012).

[GZ86] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[Han05] Jonathan Hanke, *An exact mass formula for quadratic forms over number fields*, J. Reine Angew. Math. **584** (2005), 1–27.

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[Hel01] Sigurdur Helgason, *Differential geometry, Lie groups, and symmetric spaces*, Graduate Studies in Mathematics, vol. 34, American Mathematical Society, Providence, RI, 2001, Corrected reprint of the 1978 original.

[Hir66] F. Hirzebruch, *Topological methods in algebraic geometry*, Third enlarged edition. New appendix and translation from the second German edition by R. L. E. Schwarzenberger, with an additional section by A. Borel. Die Grundlehren der Mathematischen Wissenschaften, Band 131, Springer-Verlag New York, Inc., New York, 1966.

[Hua79] L. K. Hua, *Harmonic analysis of functions of several complex variables in the classical domains*, Translations of Mathematical Monographs, vol. 6, American Mathematical Society, Providence, R.I., 1979, Translated from the Russian, which was a translation of the Chinese original, by Leo Ebner and Adam Korányi, With a foreword by M. I. Graev, Reprint of the 1963 edition.

[Jac85] Nathan Jacobson, *Basic algebra. I*, second ed., W. H. Freeman and Company, New York, 1985.

[Kat99] Hidenori Katsurada, *An explicit formula for Siegel series*, Amer. J. Math. **121** (1999), no. 2, 415–452.

[Kit93] Yoshiyuki Kitaoka, *Arithmetic of quadratic forms*, Cambridge Tracts in Mathematics, vol. 106, Cambridge University Press, Cambridge, 1993.

[KMRT98] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI, 1998, With a preface in French by J. Tits.

[Kod53] K. Kodaira, *On a differential-geometric method in the theory of analytic stacks*, Proc. Nat. Acad. Sci. U. S. A. **39** (1953), 1268–1273.

[KR99] Stephen S. Kudla and Michael Rapoport, *Arithmetic Hirzebruch-Zagier cycles*, J. Reine Angew. Math. **515** (1999), 155–244.

[Kud97a] Stephen S. Kudla, *Algebraic cycles on Shimura varieties of orthogonal type*, Duke Math. J. **86** (1997), no. 1, 39–78.

[Kud97b] ______, *Central derivatives of Eisenstein series and height pairings*, Ann. of Math. (2) **146** (1997), no. 3, 545–646.

[Kud04] ______, *Special cycles and derivatives of Eisenstein series*, Heegner points and Rankin L-series, Math. Sci. Res. Inst. Publ., vol. 49, Cambridge Univ. Press, Cambridge, 2004, pp. 243–270.

[Lam05] T. Y. Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, vol. 67, American Mathematical Society, Providence, RI, 2005.

[Lan83] Serge Lang, *Complex multiplication*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 255, Springer-Verlag, New York, 1983.

[Mil83] J. S. Milne, *The action of an automorphism of* $\mathbf{C}$ *on a Shimura variety and its special points*, Arithmetic and geometry, Vol. I, Progr.

Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 239–265.

[Mil05] ______, *Introduction to Shimura varieties*, Harmonic analysis, the trace formula, and Shimura varieties, Clay Math. Proc., vol. 4, Amer. Math. Soc., Providence, RI, 2005, pp. 265–378.

[Mil06] James S. Milne, *Complex multiplication*, 2006, Available at www.jmilne.org/math/, p. 113.

[Mum77] D. Mumford, *Hirzebruch's proportionality theorem in the noncompact case*, Invent. Math. **42** (1977), 239–272.

[Nam80] Yukihiko Namikawa, *Toroidal compactification of Siegel spaces*, Lecture Notes in Mathematics, vol. 812, Springer, Berlin, 1980.

[O'M00] O. Timothy O'Meara, *Introduction to quadratic forms*, Classics in Mathematics, Springer-Verlag, Berlin, 2000, Reprint of the 1973 edition.

[Pal65] Gordon Pall, *The weight of a genus of positive n-ary quadratic forms*, Proc. Sympos. Pure Math., Vol. VIII, Amer. Math. Soc., Providence, R.I., 1965, pp. 95–105.

[PR94] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press Inc., Boston, MA, 1994, Translated from the 1991 Russian original by Rachel Rowen.

[PR10] Gopal Prasad and Andrei S. Rapinchuk, *Local-global principles for embedding of fields with involution into simple algebras with involution*, Comment. Math. Helv. **85** (2010), no. 3, 583–645.

[Ser73] Jean-Pierre Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer-Verlag, New York, 1973, Translated from French.

[Ser79] ______, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[Ser84] ______, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comment. Math. Helv. **59** (1984), no. 4, 651–676.

[SH00] Fumihiro Sato and Yumiko Hironaka, *Local densities of representations of quadratic forms over p-adic integers (the non-dyadic case)*, J. Number Theory **83** (2000), no. 1, 106–136.

[Shi80] Goro Shimura, *The arithmetic of certain zeta functions and automorphic forms on orthogonal groups*, Ann. of Math. (2) **111** (1980), no. 2, 313–375.

[Shi99] ———, *An exact mass formula for orthogonal groups*, Duke Math. J. **97** (1999), no. 1, 1–66.

[Sie35] Carl Ludwig Siegel, *Über die analytische Theorie der quadratischen Formen*, Ann. of Math. (2) **36** (1935), no. 3, 527–606.

[Sie67] C. L. Siegel, *Lectures on quadratic forms*, Notes by K. G. Ramanathan. Tata Institute of Fundamental Research Lectures on Mathematics, No. 7, Tata Institute of Fundamental Research, Bombay, 1967.

[SP04] Rainer Schulze-Pillot, *Representation by integral quadratic forms—a survey*, Algebraic and arithmetic theory of quadratic forms, Contemp. Math., vol. 344, Amer. Math. Soc., Providence, RI, 2004, pp. 303–321.

[Tai82] Yung-Sheng Tai, *On the Kodaira dimension of the moduli space of abelian varieties*, Invent. Math. **68** (1982), no. 3, 425–439.

[Tsu80] Ryuji Tsushima, *A formula for the dimension of spaces of Siegel cusp forms of degree three*, Amer. J. Math. **102** (1980), no. 5, 937–977.

[Wat76] G. L. Watson, *The* 2*-adic density of a quadratic form*, Mathematika **23** (1976), no. 1, 94–106.

[Yan04] Tonghai Yang, *Local densities of 2-adic quadratic forms*, J. Number Theory **108** (2004), no. 2, 287–345.