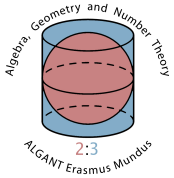


Université Bordeaux I

Stellenbosch University

Masters Thesis

Do Trace Forms Characterise Number Fields?

Author:
Frances Ogochukwu Odumodu

Supervisor:
Prof. Boas Erez

A thesis submitted in fulfilment of the requirements for the degree of Master of Science

in the

Department of Mathematics

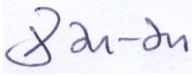
July 2013

Abstract

The discriminant completely characterises a quadratic number field. But for higher degree number fields, this is not the case. Thus, we would like to find an invariant that characterises number fields. Let K be a number field and $tr_{K/\mathbb{Q}} : K \times K \to \mathbb{Q}$ be the trace form over $\mathbb{Q}$. Then, $(K, tr_{k/\mathbb{Q}})$ is a quadratic space and so we can apply the theory of quadratic forms to the classification problem of number fields. Moreover, the discriminant of the trace form is the discriminant of the number field up to square factors. Two number fields are said to be arithmetically equivalent if their zeta functions coincide. The zeta function like the discriminant determines the decomposition of primes in a number field. Thus, it makes sense to study the isometry classes of the trace forms of arithmetically equivalent number fields.

Declaration

I, the undersigned, hereby declare that the work contained in this thesis is my original work, and that any work done by others or by myself previously has been acknowledged and referenced accordingly.



Frances Ogochukwu Odumodu, July 2013

Contents

Abstract i

1 Introduction 1

2 Quadratic Forms 2

2.1 Diagonalisation . . . 3

2.2 Isometry . . . 3

2.3 Orthogonal group . . . 4

2.4 The Hyperbolic plane . . . 6

2.5 Some invariants . . . 7

2.6 Rational equivalence . . . 9

2.7 Quadratic forms over a ring . . . 12

3 Arithmetical Equivalence 21

3.1 Algebraic Number Fields . . . 21

3.2 Trace forms . . . 24

3.3 Classification of Trace forms . . . 26

4 Totally or Non-totally Real Number Fields 32

4.1 Indefinite integral trace forms . . . 32

4.2 Positive definite integral trace forms . . . 33

5 Conclusion 34

A Integral lattices 35

A.1 Indefinite unimodular forms . . . 35

A.2 Definite unimodular forms . . . 37

References 40

1. Introduction

The classification problem is to determine when two objects in a certain collection are equivalent and to give a complete set of invariants that determine an equivalence class. It also renders a non-redundant enumeration of such objects by placing each object in exactly one class. Most of the time, a canonical form can be given for each class.

Let K be a number field of degree n over $\mathbb{Q}$. Let $w_1, \ldots, w_n$ be a $\mathbb{Q}$-basis for K and $\sigma_1, \ldots, \sigma_n$ be the distinct $\mathbb{Q}$-linear embeddings of K into a normal closure N of $\mathbb{Q}$. The discriminant of K is given by $\det(\sigma_i(w_j))^2$. The discriminant of a quadratic number field completely characterises it. But for number fields of higher degree this is no longer the case. Hermite's theorem gives that there are only finitely many number fields of a given bounded discriminant. Can we find another invariant that characterises number fields?

View a number field K as a $\mathbb{Q}$-vector space. Then, the trace form

$$tr : K \times K \to \mathbb{Q},\ tr_{K/\mathbb{Q}}(x, y) = \ \mathrm{trace}_{K/\mathbb{Q}}(xy)$$

is a quadratic form on K. The integral trace form is the trace form obtained by restricting the above map to the ring of integers $\mathcal{O}_K$ of K. The discriminant of the trace form is the discriminant of the number field up to square factors. Thus, we can consider the trace form as a refinement of the discriminant. In other words, we apply the theory of quadratic forms to the classification problem of algebraic number fields.

Let $\mathcal{O}_K$ be the ring of integers of K and $\mathfrak{a}$ a nonzero ideal of $\mathcal{O}_K$. The zeta function of K is given by

$$\zeta(s) = \sum_{\mathfrak{a} \subset \mathcal{O}_K} N(\mathfrak{a})^{-s} \quad s \in \mathbb{C}, \quad \mathrm{Re}(s) > 1$$

where $N(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})$ is the absolute norm of the ideal $\mathfrak{a}$. The zeta function is an important invariant of a number field. And like the discriminant, it determines the decomposition of primes in a number field. Two number fields are called arithmetically equivalent when their zeta functions coincide. Thus, it makes sense to study the isometry classes of the trace forms of arithmetically equivalent fields.

An outline of the thesis:

In chapter 2, we review the classical theory of quadratic forms. We discuss the classification of a general n-ary quadratic form over fields and rings of interest to arithmetic. The theory over the rational integers does not satisfy the Hasse-Minkowski theorem, hence we obtain a classification into genus. There is also the spinor genus which is an intermediate classification between the genus and the integral classification.

In chapter 3 we recall some classical theory of number fields and their trace forms. We discuss the classification of trace forms of arithmetically equivalent number fields into rational and integral isometry classes, genus and spinor genus. We ask in which case does the isometry class of the trace form characterise the number fields.

In the study of integral quadratic forms (over $\mathbb{Z}$), the problem is always separated into indefinite and positive definite forms. By a theorem of Tauskky Todd, we see that this is the same as considering totally real and non-totally real Number Fields. This is the subject of chapter 4.

2. Quadratic Forms

In this chapter, we recall the classical theory of quadratic forms that we will need for our work.

Let k be a field of characteristic $\neq 2$. Let V be a finite dimensional k-vector space. A *quadratic form* on V is a function $q : V \to k$ which satisfies the following property:

- $q(ax) = a^2 q(x)$ for all $a \in k$ and $x \in V$ and
- the function $b : V \times V \to k$; $(x, y) \mapsto \frac{1}{2}(q(x + y) - q(x) - q(y))$ is a symmetric bilinear form.

The function b is called the bilinear form associated with q. Note that if b is a symmetric bilinear form on V, then $q : V \to k$, $q(x) = b(x, x)$ is a quadratic form on V. Thus the theory of quadratic form and the theory of symmetric bilinear forms are equivalent. The pair (V, b) (or equivalently (V, q)) is called a *quadratic space*.

Let $n = \dim V$ the dimension of V. If we choose a basis $\{v_1, \ldots, v_n\}$ of V over k, we obtain a symmetric matrix $M = m_{ij} = (b(v_i, v_j))_{i,j}$. The $n \times n$ matrix M is called a (Gramm) matrix of b with respect to the basis.

Let $\{u_1, \ldots, u_n\}$ be a different basis of V. Then, we can write the u_i in terms of the v_i: $u_i = \sum_{j=1}^{n} a_{ij} v_j$. This gives $C = A^t BA$ for some $A \in \mathrm{GL}_n(k)$; where $C = (b(u_i, u_j))_{i,j}$. Thus the matrices corresponding to the different bases of V are congruent to each other.

Fix a basis $v_1, \ldots, v_n$ of V. Let $M = (m_{ij})$ be a symmetric matix. Define a bilinear form on V by $b(v_i, v_j) = m_{ij}$ and extend to all of V by bilinearity. Thus, to each symmetric matrix, we have associated a symmetric bilinear form. This association depends on a choice of basis. Therefore the set of symmetric bilinear spaces is in bijection with the symmetric matrices. The symmetric matrices allow us to do explicit computations.

Given a finite dimensional k-vector space V. Its dual V^* is defined as the set of k-linear maps

$$V^* = \mathrm{Hom}_k(V, k).$$

We have a k-linear map (*the adjoint*) for each $x \in V$

$$\mathrm{ad} : V \to V^*,\ x \mapsto b(x, y);\ y \in V.$$

Define the radical of V as the subspace

$$\mathrm{rad}(V) = V^{\perp} = \{x \in V : b(x, y) = 0 \text{ for all } y \in V\} = \ker(V \to V^*).$$

2.0.1 Definition. The quadratic space (V, b) is said to be *non-degenerate*, non-singular or regular if it satisfies one of the following equivalent statements.

1. ad: $V \to V^*$ is an isomorphism.
2. If $x \in V$ and $b(x, y) = 0$ for all $y \in V$ then $x = 0$. In otherwords, if $\mathrm{rad}(V) = 0$.
3. The determinant $\det M \neq 0$, where $M = (b(v_i, v_j))_{ij}$ is the matrix of V with respect to a basis $\{v_1, \ldots, v_n\}$.

2.1 Diagonalisation

Let (V, b) be a non-degenerate quadratic space over a field k. Let $x, y \in V$. Then x and y are said to be *orthogonal* if $b(x, y) = 0$. Two quadratic subspaces U and W of V are said to be *orthogonal* if u and w are orthogonal for every $u \in U$ and every $w \in W$.

Let $(V_1, b_1), \ldots, (V_n, b_n)$ be quadratic spaces. A quadratic space (V, b) is said to be an *orthogonal sum* of the V_i if

- V is a direct sum: $V = V_1 \oplus \ldots \oplus V_n$ and
- the V_i are pairwise orthogonal: $b(V_i, V_j) = 0;\ 1 \leq i < j \leq n$ where b is given by $b((u_1, \ldots, u_n), (v_1, \ldots, v_n)) = b_1(u_1, v_1) + \ldots + b_n(u_n, v_n)$.

Let (V, b) be a quadratic space over k. Then there exists an orthogonal sum $V = \text{ rad } V \oplus V'$ for some non-degenerate subspace V' of V. Indeed, take a basis for $\text{rad}(V)$ and extend it to a basis for V. This is called a *radical splitting* of V. The subspace V' is not unique unless V is non-degenerate. Given a quadratic space (V, b). If U is a non-degenerate vector subspace of V, then $V = U \oplus U^{\perp}$ is an orthogonal sum and U is said to split V. From now on, we will only consider non-degenerate quadratic spaces.

A basis $\{e_1, \ldots, e_n\}$ of V is said to be an orthogonal basis if $b(e_i, e_j) = 0$ for $i \neq j$. Equivalently, the matrix of the form with respect to this basis is a diagonal matrix:

$$M = (b(e_i, e_j))_{i,j} = \text{ diag } (a_1, \ldots, a_n).$$

We denote the form b with respect to a diagonal basis by $b = \langle a_1, \ldots, a_n \rangle$. If we write x as $x = \sum_i x_i e_i$, then we have $q(x) = a_1 x_1^2 + \ldots + a_n x_n^2$.

2.2 Isometry

We would like to know when two quadratic spaces are isometric and to be able to classify them into isometry classes. Also, we want a set of invariants which completely determine an isometry class of a given quadratic space. These are what we will be considering in this section.

Two quadratic spaces (V_1, b_1) and (V_2, b_2) are said to be *isometric* over k if there exists a k-linear isomorphism (isometry) $\phi : V_1 \to V_2$ such that

$$b_2(\phi(x), \phi(y)) = b_1(x, y) \text{ for all } x, y \in V_1.$$

That is, ϕ preserves the form.

Suppose we have two isometric quadratic spaces, (V_1, b_1) and (V_2, b_2). Let $\{u_1, \ldots, u_n\}$ be a basis for V_1 with matrix $M = b_1(u_i, u_j)$ and let $\{v_1, \ldots, v_n\}$ be a basis for V_2 with matrix $N = b_2(v_i, v_j)$. Then since

the $\phi(u_i)$ form a basis for V_2, we can express each $\phi(u_i)$ in terms of $\{v_1, \ldots, v_n\}$: $\phi(u_i) = \sum_j a_{ij} v_j$. Now, for some $A \in \mathsf{GL}_n(k)$, we have

$$M = b_1(u_i, u_j) = b_2(\phi(u_i), \phi(u_j)) = b_2\left(\sum_k a_{ik} v_k, \sum_l a_{jl} v_l\right)$$
$$= \sum_{k,l} a_{ik} b_2(v_k, v_l) a_{jl} = A^t N A$$

Thus, the quadratic spaces (V_1, b_1) and (V_2, b_2) are isometric over k if and only if their associated matrices are congruent. We say that the matrices M and N are equivalent over k.

We can represent ϕ by the matrix A: $\phi(x) = Ax$. Thus, the condition on ϕ then becomes, $b_1(x, y) = b_2(Ax, Ay)$. If we specify, an orthonormal basis, then A is orthogonal.

Let $a \in k^\times$, a unit and $\langle a \rangle$ be the quadratic space with basis e such that $b(e, e) = a$. Then $\langle a \rangle \cong \langle c \rangle$ if and only if $c = b^2 a$ for some $b \in k^\times$.

2.2.1 Theorem. *Every quadratic space over a field k has an orthogonal basis.* □

Scaled quadratic forms:
Let (V, b) be a quadratic space. Let $\alpha \in k^\times$. We can define a new form on V by $b^\alpha : V \times V \to k$, $b^\alpha(x, y) = \alpha b(x, y)$ for all $x, y \in V$, with associated quadratic map $q^\alpha(x) = \alpha q(x)$ for all $x \in V$. Put $V^\alpha = (V, b^\alpha)$. Then V is said to be scaled by α.

Kronecker (tensor) product of a quadratic form: Let (V_1, b_1) and (V_2, b_2) be two quadratic spaces over a field k. Then, their Kronecker product is given by: $(V, b) = (V_1, b_1) \otimes (V_2, b_2) = (V_1 \otimes V_2, b_1 \otimes b_2)$. The bilinear form b is given by $b_1 \otimes b_2(x_1 \otimes y_1, x_2 \otimes y_2) := b_1(x_1, x_2) b_2(y_1, y_2)$ for generators $x \otimes y$ of $V_1 \otimes V_2$. This extends uniquely to the whole of V. We will be particularly interested in the case where V_1 is a vector space of rank one; that is $\langle a \rangle \otimes V$ with a a unit.

If V is a diagonal form, say $V \cong \langle a_1, \ldots, a_n \rangle$. Then $\langle a \rangle \otimes V = \langle aa_1, \ldots, aa_n \rangle$ and so is just a scaling of V by a. We will denote this by $\langle a \rangle V$. Note that if M is the matrix of V, then $\langle a \rangle \otimes V$ has matrix aM.

2.3 Orthogonal group

Let (V, b) be a nondegenrate quadratic space. An isometry $\sigma : V \to V$ is called an *orthogonal transformation* of V. It follows from the definition of an isometry that an orthogonal transformation preserves the form. These orthogonal transformations form a group with respect to composition called the *orthogonal group* and is denoted by $O(V)$. Thus, $O(V)$ is a subgroup of the group of linear transformations of V denoted by $\mathsf{GL}(V)$. Thus, a linear transformation is orthogonal if and only if it preserves the form.

Let $M = b(v_i, v_j)$ be the matrix of the form b relative to the basis $(v_1, \ldots, v_n)$. Since the σv_i form a basis for V, we have

$$b(v_i, v_j) = b(\sigma v_i, \sigma v_j) = b\left(\sum_k a_{ik} v_k, \sum_l a_{jl} v_l\right) = \sum_{k,l} a_{ik} b(v_k, v_l) a_{jl}.$$

In matrix form we have $M = A^t M A$ for $A = (a_{ij})$. This is the necessary and sufficient condition on the matrix A of σ relative to $v_1, \ldots, v_n$ for σ to be orthogonal. We can write,

$$O(V) = \{A \in \mathsf{GL}_n(k) : A^t M A = M\}.$$

Now, $\det \sigma$ is the determinant of A. So it follows that $\det(M) = \det(A)^2 \det(M)$. Since, (V, b) is nondegenerate, we have that $\det(M) \neq 0$ so that $\det(A)^2 = 1$. Thus, $\det \sigma = \det(A) = \pm 1$.

If $\det \sigma = +1$, then σ is called a proper transformation or a rotation. If it has determinant -1, then it is called an improper transformation or a reflection. Let M be a diagonal matrix of (V, b) with respect to an orthogonal basis. If M has diagonal entries ± 1, it satisfies $A^t M A = M$, and so determines an orthogonal transformation. Denote by $O^+(V)$ the set of rotations and by $O^-(V)$ the set of reflections. The determinant $\det$ induces a surjective group homomorphism $\det : O(V) \to \{\pm 1\}$ with kernel $O^+(V)$. Thus, $O^+(V)$ is a normal subgroup of $O(V)$ of index 2 while $O^-(V)$ is a coset.

Symmetries:

Let $u \in V$ be such that $q(u) \neq 0$. This always exists since (V, b) is non-degenerate. Then we can associate to u a map

$$\tau_u : V \to V,\ x \mapsto x - \frac{2b(x,u)}{q(u)} u.$$

called the *symmetry* of V with respect to u. It has the following properties:

1. $\tau_u \in O(V)$.
2. Let ku be the one dimensional vector subspace of V spanned by u. We can rewrite τ_u as:

$$\tau_u(v) = \begin{cases} -v & \text{if } v \in ku \\ v & \text{if } v \in ku^\perp \end{cases}.$$

3. Since u is anisotropic, we have a decomposition $V = ku \oplus ku^\perp$. If we choose a basis for V which consists of u and a basis for $ku^\perp$, then with respect to this basis, τ_u has the diagonal matrix with diagonal entries $\{-1, 1, \ldots, 1\}$. Thus, $det \tau_u = -1$ and τ_u is improper.
4. τ_u is an involution. That is, $\tau_u^2 = 1$.
5. If $\sigma \in O(V)$, then $\sigma \tau_u \sigma^{-1} = \tau_{\sigma u}$. That is the symmetries in $O(V)$ are closed under conjugation.

2.3.1 Theorem (Cartan-Dieudonné; [O'M73]; 43:3)**.** *Let (V, b) be a non-degenerate quadratic space of dimension n. Then, every isometry $\sigma \in O(V)$ is a product of at most n symmetries.* □

2.4 The Hyperbolic plane

Let (V, b) be a quadratic space over k. Let $v \in V$ be a nonzero element. The element v is *isotropic* if $q(v) = 0$ and *anisotropic* otherwise. The quadratic space (V, b) is called isotropic if it contains an isotropic vector and anisotropic if it does not. It is totally isotropic if all its nonzero elements are isotropic.

A hyperbolic plane $\mathbb{H}$ is a non-degenerate quadratic space over k of rank two with matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ in a basis $\{v_1, v_2\}$. A quadratic space is said to be hyperbolic if it is isometric to an orthogonal sum of hyperbolic planes; thus it has an even dimension.

2.4.1 Theorem. *Let (V, b) be a 2-dimensional quadratic space. The following are equivalent:*

1. *V is a hyperbolic plane.*
2. *V is isotropic and non-degenerate.*

□

Any two hyperbolic planes are isometric. Any hyperbolic plane contains exactly two 1-dimensional totally isotropic subspaces. Indeed, if u and v form a basis for $\mathbb{H}$, then $q(\alpha u + \beta v) = \alpha\beta$. Thus, $\alpha u + \beta v$ is isotropic if and only if $\alpha = 0$ and $\beta \neq 0$ or $\alpha \neq 0$ and $\beta = 0$. So the only 1-dimensional totally isotropic subspaces are ku and kv. Hence, $\mathbb{H} = ku + kv$.

2.4.2 Theorem. *Every non-degenerate isotropic quadratic space is split by a hyperbolic plane.*

Proof. Let (V, b) be a quadratic space over k and $x \in V$ be an isotropic element. Since V is non-degenerate, we can find an element $y \in V$ such that $b(x, y) \neq 0$. Thus, $U = kx + ky$ is a non-degenerate binary isotropic space. By Theorem 2.4.1, it is a hyperbolic plane. Moreover, since it is non-degenerate, it splits V. Hence, $V = U \oplus U^{\perp}$. □

The orthogonal group of the hyperbolic plane:

Let $\sigma \in O(\mathbb{H})$ and ku and kv be the isotropic lines in $\mathbb{H}$. Then we have one of the two cases:

1. Either $\sigma(ku) = ku$ and $\sigma(kv) = kv$. In this case σ is a rotation.
2. or σ switches the two lines: $\sigma(ku) = kv$ and $\sigma(kv) = ku$. In this case σ is a symmetry.

Let $\alpha, \beta \in k^{\times}$. If the first case holds, then $\sigma(u) = \alpha u$ and $\sigma(v) = \beta v$. Thus, $b(u, v) = b(\sigma(u), \sigma(v)) = \alpha\beta b(u, v)$. Since $b(u, v) \neq 0$, we have that $\beta = \alpha^{-1}$. Hence, $\sigma(u) = \alpha u$ and $\sigma(v) = \alpha^{-1} v$ and so σ is a rotation. Similarly, in the second case we have that $\sigma(u) = \alpha v$ and $\sigma(v) = \alpha^{-1} u$ and so σ is a reflection.

Let $z = u - \alpha v \in \mathbb{H}$, with α nonzero. Then, $q(z) \neq 0$ and so z is anisotropic. Let τ_z be a symmetry in $O(\mathbb{H})$. Then, a simple calculation yields $\tau_z(u) = \alpha v$ and $\tau_z(v) = \alpha^{-1}(u)$. Thus every symmetry is of this form. Hence if σ is a symmetry, then $\sigma = \tau_{u-\alpha v}$. Moreover, if σ is not a reflection, then $\sigma = \tau_{u-v}\tau_{u-\alpha v}$.

2.4.3 Theorem (Witt Cancelation theorem)**.** *([Ger08], page 30) and ([O'M73], 42:16) Let (V, b) be a quadratic space over k and U and W non-degenerate subspaces which are isometric. Then $U^\perp \cong W^\perp$.* □

Remark: Note that this is indeed a cancellation. For if U is any regular subspace of V, we have $V = U \oplus U^\perp$. Thus, $V = U \oplus U^\perp = W \oplus W^\perp$ and $U \cong W$ gives $U^\perp \cong W^\perp$ by the theorem.

2.4.4 Theorem (Witt's extension theorem)**.** *Every isometry between two regular subspaces of a quadratic k-space (V, b) can be extended to an isometry of the whole of V.* □

Witt decomposition:

Let (V, b) be a quadratic space over k. If V is isotropic, then by theorem 2.4.2, it has a hyperbolic component $\mathbb{H}$ and so $V = \mathbb{H} \oplus \mathbb{H}^\perp$. If $\mathbb{H}^\perp$ is also isotropic, it also has a hyperbolic plane component. If we continue thus, we eventually obtain the following orthogonal sum

$$V = \mathbb{H}_1 \oplus \ldots \oplus \mathbb{H}_r \oplus V_a$$

where for each i, $\mathbb{H}_i$ is a hyperbolic plane and $r \geq 0$; and V_a is zero or anisotropic. This splitting of V is known as a *Witt decomposition* for V. The integer r is called the *Witt index* of V and is denoted by $\mathrm{ind} V$.

By cancellation theorem 2.4.3, the integer r does not depend on the way V is split. Thus, V_a is unique up to isometry; it is called the *anisotropic part* of V. ([O'M73], 42:16) yields that r is really the index of V and so satisfies $0 \leq 2r \leq \dim V$. Consequently, the classification of quadratic spaces can be reduced to the case of anisotriopic ones.

2.5 Some invariants

Two invariants of a quadratic space are the rank and the discriminant:

The **rank** of a form is the dimension of the underlying vector space. If $V \cong V_1 \oplus \ldots \oplus V_n$, an orthogonal sum, then $\mathrm{rank} V = \sum_i \mathrm{rank} V_i$. The rank $\mathrm{rk}(\langle a \rangle V) = \mathrm{rk}(V)$.

Let (V, b) be a quadratic space and M the matrix of the form with respect to some basis of V. Since the quadratic space is non-degenerate, $\det(M) \in k^\times$. If we consider another basis, we obtain

$$M' = B^t M B$$
$$\det(M') = \det(B)^2 \det(M)$$

where B is the matrix of change of basis. Thus, $\det(M) \in k^\times/(k^\times)^2$; that is, it is well defined up to multiplication by squares in $k^\times$. Define the **discriminant** of (V, b) as $d(V) = \det(M) \in k^\times/(k^\times)^2$. If V is an orthogonal sum, then $d(V) = \prod_i d(V_i)$. Moreover, if $V \cong \langle a_1, \ldots, a_n \rangle$, then $d(V) = a_1 \ldots a_n$. The discriminant, $\mathrm{disc}(\langle a \rangle V) = a^{\mathrm{rk}(V)} \mathrm{disc}(V)$. The discriminant of a hyperbolic plane is -1.

The invariants we have so far suffice to classify a quadratic spaces over the complex numbers and over a finite field up to isomorphism:

Classification over $\mathbb{C}$: For forms over the complex numbers $\mathbb{C}$, the dimension (rank) is sufficient. Every complex number is a square. Thus for a non-degenerate quadratic space (V, b), we have

$$V \cong \langle a_1, \ldots, a_n \rangle \cong \langle 1, \ldots, 1 \rangle.$$

Therefore, for two quadratic spaces (V_1, b_1) and (V_2, b_2) over $\mathbb{C}$, we have

$$(V_1, b_1) \cong (V_2, b_2) \text{ if and only if } \dim V_1 = \dim V_2.$$

Hence, there is only one isometry class for each dimension n.

Classification over the real numbers:

Let (V, b) be a quadratic space over $\mathbb{R}$ of rank n. Since, every positive real number is a square, we have

$$V \cong \langle a_1, \ldots, a_r, a_{r+1}, \ldots, a_{r+s} \rangle \cong \langle 1, \ldots, 1, -1, \ldots, -1 \rangle,$$

where r and s are the numbers of $+1$ and -1 respectively and $r + s = n$. Define (V, b) to be positive definite if $r = n$ $(s = 0)$, negative definite if $s = n$ $(r = 0)$, definite if it is either positive or negative definite and indefinite if it is not definite. Thus, (V, b) is indefinite if and only if it is isotropic. According to Sylvester's law of inertia, the numbers r and s are constant in an isometry class. Thus, we define a new invariant, the signature of (V, b) as the pair (r, s) given in an isometric diagonal form. Note that the discriminant of V is $(-1)^s$. Thus, the signature determines the discriminant.

2.5.1 Theorem. *The rank and the signature (r, s) determine completely the isometric class of a quadratic space over $\mathbb{R}$.* □

Classification over finite fields of characteristic $p \neq 2$:

Let $\mathbb{F}_q$ be a finite field of order $q = p^f$, $p \neq 2$. Consider the homomorphism,

$$\varphi : \mathbb{F}_q^\times \to (\mathbb{F}_q^\times)^2; \quad x \mapsto x^2.$$

Then, $\ker(\varphi) = \{\pm 1\}$ has two distinct elements since $p \neq 2$. Thus, we have that

$$\mathbb{F}_q^\times / \{\pm 1\} \cong (\mathbb{F}_q^\times)^2.$$

From this we can deduce that $(\mathbb{F}_q^\times)^2$ is a group of $(q-1)/2$ elements and that $\mathbb{F}_q^\times / (\mathbb{F}_q^\times)^2$ has two elements. Therefore, for every x in $\mathbb{F}_q^\times$, either $x = b^2$ for some $b \in \mathbb{F}_q^\times$ or $x = b^2 c$, where c is not a square in $\mathbb{F}_q^\times$.

2.5.2 Theorem. *Let (V, b) be a quadratic space of rank n over $\mathbb{F}_q^\times$. Then*

$$V \cong \langle 1, \ldots, 1, d \rangle, \ d \in \mathbb{F}_q^\times,$$

depending on whether d is a square or not. Thus, there are precisely two isometry classes of quadratic spaces over $\mathbb{F}_q$. □

2.5.3 Corollary. The discriminant in $\mathbb{F}_q^\times / (\mathbb{F}_q^\times)^2$ and the rank completely determine the isometry class of a quadratic space over $\mathbb{F}_q$.

For quadratic forms over other fields, we need other invariants.

2.6 Rational equivalence

To classify quadratic forms over $\mathbb{Q}$, we use the Hasse-Minkowski local to global theorem.

2.6.1 Theorem. *(Hasse-Minkowski)*
$(V_1, b_1) \cong_{\mathbb{Q}} (V_2, b_2)$ *if and only if* $(V_1, b_1) \cong_{\mathbb{Q}_p} (V_2, b_2)$ *for all* p *prime including* $p = \infty$. □

With this theorem in mind, we need to consider isometry of quadratic spaces over the real numbers and the p-adic numbers.

Equivalence over $\mathbb{Q}_p$:

Here, we need another invariant, the Hasse-Witt invariant, in order to classify quadratic forms over $\mathbb{Q}_p$. But first we have to define the Hilbert symbol.

2.6.2 Definition. Let p be a prime including $p = \infty$, so that $\mathbb{Q}_\infty = \mathbb{R}$. Let $a, b \in \mathbb{Q}_p^\times$. Then, the Hilbert symbol is defined as:

$$(a, b)_p = \begin{cases} 1 & \text{if } ax^2 + by^2 - z^2 = 0 \text{ has a nontrivial solution in } \mathbb{Q}_p^3 \\ -1 & \text{otherwise} \end{cases}.$$

The Hibert symbol $(a, b)_p$ is well defined on a and b modulo squares. Thus, it defines a map (a bilinear form): $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \times \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \to \{\pm 1\}$.

2.6.3 Proposition. Let $a, b \in \mathbb{Q}_p^\times$ and let $K = \mathbb{Q}_p(\sqrt{b})$. Then, $(a, b)_p = 1$ if and only if a is a norm in $K^\times$. □

Some properties of the Hilbert symbol. See [Ser96] and [Cas08], page 42.

1. It is symmetric $(a, b)_p = (b, a)_p$.
2. It is bilinear $(a_1 a_2, b)_p = (a_1, b)_p (a_2, b)_p$.
3. It is a non-degenerate. That is, if $b \in \mathbb{Q}_p^\times$ and $(a, b)_p = 1$ for all $a \in \mathbb{Q}_p^\times$ then $b \in (\mathbb{Q}_p^\times)^2$.
4. $(a, -a)_p = 1$ and $(a, 1 - a)_p = 1$ and $(a, c^2)_p = 1$.
5. $(a, b)_p = (a, -ab)_p = (a, (1 - a)b)_p$.

We recall the square classes group $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$.

2.6.4 Proposition. (Square classes)

1. Let p be an odd prime. Then, $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ has order 4 and has $\{1, p, r, pr\}$ as representatives; r is a quadratic nonresidue modulo p.
2. $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ has order 8 and has $\{\pm 1, \pm 2, \pm 5, \pm 10\}$ as representatives.
3. $\mathbb{R}^\times/(\mathbb{R}^\times)^2$ is a cyclic group of order 2, generated by the class of -1.

□

There is a formula expressing the Hilbert symbols explicitly in terms of the Legendre symbols. Recall the definition of the Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p \end{cases}.$$

Also put

$$\varepsilon(n) = \frac{n-1}{2} \bmod 2 = \begin{cases} 0 & \text{if } n \equiv 1 \bmod 4 \\ 1 & \text{if } n \equiv -1 \bmod 4 \end{cases}$$

and

$$\omega(n) = \frac{n^2-1}{8} \bmod 2 = \begin{cases} 0 & \text{if } n \equiv \pm 1 \bmod 8 \\ 1 & \text{if } n \equiv \pm 5 \bmod 8 \end{cases}.$$

Then, we have the following theorem:

2.6.5 Theorem. *[Ser96]*

1. *For $p = \infty$, we have*
$$(a,b)_p = \begin{cases} 1 & \text{if } a > 0 \text{ or } b > 0 \\ -1 & \text{if } a < 0 \text{ and } b < 0 \end{cases}$$
.

2. *For p a finite prime, put $a = p^\alpha u$ and $b = p^\beta v$, $u, v \in \mathbb{Z}_p^\times$, units. Then we have*
$$(a,b)_p = \begin{cases} (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha & \text{if } p \neq 2 \\ (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)} & \text{if } p = 2. \end{cases}.$$
Here, if $u \in \mathbb{Z}_p^\times$ has image $\bar{u} \in \mathbb{F}_p^\times$, then $\left(\frac{u}{p}\right) = \left(\frac{\bar{u}}{p}\right)$.

□

2.6.6 Corollary. 1. If p is an odd prime and $u, v \in \mathbb{Z}_p^\times$, then $(u,v)_p = 1$.

2. If $p = 2$, $(-1,-1)_2 = -1$. Furthermore, if ε is a unit then $(5,\varepsilon)_2 = 1$ and $(5,2\varepsilon)_2 = -1$.

□

In [Cas08], the author computes the tables of Hilbert symbols for $\mathbb{Q}_p$, p prime, including $p = \infty$ on the representatives of the square class group. These tables can be reproduced by using the formulas in theorem 2.6.5.

Now, we can define the Hasse-Witt invariant. Let (V,b) be a quadratic form. Taking an orthogonal basis for V, let $(V,b) \cong \langle a_1, \ldots, a_n \rangle$. Then the *Hasse-Witt invariant* is defined as

$$h_p(V) = \prod_{1 \leq i < j \leq n} (a_i, a_j)_p = \pm 1.$$

where $(a_i, a_j)_p$ are Hilbert symbols over $\mathbb{Q}_p$ as defined above.

If $V = V_1 \oplus V_2$ is an orthogonal sum of two quadratic spaces over a field k. Then, $h_p(V) = h_p(V_1)h_p(V_2)(\text{disc}(V_1), \text{disc}(V_2))_p$. Furthermore, $h_p(\langle a \rangle V) = h_p(V)(a, (-1)^{\frac{n(n+1)}{2}} d(V)^{n+1})_p$

2.6.7 Theorem. *The rank, discriminant and the Hasse-Witt invariant form a complete set of invariants of an isometry class of a quadratic space (V, b) over $\mathbb{Q}_p$.* □

We can compute the Hasse-Witt invariant over $\mathbb{R}$ by using the following formula: $h_\infty(V) = (-1)^{\frac{s(s-1)}{2}}$. Thus, the signature determines the Hasse invariants.

Equivalence over $\mathbb{Q}$:

Now consider the embeddings $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ for each p including $p = \infty$. Let P be the set of all primes including $p = \infty$. Then we can view the quadratic space (V, b) as a quadratic space over each $\mathbb{Q}_p$. Denote this by (V_p, b). Recall the Hasse-Minkowski's theorem: (U, b_1) is isometric to (V, b_2) if and only if (U_p, b_1) is isometric to (V_p, b_2) for all $p \in P$.

2.6.8 Theorem (Hilbert)**.** *Let $a, b \in \mathbb{Q}$. Then the Hilbert symbol $(a, b)_p = 1$ for all but a finite number of $p \in P$ and*

$$\prod_{p \in P} (a, b)_p = 1.$$

□

Let (V, b) be a quadratic space over $\mathbb{Q}$ and on choosing a diagonal basis, let $V \cong \langle a_1, \ldots, a_n \rangle$. Then the invariants of V over $\mathbb{Q}$ are:

1. The rank n.
2. The discriminant $d(V) = a_1 \ldots a_n \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. The discriminant of V_p for each p is the image of $d(V)$ under the map $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \to \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$.
3. The signature, obtained by embedding $\mathbb{Q}$ in $\mathbb{R}$.
4. The Hasse invariants $h_p(V)$ for all p prime.

2.6.9 Theorem (Hasse-Minkowski 2)**.** *The invariants above completely determine the isometry class of a quadratic space over $\mathbb{Q}$.* □

Remark: In classifying quadratic forms up to $\mathbb{Q}$ isometry, we "reduced" the problem to classification over $\mathbb{Q}_p$ for all prime p including $p = \infty$. In reality, we only need to consider a finite number of primes. Indeed, let $V \cong \langle a_1, \ldots, a_n \rangle$, where each a_i is a square-free unit. Let d be the discriminant of V. Suppose p is an odd prime and p does not divide d. Then, $h_p(V_p) = 1$. Thus, it suffices to check isometry over $\mathbb{Q}_p$ for p primes such that p divides $2d$ and for $p = \infty$.

2.7 Quadratic forms over a ring

Let R be an integral domain with fraction field k. Let (V, b) be a quadratic space of rank n over k. Let M be a finitely generated free R-module in V. An integral quadratic form is the quadratic form obtained by restricting b to $M \times M$. Put $\mathrm{rad}(M) = M^{\perp} = \{x \in M : b(x, y) = 0 \text{ for all } y \in M\}$. Thus, $\mathrm{rad}(M) = \mathrm{rad}(V) \cap R$. We will mostly be interested in the cases where R is the rational integers, p-adic integers or the ring of integers of finite extensions of the p-adic numbers.

Now, let A be a symmetric matrix. We will call A a *unimodular* matrix if its entries are in R and its determinant is a unit in R. Two matrices M and N are said to be *congruent* if there is a unimodular matrix T such that $M = T^t N T$.

Let (V, b) be a quadratic space over k and M a finitely generated free R-module in V. Then (M, b) is nondegenerate if $\mathrm{rad}(M) = 0$ (that is, if the adjoint is injective) equivalently, if $\det(M)$ is a unit in R.

2.7.1 Lattices. Let R be a principal ideal domain with fraction field k. Let V be a finite dimensional k-vector space equipped with a symmetric bilinear form b. Let $n = \dim V$.

A lattice Λ in V is a finitely generated free R-module. Thus, there is a k-basis $v_1, \ldots, v_n$ of V such that $\Lambda = Rv_1 \oplus \ldots \oplus Rv_n$.

Given such a lattice, we can associate a symmetric matrix M of Λ in a basis $v_1, \ldots, v_n$ by putting $M = (m_{ij}) = b(v_i, v_j)$. Taking a different basis $u_1, \ldots, u_n$ we get a matrix N of Λ which is congruent to M. Thus, to a lattice, we can associate a class of congruent symmetric matrices.

Two lattices Λ_1 and Λ_2 are isometric over R if there is a $\sigma \in O(V)$ such that $\sigma(\Lambda_1) = \Lambda_2$. Suppose M_1 is the matrix of Λ_1 and M_2 is the matrix of Λ_2 then Λ_1 is isometric to Λ_2 if and only if M_1 and M_2 are congruent. We say that the two matrices are equivalent over R.

We define the rank of a lattice Λ to be the dimension of V. The discriminant of Λ is the determinant of the associated matrix M in $R^{\times}/(R^{\times})^2$. Thus, two isometric lattices have the same rank and discriminant.

We give here some definitions that will be useful in the classification of lattices. Let R be a principal ideal domain with fraction field k. Let (V, b) be a quadratic space of dimension n over k. Let $\{v_1, \ldots, v_n\}$ be a basis of V and Λ be an R-lattice with respect to this basis. Then we have the following definitions:

The **scale** of Λ, $s\Lambda$ is the R-module generated by $b(\Lambda, \Lambda)$. So if $v_1, \ldots, v_n$ is a basis for Λ then $s\Lambda \subseteq \sum_{ij} b(v_i, v_j)R$. The **norm** of Λ, $n\Lambda$ is the R-module generated by $q(\Lambda)$. The **volume** of a lattice Λ, $v\Lambda$ is the ideal $(d\Lambda)$ generated by its discriminant. The **norm group** of Λ is given by $\mathfrak{g}(\Lambda) = q(\Lambda) + 2s(\Lambda)$.

Now, $q(\Lambda) \subseteq b(\Lambda, \Lambda)$ and for all $x, y \in \Lambda$, $2b(x, y) = q(x+y) - q(x) - q(y)$ and thus, $2s\Lambda \subseteq n\Lambda \subseteq s\Lambda$. If $2 \in R^{\times}$ then $n\Lambda = s\Lambda$. If on the other hand, $2 \notin R^{\times}$, then either $n\Lambda = s\Lambda$ or $n\Lambda = 2(s\Lambda)$.

The lattice defined by $\Lambda^* = \{x \in V : b(x, y) \in R \text{ for all } y \in \Lambda\}$ is called the **dual** lattice of Λ. The lattice Λ is said to be **integral** if $b(\Lambda, \Lambda) \subseteq R$ or equivalently if $\Lambda \subseteq \Lambda^*$. If $2 \notin R^{\times}$, then an integral lattice Λ is said to be **even** (properly primitive in [Cas08]) if the diagonal entries of $(b(v_i, v_j))$ lie in $2R$. Equivalently, if $n\Lambda = 2(s\Lambda)$. Otherwise, it is said to be **odd** (improperly primitive in [Cas08]).

Let $\mathfrak{a} = (a)$ be an ideal of R. We say that an R-lattice Λ is $\mathfrak{a}$-**modular** if and only if $s\Lambda = \mathfrak{a}$ and $v\Lambda = \mathfrak{a}^n$. A lattice Λ is unimodular if $s\Lambda = R$. Equivalently if $\Lambda = \Lambda^*$. If M is the matrix of Λ with respect to some basis, then Λ is unimodular if and only if M is unimodular.

Let $\mathfrak{a} = (a) = aR$. Then, Λ is $\mathfrak{a}$-**maximal** if and only if $n\Lambda \subset \mathfrak{a}$ and if M is another lattice with $nM \subset \mathfrak{a}$ then $M = \Lambda$. Unimodular lattices are always R-maximal.

2.7.2 Genus. In discussing the isometry of quadratic forms over $\mathbb{Z}$, a necessary condition is that they should be isometric over $\mathbb{Z}_p$ for all primes p, including $p = \infty$. We would hope as in the case of $\mathbb{Q}$ that this condition is also sufficient. But unfortunately, the Hasse-Minkowski local-to-global theorem does not hold for quadratic forms over $\mathbb{Z}$. Thus, we have the following definition.

2.7.3 Definition. Two quadratic forms f and g are in the same genus if and only if $f \sim_{\mathbb{Z}_p} g$ for all primes $p \in \mathbb{Z}$ including $p = \infty$.

Thus, in order to characterise the genus of a quadratic space we have to discuss first the $\mathbb{Z}_p$-isometry for each $p \in \mathbb{Z}$ prime. We have already seen isometry over $\mathbb{R}$. So for the rest of this section, $p \neq \infty$. We use the geometric language of quadratic lattices.

Classification of lattices over $\mathbb{Z}_p$ where p is an odd prime:

Let (V, b) be a non-degenerate quadratic space over $\mathbb{Q}_p$. Let Λ be a unimodular lattice in V. In this case, 2 is a unit in $\mathbb{Z}_p$ and so we have that $n\Lambda = s\Lambda$.

2.7.4 Theorem. *Let Λ be a unimodular lattice in the quadratic space (V, b), then Λ has an orthogonal basis. Moreover, for some unit ε in $\mathbb{Z}_p^\times$,*

$$\Lambda \cong \langle 1, \ldots, 1, \varepsilon \rangle.$$

Proof. Since Λ is unimodular, we have $n\Lambda = R$ and so we can find an element $v_1 \in \Lambda$ such that $q(v_1) = a_1 \in R^\times$. Thus $Rv_1 \cong \langle a_1 \rangle$ is unimodular and we have an orthogonal sum $\Lambda = Rv_1 \oplus Rv_1^\perp$. Repeating this on $Rv_1^\perp$, we eventually get an orthogonal sum $\Lambda \cong \langle a_1, \ldots, a_n \rangle$.

Now, let $M = \langle 1, \ldots, 1, \varepsilon \rangle$ be such that $\mathsf{rk}(\Lambda) = \mathsf{rk}(M)$ and $\varepsilon = a_1 \ldots a_n$. From Theorem 2.6.5, we can deduce that $(a, b)_p = 1$ for units $a, b \in \mathbb{Z}_p^\times$. Thus, L and M both have Hasse invariant 1. Therefore, $\mathbb{Q}_p M = \mathbb{Q}_p \Lambda = V$; that is, they have the same underlying vector space V. Now, since Λ and M are both unimodular, they are R-maximal. Hence, by ([O'M73]; 91:2), $\Lambda \cong M$. □

Any nonzero $a \in \mathbb{Z}_p$ has a canonical form $a = a_0 + a_1 p + a_2 p^2 + \ldots$, with $a_i \in \{0, 1, \ldots, p-1\}$. As a consequence of the surjection, $\mathbb{Z}_p \to \mathbb{F}_p$; $a \mapsto a_0$, we have that a is a unit in $\mathbb{Z}_p$ if and only if a_0 is a unit in $\mathbb{F}_p$. Hensel's lemma yields: a is a square if and only if it is a nonzero quadratic residue mod p. Since a unimodular $\mathbb{Z}_p$-lattice Λ is isometric to $\langle 1, \ldots, 1, \varepsilon \rangle$ for some $\varepsilon \in \mathbb{Z}_p^\times$, we have that if the reduction mod p of two quadratic forms are isometric and nondegenrate over $\mathbb{F}_p$, then they are isometric over $\mathbb{Z}_p$. Consequently, we have the following theorem:

2.7.5 Theorem. *Let (V, b) be a quadratic space over $\mathbb{Q}_p$ and Λ_1 and Λ_2 be two unimodular $\mathbb{Z}_p$-lattices on (V, b). Then, the lattices are isometric if and only if they have the same rank and discriminant.* □

In dealing with general lattices, it always helps to break them up into modular components and then to classify each component by the preceding theorem.

2.7.6 Theorem (Jordan decomposition)**.** *Let Λ be a $\mathbb{Z}_p$-lattice. Then Λ has the following Jordan decomposition: $\Lambda = \Lambda_0 \oplus \ldots \oplus \Lambda_t$. Each $\Lambda_i = p^i\langle a_1, \ldots, a_n\rangle \cong p^i\langle 1, \ldots, 1, u\rangle$ where each $a_j \in \mathbb{Z}_p^\times$ and u is either a quadratic residue (and hence can be replaced by 1) or a quadratic nonresidue modulo p. We also have that $s(\Lambda_i) = p^i$ and so $s(\Lambda_i) \supset s(\Lambda_{i+1})$. Moreover, if $\Lambda = \Gamma_0 \oplus \ldots \oplus \Gamma_k$ is another Jordan decomposition, then $t = k$, rank$(\Lambda_i) =$ rank(Γ_i) and $s(\Lambda_i) = s(\Gamma_i)$ for each i.*

Proof. [O'M73], §91c; [Cas08], Theorem 3.1, page 115; [Ger08], page 162; [CS98], page 378. □

2.7.7 Corollary ([Ger08], page 164; [O'M73], 92:2)**.** Let Λ and Γ be two lattices in a quadratic space of dimenstion n over $\mathbb{Q}_p$. Let $\Lambda = \Lambda_1 \oplus \ldots \oplus \Lambda_t$ and $\Gamma = \Gamma_0 \oplus \ldots \oplus \Gamma_k$. If rank$(\Lambda_i) =$ rank(Γ_i) and $s(\Lambda_i) = s(\Gamma_i)$, then $\Lambda \cong \Gamma$ if and only if disc$(\Lambda_i) =$ disc(Γ_i) for each i. □

Classification over $\mathbb{Z}_2$:

Recall that 2 is not a unit in $\mathbb{Z}_2$. Thus $n\Lambda = s\Lambda$ or $n\Lambda = 2(s\Lambda)$.

2.7.8 Theorem ([Ger08],page 168)**.** *Let Λ be a unimodular lattice in a quadratic space over $\mathbb{Q}_2$. Then,*

1. *If $n\Lambda = \mathbb{Z}_2$, then Λ has an orthogonal basis. In fact, Λ is isometric to an orthogonal sum of sublattices of the following types: $\langle 1\rangle$, $\langle 3\rangle$, $\langle 5\rangle$, $\langle 7\rangle$.*
2. *If $n\Lambda = 2\mathbb{Z}_2$ (i.e.Λ is even), then Λ is an orthogonal sum of binary sublattices of the form $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$.*

The following theorem characterises even unimodular $\mathbb{Z}_2$-lattices.

2.7.9 Theorem. *Let Λ be a unimodular $\mathbb{Z}_2$-lattice of even rank ≥ 4 such that $n\Lambda = 2\mathbb{Z}_2$. Then, Λ is isometric to $\mathbf{H}$ or $\mathbf{H} \oplus \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, where $\mathbf{H}$ is an orthogonal sum of hyperbolic planes.*

Proof. From theorem 2.7.8, we have that Λ is an orthogonal sum of binary sublattices: $\mathbb{H}$ and $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Thus, it suffices to show that

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \oplus \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

are isometric over $\mathbb{Z}_2$. Now, they have the same rank, discriminant and hasse invariants. So their underlying fields are isometric. Both lattices are (2)-maximal; hence by ([Ger08],theorem 8.8), they are isometric. □

Note that Λ is isometric to $\mathbb{H} \oplus \ldots \oplus \mathbb{H}$ if its discriminant is congruent to ± 1 mod 8 and it is isometric to $\mathbb{H} \oplus \ldots \oplus \mathbb{H} \oplus \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ if its discriminant is congruent to ± 5 mod 8; ([Cas08], page 119).

2.7.10 Corollary. Let L and M be two even unimodular lattices of the same rank. Suppose they have equal unit discriminant. Then they are isometric over $\mathbb{Z}_2$.

2.7.11 Theorem (Jordan decomposition)**.** *Let Λ be a $\mathbb{Z}_2$-lattice. Then Λ has the following Jordan decomposition: $\Lambda = \Lambda_0 \oplus \ldots \oplus \Lambda_t$. Each $\Lambda_i = 2^i A_i$ with each A_i unimodular. We have $s(\Lambda_i) = p^i$ and so $s(\Lambda_i) \supset s(\Lambda_{i+1})$. Furthermore, Theorems 2.7.8 and 2.7.9 give the form of each A_i.*

Moreover, if $\Lambda = \Gamma_0 \oplus \ldots \oplus \Gamma_k$ is another Jordan decomposition, then $t = k$, rank(Λ_i) = rank(Γ_i), $n(\Lambda_i) = n(\Gamma_i)$ and $s(\Lambda_i) = s(\Gamma_i)$ for each i.

The invariants in the last theorem are called the *Jordan invariants* of a lattice.

Let (V, b) be a quadratic space over $\mathbb{Q}$. Let Λ be a $\mathbb{Z}$-lattice on (V, b). Define the genus of Λ to be the set of lattices Γ on (V, b) such that $\Lambda_p \cong \Gamma_p$ for all p. We denote the genus of Λ by gen(Λ).

2.7.12 Lemma. Lattices in the same genus have the same discriminant.

Proof. Let Λ and Γ be two lattices on a quadratic space (V, b). Then disc(Λ_p) = disc(Γ_p) for all p. In particular, the quotient of the two discriminants must be a p-adic unit for all p and thus, must be equal to ± 1. So we have that they must have the same discriminant. Checking over $p = \infty$ shows that the two discriminant must have the same sign. □

2.7.13 Theorem. *There are only finitely many isometry classes in a genus.*

Proof. The theorem follows from Lemma 2.7.12 and the fact that for $n \geq 1$ and non-zero d, there are only finitely many isometry classes of lattices of rank n and discriminant d ([Cas08], page 128). □

Define the *class number* of a lattice Λ, $h(\Lambda)$, to be the number of isometry classes in the genus of Λ.

2.7.14 Integral Equivalence. Let (V, b) be a quadratic space over $\mathbb{Q}$ and let Λ be a lattice in (V, b). We study the isometry class of Λ over $\mathbb{Z}$.

Orthogonal group of a lattice:

Two lattices Λ and Γ are said to be isometric if for some $\sigma \in O(V)$, we have $\sigma\Lambda = \Gamma$. If $\sigma \in O^+(V)$ then they are properly isometric. Define $cls(\Lambda)$ to be the set of lattices which are isometric to Λ and $cls^+(\Lambda)$ to be the set of lattices which are properly isometric to Λ. The orthogonal transformations of Λ $O(\Lambda) = \{\sigma \in O(V) : \sigma\Lambda = \Lambda\}$ form a group. Put $O^+(\Lambda) = O(\Lambda) \cap O^+(V)$. This is the kernel of the determinant map, $\det : O(\Lambda) \to \{\pm 1\}$. Thus, $O^+(\Lambda)$ has index 1 or 2 in $O(\Lambda)$. It is 2 if there is at least a reflection $\sigma \in V$ which is contained in $O(\Lambda)$. In that case the $cls(\Lambda) = cls^+(\Lambda)$. If there is no reflection in $O(\Lambda)$, then $cls(\Lambda)$ splits into two proper isometry classes.

2.7.15 Spinor genus. The spinor genus of a lattice was introduced by Eichler. It is an intermediate classification between the genus and the integral equivalence.

2.7.16 Lemma ([O'M73]; 54:6)**.** Let (V, b) be a quadratic space over k. Let $v_1, \ldots, v_r$ be anisotropic vectors in V such that $\tau_{v_1} \ldots \tau_{v_r} = 1_V$. Then $q(v_1) \ldots q(v_r) \in (k^\times)^2$.

Spinor norm:

Let (V, b) be a quadratic space over a field k of rank n. Let $\sigma \in O(V)$. Then, by theorem 2.3.1, we can write σ as a product of symmetries:

$$\sigma = \tau_{v_1} \ldots \tau_{v_r}.$$

Since the determinant of each τ_{v_i} is -1, the determinant of σ determines the parity of r. We define the *spinor norm* of σ as

$$\theta(\sigma) := q(v_1) \ldots q(v_r).$$

This is defined only up to squares. Indeed, if $\sigma = \tau_{u_1} \ldots \tau_{u_s}$ is another expression of σ as a product of symmetries, then $\sigma\sigma^{-1} = 1_V$ gives $\tau_{v_1} \ldots \tau_{v_r} \tau_{u_1} \ldots \tau_{u_s} = 1_V$. Lemma 2.7.16 yields $q(v_1) \ldots q(v_r) \in q(u_1) \ldots q(u_s)(k^\times)^2$. Now, we have that $\theta(\sigma\tau) = \theta(\sigma)\theta(\tau)$ and so we have a well defined homomorphism of groups:

$$\theta : O(V) \to k^\times/(k^\times)^2.$$

If we restrict this to $O^+(V)$, we have

$$\theta : O^+(V) \to k^\times/(k^\times)^2.$$

The kernel of the restriction of θ is given by $\Theta(V) = \{\sigma \in O^+(V) : \theta(\sigma) = 1\}$, and is called the *spinorial kernel*. The image of $O^+(V)$ under the spinor norm map $\theta(V) = \{\theta(\sigma) : \sigma \in O^+(V)\} \subseteq k^\times/(k^\times)^2$ will be denoted by $\theta(V)$.

The spinor norm of the hyperbolic plane:

Recall that a symmetry τ of the hyperbolic plane $\mathbb{H}$ is of the form $\tau_{u-\alpha v}$.

Thus, we have $\theta(\tau) = q(u - \alpha v) = -2\alpha$. Let σ be a rotation, that is, $\sigma = \tau_{u-v}\tau_{u-\alpha v}$, then we have that $\theta(\sigma) = q(u - v)q(u - \alpha v) = \alpha \in k^\times/(k^\times)^2$.

2.7.17 Theorem. *Let (V, b) be an isotropic quadratic space over k. Then the spinor norm has image $\theta(V) = k^\times$.*

Proof. Since V is isotropic, we have that $V = \mathbb{H} \oplus \mathbb{H}^\perp$ by Theorem 2.4.2. Extend the action of $O(\mathbb{H})$ to the whole of V by the following: for each $\sigma \in O(\mathbb{H})$, $\sigma(x) = x$ for all $x \in \mathbb{H}^\perp$. □

Some results needed for later use:

2.7.18 Theorem.

1. *Let (V, b) be a quadratic space over $\mathbb{Q}_p$ of dimension $n \geq 3$. Then, $\theta(V_p) = \mathbb{Q}_p^\times$ for all p. ([O'M73], 91:6).*
2. *Let $p \neq 2$. Suppose Λ_p is a modular lattice on a quadratic space over $\mathbb{Q}_p$ and of rank ≥ 2. Then, $\theta(\Lambda_p) = \mathbb{Z}_p^\times(\mathbb{Q}_p^\times)^2$ for almost all p. ([O'M73], 92:5).*

3. *Let (V, b) be a quadratic space over $\mathbb{Q}$. Let $\dim(V) \geq 3$. Then*

$$\theta(V) = \begin{cases} \mathbb{Q}^\times & \text{if } (V,b) \text{ is indefinite} \\ \mathbb{Q}_+ & \text{if } (V,b) \text{ is definite} \end{cases}$$

where $\mathbb{Q}_+$ is the positive elements of $\mathbb{Q}^\times$, ([Cas08], lemma 3.2, page 207).

□

Let (V, b) be a quadratic space over $\mathbb{Q}$. Let Λ be a $\mathbb{Z}$-lattice in V. Let V_p and Λ_p be the quadratic space and quadratic lattice obtained by extending scalars from $\mathbb{Q}$ to $\mathbb{Q}_p$ and from $\mathbb{Z}$ to $\mathbb{Z}_p$ respectively. Equivalently, by localising with respect to rational primes. We would like to study lattices that are in the same genus. Recall that two lattices Λ_1 and Λ_2 are said to be in the same genus if for all p prime, there is exists some $\beta_p \in O^+(V)$ such that $\Lambda_2 = \beta_p(\Lambda_1)$.

2.7.19 Lemma. Let Λ and Γ be two lattices in a quadratic space (V, b) over $\mathbb{Q}$. if they are isometric, then $\theta(\Lambda) = \theta(\Gamma)$. Moreover, if they are the same genus, then $\theta(\Lambda_p) = \theta(\Gamma_p)$ for all p.

Proof. If Λ and Γ are isometric then $\Gamma = \sigma\Lambda$ and thus, $O^+(V) = \{\sigma\alpha\sigma^{-1} : \alpha \in O^+(\Lambda)\}$ and $\theta(\sigma\alpha\sigma^{-1}) = \theta(\sigma)\theta(\alpha)\theta(\sigma^{-1}) = \theta(\alpha)$. The second statement follows from the first statement, since by definition of genus, Λ_p and Γ_p are isometric. □

Spinor genus:

Define a relation $\sim_s$ on the set of lattices in a genus by: $\Lambda \sim_s \Gamma$ if there is a $\gamma \in O^+(V)$ and $\delta_p \in \Theta(V_p)$ such that $\Gamma_p = \gamma\delta_p\Lambda_p$ for all primes p.

2.7.20 Lemma ([Cas08], page 201)**.** With the definition above, we have:

1. The relation $\sim_s$ is an equivalence relation on the lattices in a genus.
2. If Γ and Λ are properly isometric, then $\Lambda \sim_s \Gamma$.
3. If $\Gamma \sim_s \Lambda$, then they are in the same genus.

Remark: From (1), we have that $\sim_s$ partitions the lattices in a genus into equivalence classes; each equivalence class is known as a *spinor genus*. Statements 2 and 3 follow from the definition of $\sim_s$ and show that the spinor genus is an intermediate classification between proper isometry and genus.

Idèle theory of spinor genus. For more details see [O'M73].

Let (V, b) be a quadratic space over $\mathbb{Q}$. Let Λ be a $\mathbb{Z}$-lattice on V and Ω be the set of all places of $\mathbb{Q}$. Let $x_1, \ldots, x_n$ be a basis of V.

We define a *norm* on V and $O^+(V)$. Let $x \in V$, then $x = a_1x_1 + \ldots + a_nx_n$. The norm of x is $\|x\|_p = \max_i|a_i|_p$. If $\sigma \in O^+(V)$, then $\sigma(x_j) = \sum_i a_{ij}x_j$ so that $\|\sigma(x_j)\|_p = \max_{i,j}|a_{ij}|_p$. Similarly, define a norm on V_p.

If ξ is an element of the direct product $\prod_{p\in\Omega} O^+(V_p)$. Then $\xi = (\xi_p)_{p\in\Omega}$ where $\xi_p \in O^+(V_p)$ and ξ_p is called the *p-coordinate* of ξ. The set

$$J_V = \{\xi \in \prod_{p\in\Omega} O^+(V_p) \ : \ \|\xi_p\|_p = 1 \text{ for almost all } p \in \Omega\}$$

is a subgroup of the direct product. It is called the *group of split rotations*. Each $\xi \in J_V$ is a split rotation of V. Note that the condition $\|\xi_p\|_p = 1$ for almost all p is equivalent to $\xi_p \in O^+(\Lambda_p)$ for almost all p. This definition is independent of the choice of basis of V.

The set

$$J'_V = \{\xi \in J_V \ : \ \xi_p \in \Theta(V) \text{ for all } p \in \Omega\}$$

is a subgroup of J_V. It contains the commutator subgroup of J_V and is a normal subgroup of J_V.

Let $\sigma \in O^+(V)$ be a rotation, and let $\sigma_p \in O^+(V_p)$ for all $p \in \Omega$ be its localisations. Let A be the matrix of σ with respect to the basis $x_1, \ldots, x_n$. Then, the entries and the determinant of A are units for almost all p. So, by the product formula, $\|\sigma_p\|_p = 1$ for almost all $p \in \Omega$. So we have a map $O^+(V) \to J_V,\ \sigma \mapsto (\sigma) = (\sigma_p)_{p\in\Omega}$.

An element $\xi \in J_V$ is called *principal* if $\xi = (\sigma)$ for some $\sigma \in O^+(V)$. These elements form a subgroup of J_V, and will be denoted by P_V. Thus, we have the following isomorphism of groups: $O^+(V) \simeq P_V$.

The *idèle group* of $\mathbb{Q}$ is given by

$$J_{\mathbb{Q}} = \{x = (x_p) \in \prod_{p\in\Omega} \mathbb{Q}_p^\times \ : \ |x_p|_p = 1 \text{ for almost all } p \in \Omega\}.$$

Let S be a set of primes in $\mathbb{Q}$. An idèle i is an *S-idèle* if $|i_p|_p = 1$ for all $p \in S$. The set of *S-idèles* form a subgroup of $J_{\mathbb{Q}}$ and will be denoted by $J_{\mathbb{Q}}^S$. The *principal idèles* of $\mathbb{Q}$ is denoted $P_{\mathbb{Q}}$ and is the idèles of the form $(\alpha)_{p\in\Omega}$ with $\alpha \in \mathbb{Q}^\times$. Thus, we have an isomorphism $\mathbb{Q}^\times \simeq P_{\mathbb{Q}}$. The image of $D = \theta(V) \subseteq \mathbb{Q}^\times$ under this isomorphism is denoted by P_D.

Let Λ be a lattice on (V, b) with respect to Ω. Define a subgroup of J_V by

$$J_\Lambda = \{\xi \in J_V \ : \ \xi_p \in O^+(\Lambda_p) \text{ for almost all } p \in \Omega\}.$$

and a subgroup of $J_{\mathbb{Q}}$ by

$$J_{\mathbb{Q}}^\Lambda = \{i \in J_{\mathbb{Q}} \ : \ i_p \in \theta(O^+(\Lambda_p) \text{ for all } p \in \Omega\}.$$

Let $\xi \in J_V$ be a split rotation and Λ a lattice on (V, b). Then, $\xi_p\Lambda_p$ is a lattice on V_p at each $p \in \Omega$. Define the lattice $\xi\Lambda$ on (V, b) by $(\xi\Lambda)_p = \xi_p\lambda_p$ for all $p \in \Omega$. This definition makes sense because $\xi_p\Lambda_p = \Lambda_p$ for almost all $p \in \Omega$. Thus, J_V acts on the lattices on (V, b). Furthermore, $(\xi\lambda)\Lambda = \xi(\lambda\Lambda)$ for all $\xi, \lambda \in J_V$. In view of the isomorphism $O^+(V) \simeq P_V$, we can describe the group J_Λ as

$$J_\Lambda = \{\xi \in J_V \ : \ \xi\Lambda = \Lambda\}.$$

The spinor genus of a lattice Λ will be denoted by $spn(\Lambda)$. Recall that a lattice Γ is in the spinor genus of Λ if there is an isometry $\sigma \in O(V)$ and a rotation $\xi_p \in \Theta(V_p)$ for each p such that $\Lambda = \sigma\xi_p\Gamma_p$.

Equivalently, if there is a $\sigma \in O(V)$ and $\xi \in J'_V$ such that $\Gamma = \sigma\xi\Lambda$. Furthermore, Γ is in the proper spinor genus of Λ if there is a $\lambda \in P_V$ and $\xi \in J'_V$ such that $\Gamma = \lambda\xi\Lambda$.

For any $\xi \in J_V$, we have $\xi spn(\Lambda) = spn(\xi\Lambda)$ and $\xi spn^+(\Lambda) = spn^+(\xi\Lambda)$. ([O'M73], 102:1).

The number of spinor genera in a genus:

Let ξ, λ be elements of J_V. Since J'_V is a normal subgroup of J_V, we have that $\xi J'_V = J'_V\xi$. Furthermore, J'_V contains the commutator subgroup of J_V, thus $\xi\lambda J'_V = \lambda\xi J'_V$. As a result, $P_V J'_V J_\Lambda$ is indepenedent of the order of P_V, J'_V and J_Λ and is the group generated by the three groups. It is a normal subgroup of J_V. Thus, we can form the quotient group $J_V/P_V J'_V J_\Lambda$.

2.7.21 Theorem ([O'M73], 102:7)**.** *The number of proper spinor genera $g^+(\Lambda)$ in the genus of Λ is given by $g^+(\Lambda) = (J_V : P_V J'_V J_\Lambda)$.* □

Now suppose $n \geq 3$, $n = \dim V$.

Let $\xi \in J_V$. Then $\xi_p\Lambda_p = \Lambda_p$ for almost all p. In other words, $\xi_p \in O^+(\Lambda_p)$ for almost all p. Thus, $\theta(\xi_p) \subseteq \mathbb{Z}_p^\times(\mathbb{Q}_p^\times)^2$ for almost all p. We have a well defined map $\Phi : J_V \to J_\mathbb{Q}/P_D J_\mathbb{Q}^\Lambda$. Indeed, for any $\xi \in J_V$ we can choose an idèle i in $J_\mathbb{Q}$ such that $i_p \in \theta(\xi_p)$ for all $p \in \Omega$. If j is another idèle satisfying the same property, then by the definition of the spinor norm, we have $j \in iJ_\mathbb{Q}^2$. Thus, $J_\mathbb{Q}^2 \subseteq J_\mathbb{Q}^\Lambda \subseteq P_D J_\mathbb{Q}^\Lambda$. This implies that i and j have the same image in $J_\mathbb{Q}/P_D J_\mathbb{Q}^\Lambda$.

The map Φ is surjective with kernel $P_V J'_V J_\Lambda$, ([O'M73], 102:9). Hence,

$$J_V/P_V J'_V J_\Lambda \cong J_\mathbb{Q}/P_D J_\mathbb{Q}^\Lambda.$$

Therefore, we have $g^+(\Lambda) = (J_V : P_V J'_V J_\Lambda) = (J_\mathbb{Q} : P_D J_\mathbb{Q}^\Lambda)$.

2.7.22 Theorem ([O'M73], 102:8a)**.** *Let Λ be a lattice in a quadratic space (V, b) over $\mathbb{Q}$. Let $\dim V \geq 1$. Then, the number of proper spinor genera $g^+(\Lambda)$ in a gen(Λ) is a power of 2.* □

2.7.23 Theorem. *Let (V, b) be a quadratic space over $\mathbb{Q}$ and let Λ be a $\mathbb{Z}$-lattice on (V, b). If the rank$(\Lambda) \geq 3$ and $\theta(\Lambda_p) \supseteq \mathbb{Z}_p^\times$ for all primes $p \in \Omega$, then $gen(\Lambda) = spn^+(\Lambda)$.*

Proof. The theorem follows from ([O'M73], 102:9):
By ([O'M73], 33:14), we can always choose a set S_0 of almost all primes of $\mathbb{Q}$ such that for any subset $S \subseteq S_0$, we have $(J_\mathbb{Q} : P_\mathbb{Q} J_\mathbb{Q}^S) = 1$. Thus $J_\mathbb{Q} = P_\mathbb{Q} J_\mathbb{Q}^S$. Now, since Theorem 2.7.18 yields that $\mathbb{Q}^\times = (\pm 1)D$ with $D = \theta(V)$, we have that $P_\mathbb{Q} = (\pm 1)P_D$. But we also have that $|-1|_p = 1$ for all p. So, $(-1) \in J_\mathbb{Q}^S$. Hence, $J_\mathbb{Q} = P_D J_\mathbb{Q}^S$. □

The following results give an efficient method for determining when the genus of a lattice contains only one spinor genus.

2.7.24 Lemma. ([Cas08], page 213) Let $p \neq 2$ and Λ_p be a $\mathbb{Z}_p$-lattice of rank 2. Suppose $\Lambda_p \sim_{\mathbb{Z}_p} \langle a_1, a_2\rangle$ with $|a_1|_p = |a_2|_p \neq 0$. Then $\mathbb{Z}_p^\times \subset \theta(\Lambda_p)$.

2.7.25 Corollary. Let $n \geq 3$ and $p \neq 2$. Suppose Λ_p is an integral lattice in V_p of discriminant D. If $\mathbb{Z}_p^\times \not\subset \theta(\Lambda_p)$, then $v_p(D) \geq \frac{n(n-1)}{2}$.

2.7.26 Lemma. ([Cas08], page 214) Let $p = 2$. Let Λ_2 be a $\mathbb{Z}_2$-lattice. If any of the following holds, then $\mathbb{Z}_2^\times \subset \theta(\Lambda_2)$:

1. The lattice Λ_2 is of rank 2 and is of the form $2^e\mathbb{H}$ or $2^e \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ with $e \geq 1$.
2. The lattice Λ has rank 3 and is of the form $\langle a_1, a_2, a_3\rangle$ with $|a_1|_2 = |a_2|_2$, and $|a_3|_2 = |a_1|_2$ or $2|a_1|_2$ or $\frac{1}{2}|a_1|_2$.
3. The lattice Λ has rank 3 and is of the form $\langle a_1, a_2, a_3\rangle$ with $|a_2|_2 = 2|a_1|_2$, and $|a_3|_2 = 4|a_1|_2$.

□

2.7.27 Theorem. *Let $n \geq 3$. Let Λ be a $\mathbb{Z}$-lattice in an n-dimensional quadratic space (V, b) over $\mathbb{Q}$. Let d be the discriminant of Λ. If Λ contains more than one spinor genus, that is $\theta(\Lambda_p) \not\supset \mathbb{Z}_p^\times(\mathbb{Q}_p^\times)^2$, Then*

For $p \neq 2$, Corollary 2.7.25 holds and for $p = 2$, the 2-adic valuation of d satisfies

1. *$v_2(d) \geq n(n-1)$ if Λ is indefinite.*
2. *$v_2(d) \geq \frac{n(n-3)}{2} + [\frac{n+1}{2}]$ if Λ is definite. Here, $[x]$ is the integer part of x.*

Proof. [EH75], Theorems 4.2 and 4.6. □

Strong approximation for rotations:

2.7.28 Theorem ([O'M73], 104:4)**.** *Let (V, b) be a quadratic space over $\mathbb{Q}$. Let S be an indefinite set of places for V and T a finite subset of S. For any $\epsilon > 0$ and any rotation $\sigma_p \in \Theta(V_p)$ for each $p \in T$, there is a rotation $\sigma \in \Theta(V)$ such that*

1. *$\|\sigma - \sigma_p\|_p < \epsilon$ for all $p \in T$, and*
2. *$\|\sigma\|_p = 1$ for all $p \in S - T$.*

The following result is due to Eichler and Kneser and is a consequence of Theorem 2.7.28:

2.7.29 Theorem ([O'M73], 104:5)**.** *Let Λ be a $\mathbb{Z}$-lattice in an indefinite quadratic space (V, b) over $\mathbb{Q}$. Then $cls^+(\Lambda) = spn^+(\Lambda)$ and $cls(\Lambda) = spn(\Lambda)$* □

3. Arithmetical Equivalence

3.1 Algebraic Number Fields

An algebraic number field K is a finite algebraic extension of $\mathbb{Q}$. Let K be an algebraic number field of degree n over $\mathbb{Q}$, then by the primitive element theorem there exists an $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$. Let f be the minimum polynomial of α over $\mathbb{Q}$. Then the roots of f: $\alpha = \alpha_1, \ldots, \alpha_n$ are the conjugates of α. Furthermore, the fields $\mathbb{Q}(\alpha_1), \ldots, \mathbb{Q}(\alpha_n)$ are the conjugate fields of $\mathbb{Q}(\alpha)$. Equivalently, two number fields, K and L are conjugates over $\mathbb{Q}$ if there exists an isomorphism $\varphi : K \to L$ such that $\varphi(a) = a$ for all $a \in \mathbb{Q}$. Conjugate fields are isomorphic.

An important invariant attached to a number field is the Dedekind zeta function:

$$\zeta_K(s) = \sum_{\{0\} \neq \mathfrak{a} \subset \mathcal{O}_K} \mathrm{N}\mathfrak{a}^{-s} = \prod_{\mathfrak{p}} (1 - \mathrm{N}\mathfrak{p}^{-s})^{-1} \quad s \in \mathbb{C}, \ \mathrm{Re}\,(s) > 1$$

where $\mathrm{N}\mathfrak{a} = \#(\mathcal{O}_K/\mathfrak{a})$ is the absolute norm of the ideal $\mathfrak{a}$ and $\mathfrak{p}$ is a prime (maximal) ideal of $\mathcal{O}_K$. Since $\zeta_K(s)$ is a field invariant, $K \cong L$ implies $\zeta_K(s) = \zeta_L(s)$. But the converse does not hold in general. Number fields for which the converse holds are called *arithmetically solitary*.

Let $p \in \mathbb{Z}$. Suppose p has exactly r primes of $\mathcal{O}_K$ dividing it and with residue degrees $f_1 \leq \ldots \leq f_r$. Then $(f_1, \ldots, f_r)$ is called the *decomposition type* of p. The Dedekind function determines and is determined by the decomposition types of all the primes in K, [Nor98].

Some representation theory; for more details see [Ser77]:

Let G be a group and V a finite dimensional $\mathbb{C}$-vector space. A linear representation of G in V is a homomorphism $\rho : G \to GL(V)$. We are only interested in the case where G is a finite group. The dimension of the vector space is the degree of the representation. A vector subspace $W \subset V$ is a subrepresentation of G if W is invariant under the action of G. A representation of G is irreducible if it has no proper subrepresentation. Every representation can be written as a direct sum of irreducible representations. The trivial representation of G is a representation of degree 1 such that $\rho(\sigma) = 1$ for all $\sigma \in G$.

Let $\rho : G \to GL(V)$ be a linear representation of G. The character of ρ is defined as $\chi_\rho : G \to \mathbb{C}$, $\chi_\rho(\sigma) = Tr(\rho(\sigma))$. Tr is the trace of the matrix obtained by making the identification $GL(V) \cong GL_n(\mathbb{C})$ with $n = \dim(V)$ and a choice of basis for V. Furthermore, $\chi(1) = n$ and χ is constant on conjugacy classes and hence a class function.

Permutation representation:

Let K be an algebraic number field and N its normal closure over $\mathbb{Q}$. Put $G = \mathrm{Gal}(N/\mathbb{Q})$ and $H = \mathrm{Gal}(N/K)$. By the primitive element theorem, we can write $K = \mathbb{Q}(\alpha)$. Let $X = \{\alpha_1, \ldots, \alpha_n\}$ the set of the conjugates of α. Now, G acts transitively on X. Put $V = \bigoplus_{i=1}^{n} \mathbb{C}e_{\alpha_i}$. Thus, we have a representation of G:

$$\rho : G \to GL(V), \ \rho(\sigma)(e_{\alpha_i}) = e_{\sigma\alpha_i} = e_{\alpha_j}$$

for all $i = 1, \ldots, n$. This is the permutation representation of G. Its character is defined by

$$\chi_\rho(\sigma) = \mathsf{trace}(\rho(\sigma)) = \sum_{i=1}^{n} \#\{\alpha_i \in X : \sigma\alpha_i = \alpha_i\}.$$

Let $\phi : H \to GL(W)$ be a linear representation of H. Let $x_1, \ldots, x_n$ be a system of representatives of $G/H =$ cosets of H. The group G acts on the cosets of H: $G \times G/H \to G/H,\ (\sigma, x_i) \mapsto \sigma x_i = x_j h$ for some $h \in H$. Put

$$V = \bigoplus_{i=1}^{n} x_i W.$$

Then, the representation ρ of G induced by the representation ϕ of H in W is given by:

$$\rho = \mathsf{Ind}_H^G : G \to GL(V),\ \sigma\left(\sum_i x_i w_i\right) = \sum_i \sigma(x_i) w_i = \sum_i x_j \phi(h) w_i.$$

If ϕ is the trivial representation 1_H of H, then $\phi(h) = 1$ for all $h \in H$ and we get back the permutation representation on G.

Regular representation:

Let G be a finite group having g elements. Let V be a $\mathbb{C}$-vector space of finite dimension g with basis (e_σ) indexed by elements of G. The regular representation of G is a homomorphism: $\rho : G \to GL(V),\ \rho_\sigma(e_\tau) = e_{\sigma\tau}$.

If $\sigma \neq 1$, then $\sigma\tau \neq \tau$ for all τ and $\mathsf{Tr}(\rho(\sigma)) = 0$. On the other hand, if $\sigma = 1$, then $\mathsf{Tr}(\rho(\sigma)) = \mathsf{Tr}(1) = \dim(V) = g$. Thus the character r_G of ρ is:

$$r_G(\sigma) = \begin{cases} g & \text{if } \sigma = 1 \\ 0 & \text{if } \sigma \neq 1 \end{cases}.$$

Moreover, the regular representation contains every irreducible representation with mulitplicity equal to its degree: $r_G = \sum_{\chi,\ \mathsf{irred}} \chi(1)\chi$. Furthermore, the regular representation of G is the induced representation $1_{\{1\}}^G$ of the trivial subgroup $\{1\}$.

Let χ be the character of a representation ϕ of H. The character ψ of the induced representation on G is given by

$$\psi(\sigma) = \frac{1}{|H|} \sum_{r \in G/H} \chi(r^{-1}\sigma r).$$

χ is 0 if its argument lies outside of H.

Now, the decomposition type of unramified primes is determined by the permutation of the cosets of H, denoted by χ_H. The Artin's L-function relates $\zeta_K(s)$ and χ_H as follows:

Let K be a number field and N be its Galois closure with $G = \mathrm{Gal}(N/K)$. Let V be a finite dimensional $\mathbb{C}$-vector space and $\rho : G \to GL(V)$ be a representation of G with character χ. Let $\mathfrak{p}$ be a prime of K and $\mathfrak{P}$ be a prime of N above $\mathfrak{p}$.

Define the *decomposition group* of $\mathfrak{P}$ in N/K:

$$D_{\mathfrak{P}} = \{\sigma \in G : \sigma\mathfrak{P} = \mathfrak{P}\} = \mathrm{Gal}(N_{\mathfrak{P}}/K_{\mathfrak{p}})$$

where $N_{\mathfrak{P}}$ and $K_{\mathfrak{P}}$ are completions of N and K at $\mathfrak{P}$ and $\mathfrak{p}$ respectively. Let $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ be the residue field extension. Hensel's lemma gives a surjection

$$D_{\mathfrak{P}} \to \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$$

with kernel $I_{\mathfrak{P}} = \{\sigma \in G : \sigma\alpha \equiv \alpha \mod \mathfrak{P} \ \forall\ \alpha \in \mathcal{O}_N\}$ the *inertia group* of $\mathfrak{P}$. Thus we have an isomorphism

$$D_{\mathfrak{P}}/I_{\mathfrak{P}} \simeq \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})),$$

and $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ is cyclic and generated by a Frobenius element $\sigma_{\mathfrak{P}}$ such that for $\alpha \in \mathcal{O}_N$, we have $\sigma_{\mathfrak{P}}(\alpha) = \alpha^{\mathsf{N}(\mathfrak{p})} \mod \mathfrak{P}$.

Since G acts transitively on the $\mathfrak{P}|\mathfrak{p}$, if $\mathfrak{P}' \neq \mathfrak{P}$ is another prime above $\mathfrak{p}$ then their corresponding decomposition group, inertia group and Frobenius elements are conjugates. Thus, the characteristic polynomials of $\sigma_{\mathfrak{P}}$ are independent of the choice of $\sigma_{\mathfrak{P}}$. Let $\sigma_{\mathfrak{p}}$ be the conjugacy class of the Frobenuis elements at all primes $\mathfrak{P}$ dividing $\mathfrak{p}$. Put $V^{I_{\mathfrak{P}}} = \{v \in V : \sigma v = v \ \forall\ \sigma \in I_{\mathfrak{P}}\}$, the subspace invariant under the action of $I_{\mathfrak{P}}$. Then, we have a representation $\rho : G_{\mathfrak{P}} \to GL(V^{I_{\mathfrak{P}}})$.

The Artin L-series attached to ρ (or to χ) is defined as

$$\mathcal{L}(N/K, \chi, s) = \prod_{\mathfrak{p}} (\det(1 - \rho(\varphi_{\mathfrak{p}})\, \mathsf{N}(\mathfrak{p})^{-s}); V^{I_{\mathfrak{P}}})^{-1}.$$

where the $\mathfrak{p}$ are the nonzero prime ideals of $\mathcal{O}_K$. If we take the trivial character $\chi = \mathbf{1}_G$, then

$$\mathcal{L}(N/K, \mathbf{1}_G, s) = \prod_{\mathfrak{p}} (\det(1 - \ \mathsf{N}(\mathfrak{p})^{-s}))^{-1} = \zeta_K(s).$$

the Dedekind zeta function of K.

Artin's conductor:

Let N/L be a finite Galois extension of algebraic number fields with Galois group $G = \mathrm{Gal}(N/L)$. Let $\mathfrak{p}$ be a prime of L and $\mathfrak{P}$ be a prime of N above $\mathfrak{p}$. Let $\rho : G \to GL(V)$ be a representation of G with character χ where V is a finite dimensional $\mathbb{C}$-vector space.

Define the ith ramification groups G_i of $\mathfrak{P}$, $G_i = \{\sigma \in G :$ for all $x \in \mathcal{O}_N,\ \sigma(x) \equiv x \bmod \mathfrak{P}^{i+1}\}$. Let g_i be the order of G_i. Put

$$n(\chi, \mathfrak{p}) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \ \mathsf{codim}\ V^{G_i}.$$

This is independent of the choice of $\mathfrak{P}$ lying above $\mathfrak{p}$. Artin proved that $n(\chi, \mathfrak{p})$ is an integer. Note that: If N/L is unramified at $\mathfrak{p}$, then $n(\chi, \mathfrak{p}) = 0$.

Define the Artin conductor by

$$\mathfrak{f}(\chi, N/L) = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\chi, \mathfrak{p})}.$$

Among the properties satisfied by the Artin conductor are the induction property and the fact that $f(\mathbf{1}) = 1$ where $\mathbf{1}$ is the trivial character. Induction property: Let H be a subgroup of G corresponding to a subfield K of N. Let χ be a character of H and χ^* be the character of G induced by χ, that is, $\chi^* = \mathsf{Ind}_H^G \chi$. Then,

$$\mathfrak{f}(\chi^*) = N_{K/L}(\mathfrak{f}(\chi)) D_{K/L}^{\chi(1)}.$$

If we let $L = \mathbb{Q}$ and let $\chi = \mathbf{1}_H$ be the trivial character of H so that $\chi^* = \mathbf{1}_G^H$ is the character of G induced by H, then we have that

$$f(\mathbf{1}_G^H, N/\mathbb{Q}) = D_{K/\mathbb{Q}}. \tag{3.1.1}$$

3.1.1 Definition. Let K and L be two field extensions over k. They are arithmetically equivalent over k if and only if the decomposition type of primes of k in K and L coincide for almost all primes of k.

Since the Dedekind zeta function determines the decomposition types of primes in K, we have the following:

Two number fields K and L are arithmetically equivalent over $\mathbb{Q}$ if and only if their Dedekind zeta function coincide for all complex numbers.

A characterisation of arithmetical equivalence:

3.1.2 Theorem. *[Per77a] Let K and L be two algebraic number fields. Let N be the galois closure of KL over $\mathbb{Q}$. Let $G = \mathrm{Gal}(N/\mathbb{Q})$ and H and H' be $\mathrm{Gal}(N/K)$ and $\mathrm{Gal}(N/L)$ respectively. Then the following are equivalent:*

1. *K and L are arithmetically equivalent.*
2. *$1_H^G = 1_{H'}^G$.*
3. *For every conjugacy class C of G, $\#(C \cap H) = \#(C \cap H')$.*

Two subgroups H and H' of a finite group G satisfying 3 are said to be *Gassmann conjugate* or *almost conjugate*.

3.1.3 Theorem. *Two number fields K and L which are arithmetically equivalent have a common normal closure.*

Proof. Let K be a number field and N its Galois closure. Let $G =$ Gal $(N/\mathbb{Q})$ and $H =$ Gal (N/K). By definition, the Galois closure is the smallest Galois extension of $\mathbb{Q}$ containing K. By Galois theory, it corresponds to the largest normal subgroup contained in H. But this is the kernel of the permutation representation $\rho_H : G \times G/H \to G/H$ and this kernel is determined by its character: $\ker \rho_H = ker 1_H^G = \{\sigma \in G : 1_H^G(\sigma) = 1_H^G(e)\}$ where e is the identity element of G. Since L is arithmetically equivalent to K, the result follows from Theorem 3.1.2.

□

3.2 Trace forms

Let K be an algebraic number field with degree $[K : \mathbb{Q}] = n$. The trace form on K is the quadratic form $tr_K : K \to \mathbb{Q}, \quad x \mapsto \mathrm{trace}_{K/\mathbb{Q}}(x^2)$, with corresponding symmetric bilinear form $b_K(x, y) \mapsto \mathrm{trace}_{K/\mathbb{Q}}(xy)$. Thus (K, tr_K) is a quadratic space over $\mathbb{Q}$.

By the primitive element theorem, $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$ where f is the minimum polynomial of α over $\mathbb{Q}$. Thus $K = \oplus K_i$ where $K_i = \mathbb{Q}[x]/(f_i)$ and $\sum_i [K_i : \mathbb{Q}] = n$. Now, $tr_K = \oplus tr_{K_i}$ with $tr_{K_i}(x) = \text{trace}_{K_i/\mathbb{Q}}(x^2)$.

On choosing a basis $\{v_1, \ldots, v_n\}$ for K we obtain a matrix of tr_K with respect to this basis: $M = \text{trace}_{K/\mathbb{Q}}(v_i v_j)$.

The trace form tr_K is nondegenerate:

Let $\{v_1, \ldots, v_n\}$ be a basis of K and M a matrix of tr_K with respect to this basis, then

$$\det(M) = \det(\text{trace}_{K/\mathbb{Q}}(v_i v_j)) \neq 0.$$

Equivalently, Suppose it is degenerate, then there is a nonzero $\alpha \in K$ such that for all $\beta \in K$, $\text{trace}_{K/\mathbb{Q}}(\alpha\beta) = 0$. So, for $\beta = \alpha^{-1}$, we have

$$0 = \text{trace}_{K/\mathbb{Q}}(\alpha\alpha^{-1}) = \text{trace}_{K/\mathbb{Q}}(1) = [K : \mathbb{Q}] = n.$$

contradicting the characteristic of K.

The rational invariants of the trace form are:

1. $\text{rank}(tr_K) = \dim_{\mathbb{Q}}(K) = \deg f$.
2. $\text{disc}(tr_K) = \text{disc } K \text{ in } \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$
3. $\text{sign}(tr_K) = (r_1, r_2)$ where r_1 is the number of real embeddings of K and r_2 is the number of pairs of complex embeddings.
4. Hasse-Witt invariants

Integral trace form.

Let K be a number field of degree n over $\mathbb{Q}$. An additive subgroup A of K is a $\mathbb{Z}$-lattice in K if there is a $\mathbb{Q}$-basis $\alpha_1, \ldots, \alpha_n$ of K such that $A = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$. Examples $\mathcal{O}_K$, fractional fields, orders.

An algebraic number field K is a finite dimensional $\mathbb{Q}$-vector space. Its ring of integers $\mathcal{O}_K$ is a $\mathbb{Z}$-lattice of rank n, where $n = [K : \mathbb{Q}]$. The dual of $\mathcal{O}_K$ is given by $\mathcal{O}_K^\vee = \{x \in \mathcal{O}_K : tr_{K/\mathbb{Q}}(x\mathcal{O}_K) \subset \mathbb{Z}\}$. The trace $tr_{K/\mathbb{Q}}(\mathcal{O}_K) \subset \mathbb{Z}$ and thus $\mathcal{O}_K \subset \mathcal{O}_K^\vee$. Now $\mathcal{O}_K^\vee$ is strictly larger than $\mathcal{O}_K$ if and only if the discriminant of K is larger than 1. But for all $K \neq \mathbb{Q}$, we have that $\text{disc}(K) > 1$. Thus, if $K \neq \mathbb{Q}$ then $\mathcal{O}_K \neq \mathcal{O}_K^\vee$ and hence, $\mathcal{O}_K$ cannot be unimodular.

The integral trace form is the quadratic form $tr_K : \mathcal{O}_K \to \mathbb{Z}$ obtained by restricting the quadratic form defined above to the ring of integers $\mathcal{O}_K$.

3.3 Classification of Trace forms

3.3.1 Rational equivalence. Perlis in his paper [Per85] proved that arithmetical equivalence determines the rational isometric class of the trace form of a number field. We will follow closely the account given in [Nor98].

3.3.2 Theorem. *Let K and L be two algebraic number fields. If their Dedekind zeta function coincide then they have rationally equivalent trace forms.*

Proof. Let K and L be two number fields with common Galois closure N. Put $G = \mathrm{Gal}(N/\mathbb{Q})$ and let $H = \mathrm{Gal}(N/K)$ and $H' = \mathrm{Gal}(N/L)$ be subgroups of G. Let q_K and q_L be the corresponding trace forms over K and L respectively. By Hasse-Minkowski theorem, the two trace forms are rationally equivalent if and only if they have the same rank, discriminant, signature and Hasse invariants.

Now, since K and L are arithmetically equivalent, we have that $1_H^G = 1_{H'}^G$. From this we can deduce the following:

The ranks coincide since $\mathrm{rk}\,(q_K) = \dim_{\mathbb{Q}}(K) = [K:\mathbb{Q}] = (G:H) = 1_H^G(1)$.

From the conductordiscriminant formula in equation (3.1.1), we see that the discriminant of a number field is determined by the character $\mathbf{1}_G^H$. Thus, we have that $D_{K/\mathbb{Q}} = D_{L/\mathbb{Q}}$. Hence, $d_K = d_L$.

Signature: Let σ be the inclusion $\mathbb{Q} \subset \mathbb{R}$ and embed N into $\mathbb{C}$. The complex conjugation $\iota : \mathbb{C} \to \mathbb{C}$ induces an automorphism $c : N \to \mathbb{C},\ c = \sigma^{-1}\iota\sigma$. Now, $c \in \mathrm{Gal}(N/\mathbb{Q})$ since it fixes $\mathbb{Q}$. Thus, we can compute $1_H^G(c)$.

Let $\rho_i,\ i = 1, \ldots, n$ be a complete list of representatives for the cosets of H. That is, $\rho_i \in G$ and $\rho_i H \neq \rho_j H$ if $i \neq j$ and $G = \cup \rho_i H$. Now, restricting the ρ_i to K gives the n distinct embeddings $K \to \mathbb{C}$ which fix $\mathbb{Q}$ and $\sigma\rho$ are the n distinct embeddings $K \to \mathbb{C}$ extending σ. Thus we have:

$$\begin{aligned}
1_H^G(c) &= \#\{i : c\rho_i H = \rho_i H\} \\
&= \#\{i : \rho_i^{-1} c \rho_i \in H\} \\
&= \#\{i : \rho_i^{-1}\sigma^{-1}\iota\sigma\rho_i|_K = id_K\} \\
&= \#\{i : \iota\sigma\rho_i|_K = \sigma\rho_i|_K\} \\
&= \#\{i : \sigma\rho_i(K) \subset \mathbb{R}\} \\
&= \#\{\tau : K \to \mathbb{C} \text{ such that } \tau|_{\mathbb{Q}} = \sigma;\ \tau(K) \subset \mathbb{R}\} \\
&= r_\sigma(K/\mathbb{Q}).
\end{aligned}$$

Thus, the signature of K is also determined by $\mathbf{1}_G^H$.

In [Ser84], Serre expresses the Hasse invariant of trace forms in terms of cohomology classes which are defined by the discriminant and classes which can be viewed as the obstruction to a certain "embedding problem". Perlis, in [Per77a], uses this result to show that for arithmetically equivalent number fields, the Hasse invariants coincide at all primes.

□

3.3.3 Genus. In [EMP87], the authors proved that arithmetical equivalence determines the genus of the integral trace form of a *tamely* ramified number field. We shall discuss this in this section following [EMP87].

Let K be a number field and $\mathcal{O}_K$ its ring of integers. Let p be a prime number. Then p splits in $\mathcal{O}_K$ as $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$, where $e_i = e_i(\mathfrak{p}|p)$ is the ramification indices. Also, let $f_i = f_i(\mathfrak{p}_i|p) = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p]$ be the residue degrees. The extension $K/\mathbb{Q}$ is said to be tamely ramified if and only if p does not divide the residue degrees e_i for all primes $p \in \mathbb{Z}$. If D_K is the absolute discriminant of K then $\text{ord}_p(D_K) = \sum_{i=1}^{g} f_i(e_i - 1) = n - s$ where $n = \sum_i e_i f_i$ and $s = \sum_i f_i$.

3.3.4 Theorem ([EMP87])**.** *Let K be a tamely ramified algebraic number field. Let $p \in \mathbb{Z}$ be a prime number and $\mathfrak{p}$ be a prime of K above p. Denote by $K_\mathfrak{p}$ the localisation and completion of K at $\mathfrak{p}$. Let tr_K be the integral trace form over $\mathcal{O}_K$. Then tr_K has the following Jordan canonical decomposition:*

$$tr_K \sim_{\mathbb{Z}_p} U \oplus \langle p \rangle V$$

where $U \sim_{\mathbb{Z}_p} \langle e_1 \rangle tr_{F_1} \oplus \dots \oplus \langle e_g \rangle tr_{F_g}$; F_i is the maximal unramified subextension of $K_{\mathfrak{p}_i}/\mathbb{Q}$ and tr_{F_i} is the trace form over the ring of integers of F_i; U is $\mathbb{Z}_p$-unimodular with discriminant $\left(\prod_i e_i^{f_i}\right) \varepsilon^{s-g} \in \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$; ε is a non-square unit of $\mathbb{Z}_p$ for p odd prime and $\varepsilon = 5$ for $p = 2$. Furthermore, V is $\mathbb{Z}_p$-unimodular of rank $n - s$ and if $p = 2$ then V is even.

Proof. Let K be a tamely ramified number field with ring of integers $\mathcal{O}_K$. Let p be a prime of $\mathbb{Z}$ and $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ be the primes of $\mathcal{O}_K$ above p. For each extension $K_{\mathfrak{p}_i}/\mathbb{Q}_p$, let $F_i/\mathbb{Q}_p$ be the maximal unramified subextension. We have that $K \otimes_\mathbb{Q} \mathbb{Q}_p \cong \oplus_{i=1}^{g} K_{\mathfrak{p}_i}$ and $tr_{K/\mathbb{Q}} = \oplus_{i=1}^{g} tr_{K_{\mathfrak{p}_i}/\mathbb{Q}_p}$ ([Jan96] pages 114-115). Thus, we can reduce the proof of the theorem to the local case: $K_{\mathfrak{p}_i} \supseteq F_i \supseteq \mathbb{Q}_p$ where $[K_\mathfrak{p} : F_i] = e_i$ and $[F_i : \mathbb{Q}_p] = f_i$.

Fix a prime p and $\mathfrak{p} = \mathfrak{p}_i$ dividing p. Put $F = F_i$ the maximal unramified subextension in $K_\mathfrak{p}/\mathbb{Q}_p$: $K_\mathfrak{p} \supseteq F \supseteq \mathbb{Q}_p$.

By Scharlau transfer ([Lam05], page 187 and [Sch85], page 47) we have,

$$tr_{K_{\mathfrak{p}/\mathbb{Q}_p}} = tr_{F/\mathbb{Q}_p} \circ tr_{K_{\mathfrak{p}/F}}.$$

Thus, we can do the proof in two parts:

Part 1: Description of $tr_{K_\mathfrak{p}}$ over the totally ramified extension $K_{\mathfrak{p}/F}$. Still keeping the notation as above, we have the following lemma:

3.3.5 Lemma. Over $\mathcal{O}_F$, we have the decomposition

$$tr_{K_{\mathfrak{p}/F}} \sim_{\mathcal{O}_F} \langle e \rangle \oplus \langle p \rangle V$$

where V is unimodular. Furthermore, if $p = 2$ then V is even.

Proof. Since we are working in a tamely ramified extension, $p \not| e$ and so e is a unit. Now $tr_{K_{\mathfrak{p}/F}}(1 \cdot 1) = e$. Thus $\langle e \rangle$ is unimodular and we have an orthogonal sum

$$tr_{K_{\mathfrak{p}/F}} \sim_{\mathcal{O}_F} \langle e \rangle \oplus V"$$

where $V" = \ker(tr_{K_\mathfrak{p}/F}) \cap \mathcal{O}_{K_\mathfrak{p}}$.

Now, since $K_\mathfrak{p}/F$ is a totally and tamely ramified extension, we have that $\mathcal{O}_{K_\mathfrak{p}} = \mathcal{O}_F(\pi)$ where π is a uniformiser and a root of a polynomial of the form $X^e - p$. Thus $\{1, \pi, \pi^2, \ldots, \pi^{e-1}\}$ is a basis of $\mathcal{O}_{K_\mathfrak{p}}$. From ([CP84], page 139), we have that

$$tr_{K_\mathfrak{p}/F}(\pi^j) = 0 \text{ for } 1 \leq j \leq e-1. \tag{3.3.1}$$

This yields that $\{\pi, \pi^2, \ldots, \pi^{e-1}\}$ is a basis for $V"$. From (3.3.1), we have

$$tr_{K_\mathfrak{p}/F}(\pi^i\pi^j) = \begin{cases} 0 & i+j \neq e \\ pe & i+j = e \end{cases} \text{ for } 1 \leq i,j \leq e-1.$$

Hence, with respect to the basis $\{\pi, \pi^2, \ldots, \pi^{e-1}\}$, $tr_{K_\mathfrak{p}/F}$ has the diagonal form $\langle e, 0, \ldots, 0\rangle$ mod p. Therefore, $V" \equiv 0$ mod p which means that $V" = \langle p\rangle V$ for some quadratic form V. Calculating the discriminant yields that V is unimodular.

Now, let $p = 2$. We show that V is even. That is, for all $\alpha \in ker(tr_{K_\mathfrak{p}/F}) \cap \mathcal{O}_{K_\mathfrak{p}}$, $V(\alpha) \equiv 0$ mod 2. Let N be a normal closure of $K_\mathfrak{p}/F$ with a uniformiser π'. Let $\alpha = \alpha_1, \ldots, \alpha_e$ be the conjugates of α in N. For $\alpha \in \mathcal{O}_{K_\mathfrak{p}}$, write $\alpha = \sum a_j\pi^j$ $j = 0, \ldots, e-1$. Then, since $tr_{K_\mathfrak{p}/F}(\pi^j) = 0$ for $j \neq 0$, $tr_{K_\mathfrak{p}/F}(\alpha) = 0$ yields that $a_0 = 0$. That is $\alpha \equiv 0 \mod \pi'$. Thus $\alpha_i \equiv 0 \mod \pi'$ for each $i = 1, \ldots, e$. Now, using

$$\begin{aligned} tr_{K_\mathfrak{p}/F}(\alpha) &= \alpha_1 + \ldots + \alpha_e \\ tr_{K_\mathfrak{p}/F}(\alpha^2) &= \alpha_1^2 + \ldots + \alpha_e^2 \\ (tr_{K_\mathfrak{p}/F}(\alpha))^2 &= \alpha_1^2 + \ldots + \alpha_e^2 + 2\sum_{i<j} \alpha_i\alpha_j \end{aligned}$$

and the fact that $\alpha_i \equiv 0 \mod \pi'$ for each $i = 1, \ldots, e$, we obtain the result. □

Part 2: Description of tr_F over the maximal unramified extension $F/\mathbb{Q}_p$. For this we need a theorem:

3.3.6 Theorem ([CP84]). *Let F be a Galois extension of L. Then the discriminant of F/L is a square in $L^\times$ if and only if $\mathrm{Gal}(F/L)$ has a trivial or noncyclic sylow 2 subgroup.*

3.3.7 Lemma. Over $\mathbb{Q}_p$, we have $tr_F \sim_{\mathbb{Q}_p} \langle 1, \ldots, 1, 2, 2\varepsilon^{f-1}\rangle$, where for $p \neq 2$, ε generates $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$ and for $p = 2$, $\varepsilon = 5$.

Proof. To prove this isometry we only need to calculate the discriminants and Hasse-Witt invariants. From Theorem 3.3.6 it follows that the discriminant D_F of tr_F modulo squares is given by

$$D_F = \begin{cases} \varepsilon^{f-1} & \text{if } p \neq 2 \\ 5^{f-1} & \text{if } p = 2. \end{cases}$$

If we let $\mathrm{Gal}(F/\mathbb{Q}_p) = \{\sigma_1, \ldots, \sigma_f\}$ and $\{x_1, \ldots, x_f\}$ a $\mathbb{Q}_p$-basis for F. Then, since $F/\mathbb{Q}_p$ is Galois, it contains the square root of the discriminant; $\sqrt{D_F} = \det(\sigma_i(x_j))$. Thus, either $\sqrt{D_F} \in \mathbb{Q}_p$ that is, D_F is a square or $\mathbb{Q}_p(\sqrt{D_F})$ is the unique unramified quadratic extension of $\mathbb{Q}_p$. The unique unramified quadratic extension of $\mathbb{Q}_p$ is given by $\mathbb{Q}_p(\sqrt{D_F}) = \mathbb{Q}_p(\sqrt{\varepsilon})$, where ε is a quadratic non-residue mod p

for $p \neq 2$ and $\varepsilon = 5$ for $p = 2$. Thus, the discriminant is as given and ε^{f-1} is a square or not according as $f = [F : \mathbb{Q}_p]$ is odd or even.

We calculate the Hasse invariants: $h_p(tr_F)$: For $p \neq 2$, we have that p does not divide $2D_F$. Thus, $h_p(tr_F) = 1$. For $p = 2$, we have that $h_2(tr_F) = (2, D_F)_2$. The lemma follows since $(2, 2)_2 = 1$. □

The theorem can be deduced from Lemmas 3.3.5 and 3.3.7 by the elementary properties of the transfer. □

The following lemma makes theorem 3.3.4 precise for $p = 2$.

3.3.8 Lemma. We have the following isometry over $\mathbb{Z}_2$

$$tr_K \sim_{\mathbb{Z}_2} U \oplus 2(\mathbb{H} \oplus \ldots \oplus \mathbb{H})$$

where U is odd and $\mathbb{H}$ is a hyperbolic plane.

Proof. By theorem 3.3.4, $tr_K \sim_{\mathbb{Z}_2} U \oplus \langle 2 \rangle V$ and V is even. Now, if U were even, then reducing mod 2 would yield a degenerate trace form over the residue class field and by ([Mau73], page 381) would contradict the fact that $K/\mathbb{Q}$ is tamely ramified. Thus U is odd.

Since V is even, we have by theorem 2.7.8 that it is an orthogonal sum of binary forms isometric to the hyperbolic plane or to $S = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Theorem 2.7.9 gives that it is isometric to either $\mathbb{H} \oplus \ldots \oplus \mathbb{H}$ or $\mathbb{H} \oplus \ldots \oplus \mathbb{H} \oplus S$. If it of the first type then we are done. Suppose it is of the second type. The norm from the unramified field $\mathbb{Q}_2(\sqrt{-3})$ is surjective on the units and is equal to $y^2 + yz + z^2$. Thus $ux^2 + 2(2y^2 + 2yz + 2z^2)$ represents $5u$ with $x = 1$. So we have, $\langle u \rangle \oplus 2S \sim_{\mathbb{Z}_2} \langle 5u \rangle \oplus 2M$ for some binary lattice M. Indeed, they have the same rank and comparing discriminant gives $\text{disc}(2M) = -1$. so that $M = \mathbb{H}$. Isometry follows from Corollary 2.7.10. □

3.3.9 Theorem. *Let $K/\mathbb{Q}$ be a tamely ramified extension with integral trace form tr_K. Then the discriminant and the rational class of tr_K determines its genus.*

Proof. Let K and L be two tamely ramified number fields with integral trace forms tr_K and tr_L respectively. Suppose tr_K and tr_L are in the same genus then by ([Wat60], theorem 50, page 78), they are rationally equivalent.

On the other hand suppose that tr_K and tr_L are rationally equivalent and have the same discriminant over $\mathbb{Z}$. By theorem 3.3.4 we have that $tr_K \sim U \oplus \langle p \rangle V$ and $tr_L \sim U' \oplus \langle p \rangle V'$. Thus we only need to show that $U \sim U'$ and $V \sim V'$.

Since the rank and discriminant of K and L over $\mathbb{Q}$ are equal, we have that $s = \text{rank} U = \text{rank } U' = s'$.

For $p = 2$:

By hypothesis, tr_K and $tr_{K'}$ are isometric over $\mathbb{Q}_2$. Since K and K' are both tamely ramified, Lemma 1 of [Mau73] yields that the two forms are primitive and so have scale $\mathbb{Z}_2$. Thus, we have the following decomposition from Lemma 3.3.8: $tr_K \sim_{\mathbb{Z}_2} U \oplus 2(\mathbb{H} \oplus \ldots \oplus \mathbb{H})$ and $tr_{K'} \sim_{\mathbb{Z}_2} U' \oplus 2(\mathbb{H} \oplus \ldots \oplus \mathbb{H})$. Since U and U' have the same rank and discriminant, the hyperbolic parts of tr_K and $tr_{K'}$ are isometric.

So we just have to show that U and U' are isometric over $\mathbb{Z}_2$. Now, U and U' are unimodular and so by ([O'M73], 93:16), we only need to show that $\mathfrak{g}(U) = \mathfrak{g}(U')$. We have $\mathfrak{g}(U) = n(U) = \mathbb{Z}_2$ since U is odd. Similarly for $\mathfrak{g}(U')$. Thus, the result is proved. Hence, the rank and discriminant completely determines the isometry class of tr_K over $\mathbb{Z}_2$.

For $p \neq 2$:

We have by hypothesis that tr_K and tr_L are rationally isometric. Thus, they are isometric over $\mathbb{Q}_p$. The residue class map $\mathbb{Z}_p \to \mathbb{F}_p,\ u \mapsto \bar{u}$ yields an isomorphism $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \cong \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$. Recall that $\langle u \rangle = ux^2$. For $a \in \mathbb{Q}_p$, we have $a = p^i u$, where $i \in \mathbb{Z}$ and $u \in \mathbb{Z}_p$. Thus, we can define a residue class homomorphism,

$$\langle a \rangle \mapsto \begin{cases} 0 & \text{if } i \text{ is odd} \\ \langle \bar{u} \rangle & \text{if } i \text{ is even} \end{cases}.$$

So, we reduce mod p and check that U and U' are isometric over $\mathbb{Z}_p$. But we already have that they have the same rank and discriminant; these two invariants determine the isometry class of a form over $\mathbb{F}_p$. Thus tr_K and tr_L are isometric over $\mathbb{F}_p$. Hence, they are isometric over $\mathbb{Z}_p$. □

From theorem 3.3.2 and theorem 3.3.9 we can deduce the following corollary:

3.3.10 Corollary. Let $K/\mathbb{Q}$ be a tamely ramified extension. Then the genus of tr_K is determined by the Dedekind zeta function of tr_K. □

3.3.11 Integral equivalence. In ([Per77a], page 355), the author showed that if K and L are two arithmetically equivalent number fields whose respective degrees over $\mathbb{Q}$ are less than 7, then K and L are conjugated. Thus, we need only consider number fields of degree ≥ 7. The following theorem shows that under arithmetical equivalence, the integral trace form does not characterise a number field.

3.3.12 Theorem ([MS12]). *Let K and L be two number fields defined by $p_K = x^7 - 3x^6 + 4x^4 + x^3 - 4x^2 - x + 1$ and $p_L = x^7 - 3x^6 + 2x^5 + 4x^4 - 3x^3 - 2x^2 - x - 1$ respectively. Then their integral trace forms are isometric.*

Proof. The number fields K and L have a common discriminant $(2741)^2$ and we have the following factorisation of the prime 2741 in the respective ring of integers:

- $2741\mathcal{O}_K = P_1P_2P_3P_4^2$
- $2741\mathcal{O}_L = Q_1Q_2^2Q_3^2Q_4$

where the residue degree of P_4 and Q_4 is 2 and for the others it is 1. Thus, K and L are not conjugate fields.

Two number fields are said to be linearly disjoint if and only if $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$. But we have $[KL : \mathbb{Q}] \leq 28$, and so K and L are not linearly disjoint. Thus, it follows from [Per77b] that K and L are arithmetically equivalent.

Furthermore, K and L have the same signature $(3, 2)$ and the same discriminant and so they satisfy the hypothesis of Theorem 4.1.1. Hence, they have equivalent integral trace forms.

□

3.3.13 Spinor genus. The genus of a lattice is partitioned into (proper) spinor genera. For indefinite lattices, the theorem of Eichler-Kneser yields that the (proper) spinor genus and the (proper) class coincide. So the question is then, "what happens for definite lattices?"

3.3.14 Theorem ([MS13]). *Let K be a tamely ramified number field of degree $n \geq 3$ over $\mathbb{Q}$. Then the genus of the integral trace form q_K contains only one proper spinor genus.*

Proof. Let K be a tamely ramified number field of degree $n \geq 3$ and $\mathcal{O}_K$ be its ring of integers. Let q_K be the integral trace form obtained by restricting $tr_{K/\mathbb{Q}}$ to $\mathcal{O}_K$. Thus, $\mathcal{O}_K$ is an integral $\mathbb{Z}$-lattice in the quadratic space $(K, tr_{K/\mathbb{Q}})$. Put $\Lambda = \mathcal{O}_K$. We need to show that $spn^+(\Lambda) = gen(\Lambda)$. By Theorem 2.7.23, it suffices to show that $\theta_p(\Lambda_p) \supseteq \mathbb{Z}_p^\times \mod (\mathbb{Q}_p^\times)^2$ for all p.

Let $p \neq 2$, be a prime number. From Theorem 3.3.4 , we have the following Jordan decomposition $\Lambda_p \sim_{\mathbb{Z}_p} U \oplus \langle p \rangle V$ where U and V are $\mathbb{Z}_p$-unimodular. By the classification of unimodular lattices in Theorem 2.7.4, we have the isometry, $\Lambda_p \sim_{\mathbb{Z}_p} \langle 1, \ldots, 1, \alpha \rangle \oplus \langle p, \ldots, p, p\beta \rangle$ for some $\alpha, \beta \in \mathbb{Z}_p^\times$. Now, since the rank of $\Lambda_p \geq 3$, we have that either one of the components of the decomposition has rank ≥ 2. Thus, Λ_p has an orthogonal summand Γ_p of rank 2 of the form $\langle 1, \alpha \rangle$ or $\langle p, p\beta \rangle$.

Let $p = 2$. From Lemma 3.3.8, we have $\Lambda_2 \sim_{\mathbb{Z}_2} U \oplus 2(\mathbb{H} \oplus \ldots \oplus \mathbb{H})$ where U is $\mathbb{Z}_p$-unimodular and odd. Since U is odd, by Theorem 2.7.8, $U \cong_{\mathbb{Z}_2} \langle \alpha_1, \ldots, \alpha_m \rangle$ with $\alpha_i \in \mathbb{Z}_2^\times$. Thus, Λ_2 contains an orthogonal summand Γ_2 of the form $2\mathbb{H}$ or $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$.

Thus, by Lemmas 2.7.24 and 2.7.26, it follows that $\theta(\Lambda_p) \supset \theta(\Gamma_p) \supset \mathbb{Z}_p^\times (\mathbb{Q}_p^\times)^2$.

□

3.3.15 Corollary. Let $K/\mathbb{Q}$ be a tamely ramified extension. From Corollary 3.3.10 and Theorem 3.3.14, we have that the spinor genus of the integral trace form of K is determined by the Dedekind zeta function. □

4. Totally or Non-totally Real Number Fields

In the classification of quadratic forms over $\mathbb{Z}$, the problem is broken down into two by considering the definite and indefinite cases.

Let K be a number field. K is totally real if for each embedding $\tau : K \to \mathbb{C}$, $\tau(K) \subset \mathbb{R}$. Equivalently, if $K = \mathbb{Q}(\alpha)$ and the minimum polynomial of α over $\mathbb{Q}$ has only real roots. If K cannot be embedded into $\mathbb{R}$ then K is totally imaginary.

Recall that the definiteness of a quadratic form of rank n is determined by considering it as a quadratic space over $\mathbb{R}$. We first diagonalise it to get $q \cong \langle 1, \ldots, 1, -1, \ldots, -1\rangle$ where r is the number of $+1$ and s is the number of -1. Hence, it has signature (r, s). Now, if $r = n$ (or $s = n$) then the quadratic form is positive (negative) definite and if $0 < r < n$ then it is indefinite.

Now, Taussky's theorem ([Tau68]) states that the signature of the trace form of a number field K is the number of real places r of K. Thus, the trace form is positive (negative) definite if K is totally real (totally imaginary) and indefinite if K is non-totally real.

4.1 Indefinite integral trace forms

These are the integral trace forms of non-totally real number fields. In [MS12], the author showed that the integral trace form does not characterise number fields in this case.

4.1.1 Theorem ([MS12]). *Let K and L be two non-totally real number fields with the same discriminant, signature and degree. Furthermore, suppose there is only one prime p which ramifies on K and that p is tamely ramified. Then the integral trace forms of K and L are isometric.*

Proof. We may assume that $[K : \mathbb{Q}] > 2$.

Let tr_K and tr_L be the respective trace forms of K and L over $\mathbb{Q}$. We first show that they are rationally isometric. By hypothesis, we need only show that the share the same Hasse invariants h_ℓ:

- $\ell = \infty$: Let (r_K, s_K) be the signature of tr_K. By Tauskky Todd's theorem, tr_K is isometric over $\mathbb{R}$ to the orthogonal sum $(r_K + s_K)\langle 1\rangle \oplus s_K\langle -1\rangle$. The signature determines the Hasse invariant over $\mathbb{R}$ and by hypothesis, K and L have equal signature. Consequently, $h_\ell(tr_K) = h_\ell(tr_L)$.
- $\ell = 2$: Since K and L are tamely ramified, the degree and discriminant determine their trace forms over $\mathbb{Z}_2$. Thus, their trace forms are isometric over $\mathbb{Z}_2$. Hence, $h_2(tr_K) = h_2(tr_L)$.
- $\ell \neq p, 2$: Since ℓ does not divide p nor 2. It follows that ℓ does not divide $2d$ where d is the common discriminant. Thus, $h_\ell(tr_K) = 1 = h_\ell(tr_L)$.
- $\ell = p$: Since $h_\ell(tr_K) = h_\ell(tr_L)$ for all prime $\ell \neq p$, Theorem 2.6.8 yields that $h_p(tr_K) = h_p(tr_L)$

Since K and L are tamely ramified, and since tr_K and tr_L are rationally isometric and have the same discriminant, Theorem 3.3.9 yields that they are in the same genus.

Next we show that they are in the same spinor genus: Let $d = p^m$ be the common discriminant of F and L. Since F is tamely ramified, $\text{ord}_p(d) = n - t$ where $n = [F : \mathbb{Q}]$ and t is the sum of residue degrees at p. Therefore, $m < n$. So, we have that the discriminant d is not divisible by the $(\frac{n(n-1)}{2})$th power of p for any $n > 2$. Thus by Theorem 2.7.27 of chapter 2, the spinor genus and genus of tr_K coincide. Hence, tr_F and tr_L are in the same spinor genus.

Since $n \geq 3$ and since tr_F and tr_L are indefinite, Theorem 2.7.29 yields that they are integrally isometric. □

4.1.2 Corollary ([MS12]). Let K and L be two non-totally real number fields having the same signature. Suppose also that they have a common discriminant which is a power of a prime. Then their corresponding integral trace forms are isometric. □

4.2 Positive definite integral trace forms

These are the integral trace forms of totally real number fields. In the last section, we saw that the integral trace forms do not characterise non-totally real number fields. Thus, we would like to know if they characterise totally real number fields. General positive definite n-ary quadratic forms have only been classified for rank $n \leq 24$. So essentially, it is still an open question. The theorem that follows gives a partial solution to the problem for $n < 11$ and for a given bounded discriminant.

The trace zero module is given by $\mathcal{O}_K^\circ := \{x \in \mathcal{O}_K : tr_{K/\mathbb{Q}}(x) = 0\}$.

4.2.1 Theorem ([MS12]). *Let $n < 11$ be a positive integer. Let X_n be given by ∞ for $n = 1, 2, 3$; 1×10^9 for $n = 4, 5, 6$; and 8.9×10^{10}, 2.5×10^9, 2.8×10^{10}, 2.8×10^{11} for $n = 7, 8, 9, 10$ respectively. Let K be a totally real number field of degree n over $\mathbb{Q}$ having fundamental discriminant bounded by X_n. Suppose L is a tamely ramified number field such that there is an isomorphism of quadratic modules*

$$\langle \mathcal{O}_K^\circ, tr_{K/\mathbb{Q}}(x^2)|_{\mathcal{O}_K^\circ} \rangle \cong \langle \mathcal{O}_L^\circ, tr_{L/\mathbb{Q}}(x^2)|_{\mathcal{O}_L^\circ} \rangle.$$

Then $K \cong L$.

5. Conclusion

Classification of number fields into isometry classes renders an enumeration of number fields. Number fields are usually counted by ordering them with respect to their discriminant. The discriminant is an invariant of the isometry class of the trace form. Hence, we would like to know whether the trace form characterises number fields.

In this thesis, we studied the answer to the question," Do Trace Forms Characterise Number Fields?" In chapter 3, we saw that the Dedekind zeta function determines the rational equivalence of a number field. It also determines the genus and the spinor genus of a tamely ramified number field. But even under arithmetical equivalence, the integral trace form does not characterise its number field.

In chapter 4, we saw that for non-totally real number fields, the integral trace form does not characterise its number field. The question is still open for totally real number fields. In [MS12], the author gives a partial solution with restrictions on the rank and discriminant.

We have not considered the genus and spinor genus of the trace form of a wildly ramified number field. In [MS13], which appeared in arxiv last month, the author showed that the genus of the trace form of a wildly ramified number field contains only one proper spinor genus.

Appendix A. Integral lattices

Classification of $\mathbb{Z}$-lattices on a quadratic space (V, b) over $\mathbb{Q}$:

Let (V, b) be a quadratic space over $\mathbb{Q}$. Let Λ be a unimodular $\mathbb{Z}$-lattice. The lattice Λ is said to be positive definite if $b(x, x) > 0$ for all nonzero $x \in \Lambda$. It is negative definite if $b(x, x) < 0$ for all nonzero $x \in \Lambda$. It is definite if it is either positive or negative definite and indefinite if it is not definite.

The invariants of a unimodular lattice Λ are:

Its **rank** denoted by n; it is the dimension of the vector space V.

The **signature** (r, s) obtained by considering Λ as a quadratic form over $\mathbb{R}$ (localising or extending scalars). Define the index τ to be $r - s$. Note that the signature can always be recovered from the rank and the index, since $r + s = n$.

The **discriminant** d of Λ does not depend on the choice of basis and is equal to ± 1. If Λ has signature (r, s) then the sign of the discriminant is $(-1)^s$.

Type: Let Λ be a unimodular $\mathbb{Z}$-lattice. Then, Λ is of type II if it is even that is, if $n\Lambda \subseteq 2\mathbb{Z}$; and it is of type I if it is odd. The lattice $\langle 1, \ldots, 1, -1, \ldots, -1\rangle$ is of type I while the hyperbolic plane $\mathbb{H} \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is of type II. If $\Lambda = \Lambda_1 \oplus \Lambda_2$. Then Λ is of type II if and only if Λ_1 and Λ_2 are of type II.

Invariant mod 8: Let Λ be a unimodular $\mathbb{Z}$-lattice. Then, $\Lambda \to \mathbb{F}_2,\ x \mapsto b(x, x) \bmod 2$ is a homomorphism. Now, let $L = \Lambda/2\Lambda$ be the reduction of Λ mod 2. Then L is an $\mathbb{F}_2$-vector space. The bilinear form $b(x, y)$ on Λ induces an $\mathbb{F}_2$-valued form $b(\bar{x}, \bar{y})$ on $\Lambda/2\Lambda$. The associated quadratic form $\Lambda/2\Lambda \to \mathbb{F}_2,\ \bar{x} \mapsto b(\bar{x}, \bar{x})$ is linear over $\mathbb{F}_2$ and so it is an element of the dual. Since $b(\bar{x}, \bar{y})$ is non-degenerate, we have an isomorphism onto the dual $L \cong L^\vee$. Thus, there exists a canonical element $\bar{u}$ such that $b(\bar{u}, \bar{x}) \equiv b(\bar{x}, \bar{x})$ for all $\bar{x} \in L$. If we life $\bar{u}$ to u in Λ, unique mod 2Λ and satisfying $b(u, x) \equiv b(x, x) \bmod 2$. Such a u is called a parity or characteristic vector.

If u' and u are two lifting of $\bar{u}$ to Λ, then $u' = u + 2v$ for some $v \in \Lambda$. Thus, $b(u', u') = b(u+2v, u+2v) = b(u, u) + 4(b(u, v) + b(v, v)) = b(u, u) \bmod 8$. The residue class of $b(u, u) \bmod 8$ is an invariant of Λ and we shall denote it by σ.

If Λ is of type II, then $b(\bar{x}, \bar{x})$ is zero and we can take $\sigma = 0$ in that case. See ([Ser96],page49) and ([MH73], page 24).

A.1 Indefinite unimodular forms

A.1.1 Theorem. *Every indefinite unimodular $\mathbb{Z}$-lattice is isotropic.*

Proof. Let Λ be an indefinite unimodular $\mathbb{Z}$-lattice on a quadratic space (V, b) over $\mathbb{Q}$. If Λ has rank $n \leq 4$. Then it is isotropic by ([Ser96], page 56).

If the rank of Λ is ≥ 5, then it follows from Meyer's theorem ([MH73], page 20). □

We discuss the structure theorem for unimodular $\mathbb{Z}$-lattices of type I. First we need a lemma.

A.1.2 Lemma. Let Λ be an indefinite unimodular $\mathbb{Z}$-lattice of type I and rank n. Then there exists a unimodular sublattice Γ of Λ of rank $n-2$ such that $\Lambda \cong \langle 1,-1\rangle \oplus \Gamma$.

Proof. Let Λ be an indefinite unimodular $\mathbb{Z}$-lattice of type I. Then by Theorem A.1.1, Λ is isotropic. let $v \in \Lambda$ be primivite and isotropic. Extend v to a basis of Λ and choose the first element w in the dual basis. Thus, $b(v,w) = 1$.

Since Λ is of type I, there is a $w \in \Lambda$ such that $b(w,w)$ is odd. In fact, if $b(w,w)$ is even. Find an $x \in \Lambda$ with $b(x,x)$ odd and replace w with $w' = x + (1 - b(v,x))w$. Thus, $b(w',w')$ is odd and $b(v,w') = 1$.

So we may now suppose that $b(w,w)$ is odd. Thus $b(w,w) = 2m+1$ for some m. Put $v_1 = w - mv$ and $v_2 = w - (m+1)v$. Then, we see that $M = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 = \langle 1,-1\rangle$ is a unimodular sublattice of Λ and so $L = M \oplus M^{\perp}$. □

A.1.3 Theorem. *Let Λ be an indefinite unimodular $\mathbb{Z}$-lattice of type I. Then, Λ has an orthogonal basis and so is isometric to an orthogonal sum $\langle 1,\ldots,1,-1,\ldots,-1\rangle$.*

Proof. Let Λ be an indefinite unimodular $\mathbb{Z}$-lattice of type I. We prove the theorem by induction on the rank n of Λ. For $n = 1$, this is trivial. For $n = 2$, we have that $M^{\perp} = 0$. Assume the theorem holds for ranks smaller than n. Then for $n > 2$, $M^{\perp} \neq 0$. Choose ± 1 such that $\langle \pm 1\rangle \oplus M^{\perp}$ is indefinite; say $\langle 1\rangle \oplus M^{\perp}$. Then by hypothesis, it is of the form $a\langle 1\rangle \oplus b\langle -1\rangle$. Hence $\Lambda \cong a\langle 1\rangle \oplus (b+1)\langle -1\rangle$. ([Ger08], page 189; [Ser96], page 57; [MH73], page 22). □

A.1.4 Corollary. Let Λ be as in the theorem above. Then, the isometry class of Λ is determined by its rank and signature.

We now give a structure theorem for indefinite unimodular lattices of type II.

A.1.5 Lemma. Let Λ be an indefinite unimodular $\mathbb{Z}$-lattice of type II. Then there exists a unimodular sublattice F of Λ such that Λ is an orthogonal sum: $\Lambda \cong \mathbb{H} \oplus F$.

Proof. The lattice Λ is isotropic and so we can find an $x \in \Lambda$ such that $b(x,x) = 0$ and a $y \in \Lambda$ such $b(x,y) = 1$. If $b(y,y) = 2a$ for some a, replace y with $z = y - ax$. Thus, the lattice generated by $\{x,z\}$ is isomorphic to $\mathbb{H}$. Hence, $L \cong \mathbb{H} \oplus F$. □

A.1.6 Lemma. If Λ and Γ are two unimodular $\mathbb{Z}$-lattices of type II and $\Lambda \oplus \langle 1,-1\rangle \cong \Gamma \oplus \langle 1,-1\rangle$. Then, $\Lambda \oplus \mathbb{H} \cong \Gamma \oplus \mathbb{H}$.

Proof. [Ser96], lemma 6, page 57. □

A.1.7 Theorem. *Two indefinite unimodular $\mathbb{Z}$-lattices of type II and having the same rank and index are isometric.*

Proof. Let Λ_1 and Λ_2 be as in the statement of the theorem. By Lemma A.1.5, we have that $\Lambda_1 = \mathbb{H} \oplus F_1$ and $\Lambda_2 = \mathbb{H} \oplus F_2$. Now, F_1 and F_2 are of same rank, index and type II. Thus, $\langle 1,-1\rangle \oplus F_1$ and $\langle 1,-1\rangle \oplus F_2$ are indefinite and of type I. They also have the same rank and index and so are isomorphic by Theorem A.1.3. Hence, Λ_1 and Λ_2 are isometric by Lemma A.1.6. ([Ser96], page 58). □

In summary, we have the following theorem:

A.1.8 Theorem. *Two indefinite unimodular $\mathbb{Z}$-lattices are isometric if and only if they have the same rank, type and signature.*

A.2 Definite unimodular forms

We only need to consider positive definite forms since we can always scale a negative definite form to a positive definite form by -1. From now on, all our lattices will be positive definite.

Let Λ be a $\mathbb{Z}$-lattice in a quadratic space (V, b) over $\mathbb{Q}$. The lattice Λ is said to be decomposable if we can find two nonzero lattices A and B in Λ such that $\Lambda = A \oplus B$ is an orthogonal sum.

A.2.1 Theorem (Eichler-Kneser)**.** *Let (V, b) be a quadratic space over $\mathbb{Q}$ and Λ a positive definite $\mathbb{Z}$-lattice in V. Then, Λ has a unique (up to order of summands) decomposition as an orthogonal sum : $\Lambda = \Lambda_1 \oplus \ldots \oplus \Lambda_t$ where each Λ_i is indecomposable.*

Let (V, b) be a quadratic space over $\mathbb{Q}$ which is positive definite. Let Λ be a unimodular lattice in V, then since it is positive definite, we have that $\text{disc}(\Lambda) = 1$. This yields in particular that $\text{disc}(V) = 1$.

If there is a unimodular $\mathbb{Z}$-lattice on V, then there is a unimodular lattice on the localisation V_p for each p. Hence, $h_p(V) = 1$ for $p = 3, 5, 7, \ldots$ since the determinant is ± 1. Since V_∞ is positive defininte, $h_\infty = 1$. Thus, by Hilbert reciprocity, $h_2(V) = 1$. Hence by Hasse-Minkowski theorem and the clasification of quadratic spaces over $\mathbb{Q}_p$, we have that $V \cong \langle 1, \ldots, 1 \rangle$. Furthermore, the matrix associated to V is the $n \times n$ identity matrix I_n, where n is the rank of V. We will say that a lattice in V is completely decomposable if it can be written as an orthogonal sum of rank 1 lattices.

A.2.2 Theorem. *Let V be a quadratic space isometric to $\langle 1, \ldots, 1 \rangle$. Then, there is an even unimodular $\mathbb{Z}$-lattice in (V, b) if and only if $n \equiv 0 \mod 8$.*

Proof. [O'M73], 106:1 and [Ger08], page188. □

Positive definite quadratic forms have been classified only up to rank 25. Kneser determined all the indecomposable lattices of rank ≤ 16. He used the method of neighbouring lattices which he developed. Other mathematicians, Niemer, Borcherds and Venkov, extended the result to lattices of rank through rank 25, using Siegel's mass formular from the analytical theory of quadratic forms. For lattices of rank greater than 25, the Smith-Minkowski-Siegel mass formular shows that the number of isometry classes of a lattices grows exponentially with rank making the complete classification of positive definite lattices really difficult. This problem is still open.

Acknowledgements

I am grateful to God for life, health and for seeing me through. My sincere gratitude goes to my supervisor, Prof. Boas EREZ, whose support, advice and suggestions made this work a reality. To the African Institute for Mathematical Sciences (AIMS), The ALGANT Consortium and the Stellenbosch University for funding my masters program. To all the 2012-2013 Algant-Bordeaux students. And to my family and friends for their support.

References

[Cas08] J. W. S. Cassels, *Rational quadratic forms*, Dover Publications Inc New York, 2008.

[CP84] P E Conner and Robert Perlis, *A survey of trace forms of algebraic number fields*, Series in pure mathematics, vol. 2, World Scientific publishing company, 1984.

[CS98] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, Grundlehren der mathematischen Wissenschaften, vol. 290, Springer, 1998.

[EH75] A. G. Earnest and J. S. Hsia, *Spinor norms of local integral rotations II*, Pacific Journal of Mathematics **61** (1975), no. 1, 71–86.

[EMP87] Boas Erez, J. Morales, and Robert Perlis, *Sur le genre de la forme trace*, Séminaire de théorie des nombres de Bordeaux **16** (1987), 1–16.

[Ger08] Larry J. Gerstein, *Basic quadratic forms*, Graduate Studies in Mathematics, vol. 90, American Mathematical Society, 2008.

[Gou97] Fernando Gouvêa, *p-adic numbers: An introduction*, Springer Verlag, 1997.

[Jan96] Gerald J. Janusz, *Algebraic number fields*, second ed., Graduate studies in mathematics, vol. 7, American Mathematical Society, 1996.

[Lam05] T. Y. Lam, *Introduction to quadratic forms over fields*, Graduate studies in mathematics, vol. 67, American Mathematical Society, 2005.

[Mau73] Donald Maurer, *The trace-form of an algebraic number field*, Journal of Number theory **5** (1973), 379–384.

[MH73] J. Milnor and D. Husemöller, *Symmetric bilinear forms*, Ergebnisse der mathematik und ihrer Grenzgebiete neue Folge, vol. 73, Springer-Verlag Berlin-Heidelberg-New York, 1973.

[MS12] Guillermo Mantilla-Soler, *On number fields with equivalent integral trace forms*, International journal of number theory **8** (2012), no. 7, 1569–1580.

[MS13] ———, *The spinor genus of the integral trace*, preprint, http://arxiv.org/abs/1306.3998, 2013.

[Nor98] K. Norbert, *Arithmetical similarities. prime decomposition and finite group theory*, Oxford university press New York, 1998.

[O'M73] O. T. O'Meara, *Introduction to quadratic forms*, Die Grundlehren der mathematischen wissenschaften in einzeldarstellungen, vol. 117, Springer Verlag, 1973.

[Per77a] R. Perlis, *On the equation* $\zeta_K(s) = \zeta_{K'}(s)$, Journal of number theory **9** (1977), no. 3, 342–360.

[Per77b] ———, *A remark about zeta functions of number fields of prime degree*, Journal für die reine und angewandte Mathematik **0293_0294** (1977), 435–436.

[Per85] ———, *On the analytic determination of the trace form*, Canadian Journal of Math **28** (1985), no. 4, 422–430.

[Sch85] Winfried Scharlau, *Quadratic and hermitian forms*, Grundlehren der mathematischen wissenschaften, vol. 270, Springer-Verlag, 1985.

[Ser77] J.-P. Serre, *Linear representations of finite groups*, Springer-Verlag New York, 1977.

[Ser84] _____, *L'invariant de witt de la forme* $tr(x^2)$, Commentarii Mathematici Helvetici **59** (1984), 651–676.

[Ser96] _____, *A course in arithmetic*, corrected fifth printing ed., Graduate Studies in Mathematics, vol. 7, Springer New-York, 1996.

[Tau68] Olga Tauskky, *The discriminant matrices of an algebraic number field*, Journal of the London Mathematical Society **1** (1968), no. 1, 152–154.

[Wat60] G. L. Watson, *Integral quadratic forms*, Cambridge tracts in mathematics and mathematical physics, vol. 51, Cambridge, 1960.

[Yos99] Kitaoka Yoshiyuki, *Arithmetic of quadratic forms*, Cambridge tracts in mathematics, vol. 106, Cambridge University Press, 1999.