Representations of integral Hermitian forms
by sums of norms

By
Jingbo Liu

Faculty Advisor: Wai Kiu Chan
Professor of Mathematics

A Dissertation in Mathematics
submitted in partial fulfillment of the
requirements for the degree of Doctor of Philosophy
at Wesleyan University

Middletown, CT May, 2016
For my daughter, Jacquelyn Han
Abstract

In 1770, Lagrange proved the famous four square theorem, which says that each positive integer \(a\) can be written as a sum of four squares. This theorem has been generalized in many directions since then. One interesting generalization is to consider the representation of positive definite integral quadratic forms in more variables by sums of squares.

Let \(g_Z(n)\) be the smallest number of squares whose sum represents all positive definite integral quadratic forms in \(n\) variables over \(Z\) that are represented by some sums of squares. In 1996, Icaza first proved the existence of \(g_Z(n)\) and she also gave an explicit upper bound for it. An improved upper bound was obtained later by Kim and Oh in 2005.

In this thesis, we consider the Hermitian analog of the above representation problem. Let \(E\) be an imaginary quadratic field and \(\mathcal{O}\) be its ring of integers. For any positive integer \(m\), let \(I_m\) be the free Hermitian lattice over \(\mathcal{O}\) with an orthonormal basis. Via the standard correspondence between free Hermitian lattices and Hermitian forms, \(I_m\) corresponds to the integral Hermitian form \(x_1\overline{x}_1 + \cdots + x_m\overline{x}_m\) over \(\mathcal{O}\). For any positive integer \(n\), let \(\mathcal{S}_E(n)\) be the set consisting of all positive definite integral Hermitian lattices of rank \(n\) over \(\mathcal{O}\) that are represented by some \(I_m\). We define \(g_E(n)\) to be the smallest positive integer \(g\) such that every Hermitian lattice in \(\mathcal{S}_E(n)\) is represented by \(I_g\). Our main result is an explicit upper bound for \(g_E(n)\) for any imaginary quadratic field \(E\) and positive integer \(n\).
Acknowledgements

I would like to express my most sincere gratitude to my advisor, Professor Wai Kiu Chan, for his consistent encouragement, guidance, inspiration, and patience. I feel extremely honored to have him as my Ph.D. advisor, he is not only an excellent mathematician, but also a wonderful teacher. Without his support, this work could never have been done.

I am grateful to Professor David Pollack and Professor Chris Rasmussen for being my committee members and spending their time reading this thesis carefully. I also want to thank them for introducing me to various topics in number theory.

Thank all my fellow graduate students past and present. Special thanks to the number theory group; it was such a pleasure to learn with and from all of you.

Finally and foremost, I would like to thank my parents and my husband for their continuous understanding and unconditional support. I love you.
# Contents

Abstract ii

Acknowledgements iii

Introduction 1

Chapter 1. Hermitian Spaces 5
  1.1. Basic Results and Definitions 5
  1.2. The induced quadratic space 10
  1.3. Local and Global Hermitian spaces 13

Chapter 2. Hermitian lattices 18
  2.1. Generalities 18
  2.2. Local theory of Hermitian lattices 25
  2.3. Representations of Hermitian lattices over local field 27
  2.4. The induced quadratic lattice 32

Chapter 3. Neighbors of Hermitian lattices over number fields 36
  3.1. Basic definitions 36
  3.2. Neighborhood, genus and special genus 38

Chapter 4. The \(g\)-invariants of imaginary quadratic fields 41
  4.1. The \(g\)-invariant 41
  4.2. Local density 42
  4.3. The smallest universal number 51
  4.4. Main theorem 57

Bibliography 66
**Introduction**

A positive integer $a$ is said to be represented by a given quadratic form $f$, written $a \rightarrow f$, if there exist integers $x_1, ..., x_m$ such that $f(x_1, ..., x_m) = a$. A typical question is to determine those positive integers that can be represented by the quadratic form $I_m = x_1^2 + \cdots + x_m^2$, where $m$ is a positive integer. Following the work of Fermat, Euler, Legendre and Lagrange on sums of squares, it is well known that every positive integer can be written as a sum of at most four squares.

This result has been generalized in many different ways. For example, Waring’s Problem seeks for the smallest positive integer $r(k)$, such that every positive integer is a sum of $r$ $k$-th powers. There is also a higher dimensional generalization in terms of the representations of positive definite integral quadratic forms. To each quadratic form

$$f(x_1, ..., x_m) = \sum_{i,j=1}^{m} a_{ij}x_i x_j,$$

we can associate a Gram matrix $M_f = (a_{ij})$. Let $g$ be a quadratic form in $n$ variables with $m \leq n$. We say that $f$ is represented by $g$, written $f \rightarrow g$, if there exists an $n \times m$ integral matrix $T$ such that $M_f = T^t M_g T$. We say that $f$ is equivalent to $g$ if $T$ is an invertible square matrix.

In general, a quadratic form is represented by $I_m$ if and only if it is the sum of $m$ squares of integral linear forms. Lagrange’s Four-Square Theorem tells us that every unary positive definite integral quadratic form is represented by $I_4$. Mordell [20] made the first step of generalization along this direction by proving that every binary positive definite integral quadratic form is represented by $I_5$, but not by any $I_m$ with $m \leq 4$. In the same paper, he posed the following which he called a new Waring’s Problem: can every positive definite integral quadratic form in $n$ variables be written as a sum of $n + 3$ squares of integral linear forms? This was proven to be
true when \( n \leq 5 \) by Ko \([16]\), but around the same time Mordell \([21]\) showed that the following 6-variable quadratic form
\[
q(x) = \sum_{i=1}^{6} x_i^2 + \left( \sum_{i=1}^{6} x_i \right)^2 - 2x_1x_2 - 2x_2x_6,
\]
which corresponds to the root system \( E_6 \), cannot be represented by any sum of squares. More precisely, he proved that this quadratic form cannot be written as the sum of two positive semi-definite integral quadratic forms. This leads to the consideration of the set \( \mathcal{S}_Z(n) \) of all positive definite integral quadratic forms in \( n \) variables that can be represented by some sums of squares and the following definition of the \( g \)-invariants of \( Z \):
\[
g_Z(n) := \min \{ g : f \to I_g \text{ for any } f \in \mathcal{S}_Z(n) \}.
\]
All the results mentioned so far can be summarized as \( g_Z(n) = n + 3 \) for \( n \leq 5 \).
Ko \([17]\) conjectured that \( g_Z(6) = 9 \), but this is disproved almost sixty years later by Kim and Oh \([12]\) who show that \( g_Z(6) \) is actually equal to 10. This is the last known exact value of \( g_Z(n) \).

For larger values of \( n \), Icaza \([10]\) first proves the existence of the \( g_Z(n) \), and she also obtains an upper bound by computing the so called HKK-constant. But her bound contains a factor \( n^{n+1}2^{h(I_n+1)} \), where \( h(I_n) \) denotes the class number of the genus of \( I_n \) which can be shown to be of the form \( h(I_n) = n^{\Theta(n^2)} \) for some arithmetic function \( \Theta(n^2) \) bounded between constant multiples of \( n^2 \) for all \( n \gg 0 \). A much better upper bound \( g_Z(n) = O(3^{n/2}n \log n) \) is later obtained by Kim and Oh \([13]\) which is the best upper bound for \( g_Z(n) \) so far.

In this thesis, we consider the Hermitian analog of this representation problem. Let \( E = \mathbb{Q}(\sqrt{-\ell}) \) be an imaginary quadratic extension of \( \mathbb{Q} \), where \( \ell \) is a square-free positive integer, and \( \mathcal{O} \) be its ring of integers. Since \( \mathcal{O} \) is not necessarily a principle ideal domain in general, every Hermitian form corresponds to a Hermitian lattice, but not vice versa. Therefore, instead of Hermitian forms, the more general notion of Hermitian lattices will be considered.

For a Hermitian space \( V \), we define the unitary group \( U(V) \) to be the set of all \( E \)-isomorphisms \( \sigma \) of \( V \) onto itself which preserve the Hermitian map. Given two
Hermitian lattices $K$ and $L$ in $V$, we say that $K$ is represented by $L$ if there is some $\phi \in U(V)$ such that $\phi K \subseteq L$, and $K$ is isometric to $L$ if $\phi K = L$.

For any integer $m \geq 1$, let $I_m$ be the free Hermitian lattice of rank $m$ with an orthonormal basis. Via the standard correspondence between free Hermitian lattices and Hermitian forms, $I_m$ corresponds to the integral Hermitian form $x_1 \overline{x}_1 + \cdots + x_m \overline{x}_m$. For each integer $n \geq 1$, let $\mathcal{S}_E(n)$ be the set consisting of all positive definite integral Hermitian lattices of rank $n$ that can be represented by some $I_m$. We define

$$g_E(n) := \min\{g : L \to I_g \text{ for any } L \in \mathcal{S}_E(n)\}.$$ 

The finiteness of $g_E(n)$ can be proved in the same way as $g_Z(n)$. Using the results of local representation theory in [2] and [9], every positive definite integral Hermitian lattice $L$ of rank $n$ is locally represented by $I_m$ at every prime $p$, for any integer $m > n$. A theorem of Hsia and Prieto-Cox [4, Theorem 2.12] says that for a positive definite Hermitian lattice $M$ of rank $2n + 1$, there exists a constant $C$, depending only on $M$, such that $M$ represents any positive definite Hermitian lattice $N$ of rank $n$ satisfying that $N$ is represented by $M$ at every prime $p$ and the smallest positive number represented by $N$ is no less than $C$. All these observations together provide one way of showing the existence of $g_E(n)$.

In this thesis, we obtain an explicit upper bound for $g_E(n)$ which only depends on the imaginary quadratic field $E$ and the rank $n$. In Chapters 1 and 2 we give the necessary background on Hermitian spaces and Hermitian lattices. In Chapter 3, we introduce the theory of neighbors of Hermitian lattices over number fields, which is due to Schiemann [25] and is considered to be the Hermitian analog of the theory of neighbors of quadratic lattices developed by Kneser [14]. This theory is very useful in finding a condition when a Hermitian lattice $L$ of rank $n$ is represented by $I_{n+2}$. In Chapter 4, we present and prove the main result of this thesis.

Let $p$ be the smallest inert prime in the extension $E/\mathbb{Q}$. For any integer $n \geq 1$, define

$$\delta(n) := \begin{cases} n - 3, & \text{if } n \geq 3 \text{ and } 2 \text{ is ramified;} \\ 0, & \text{otherwise.} \end{cases}$$
Let $\chi$ be the Dirichlet character associated to $E$ and $B_{3,\chi}$ be the third Bernoulli number twisted by $\chi$. Then the main result is the following:

**Theorem 0.1.**

$$g_E(n) \leq \frac{3^{n+2}}{2}\delta(n + 1) + \frac{9(p - 1)(p + 5)^{n+1}}{2^{n+2}}\left[\sum_{i=3}^{n+1} \lceil 10\log_p(i\ell) \rceil + G(\ell)\right] + n + 6,$$

where

$$G(\ell) = \begin{cases} 
\ell B_{3,\chi}/36 + 64\ell^3, & \text{if } 2 \text{ is ramified;} \\
\ell B_{3,\chi}/144 + \ell^3, & \text{otherwise.}
\end{cases}$$
CHAPTER 1

Hermitian Spaces

In this chapter we provide the background on the algebraic theory of Hermitian spaces. In the first section, we introduce the basic definitions and classical results. Then in the second section, we present the correspondence between Hermitian and quadratic spaces. Finally in the third section we present the classical results for local and global Hermitian spaces.

Let $F$ be either a number field or a $p$-adic field, and $E$ either a quadratic extension $F(\sqrt{\theta})$ of $F$ or the direct sum $F \times F$ of two copies of $F$. By $O$, $\mathfrak{o}$ we denote the ring of integers of $E$ and $F$ respectively, and by $V$ we denote a finitely generated free $E$-module.

1.1. Basic Results and Definitions

Let $E$ be either a quadratic extension $F(\sqrt{\theta})$ of $F$ where $\theta$ is a non-square in $F$, or the direct sum $F \times F$ of two copies of $F$. In both cases $E$ has a non-trivial involution whose fixed field is $F$. We usually call this involution the conjugation and denote it by $\overline{\cdot}$. In the first case this involution is defined by the generator of the Galois group, i.e., $\overline{\alpha + \beta \sqrt{\theta}} = \alpha - \beta \sqrt{\theta}$, where $\alpha$ and $\beta$ are in $F$. In the second case it is defined by $(a,b) := (b,a)$. Here $F$ is embedded into $E$ diagonally, i.e., $a \mapsto (a,a)$.

**Definition 1.1.** The *norm* and *trace* of an element $a$ of $E$ are defined respectively by:

\[ N(a) = a\overline{a}; \quad T(a) = a + \overline{a}. \]
1.1.1. Hermitian spaces.

**Definition 1.2.** A Hermitian space \((V, h)\) is a finitely generated free \(E\)-module with a Hermitian map \(h : V \times V \to E\) satisfying the following conditions:

1. \(h(v, w) = \overline{h(w, v)}\) for any \(v, w \in V\);
2. \(h(v_1 + v_2, w) = h(v_1, w) + h(v_2, w)\) for any \(v_1, v_2, w \in V\);
3. \(h(\alpha v, w) = \alpha h(v, w)\) for any \(\alpha \in E\) and \(v, w \in V\).

The following three consequences are straightforward:

1. \(h(v, \alpha w) = \overline{\alpha} h(v, w)\) for any \(\alpha \in E\) and \(v, w \in V\);
2. \(h(\alpha v, \alpha w) = N(\alpha) h(v, w)\) for any \(\alpha \in E\) and \(v, w \in V\);
3. \(h(v, v) \in F\) for any \(v \in V\).

Throughout this thesis \(h(v, v)\) is abbreviated simply to \(h(v)\). If there is no fear of confusion we will denote the Hermitian space \((V, h)\) by \(V\) alone.

**Definition 1.3.** A Hermitian space \((V, h)\) is said to be represented by another Hermitian space \((V_1, h_1)\) if there is an \(E\)-linear map \(\sigma : V \to V_1\), such that \(h(v, w) = h_1(\sigma(v), \sigma(w))\), for all \(v, w\) in \(V\). Such \(\sigma\) is called a representation from \(V\) into \(V_1\), and we say that \(\sigma\) is an isometry of \(V\) onto \(V_1\) if it is bijective.

**Definition 1.4.** Two Hermitian spaces \((V, h)\) and \((V_1, h_1)\) are said to be isometric if there is an isometry \(\sigma\) from \(V\) onto \(V_1\).

The unitary group of a Hermitian space \(V\) is the group of isometries from \(V\) onto itself, denoted by \(U(V)\). These elements in \(U(V)\) with determinant 1 form a subgroup \(SU(V)\), which is called the special unitary group of \(V\).

1.1.2. Hermitian matrices.

**Definition 1.5.** A matrix \(H = (a_{ij}) \in M_n(E)\) is said to be Hermitian if \(H^* = H\), where \(H^* := (\overline{a_{ij}})\) is the conjugate transpose of \(H\).
Definition 1.6. Let $H$ be an $m \times m$ Hermitian matrix and $K$ an $n \times n$ Hermitian matrix over $E$. We write

$$H \rightarrow K \quad \text{(over $E$)}$$

and say that $H$ is represented by $K$ (fractionally) if there is an $n \times m$ matrix $T$ with coefficients in $E$ such that

$$H = T^*KT.$$ 

If this can be done with an invertible $T$ over $E$, we say that $H$ is equivalent to $K$ and write

$$H \cong K \quad \text{(over $E$)}.$$ 

Given a basis $\{v_1, \ldots, v_n\}$ of a Hermitian space $V$, let $H$ be the $n \times n$ Hermitian matrix whose $(i,j)$ entry is $h(v_i,v_j)$. We call $H$ the Gram matrix of $V$ in the basis $\{v_1, \ldots, v_n\}$. Suppose $K$ is the Gram matrix of $V$ in another basis $\{w_1, \ldots, w_n\}$ and let $T \in \text{GL}_n(E)$ be the matrix that carries the first basis to the second. Then $H$ is equivalent to $K$ and we have the equality $K = T^*HT$. Hence

$$\det K = N(\det T)\det H,$$

i.e., $\det K$ and $\det H$ differ by a factor in $N(E^\times)$. Accordingly, we define the determinant of $V$ as the class of $\det H$ in $F^\times/N(E^\times) \cup \{0\}$ and denote it by $dV$. When there is no fear of confusion we use a representative of $dV$ to denote the determinant of $V$.

Definition 1.7. A Hermitian space $V$ is called non-degenerate if $dV \neq 0$. Otherwise, we say that $V$ is degenerate.

1.1.3. Hermitian spaces and Hermitian forms over $E$.

Definition 1.8. A Hermitian form $f$ over $E$ in variables $x_1, \ldots, x_n$ is an algebraic expression of the form

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^n a_{ij}x_i\overline{x}_j,$$

where $a_{ij} = \overline{a}_{ji} \in E$. 
1.1. BASIC RESULTS AND DEFINITIONS

Definition 1.9. A Hermitian form $f$ over $E$ is said to be represented by another Hermitian form $g$ over $E$ if there is a homogeneous linear substitution over $E$ which takes the form $g$ to the form $f$. We say that two $n$-ary Hermitian forms $f$ and $g$ are equivalent if they can represent each other.

For an $n$-dimensional Hermitian space $V$, associated with a basis $\{v_1, ..., v_n\}$ is the Hermitian form

$$f_V(x_1, ..., x_n) = \sum_{i,j=1}^{n} h(v_i, v_j)x_ix_j.$$ 

Conversely, given a Hermitian form $f(x_1, ..., x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$ over $E$, we can associate with it a Hermitian space

$$V_f = Ev_1 + \cdots + Ev_n,$$

where the Hermitian map defined on $V_f$ is $h(v_i, v_j) = a_{ij}$.

This “correspondence” is certainly not one-to-one, on the one hand it depends on the basis chosen to construct the Hermitian form and on the other hand it depends on the free $E$-module used to support the Hermitian form. However, this will induce a one-to-one correspondence between the set of isometry classes of Hermitian spaces and the equivalence classes of Hermitian forms.

1.1.4. Orthogonal sums.

Definition 1.10. Let $V$ be a Hermitian space. Two subspaces $U$ and $W$ of $V$ are said to be orthogonal if $h(u, w) = 0$ for all $u \in U$ and $w \in W$.

We say that $V$ has the orthogonal splitting

$$V = V_1 \perp \cdots \perp V_k$$

into subspaces $V_1, ..., V_k$, if $V$ is the direct sum $V_1 \oplus \cdots \oplus V_k$ and the $V_i$ are pairwise orthogonal. We call these $V_1, ..., V_k$ the components of this splitting. In particular, every Hermitian space $V$ has an orthogonal splitting into lines, i.e., $V = Ev_1 \perp$
1.1. BASIC RESULTS AND DEFINITIONS

\[ \cdots \perp Ev_n \] with some linearly independent vectors \( v_1, \ldots, v_n \in V \). In this case we call \( \{v_1, \ldots, v_n\} \) an orthogonal basis of \( V \) and write

\[ V \cong [a_1] \perp \cdots \perp [a_n], \]

where \( a_i = h(v_i, v_i) \).

Let \( U \) be a subspace of \( V \). We say that \( U \) splits \( V \), or that it is a component of \( V \), if there exists a subspace \( W \) such that \( V = U \perp W \). By the orthogonal complement \( U^\perp \) of \( U \) in \( V \) we mean the subspace

\[ U^\perp = \{v \in V : h(v, U) = 0\}. \]

When \( U \) is non-degenerate, \( U \) splits \( V \), and \( V = U \perp U^\perp \). If \( V = U \perp W \) is another splitting, then \( W = U^\perp \).

In particular, we call the orthogonal complement \( V^\perp \) of \( V \) the radical of \( V \), denoted \( \text{rad}V \). The space \( V \) is non-degenerate if and only if \( \text{rad}V = \{0\} \). Every Hermitian space \( V \) can be written as \( V = V' \perp \text{rad}V \) where \( V' \) is non-degenerate. It is well known that two Hermitian spaces \( V = V' \perp \text{rad}V \) and \( W = W' \perp \text{rad}W \) are isometric iff \( V' \cong W' \) and \( \dim(\text{rad}V) = \dim(\text{rad}W) \).

For the above reason, we assume that all Hermitian spaces are non-degenerate from now on, though subspaces arising from our discussion are not necessarily non-degenerate.

1.1.5. Isotropy.

DEFINITION 1.11. A vector \( v \neq 0 \) in \( V \) is called isotropic if \( h(v, v) = 0 \); otherwise, it is called anisotropic.

A Hermitian space \( V \) is called isotropic if it contains an isotropic vector, otherwise it is called anisotropic. A subspace \( W \) of \( V \) is called totally isotropic if \( h(v, v) = 0 \) for all vectors \( v \) in \( W \).
1.2. THE INDUCED QUADRATIC SPACE

The simplest but most important example of a non-degenerate isotropic Hermitian space is the *hyperbolic plane*. It is a binary Hermitian space $\mathbb{H}$ which satisfies one of the following equivalent conditions:

1. $\mathbb{H}$ is non-degenerate and isotropic;
2. $\mathbb{H}$ has the matrix \[
\begin{pmatrix}
0 & 1 \\
1 & 0 \\
\end{pmatrix}
\] in some suitable basis;
3. $d\mathbb{H} = -1$.

An isotropic non-degenerate space $V$ always contains an hyperbolic plane which splits $V$, i.e., $V = \mathbb{H} \perp U$. A *hyperbolic space* is an orthogonal sum of hyperbolic planes.

1.2. The induced quadratic space

Two fundamental problems in the theory of Hermitian spaces are classification and representation. The *classification* problem asks for an effective procedure to determine whether two Hermitian spaces are isometric, and the *representation* problem asks for an effective procedure to decide if a Hermitian space is represented by another Hermitian space.

To answer these two questions, we can use the trace from $E$ to $F$ to associate to every Hermitian space over $E$ a quadratic space over $F$, whose theory has been extensively studied. This idea was introduced by Jacobson ([8, page267]).

For each Hermitian space $(V, h)$ over $E$, Jacobson considered a quadratic space $(\hat{V}, b_h)$ over $F$ defined as follows:

1. $\hat{V} = V$ setwise but viewed as a vector space over $F$;
2. $b_h = \frac{1}{2}T \circ h$ where $T : E \to F$ is the trace.

The bilinear form $b_h$ is called the *trace form induced by $h$*. If we denote by $Q_h$ the quadratic form associated with $b_h$ (i.e., $Q_h(x) = b_h(x, x)$), then $Q_h(x) = h(x, x)$ and hence $Q_h$ and $h$ represent the same elements in $F$. When there is no fear of confusion, we will simply write $b$ and $Q$ for $b_h$ and $Q_h$, respectively.
Remark 1.12. In a few instances we will use $T \circ h$ as $b_h$ instead.

1.2.1. The non-split case. Suppose that $E = F(\sqrt{\theta})$ is a quadratic extension of $F$, and we take $b = \frac{1}{2} T \circ h$ in this case.

Let $H$ be the Gram matrix of $V$ in some basis $\{v_1, ..., v_n\}$, and we write $H = B + \sqrt{\theta} A$, where $B$ is symmetric and $A$ is alternating. Then the Gram matrix $\hat{H}$ of the associated quadratic space $\hat{V}$ in the basis $\{v_1, ..., v_n, \sqrt{\theta}v_1, ..., \sqrt{\theta}v_n\}$ is

$$\hat{H} = \begin{pmatrix} B & -\theta A \\ \theta A & -\theta B \end{pmatrix}.$$ 

On the other hand, we can recover the Hermitian form $h$ from its induced bilinear form $b$ as follows. Note that

$$h(v, w) = b(v, w) + a(v, w)\sqrt{\theta},$$

where $a(v, w)$ is an alternating form. Now

$$b(\sqrt{\theta}v, w) = \frac{1}{2} T(\sqrt{\theta} h(v, w)) = a(v, w)\theta.$$ 

Therefore

$$h(v, w) = b(v, w) + \frac{1}{\sqrt{\theta}} b(\sqrt{\theta}v, w).$$

The following theorem is important in addressing the problem of classification of Hermitian spaces. With this result, the problem of classification of Hermitian spaces is reduced to the corresponding problem for quadratic spaces.

Theorem 1.13. (Jacobson [8]) Let $E = F(\sqrt{\theta})$ be a quadratic extension of $F$, and let $(V, h), (W, g)$ be Hermitian spaces over $E$. Then

1. $(V, h)$ is non-degenerate $\iff$ $(\hat{V}, b)$ is non-degenerate.
2. $(V, h) \cong (W, g) \iff (\hat{V}, b_h) \cong (\hat{W}, b_g)$.
3. $(V, h)$ is isotropic $\iff (\hat{V}, b)$ is isotropic.

A natural question is: Which quadratic spaces can be obtained in this way? This question was answered by Lewis in 1979.
1.2. THE INDUCED QUADRATIC SPACE

Proposition 1.14. (Lewis, [19, page 266]) Let $E = F(\sqrt{\theta})$ be a quadratic extension of $F$. A quadratic space $(W, b)$ over $F$ is the induced quadratic space of a Hermitian space over $E$ if and only if

1. $\dim_F W = 2n$;
2. $W \otimes E$ is hyperbolic;
3. $dW \equiv (-\theta)^n$ mod $F^\times 2$.

1.2.2. The split case. Now we assume that $E = F \times F$ is the direct sum of two copies of $F$, and take $b = T \circ h$ in this case.

Let $V$ be a Hermitian space over $E$. In this special case, $N(E^\times) = F^\times$, since $N(a, b) = (a, b)(b, a) = (ab, ab)$. Therefore, $dV = 1$. In contrast with the non-split case, every Hermitian space in the split case is isotropic because $N(a, 0) = 0$ for any $a \in F$.

Let $e = (1, 0)$ and $\bar{e} = (0, 1)$. We can write $h : V \to F \times F$ in the form

$$h(v, w) = f(v, w)e + g(v, w)\bar{e}.$$ 

Since $h$ is a Hermitian form, it follows that $g(v, w) = f(w, v)$ and $f(v, w)$ is $F$-bilinear. To compute the determinant of $V$, we take a basis $\{v_1, ..., v_n\}$ of $V$ and denote $h(v_i, v_j) = h_{ij}$ and $f(v_i, v_j) = f_{ij}$. Then $h_{ij} = f_{ij}e + f_{ji}\bar{e}$, and since the arithmetic operations are defined componentwise,

$$\det(h_{ij}) = \det(f_{ij})e + \det(f_{ij})\bar{e} = \det(f_{ij})$$

The non-degeneracy of $V$ implies that $\det(f_{ij}) \neq 0$. Let $(a_{ij}) = (f_{ij})^{-1}$ and put

$$w_i = \sum_{j=1}^{n} (a_{ij}e + \delta_{ij}\bar{e})v_j$$

for $i = 1, ..., n$, where $\delta_{ij}$ denotes Kronecker’s delta. Clearly $(a_{ij}e + \delta_{ij}\bar{e})$ is an invertible matrix. Therefore $\{w_1, ..., w_n\}$ is a basis for $V$ and the Gram matrix of $V$ with respect to this basis is $I_n \in GL_n(E)$. Thus we have proved:

Proposition 1.15. Every Hermitian space over $F \times F$ has an orthonormal basis.
For the induced quadratic space, if \( H = ((f_{ij}e + f_{ji}\overline{e})) \) is the Gram matrix of the Hermitian space \( V \) in some basis \( \{v_1, ..., v_n\} \), then the Gram matrix of \( \hat{V} \) in the basis \( \{ev_1, ..., ev_n, \overline{ev}_1, ..., \overline{ev}_n\} \) is

\[
\begin{pmatrix}
0 & (f_{ij}) \\
(f_{ji}) & 0
\end{pmatrix}.
\]

In particular, since every Hermitian space has an orthonormal basis, \( \hat{V} \) always has a Gram matrix of the form

\[
\begin{pmatrix}
0 & I_n \\
I_n & 0
\end{pmatrix}.
\]

That is, \( \hat{V} \) is a hyperbolic space. Consequently, the conclusions of Theorem 1.13 are still true in the split case.

**Remark 1.16.** In the split case, note that only the hyperbolic spaces can be obtained by taking the trace form of Hermitian spaces.

As in the non-split case, we can recover \( h \) from its induced form \( b = T \circ h \) as follows. Note that

\[
b(ev, w) = T(eh(v, w)) = T(f(v, w)e) = f(v, w).
\]

Similarly, \( b(v, ew) = f(w, v) \). Therefore

\[
h(v, w) = b(ev, w)e + b(v, ew)e.
\]

### 1.3. Local and Global Hermitian spaces

Let \( F \) be a number field, and \( E = F(\sqrt{\theta}) \) be a quadratic extension of \( F \), where \( \theta \) is a non-square in \( F \).
1.3. LOCAL AND GLOBAL HERMITIAN SPACES

1.3.1. Local Hermitian spaces. For any finite prime \( p \) of \( F \), \( p \) ramifies, remains inert or splits completely in \( E \). In the first two cases the local degree

\[
n_p := [E_P : F_p] = 2,
\]

where \( P \) is the unique prime of \( E \) which divides \( p \), and we say that \( p \) is non-split in \( E/F \). In the third case,

\[
n_p := [E_{P_1} : F_p] = [E_{P_2} : F_p] = 1,
\]

where \( P_1 \) and \( P_2 \) are the two primes of \( E \) above \( p \), and we say that \( p \) splits in \( E/F \). Then \( n_p = 1 \) or \( 2 \) according to whether or not \( \theta \) is a square in \( F_p \). It is well-known that there are infinitely many split, as well as non-split, primes in \( F \) (see [22, §65]).

Let \( p \) be a finite or infinite prime of \( F \). The localization \( E_p \) is defined as

\[
E_p = E \otimes_F F_p.
\]

For a vector space \( V \) over \( E \), we define \( V_p = V \otimes_F F_p \). Then \( V_p \) is just the extension of scalars \( E_p V \).

When \( n_p = 2 \), that is, when \( p \) is ramified or inert in \( E \), it is well-known that \( E_p = E_P = F_p(\sqrt{\theta}) \), where \( P \) is the unique prime of \( E \) dividing \( p \). The involution extends to a unique \( F_p \)-involution on \( E_p \) that coincides with the involution of \( F_p(\sqrt{\theta}) \) over \( F_p \).

When \( n_p = 1 \), that is, when \( p \) splits in \( E \), there is a ring isomorphism

\[
E_p = E \otimes_F F_p \cong F_p \times F_p
\]

defined by \( \alpha \otimes \beta \mapsto (\alpha \beta, \overline{\alpha} \beta) \), where \( \alpha \in E = F(\sqrt{\theta}) \subseteq F_p(\sqrt{\theta}) = F_p \) and \( \beta \in F_p \).

From now on, we will simply write \( E_p = F_p \times F_p \) with the understanding that they are identified via this ring isomorphism. Again the involution on \( E \) extends uniquely to an \( F_p \)-involution of \( E_p \) given by \( (\alpha \otimes \beta) = \overline{\alpha} \otimes \beta \). So the effect of the involution on \( F_p \times F_p \) is \( (a, b) = (b, a) \).

In both cases the Hermitian form on \( V \) extends to a unique Hermitian form on \( V_p \), that we still denote by \( h \).
1.3. Local representations. Let \( p \) be a finite prime of \( F \) and \( F_p \) be the localization of \( F \) at \( p \).

When \( E_p = F_p(\sqrt{\theta}) \) is a quadratic extension of \( F_p \), we essentially use Jacobson’s theory, together with the corresponding classification of quadratic spaces over local fields. It is well-known that every quaternary quadratic space over \( F_p \) is universal, i.e., represents all the elements of \( F_p \). By Theorem 1.13, it follows that every binary Hermitian space over \( E_p \) is universal, and therefore every Hermitian space over \( E_p \) of dimension 3 or higher is isotropic. In fact we have

**Proposition 1.17.** Suppose \( E_p \) is a quadratic extension of a \( p \)-adic field. Let \( V \) and \( W \) be Hermitian spaces over \( E_p \).

1. When \( \dim V > 2 \), \( V \) is isotropic. When \( \dim V = 2 \), \( V \) is isotropic or anisotropic according to whether or not \( dV \equiv -1 \mod \mathbb{N}(E_p^\times) \). When \( \dim V = 1 \), \( V \) is anisotropic.

2. \( W \to V \) if and only if \( \dim W < \dim V \) or \( \dim W = \dim V \) and \( dW \equiv dV \mod \mathbb{N}(E_p^\times) \).

Suppose now that \( E_p = F_p \times F_p \) is the direct sum of two copies of \( F_p \). As a straightforward consequence of Proposition 1.15, we obtain necessary and sufficient conditions for the representation of Hermitian spaces over \( F_p \times F_p \).

**Corollary 1.18.** Let \( V \) and \( W \) be two Hermitian spaces over \( F_p \times F_p \). Then

1. \( V \) and \( W \) are isometric if and only if they have the same rank;

2. \( V \) represents \( W \) if and only if \( \text{rank} V \geq \text{rank} W \).

1.3.3. Local-global principle. Now we present the classical local-global principle of Landherr.

Let \( V \) be a Hermitian space over \( E \). Denote by \( \infty_1, \ldots, \infty_t \) the distinct infinite real prime spots on \( F \). As before, denote by \( E_{\infty_i} \) the localization \( E \otimes_F F_{\infty_i} \). Reorder the prime spots so that for \( 1 \leq i \leq s \), \( E_{\infty_i}/F_{\infty_i} \cong \mathbb{C}/\mathbb{R} \), and for \( s + 1 \leq i \leq t \),
\[ E_\infty / F_\infty \cong (\mathbb{R} \times \mathbb{R}) / \mathbb{R}. \]  
For \( 1 \leq i \leq s \) denote by \( r(V_\infty) \) the number of negative entries in any diagonalization of \( V_\infty \).

**Theorem 1.19.** (Landherr, [18]) Let \( V, W \) be two Hermitian spaces over \( E \) of dimension \( m \) and \( n \) respectively. Then, \( V \) represents \( W \) if and only if

1. (when \( m > n \)) \( 0 \leq r(V_\infty) - r(W_\infty) \leq m - n \) for \( 1 \leq i \leq s \);
2. (when \( m = n \)) \( r(V_\infty) = r(W_\infty) \) for \( 1 \leq i \leq s \), and \( dV \equiv dW \mod N(E_\mathbb{F}^\times) \) for every finite prime spot \( p \) on \( F \).

In fact, for all (finite and infinite) prime spots \( p \) on \( F \)

\[ (1) \iff W_p \to V_p \quad \text{and} \quad (2) \iff W_p \cong V_p. \]

Thus the above theorem can be stated as a local-global principle in the Hermitian case, i.e.,

\[ W \to V \iff W_p \to V_p \quad \text{for all prime spots } p. \]

**1.3.4. Definite and indefinite spaces.** Finally, we introduce the notion of definite and indefinite Hermitian spaces.

**Definition 1.20.** The quadratic extension \( E/F \) is called a **CM-extension** if \( F \) is a totally real number field and \( E \) is a totally imaginary quadratic extension of \( F \).

Let \( E/F \) be a quadratic extension of number fields. We say that a Hermitian space \( V \) over \( E \) is **positive definite** if:

1. \( E_\infty / F_\infty \cong \mathbb{C}/\mathbb{R} \) at each infinite prime spot \( \infty \) on \( F \), i.e., the extension \( E/F \) is a CM-extension, and
2. \( V_\infty \) is positive definite at each infinite prime spot \( \infty \) on \( F \), i.e., in any diagonalization of \( V_\infty \) the diagonal entries are all positive.

Similarly we can define **negative definite** space. The Hermitian space \( V \) is said to be **definite**, if it is either positive definite or negative definite. Otherwise we say that \( V \) is **indefinite**.
Recall that $(\hat{V}, b)$ denote the associated quadratic space of Hermitian space $(V, h)$ by taking the trace form of $h$.

**Lemma 1.21.** Let $(V, h)$ be a Hermitian space over $E$, where $E/F$ is a CM-extension. Then $(V, h)$ is positive definite if and only if $(\hat{V}, b)$ is a positive definite quadratic space over $F$. 
CHAPTER 2

Hermitian lattices

In this chapter we present the integral theory of Hermitian forms. We introduce Hermitian lattices in Section 1 and look more closely at their local structure in the next section. The local theory of Hermitian lattices is very important in our work, in particular the representation theory is essential for what follows. In Section 3, we describe the results of Gerstein and Johnson needed for the representation problem in the local cases. Then in Section 4 we exhibit the relation between Hermitian and quadratic lattices.

Let $F$ be either a number field or a $p$-adic field, and $E$ be either a quadratic extension $F(\sqrt{\theta})$ of $F$ or the direct sum $F \times F$ of two copies of $F$. By $\mathcal{O}$, $\mathfrak{o}$ we denote the ring of integers of $E$ and $F$ respectively, and by $\mathcal{O}^\times$, $\mathfrak{o}^\times$ the groups of units of $\mathcal{O}$ and $\mathfrak{o}$ respectively. Let $(V, h)$ be a Hermitian space over $E$.

2.1. Generalities

**Definition 2.1.** A Hermitian lattice $(L, h)$ over $\mathcal{O}$ in $(V, h)$ consists a finitely generated $\mathcal{O}$-submodule $L$ of $V$, together with the Hermitian map $h$. We say that $(L, h)$ is a Hermitian lattice on $(V, h)$ if, in addition to the above property, we have $EL = V$.

We usually denote the pair $(L, h)$ by $L$ for convenience, with the assumption that the Hermitian map is understood. $L$ is said to be non-degenerate if the underlying Hermitian space $V$ is non-degenerate.
Any Hermitian lattice $L$ over $\mathcal{O}$ on $V$ can be written in the form

$$L = a_1 v_1 + \cdots + a_n v_n,$$

where $a_1, \ldots, a_n$ are fractional ideals in $E$ and $\{v_1, \ldots, v_n\}$ is a basis of $V$. We call $n$ the rank of $L$. There is always a basis $\{w_1, \ldots, w_n\}$ of $V$ such that $L$ can be written as

$$L = \mathcal{O}w_1 + \cdots + \mathcal{O}w_{n-1} + \mathfrak{A}w_n,$$

where $\mathfrak{A}$ is a fractional ideal in $E$. We say that $L$ is a free Hermitian lattice if $\mathfrak{A}$ can be taken to be $\mathcal{O}$, and we call $\{w_1, \ldots, w_n\}$ a basis of $L$. When $\mathcal{O}$ is a principal ideal domain, $\mathfrak{A} = a \mathcal{O}$ for some $a \in E^\times$, and thus

$$L = \mathcal{O}w_1 + \cdots + \mathcal{O}w_{n-1} + \mathcal{O}(aw_n)$$

is a free Hermitian lattice.

**Theorem 2.2. (Invariant Factor Theorem)** Let $K$ and $L$ be Hermitian lattices over $\mathcal{O}$ on $V$, where $\dim V = n$. Then there are fractional ideals $a_1, \ldots, a_n, r_1, \ldots, r_n$ with $r_1 \supseteq \cdots \supseteq r_n$, and a basis $\{v_1, \ldots, v_n\}$ of $V$ such that

$$K = a_1 v_1 + \cdots + a_n v_n \quad \text{and} \quad L = r_1 a_1 v_1 + \cdots + r_n a_n v_n.$$

Further, the fractional ideals $r_1, \ldots, r_n$ are uniquely determined by $K$ and $L$, and we call them the invariant factors of $L$ in $K$.

**Definition 2.3.** Let $(V, h)$, $(W, g)$ be two Hermitian spaces over $E$. Let $L$ and $K$ be Hermitian $\mathcal{O}$-lattices on $V$ and $W$ respectively. We say that $L$ represents $K$, written $K \to L$, if there is a representation $\sigma$ from $W$ into $V$ such that $\sigma(K) \subseteq L$. Likewise, we say that $L$ and $K$ are isometric, and write $K \cong L$, if there is an isometry $\sigma$ from $W$ onto $V$ such that $\sigma K = L$.

Whenever we study classification or representation of a Hermitian lattice $K$ by another Hermitian lattice $L$, there is no loss of generality in assuming that they are in the same space $V$. In this setting, $K$ is represented by $L$ if and only if there exists $\sigma \in \text{U}(V)$ such that $\sigma K \subseteq L$, and $K$ is isometric to $L$ if and only if there
exists \( \sigma \in U(V) \) such that \( \sigma K = L \). The Hermitian lattice \( K \) is said to be properly represented by \( L \), written \( K \xrightarrow{SU} L \), if there is some \( \sigma \in SU(V) \) such that \( \sigma K \subseteq L \).

We are interested in the following fundamental question: can we determine, say by means of invariants, whether or not two given lattices \( K \) and \( L \) are isometric? This should be regarded as the integral analog of the work on Hermitian spaces in Chapter 1. And just as the question for spaces is a geometric interpretation of the classical problem on the fractional equivalence of Hermitian forms, the question for lattices can be regarded as a geometric interpretation of the classical question on the integral equivalence of Hermitian forms, although the set of Hermitian lattices is a more general category than the set of Hermitian forms. In fact it will be shown that finding the set of lattices isometric to a given free Hermitian lattice is the same as finding the integral equivalence class of a Hermitian form.

For each free Hermitian lattice \( L \), each choice of basis \( \{v_1, \ldots, v_n\} \) of \( L \) gives rise to a function \( f_L : \mathcal{O}^n \rightarrow F \) defined by

\[
f_L(x_1, \ldots, x_n) := h\left( \sum_{i=1}^n x_i v_i \right) = \sum_{i,j=1}^n h(v_i, v_j)x_i x_j.
\]

Such a function is called a Hermitian form associated to \( L \). Conversely, each Hermitian form \( f(x_1, \ldots, x_n) = \sum a_{ij} x_i x_j \) gives rise to a free Hermitian lattice

\[ L_f = \mathcal{O}v_1 + \cdots + \mathcal{O}v_n \]

with \( h(v_i, v_j) = a_{ij} \). In this way, an isometry class of free Hermitian lattices on a fixed Hermitian space corresponds to a class of Hermitian forms equivalent under integral invertible transformations.

When \( \mathcal{O} \) is not a principal ideal domain, not every Hermitian lattice is free. For this reason, we will adopt the more general definition Hermitian lattices.

**Definition 2.4.** Let \( L \) be a Hermitian lattice over \( \mathcal{O} \). The scale \( sL \) of \( L \) is the fractional ideal generated by the set \( \{h(v, w) : v, w \in L\} \), and the norm \( nL \) of \( L \) is the fractional ideal generated by the set \( \{h(v, v) : v \in L\} \).
2.1. GENERALITIES

Definition 2.5. A Hermitian lattice $L$ over $\mathcal{O}$ is said to be integral if $sL \subseteq \mathcal{O}$. And $L$ is said to be positive definite if $h(v, v) > 0$ for any non-zero vector $v \in L$.

Definition 2.6. A Hermitian lattice $L$ over $\mathcal{O}$ is said to be normal if $nL = sL$. Otherwise it is called subnormal.

Let $D_{E/F}^{-1} = \{a \in E : T(a\mathcal{O}) \subseteq \mathfrak{o}\}$, which is a fractional ideal in $E$ containing $\mathcal{O}$. The different of $E/F$ is defined to be the integral $\mathcal{O}$-ideal $D_{E/F}$. When there is no fear of confusion we will write $D$ for $D_{E/F}$. It follows that when $E/F$ is unramified or split, $D = \mathcal{O}$. For a fractional ideal $\mathfrak{a}$ in $E$, we define the trace $T(\mathfrak{a})$ of $\mathfrak{a}$ as the fractional $\mathcal{O}$-ideal generated by the traces of the elements of $\mathfrak{a}$. Similarly we define the norm $N(\mathfrak{a})$ of $\mathfrak{a}$ as the fractional $\mathcal{O}$-ideal generated by the norms of the elements in $\mathfrak{a}$.

Theorem 2.7. Let $L$ be a Hermitian lattice over $\mathcal{O}$. Then

\begin{equation}
T(sL) \subseteq nL \subseteq sL \subseteq D^{-1}nL.
\end{equation}

Proof. The second inclusion is trivial. We only need to check the first and the last ones. Let $v, w \in L$ and $a \in \mathcal{O}$. Then

$$T(ah(v, w)) = h(av + w, av + w) - h(av, av) - h(w, w) \in nL.$$  

Thus the first inclusion holds.

Let $\hat{n}L$ be the $\mathfrak{o}$-ideal generated by the set $\{h(v, v) : v \in L\}$. Then $nL = (\hat{n}L)\mathcal{O}$ and $(nL)^{-1} = (\hat{n}L)^{-1}\mathcal{O}$. In order to show that $sL(nL)^{-1} \subseteq D^{-1}$, it is enough to show that $h(v, w)b \in D^{-1}$ for any $v, w \in L$ and $b \in \hat{n}L$. Let $a$ be an element in $\mathcal{O}$, we can conclude that $T(h(v, w)ba) = bT(h(v, w)a) \in \mathfrak{o}$ by the first part of the proof.

Proposition 2.8. When $E/F$ is unramified or split, all Hermitian lattices over $\mathcal{O}$ are normal.

Proof. It follows Theorem 2.7 immediately.
2.1. GENERALITIES

**Definition 2.9.** Let \( L = a_1v_1 + \cdots + a_nv_n \). The dual of \( L \) is the Hermitian lattice \( L^\# := \{ v \in V : h(v, L) \subseteq \mathcal{O} \} \). The volume \( vL \) of \( L \) is defined to be the fractional ideal

\[
a_1\bar{a}_1 \cdots a_n\bar{a}_n\det(h(v_i, v_j)),
\]

where \( \bar{a}_i = \{ \bar{a} : a \in a_i \} \).

When \( L = \mathcal{O}v_1 + \cdots + \mathcal{O}v_n \) is a free Hermitian lattice, the volume \( vL \) is generated by \( \det(h(v_i, v_j)) \), which is called the determinant of \( L \), denoted by \( dL \). Suppose \( \{ w_1, \ldots, w_n \} \) is another basis of \( L \), then there is an integral invertible matrix \( T \) such that \( (h(v_i, v_j)) = T^*(h(w_i, w_j))T \). Therefore \( dL \) is well defined modulo the norms of units.

The following observations for the dual lattice are straightforward:

1. \( L^\# = \bar{a}_1^{-1}w_1 + \cdots + \bar{a}_n^{-1}w_n \), where \( \{ w_1, \ldots, w_n \} \) is the dual basis of \( \{ v_1, \ldots, v_n \} \), i.e., \( \{ w_1, \ldots, w_n \} \) is another basis of \( V \) such that \( h(v_i, w_j) = 1 \) when \( i = j \) and 0 otherwise;
2. \( vL^\# = (vL)^{-1} \);
3. \( (bL)^\# = \bar{b}^{-1}L^\# \) for any fractional \( \mathcal{O} \)-ideal \( b \).

**Definition 2.10.** A Hermitian lattice \( L \) is said to be \( a \)-modular if \( vL = (aL)^n \) and \( a = sL \), where \( n \) is the rank of \( L \). A Hermitian lattice \( L \) is called \( a \)-maximal if \( nL \subseteq a \), and if \( L \subseteq K \) with \( nK \subseteq a \) implies \( L = K \).

We will state without proof the following results, which follows from the proofs of the analogous results for quadratic forms (see \([22, \S 82G]\)). Let \( L \) be a Hermitian lattice over \( \mathcal{O} \).

**Proposition 2.11.** \( L \) is \( a \)-modular if and only if \( L = aL^\# = \{ v \in EL : h(v, L) \subseteq a \} \).

**Definition 2.12.** Let \( M \) be a sublattice of \( L \). We say that \( M \) splits \( L \) if \( L = M \perp J \). In this case \( M \) (as well as \( J \)) is called a component of \( L \).
PROPOSITION 2.13. Let $M$ be an $\mathfrak{a}$-modular sublattice of $L$. Then $M$ splits $L$ if and only if $h(M, L) \subseteq \mathfrak{a}$.

COROLLARY 2.14. If $M$ is an $\mathfrak{a}$-modular sublattice of $L$ with $\mathfrak{a}(L) = \mathfrak{a}$, then $M$ splits $L$.

2.1.1. The localization of Hermitian lattices. Throughout this section we assume that $F$ is a number field and $E$ is a quadratic extension of $F$.

For a finite prime $p$ of $F$, recall that $E_p = E \otimes_F F_p$ and $n_p = [E_{\mathfrak{P}} : F_p]$ where $\mathfrak{P}$ is a prime in $E$ dividing $p$.

Let $\mathfrak{a}$ be a fractional ideal in $E$ and define $\mathfrak{a}_p$ to be the closure of $\mathfrak{a}$ in $E_p$. When $n_p = 2$, there is only one prime $\mathfrak{P}$ in $E$ lying above $p$, then $\mathfrak{a}_p = \mathfrak{a}_0$. When $n_p = 1$, there are two primes $\mathfrak{P}_1$ and $\mathfrak{P}_2$ in $E$ lying above $p$, then $\mathfrak{a}_p = p^{e_1} \times p^{e_2}$, where $e_i$ is the order of $\mathfrak{a}$ at $\mathfrak{P}_i$.

Let $L$ be a Hermitian $\mathcal{O}$-lattice on $V$. By the localization $L_p$ of $L$ in $V_p$ at the prime $p$ we mean the $\mathcal{O}_p$-module generated by $L$ in $V_p$. If we take a basis $\{v_1, \ldots, v_n\}$ for $V$ such that

$$L = \mathfrak{a}_1v_1 + \cdots + \mathfrak{a}_nv_n,$$

then

$$L_p = \mathfrak{a}_1pv_1 + \cdots + \mathfrak{a}_npv_n.$$

REMARK 2.15. Let $\mathfrak{a}$ be a fractional ideal in $E$. Then $\mathfrak{a}_p = \mathcal{O}_p$ for almost all primes spots $p$ on $F$.

REMARK 2.16. Let $L, M$ be two Hermitian $\mathcal{O}$-lattices on $V$. Then $L_p = M_p$ for almost all prime spots $p$ on $F$. 
Definition 2.17. Let $L$ be a Hermitian $\mathcal{O}$-lattice on $V$. The class, genus and special genus of $L$ are defined respectively by

$$
\text{cls}(L) := \{ K \text{ on } V : K = \sigma L, \ \sigma \in U(V) \};
$$

$$
\text{gen}(L) := \{ K \text{ on } V : K_p = \sigma_p L_p, \ \sigma_p \in U(V_p) \text{ for all finite primes } p \};
$$

$$
\text{gen}^0(L) := \{ K \text{ on } V : K_p = \varphi \circ \phi_p L_p \text{ for some } \varphi \in U(V) \text{ and } \phi_p \in SU(V_p) \text{ for each finite prime } p \}.
$$

Proposition 2.18. (Shimura, [27, Lemma 5.2]) Let $L$ be a Hermitian $\mathcal{O}$-lattice on $V$. Let $M_p$ be a Hermitian $\mathcal{O}_p$-lattice on $V_p$ for each finite prime spot $p$ on $F$. Then there exists a Hermitian $\mathcal{O}$-lattice $M$ on $V$ such that $M_p = M_p$ for every $p$ if and only if $M_p = L_p$ for all but a finite number of $p$. If such a lattice $M$ exists, we have $M = \cap_p (M_p \cap V)$.

Let $K$ and $L$ be Hermitian lattices on $V$. We usually use the notation “$K \rightarrow \text{gen}(L)$” when there is a representation $K_p \rightarrow L_p$ at each finite prime $p$ of $F$. The following proposition is very important in the representation theory of Hermitian lattices.

Proposition 2.19. Let $L$ be a Hermitian lattice on $V$, and let $K$ be a non-degenerate Hermitian lattice in $V$ such that $K \rightarrow \text{gen}(L)$. Then $K$ is represented by some Hermitian lattice $M \in \text{gen}(L)$. Moreover, if $\text{rank} K < \text{rank} L$, there is some Hermitian lattice $N \in \text{gen}^0(L)$ such that $K \rightarrow N$.

Proof. Let $S$ be the set of all finite prime spots on $F$. We take a finite subset $T$ of $S$ such that $K_p \subseteq L_p$ for any $p \in S \setminus T$. Since there is a representation $K_p \rightarrow L_p$ for each $p$ in $T$, there is an isometry $\varphi_p \in U(V_p)$ such that $K_p \subseteq \varphi_p L_p$.

For the first assertion, we define $M$ to be the Hermitian lattice on $V$ for which

$$
M = \begin{cases} 
\varphi_p L_p, & \text{if } p \in T; \\
L_p, & \text{otherwise}.
\end{cases}
$$
Then $K_p \subseteq M_p$ for all $p$ in $S$, hence $K \subseteq M$. Clearly $M \in \text{gen}(L)$.

Now let us consider the second assertion. Suppose that $\det \varphi_p = \alpha \neq 1$, and $V_p = W_p \perp E_p v_0$ where $E_p K_p \subseteq W_p$. Since $N\alpha = 1$, the map $\tau_p : V_p \rightarrow V_p$ defined by

$$\tau_p v = \begin{cases} v, & \text{if } v \in W_p; \\ \alpha^{-1}v, & \text{if } v \in E_p v_0, \end{cases}$$

is an isometry in $U(V_p)$ and $\det \tau_p = \alpha^{-1}$. Thus $\tau_p \varphi_p \in \text{SU}(V_p)$ and $K_p \subseteq \tau_p \varphi_p L_p$ for each $p \in T$. Define a Hermitian lattice

$$N = \begin{cases} \tau_p \varphi_p L_p, & \text{if } p \in T; \\ L_p, & \text{otherwise.} \end{cases}$$

Then $K \rightarrow N$ and $N \in \text{gen}^0(L)$. \hfill \qed

### 2.2. Local theory of Hermitian lattices

Throughout this section, unless we state otherwise, $F_p$ will denote a $p$-adic field and $E_p$ a quadratic extension of $F_p$ or the direct sum $F_p \times F_p$ of two copies of $F_p$. As usual, we use $O_p$ and $\mathfrak{o}_p$ to denote the rings of integers of $E_p$ and $F_p$ respectively. We let $\pi_p$ stand for a generator of the maximal ideal $p$ of $\mathfrak{o}_p$.

**Proposition 2.20.** Let $L$ be a Hermitian lattice over $O_p$. Then

$$L = M_1 \perp \cdots \perp M_t,$$

where all the $M_i$ are modular lattices of rank 1 or 2. Moreover, when $E_p/F_p$ is inert or split, we can choose all the $L_i$ to be of rank 1.

**Proof.** First suppose that $L$ is normal. Then there is a vector $v \in L$ such that $h(v, v)O_p = nL = sL$. Let $M = O_p v$, which is a $sL$-modular sublattice of $L$. Hence by Corollary 2.14, $M$ splits $L$.

Now suppose that $L$ is subnormal. Then $nL \subseteq sL$. Hence $sL = (\pi_p)^s$ and $nL = (\pi_p)^f$, with $f > s$. Take $v, w \in L$ such that $h(v, w)O_p = sL$. We claim that
$M = \mathcal{O}_p v + \mathcal{O}_p w$ is a $sL$-modular sublattice of $L$, and thus it splits $L$. Clearly, $sM = h(v, w)\mathcal{O}_p = sL$. Now,

$$vM = \left( h(v, v)h(w, w) - h(v, w)\overline{h(v, w)} \right) \mathcal{O}_p$$

$$= (\pi_p^{2f} a - \pi_p^{2s} u)\mathcal{O}_p$$

$$= \pi_p^{2s} \mathcal{O}_p,$$

where $a \in \mathcal{O}_p$ and $u \in \mathcal{O}_p^\times$. Thus $vM = (sM)^2$ and we prove our claim.

In particular, when $p$ is inert or split, by Proposition 2.8 every Hermitian lattice $L$ over $\mathcal{O}_p$ is normal. By the above discussion, $L$ has an orthogonal basis. $\square$

**Definition 2.21.** (Jordan splitting) A Jordan splitting of $L$ is a decomposition

$$L = L_1 \perp \cdots \perp L_t,$$

where $L_i$ are modular and $sL_1 \nmid sL_2 \nmid \cdots \nmid sL_t$.

The previous proposition shows that any Hermitian lattice over $\mathcal{O}_p$ has a Jordan splitting. Two Jordan splittings $L = L_1 \perp \cdots \perp L_t$ and $K = K_1 \perp \cdots \perp K_s$ are said to be of the same type if $t = s$, $\text{rank} L_i = \text{rank} K_i$, $sL_i = sK_i$, and $L_i$ and $K_i$ are both normal or both subnormal for every $i$. The next result is the Hermitian analogue of Proposition 91:9 in [22].

**Proposition 2.22.** Two Jordan splittings of isometric lattices are always of the same type.

Jordan splittings play a crucial role in the classification problem and the representation problem. It is from these splittings that Jacobowitz and Johnson obtained the complete solution of these two problems in the local case.
2.3. Representations of Hermitian lattices over local field

We present here necessary and sufficient conditions for the integral representation of Hermitian lattices over local fields. The discussion will be divided into the following four cases, namely those where $E_p$ is

1. the sum $F_p \times F_p$ of two copies of $F_p$;
2. an unramified quadratic extension of $F_p$;
3. a non-dyadic ramified quadratic extension of $F_p$;
4. a dyadic ramified quadratic extension of $F_p$.

2.3.1. The split case. Let $E_p = F_p \times F_p$ and $L$ be a Hermitian lattice over $O_p$. The next result shows how much simpler the structure of a Hermitian $O_p$-lattice is in this split case.

**Proposition 2.23.** (Shimura, [27, Proposition 3.2]) Assume that $E_p = F_p \times F_p$. Let $V$ be a Hermitian space over $E_p$ and $L$ be an $O_p$-lattice on $V$. Then there exists a basis $\{z_1, \ldots, z_n\}$ of $V$ and fractional ideals $a_1O_p \supset a_2O_p \supset \cdots \supset a_nO_p$ such that:

1. $L = \sum_{i=1}^{n}(o_p + o_pa_i)e_iz_i$;
2. $h(z_i, z_j) = \delta_{ij}$;
3. $nL = sL = a_1O_p$;
4. $L$ is maximal if and only if $a_1O_p = \cdots = a_nO_p$.

This proposition implies that $L = O_p(1, a_1)z_1 + \cdots + O_p(1, a_n)z_n$. It is easy to check that $\{(1, a_i)z_i\}_{1 \leq i \leq n}$ is a basis of $L$, and with this basis

$L \cong \langle a_1 \rangle \perp \cdots \perp \langle a_n \rangle$,

where $a_1O_p \supset \cdots \supset a_nO_p$. We call such a splitting a *canonical decomposition* for $L$.

The following lemma is the necessary and sufficient condition for the representation of Hermitian lattices in the split case.
Lemma 2.24. (Gerstein, [3, Lemma 1.1]) Let $L$ and $M$ be Hermitian lattices over $\mathcal{O}_p$ with canonical decompositions $L \cong \langle a_1 \rangle \perp \cdots \perp \langle a_n \rangle$ and $M \cong \langle b_1 \rangle \perp \cdots \perp \langle b_m \rangle$. Then $M \to L$ if and only if $m \leq n$ and $b_i \mathcal{O}_p \subseteq a_i \mathcal{O}_p$ for $1 \leq i \leq m$.

Corollary 2.25. Let $L$ and $M$ be Hermitian lattices over $\mathcal{O}_p$ with canonical decompositions $L \cong \langle a_1 \rangle \perp \cdots \perp \langle a_n \rangle$ and $M \cong \langle b_1 \rangle \perp \cdots \perp \langle b_m \rangle$. Then $L \cong M$ if and only if $m = n$ and $a_i \mathcal{O}_p = b_i \mathcal{O}_p$ for every $1 \leq i \leq n$.

A Hermitian lattice $L$ over $\mathcal{O}_p$ is $\mathfrak{a}$-modular if and only if $\mathfrak{a} = a_1 \mathcal{O}_p = a_2 \mathcal{O}_p = \cdots = a_n \mathcal{O}_p$. An $\mathfrak{a}$-modular lattice is also $\mathfrak{a}$-maximal. The following two corollaries follow from Lemma 2.24 directly:

Corollary 2.26. Up to isometry, there is only one $\mathfrak{a}$-modular (or $\mathfrak{a}$-maximal) Hermitian lattice over $\mathcal{O}_p$ of a given rank.

Corollary 2.27. Two Hermitian lattices over $\mathcal{O}_p$ are isometric if and only if they have the same Jordan type.

In the following subsections, we assume that $E_p$ is a quadratic extension of the $p$-adic field $F_p$ and let $\mathfrak{P} = \pi \mathcal{O}_p$ be the prime ideal lying above $p$.

Definition 2.28. For each integer $i$, we define
\[
H(i) = \begin{pmatrix} 0 & \pi^i \mathfrak{P} \\ \pi^i \mathfrak{P} & 0 \end{pmatrix}.
\]

For a giving Jordan splitting $L = L_1 \perp \cdots \perp L_t$ and for all $i$, we write $L(i) = 0$ if $\mathfrak{P}^i \supset sL$ and otherwise
\[
L(i) = L_1 \perp \cdots \perp L_\mu
\]
where $L_1, \ldots, L_\mu$ are all the components of the splitting whose scales contain $\mathfrak{P}^i$. For $1 \leq j \leq t$, we write
\[
L[j] = L_1 \perp \cdots \perp L_j.
\]
2.3. REPRESENTATIONS OF HERMITIAN LATTICES OVER LOCAL FIELD

2.3.2. The unramified case. Here we assume that the field extension $E_p/F_p$ is unramified. Then $\pi_p$ is also a generator of the maximal ideal $\mathfrak{p}$ of $\mathcal{O}_p$. Following from 63:16 in [22], we have $\mathcal{N}(E_p^x) = \mathfrak{o}_p^x F^\times 2$ and $\mathcal{N}(\mathcal{O}_p^x) = \mathfrak{o}_p^x$.

**Theorem 2.29.** (Johnson, [9, Theorem 4.4]) Suppose $E_p/F_p$ is an unramified extension. Let $L$ and $K$ be two Hermitian lattices over $\mathcal{O}_p$ with Jordan splittings $L = L_1 \perp \cdots \perp L_t$ and $K = K_1 \perp \cdots \perp K_s$. Then $L \to K$ if and only if $E_p L(i) \to E_p K(i)$ for all $i$.

We have a similar result for $\mathfrak{a}$-modular Hermitian lattices over $\mathcal{O}_p$ as in split case.

**Corollary 2.30.** Let $K$ and $L$ be two $\mathfrak{a}$-modular Hermitian lattices over $\mathcal{O}_p$. Then $K \cong L$ if and only if they have the same rank.

**Proof.** We only need to show that $\text{rank} K = \text{rank} L$ implies $K \cong L$; the other direction is obvious.

Without loss of generality, we may assume that $L$ and $K$ are unimodular. Recall that every Hermitian lattice over $\mathcal{O}_p$ are free, and since they are both unimodular, we have $dK \mathcal{O}_p = \mathfrak{v} K = \mathfrak{v} L = dL \mathcal{O}_p$. Thus $dK \equiv dL \pmod{\mathfrak{o}_p^x}$. This implies that $dK \equiv dL \pmod{\mathcal{N}(\mathcal{O}_p^x)}$ as $\mathcal{N}(\mathcal{O}_p^x) = \mathfrak{o}_p^x$ in this case.

Note that when $i < 0$, $E_p K(i) = E_p L(i) = 0$; when $i \geq 0$, $E_p K(i) = E_p K$ and $E_p L(i) = E_p L$. By Proposition 1.17, $E_p K(i) \cong E_p L(i)$ for any integer $i$. Thus we have proved our statement by applying the above theorem.

From the above corollary, we see that a $\mathfrak{P}^i$-modular Hermitian lattice over $\mathcal{O}_p$ can be written as

$$L \cong \langle \pi_p^1 \rangle \perp \cdots \perp \langle \pi_p^i \rangle$$

for any integer $i$. The following corollary is straightforward.

**Corollary 2.31.** (Jacobowitz, [7, Theorem 7.1]) Two Hermitian lattices over $\mathcal{O}_p$ are isometric if and only if they have the same Jordan type.
2.3.3. The non-dyadic ramified case. We assume that \( E_p/F_p \) is a non-dyadic ramified extension. In this case \( E_p = F_p(\sqrt{\theta}) \) where \( \theta \) is a generator of \( \mathfrak{p} \) and we can take \( \pi \mathfrak{p} = \sqrt{\theta} \) as a generator of \( \mathfrak{P} \). The following proposition describes every \( \mathfrak{P}^i \)-modular Hermitian lattice over \( O_p \).

**Proposition 2.32.** (Jacobowitz, [7, Proposition 8.1]) Let \( E_p/F_p \) be a non-dyadic ramified extension and \( L \) be a \( \mathfrak{P}^i \)-modular Hermitian lattice over \( O_p \) of rank \( n \). Then

1. when \( i \) is even, \( L \cong \langle \theta^{i/2} \rangle \perp \cdots \perp \langle \theta^{i/2} \rangle \perp \langle \theta^{-(n-1)i/2}dL \rangle \);
2. when \( i \) is odd, \( L \cong \mathbb{H}(i) \perp \cdots \perp \mathbb{H}(i) \).

The next theorem provides us a sufficient and necessary condition for the representing a Hermitian lattice by another Hermitian lattice, which is similar to the unramified case.

**Theorem 2.33.** (Johnson, [9, Theorem 5.5])) Suppose \( E_p/F_p \) is a non-dyadic ramified extension. Let \( K \) and \( L \) be two Hermitian lattices over \( O_p \) with the Jordan splittings \( K = K_1 \perp \cdots \perp K_s \) and \( L = L_1 \perp \cdots \perp L_t \). Then \( K \rightarrow L \) if and only if \( E_pK(i) \rightarrow E_pL(i) \) for all \( i \).

2.3.4. The dyadic ramified case. Now we assume that \( E_p/F_p \) is a dyadic ramified extension. In this case \( E_p = F_p(\sqrt{\theta}) \) where \( \theta \) is either a prime element or a unit in \( F_p \).

The solution of the representation problem for two modular Hermitian lattices can be easily stated as follows.

**Theorem 2.34.** (Johnson, [9, Theorem 7.5]) Suppose \( E_p/F_p \) is a dyadic ramified extension. Let \( K \) and \( L \) be two modular lattices with \( sK \subseteq sL, nK \subseteq nL, \) and \( E_pK \rightarrow E_pL \). Then \( K \rightarrow L \) if and only if \( \text{rank}K < \text{rank}L \) or \( (sK)^2(nK)^{-1} \subseteq (sL)^2(nL)^{-1} \) when \( \text{rank}K = \text{rank}L \). In particular, \( L \) contains a sublattice \( L' \) on \( E_pL \) such that

\[
L' \cong J \perp K,
\]
where \( J \) is modular with \( s(J) \supseteq s(K) \) and \( (sJ)^2(nJ)^{-1} = (sK)^2(nK)^{-1} \cap (sL)^2(nL)^{-1} \).

Suppose now that \( K \) and \( L \) are Hermitian lattices which are not necessarily modular. First we introduce the concept of a saturated Jordan splitting. We know that if \( L = \perp L_i = \perp M_i \) are two Jordan splittings of \( L \), then \( sL_i = sM_i \) for all \( i \). Thus we define the \( i^{th} \) fundamental scale of \( L \) to be the fractional ideal \( s_i = sL_i \). We also define the \( i^{th} \) fundamental norm of \( L \) to be the fractional ideal \( n_i = nL_{s_i} \), where \( L_{s_i} = \{ v \in L : h(v, L) \subseteq s_i \} \).

**Definition 2.35.** A Jordan splitting

\[
L = L_1 \perp \cdots \perp L_t
\]
satisfying \( nL_i = n_i \) for \( 1 \leq i \leq t \), is called a saturated Jordan splitting.

The existence of saturated Jordan splittings was given by Johnson.

**Proposition 2.36.** (Johnson, [9, Proposition 8.1]) Every Hermitian lattice over \( \mathcal{O}_p \) has a saturated Jordan splitting.

Now let \( K = K_1 \perp \cdots \perp K_t \) and \( L = L_1 \perp \cdots \perp L_s \) be Jordan splittings of Hermitian lattices \( K \) and \( L \), respectively, where \( sK \subseteq sL \). We define a map \( \lambda : \{1, 2, \cdots, t\} \to \{1, 2, \cdots, s\} \) by setting \( \lambda(j) = \mu \) if \( sL_{\mu} \supseteq sK_j \supset sL_{\mu+1} \), and \( \lambda(j) = s \) otherwise.

Because we shall be working with fundamental scales and norms of Hermitian lattices, let us adopt a new notation to distinguish them from the scales and norms we defined before. We write \( s_j L \) and \( n_j L \) to denote the \( j^{th} \) fundamental scale and norm of a Hermitian lattice \( L \), respectively.

With these added notations, we can present the theorem for the general dyadic ramified case.

**Theorem 2.37.** (Johnson, [9, Proposition 9.4]) Let \( E_p/F_p \) be a dyadic ramified extension, and let \( K \) and \( L \) be two Hermitian lattices over \( \mathcal{O}_p \) with Jordan splittings
2.4. THE INDUCED QUADRATIC LATTICE

The induced quadratic lattice

It was shown in Chapter 1.2 that for every Hermitian space \((V,h)\) over \(E\), we can associate with it a quadratic space \((\hat{V},b)\) over \(F\). Now we turn to the integral side of this problem.

Given any Hermitian \(\mathcal{O}\)-lattice \(L\) on a Hermitian space \((V,h)\), we can view \(L\) as a quadratic \(\mathcal{O}\)-lattice on the quadratic space \((\hat{V},b)\). We denote this \(\mathcal{O}\)-lattice by \(\hat{L}\). In this section, we only outline those results we need. The proofs of Proposition 2.40 and Proposition 2.41 are from [24].

**Lemma 2.38.** Let \(K\) and \(L\) be Hermitian lattices over \(\mathcal{O}\). If \(K \in \text{gen}(L)\), then the corresponding quadratic lattice \(\hat{K} \in \text{gen}(\hat{L})\).

**Proof.** It is clear that \(\hat{K}\) and \(\hat{L}\) are on the same quadratic space. Since \(K \in \text{gen}(L)\), for any finite prime spot \(p\) on \(F\), there exists some \(\sigma_p \in U(V_p)\) such that \(\sigma_p K_p = L_p\). Since an \(E_p\)-linear map is definitely an \(F_p\)-linear map, we can also view \(\sigma_p\) as an element in \(U(V_p)\). Therefore \(\hat{K} \in \text{gen}(\hat{L})\).

In the remaining part of this section, we want to describe the relation between the volumes \(v\hat{L}\) and \(vL\), which is useful in the proof of the main theorem.
Let \( p \) be a finite prime spot on \( F \). Then \( E_p \) is either a quadratic extension of \( F_p \) or the direct sum \( F_p \times F_p \) of two copies of \( F_p \). In the local case, we can always choose an integral basis of the form \( \{1, \omega\} \), and the discriminant \( d_{E_p} \) of \( E_p \) over \( F_p \) is \((\omega - \overline{\omega})^2\). Note that in the split case we can choose \( \omega = (1, 0) \) and hence \( d_{E_p} = 1 \).

Put \( \alpha := \mathbb{T}(\omega) \).

**Lemma 2.39.** Let \( \phi \) be an element in \( \text{End}_{E_p}(V_p) \), and denote by \( \hat{\phi} \) the endomorphism \( \phi \) considered as an \( F_p \)-endomorphism. Then

\[
\det \hat{\phi} = \mathbb{N}(\det \phi).
\]

**Proof.** When \( E_p = F_p(\omega) \) is a quadratic extension of \( F_p \). Let \( \{v_1, ..., v_n\} \) be a basis of \( V_p \) over \( E_p \), and write

\[
\phi(v_j) = \sum_{i=1}^{n} a_{ij}v_i = \sum_{i=1}^{n} (b_{ij} + c_{ij}\omega)v_i.
\]

Now let \( \{v_1, ..., v_n, \omega v_1, ..., \omega v_n\} \) be the induced basis of \( \hat{V}_p \) over \( F_p \). Then the matrix of \( \hat{\phi} \) is of the form

\[
\begin{pmatrix}
(b_{ij}) & (\omega^2 c_{ij}) \\
(c_{ij}) & (b_{ij})
\end{pmatrix},
\]

and

\[
\det \hat{\phi} = \det \begin{pmatrix}
(b_{ij}) & (\omega^2 c_{ij}) \\
(c_{ij}) & (b_{ij})
\end{pmatrix} = \det \begin{pmatrix}
(b_{ij} + \omega c_{ij}) & (0) \\
(0) & (b_{ij} - \omega c_{ij})
\end{pmatrix} = \mathbb{N}(\det \phi).
\]

When \( E_p = F_p \times F_p \), we can show that this statement is also true by the similar argument.

In the next proposition, recall that for a Hermitian lattice \( L_p \) over \( \mathcal{O}_p \), its volume \( vL_p \) is generated by its discriminant \( dL_p \).

**Proposition 2.40.** Let \( E_p \) be a quadratic extension over \( F_p \) or the direct sum \( F_p \times F_p \) of two copies of \( F_p \), and let \( L_p \) be a Hermitian \( \mathcal{O}_p \)-lattice on \( V_p \) of rank \( n \). Suppose \( \hat{L}_p \) is the underlying quadratic lattice over \( \mathcal{o}_p \) with the bilinear form \( b = \frac{1}{2} \mathbb{T} \circ h \). Then

\[
d\hat{L}_p = (dL_p)^2(-d_{E_p}/4)^n.
\]
If we take \( b = T \circ h \) instead, then

\[
dL_p = (dL_p)^2(-d_{E_p})^n.
\]

**Proof.** We only deal with the case when \( b = \frac{1}{2} T \circ h \). When we take \( b = T \circ h \) instead, the proof is similar.

Let \( H \) be the Gram matrix of \( L_p \) with respect to the basis \( \{v_1, ..., v_n\} \), and \( B \) be the Gram matrix of \( \hat{L}_p \) with respect to the basis \( \{v_1, ..., v_n, \omega v_1, ..., \omega v_n\} \). Since in the local case, every Hermitian space has an orthogonal basis, we can find some matrix \( T \in \text{GL}_n(E_p) \) such that

(2.2) \[
T^* HT = \text{diag}(a_1, ..., a_m) =: D.
\]

We denote also by \( T \) the corresponding endomorphism of \( V_p \) over \( E_p \).

Now we view \( T \) as an endomorphism of \( \hat{V}_p \) over \( F_p \), and let \( \hat{T} \) denote the matrix of this linear map with respect to the basis \( \{v_1, ..., v_n, \omega v_1, ..., \omega v_n\} \). We claim that

(2.3) \[
\hat{T}^* B \hat{T} = \begin{pmatrix}
D & \frac{1}{2} \alpha D \\
\frac{1}{2} \alpha D & N(\omega) D
\end{pmatrix}.
\]

In terms of the form \( h \), equation (2.2) says: \( h(Tv_i, Tv_j) = \delta_{ij} a_i \), where \( \delta_{ij} \) is Kronecker’s delta. Therefore for \( b \) we have

\[
b(\hat{T}v_i, \hat{T}v_j) = \frac{1}{2} T(h(Tv_i, Tv_j)) = \delta_{ij} a_i;
\]

\[
b(\hat{T}\omega v_i, \hat{T}\omega v_j) = \frac{1}{2} T(\omega \overline{h}(Tv_i, Tv_j)) = N(\omega) \delta_{ij} a_i;
\]

\[
b(\hat{T}v_i, \hat{T}\omega v_j) = \frac{1}{2} T(\overline{h}(Tv_i, Tv_j)) = \frac{1}{2} \alpha \delta_{ij} a_i;
\]

\[
b(\hat{T}\omega v_i, \hat{T}v_j) = \frac{1}{2} T(h(Tv_i, Tv_j)) = \frac{1}{2} \alpha \delta_{ij} a_i.
\]

This proves our claim.

Combining the results from (2.2) and (2.3), we obtain that

\[
\det B (\det \hat{T})^2 = (\det H)^2 (N(\det T))^2 (-d_{E_p}/4)^n.
\]

By Lemma 2.39, \( N(\det T) = \det \hat{T} \). Therefore

\[
\det B = (\det H)^2 (-d_{E_p}/4)^n,
\]
that is
\[ d \hat{L}_p = (dL_p)^2(-d_{E_p}/4)^n. \]

In the global case, we define the discriminant \( D_{E/F} \) of \( E \) over \( F \) to be the integral ideal of \( \mathfrak{o} \) which is generated by the discriminants \( d(\omega_1, \omega_2) \) of all the bases \( \omega_1, \omega_2 \) of \( E/F \) contained in \( \mathcal{O} \). If there is no fear of confusion, we will write \( D_E \) simply. We have the following relation between the volumes \( v\hat{L} \) and \( vL \).

**Proposition 2.41.** Let \( E/F \) be a quadratic extension of number fields, and let \( L \) be a Hermitian \( \mathcal{O} \)-lattice of rank \( n \). Suppose \( \hat{L} \) is the underlying quadratic \( \mathbb{Z} \)-lattice with \( b = \frac{1}{2} T \circ h \). Then
\[ v\hat{L} = (vL)^2(D_{E}/4)^n \]
as \( \mathcal{O} \) ideals. If we take \( b = T \circ h \) instead, then
\[ v\hat{L} = (vL)^2(D_{E})^n. \]

**Proof.** We only consider the case when \( b = \frac{1}{2} T \circ h \). The proof when \( b = T \circ h \) is similar.

It suffices to show that
\[ (v\hat{L})_p = ((vL)^2(D_{E}/4)^n)_p \]
as \( \mathcal{O}_p \) ideals for all finite primes \( p \). By Proposition 2.40, we have
\[ v\hat{L}_p = (vL_p)^2(d_{E_p}/4)^n \]
as \( \mathcal{O}_p \) ideals for all finite primes \( p \). By the definition of localization, we know that for any Hermitian lattice \( L \) over \( \mathcal{O} \), \((vL)_p = vL_p \) and \((\hat{L})_p = \hat{L}_p \). If \( p \) is non-split, clearly \( (D_{E})_p = d_{E_p} \mathfrak{o}_p \). If \( p \) splits, then by definition \( d_{E_p} \mathfrak{o}_p = \mathfrak{o}_p \), and on the other hand \( p \nmid D_E \), thus \( (D_{E})_p = \mathfrak{o}_p \). Hence \( (D_{E})_p = d_{E_p} \mathfrak{o}_p \) for all finite primes \( p \). Therefore (2.5) holds.

\[ \Box \]
CHAPTER 3

Neighbors of Hermitian lattices over number fields

In this chapter we present the theory of neighbors of Hermitian lattices over number fields, which is due to Schiemann [25] and is considered to be the Hermitian analog of the theory of neighbors of quadratic lattices developed by Kneser [14]. In Section 1, we present the basic definitions in the theory of neighbors. Then in Section 2, we present the relation among the neighborhood, genus, and special genus of a Hermitian lattice $L$.

Let $E/F$ be a quadratic extension of number fields, and let $V$ be a Hermitian space over $E$. By $\mathcal{O}$, $\mathfrak{o}$ we denote the ring of integers of $E$ and $F$, respectively. We use $\Omega_F$ to denote the set of all finite prime spots on $F$.

3.1. Basic definitions

**Definition 3.1.** Let $L$ be an integral Hermitian lattice over $\mathcal{O}$ on $V$, $\mathfrak{P}$ be a prime ideal in $\mathcal{O}$ which does not divide $\nu(L)$. An integral Hermitian lattice $M$ over $\mathcal{O}$ on $V$ is called a $\mathfrak{P}$-neighbor of $L$ if and only if we have the following $\mathcal{O}$-module isomorphisms:

$$M/(L \cap M) \cong \mathcal{O}/\mathfrak{P} \quad \text{and} \quad L/(L \cap M) \cong \mathcal{O}/\mathfrak{P}.$$

**Remark 3.2.** Suppose that the Hermitian lattice $M$ is a $\mathfrak{P}$-neighbor of $L$. Based on the above definition, we have the following observations:

1. $L$ is a $\mathfrak{P}$-neighbor of $M$. 

36
(2) By the Invariant Factor Theorem, there are fractional ideals \(a_1, \ldots, a_n\) in \(E\) and a basis \(\{v_1, \ldots, v_n\}\) of \(V\), such that

\[
L = a_1v_1 + a_2v_2 + \cdots + a_{n-1}v_{n-1} + a_nv_n
\]

and

\[
M = p^{-1}a_1v_1 + a_2v_2 + \cdots + a_{n-1}v_{n-1} + pa_nv_n.
\]

(3) \(vL = vM\). Moreover, \(L\) is unimodular if and only if \(M\) is unimodular.

(4) \(PM \subseteq L\) and \(PL \subseteq M\).

**Definition 3.3.** Let \(L\) be an integral Hermitian lattice over \(O\) on \(V\), \(\mathfrak{P}\) be a prime ideal in \(O\) which does not divide \(v(L)\). A vector \(v \in L \setminus \mathfrak{P}L\) is called *admissible* if \(h(v, v) \in \mathfrak{P}\mathfrak{P}\). We define the Hermitian lattice

\[
L(\mathfrak{P}, v) := \mathfrak{P}^{-1}v + \{w \in L \mid h(v, w) \in \mathfrak{P}\}.
\]

If there are only neighbors of one prime ideal \(\mathfrak{P}\) in a specific context, we use the notation \(L(v)\) instead of \(L(\mathfrak{P}, v)\). The following lemma indicates the fact that a Hermitian lattice \(M\) is a \(\mathfrak{P}\)-neighbor of \(L\) if and only if it is defined at some admissible vector \(v\).

**Lemma 3.4. (Schiemann, [25, Lemma 2.2])** Let \(L\) be an integral Hermitian lattice over \(O\) on \(V\), and \(\mathfrak{P}\) be a prime ideal in \(O\) which does not divide \(v(L)\). A Hermitian lattice \(M\) over \(O\) is a \(\mathfrak{P}\)-neighbor of \(L\) if and only if there is an admissible vector \(v \in L\) such that \(M = L(v)\).

What makes this notion so valuable is the following fact: starting with a Hermitian lattice \(L\), by successive construction of \(\mathfrak{P}\)-neighbors, we can obtain every isometry classes of Hermitian lattices containing a representative \(M\) which is locally equal to \(L\) at all prime spots \(q \in \Omega_F \setminus \{p\}\) and \(vM = vL\).

**Definition 3.5.** Let \(K\) and \(L\) be integral Hermitian \(O\)-lattices on \(V\), and \(\mathfrak{P}\) be a prime ideal in \(O\) which does not divide \(vL\). We write “\(L \sim K\)” when there are
lattices $L_0 = L, L_1, \ldots, L_t = K$ such that $L_{i+1}$ is a $\mathfrak{P}$-neighbor of $L_i$ for $0 \leq i \leq t-1$.

The neighborhood of $L$ at $\mathfrak{P}$ is

$$\mathfrak{N}(L, \mathfrak{P}) := \{M \text{ on } V : L \sim K \text{ for some } K \in \text{cls}(M)\}.$$ 

The (oriented) neighbor graph $\text{NG}(L, \mathfrak{P})$ of $L$ at $\mathfrak{P}$ is the graph with vertices from $\{\text{cls}(M) \mid M \in \mathfrak{N}(L, \mathfrak{P})\}$ and the edges $\text{cls}(M) \to \text{cls}(N)$ for $M, N \in \mathfrak{N}(L, \mathfrak{P})$ with $M$ a $\mathfrak{P}$-neighbor of $N$.

The following proposition shows that if there is some non-negative integer $e$ such that $\mathfrak{P}^e K \subseteq L$, then we can always construct a sequence of integral Hermitian lattices such that $L \sim K$ through them.

**Proposition 3.6.** (Schiemann, [25, Proposition 2.4]) Let $K$ and $L$ be integral Hermitian $\mathcal{O}$-lattices on $V$ such that $vL = vK$. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}$ such that $\mathfrak{P} \nmid vL$. Assume that there is an $e \in \mathbb{N} \cup \{0\}$ such that $\mathfrak{P}^e K \subseteq L$. Then there are integral Hermitian lattices $L_0 = L, L_1, \ldots, L_k = K$ such that $L_{i+1}$ is a $\mathfrak{P}$-neighbor of $L_i$ for all $0 \leq i \leq k-1$.

The proposition below is essential in showing the relation among the neighborhood, genus and special genus of a Hermitian lattice $L$, which will be stated in the next section.

**Proposition 3.7.** (Schiemann, [25, Proposition 2.5]) Let $L$ be an integral Hermitian lattice over $\mathcal{O}$. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}$ such that $\mathfrak{P} \nmid vL$, and set $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}$. Then

$$\mathfrak{N}(L, \mathfrak{P}) = \{M \text{ on } V : vL = vM \text{ and there exists some } \phi \in U(V) \text{ such that } L_q = \phi M_q \text{ for each } q \in \Omega_F \setminus \{\mathfrak{p}\}\}.$$ 

3.2. Neighborhood, genus and special genus

Let $L$ be a Hermitian lattice over $\mathcal{O}$. At some suitable $\mathfrak{P}$, the Strong Approximation Theorem for $SU(V)$ implies that a neighborhood $\mathfrak{N}(L, \mathfrak{P})$ contains at least
3.2. NEIGHBORHOOD, GENUS AND SPECIAL GENUS

the special genus of $L$ when $\text{rank} L \geq 2$. Strong Approximation on $\text{SU}(V)$ for indefinite Hermitian space $V$ was proved by Shimura [27]. For a survey of the general situation for classical groups, we refer the readers to the article of Kneser [15].

**Theorem 3.8. (Strong approximation)** Let $V$ be a Hermitian space over $E$ with $\dim V \geq 2$ and let $S \subseteq \Omega_F$. Assume that $V$ is indefinite or that $V_q$ is isotropic at a prime $q \in \Omega_F \setminus S$. Let $T$ be a finite set of primes with $T \subset S$. Let $L$ be a Hermitian lattice over $\mathcal{O}$ on $V$ and for all $p \in T$ let $\sigma_p \in \text{SU}(V_p)$. Then for every positive integer $e$ there exists $\sigma \in \text{SU}(V)$ such that

$$(\sigma - \sigma_p)L_p \subset p^e L_p, \ \forall \ p \in T \quad \text{and} \quad \sigma L_p = L_p, \ \forall \ p \in S \setminus T.$$  

**Remark 3.9.** We can choose $e$ large enough that $p^e L_p \subseteq \sigma_p L_p$ for each $p \in T$, which implies that $\sigma L_p \subseteq \sigma_p L_p$. Since $\sigma \in \text{SU}(V)$ and $\sigma_p \in \text{SU}(V_p)$, they preserve the volume of $L_p$, and hence $v(\sigma L_p) = vL_p = v(\sigma_p L_p)$. Thus $\sigma L_p = \sigma_p L_p$ for all $p \in T$.

**Corollary 3.10. (Schiemann, [25, Proposition 2.7])** Let $V$ be a Hermitian space on $E$ with $\dim V \geq 2$ and $L$ be a Hermitian lattice over $\mathcal{O}$ on $V$. Let $\mathfrak{P}$ be a prime in $\mathcal{O}$ such that $\mathfrak{P} \mid v(L)$, and set $p = \mathfrak{P} \cap \mathfrak{o}$. Assume that $V_p$ is isotropic or $V$ is indefinite. Then

$$\mathfrak{M}(L, \mathfrak{P}) \supseteq \gen^0(L).$$

**Proof.** Let $M \in \gen^0(L)$. Suppose that there is some $\tau \in U(V)$ and $\sigma_q \in \text{SU}(V_q)$ for each $q \in \Omega_F$ such that $\tau \sigma_q L_q = M_q$. Apply the Strong Approximation Theorem with $S = \Omega_F \setminus \{p\}$, $T = \{q : \tau^{-1} M_q \neq L_q\}$, and $e$ such that $q^e L_q \subseteq \sigma_q L_q$ for $q \in T$. Then we can find some $\sigma \in \text{SU}(V)$ with $\sigma L_q = \tau^{-1} M_q$ for all $q \in S$. Then the assertion is a consequence of Proposition 3.7. \qed

Notice that in the definite case, the hypothesis that $V_p$ is isotropic is true for all split primes $\mathfrak{P}$ as well as for $\dim V \geq 3$. So in these situations, the special genus is always contained in the neighborhood of $L$. The following proposition describes the relation between the neighborhood and genus of $L$. 

Proposition 3.11. Let $L$ be a Hermitian lattice over $\mathcal{O}$, $\mathfrak{P}$ be a prime in $\mathcal{O}$ such that $\mathfrak{P} \nmid v(L)$, and set $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}$. When $\mathfrak{p}$ is split or inert or non-dyadic ramified, $\mathfrak{n}(L, \mathfrak{P}) \subseteq \text{gen}(L)$. When $\mathfrak{p}$ is dyadic ramified, for any $M \in \mathfrak{n}(L, \mathfrak{P})$, we have $M \in \text{gen}(L)$ if and only if $nM = nL$.

Proof. Let $M$ be a Hermitian lattice in $\mathfrak{n}(L, \mathfrak{P})$. By Proposition 3.7, it suffices to show that $M_p$ and $L_p$ are isometric. By the assumption that $\mathfrak{P}$ does not divide the volume $vL$ and the fact that $vM = vL$, we have that $L_p$ and $M_p$ are unimodular.

For the classification of unimodular Hermitian lattices, when $\mathfrak{p}$ is dyadic ramified, two unimodular Hermitian lattices over $\mathcal{O}_p$ of the same rank are isometric if and only if they have the same norm ideal. In the remaining cases, all the unimodular Hermitian lattices over $\mathcal{O}_p$ of the same rank are always isometric. □
CHAPTER 4

The $g$-invariants of imaginary quadratic fields

In this chapter, we present and prove the main result of this thesis. In Section 1 we introduce the definition of the $g$-invariants of imaginary quadratic fields. In Section 2, given a Hermitian lattice $K$ in the genus of $I_m$, where $I_m$ is the free Hermitian lattice of rank $m$ with an orthonormal basis, we calculate the local density of the associated quadratic lattice $\hat{K}$. Then in Section 3 we use the result of the local density to obtain an upper bound of the smallest universal number $c(m)$. Finally in Section 4 we give an upper bound for the $g$-invariants of imaginary number fields.

From now on, we assume that $E$ is the imaginary quadratic field $\mathbb{Q}(\sqrt{-\ell})$, where $\ell$ is a squarefree positive integer. Let $\mathcal{O}$ be the ring of integers of $E$. Unless we state otherwise, all Hermitian spaces and lattices considered here are over $E$ and over $\mathcal{O}$, respectively; and all quadratic spaces and lattices considered here are over $\mathbb{Q}$ and over $\mathbb{Z}$, respectively.

4.1. The $g$-invariant

For any integer $n \geq 1$, let $\mathcal{G}_E(n)$ be the set of all positive definite integral Hermitian lattices of rank $n$ which can be represented by some $I_m$, where $I_m$ is the free Hermitian lattice of rank $m$ with an orthonormal basis. Via the standard correspondence between free Hermitian lattices and Hermitian forms, $I_m$ corresponds to the integral Hermitian form $x_1\bar{x}_1 + \cdots + x_m\bar{x}_m$.

DEFINITION 4.1. Let $E$ be an imaginary quadratic field. For any positive integer $n$, we define the $g$-invariant

$$g_E(n) := \min \{ g \mid L \to I_g, \forall L \in \mathcal{G}_E(n) \}.$$
The aim of this chapter is to find an upper bound for \( g_E(n) \). A special case is when the class number \( h(I_{n+1}) = 1 \). By applying the results of the representation theory of Hermitian lattices over local fields, we obtain in that case every positive definite integral Hermitian lattice \( L \) of rank \( n \) is represented by the genus of \( I_{n+1} \), thus \( L \rightarrow I_{n+1} \) and \( g_E(n) = n + 1 \).

However, the class number of \( I_m \) is seldom equal to 1. For example, Otremba \cite{23} used the analytical results of Braun \cite{1} to show that when \( m \geq 6 \), the class number of \( I_m \) is always at least 2. In the remainder of this chapter we are going to find an upper bound for \( g_E(n) \) where \( n \) and \( \ell \) are arbitrary.

4.2. Local density

**Definition 4.2.** Let \((K,b)\) be a positive definite integral quadratic lattice of rank \( n \). For any positive integer \( t \) and prime \( q \), the local density of representing \( t \) by \( K \) at \( q \) is defined to be

\[
\alpha_q(t,K) = \lim_{a \to \infty} q^{a(1-n)} \# \{ v \in K : b(v,v) \equiv t \pmod{q^a} \}.
\]

As we introduced in Section 1.2, for any Hermitian space \((V,h)\), we can associate with it a quadratic space \((\hat{V},b)\). Our choice of \( b \) is as follows:

\[
b := \begin{cases} 
\frac{1}{2} \mathbb{T} \circ h, & \text{when } \ell \equiv 1, 2 \pmod{4}; \\
\mathbb{T} \circ h, & \text{when } \ell \equiv 3 \pmod{4}.
\end{cases}
\]

Similarly, we can associate a Hermitian lattice \((L,h)\) with a quadratic lattice \((\hat{L},b)\).

Given a Hermitian lattice \( L \), we use \((\hat{L})^\sharp\) to denote the dual lattice of \( \hat{L} \) as a quadratic lattice over \( \mathbb{Z} \), and use \( \hat{\mathbb{L}}^\sharp \) to denote the corresponding quadratic lattice of the dual lattice of \( L \). In the following proposition, we will describe the relation between these two quadratic lattices under the assumption that \( L \) is integral.

**Lemma 4.3.** Let \( E \) be an imaginary quadratic field and let \( L \) be an integral Hermitian lattice of rank \( n \). Suppose \( \hat{L} \) is the underlying quadratic lattice with
\[ b = \mathbb{T} \circ h. \] Then
\[ (\hat{L})^\sharp = D^{-1}\hat{L}^\sharp. \]

Similarly, if we take \( b = \frac{1}{\mathbb{T}} \circ h \), then
\[ (\hat{L})^\sharp = 2D^{-1}\hat{L}^\sharp. \]

**Proof.** Recall that \( D^{-1} = \{ a \in E : \mathbb{T}(a\mathcal{O}) \subseteq \mathbb{Z} \} \). We only give the proof when \( b = \mathbb{T} \circ h \). For any \( \alpha \in D^{-1}, v \in \hat{L}^\sharp \) and \( w \in \hat{L} \), we have \( b(\alpha v, w) = \mathbb{T} \circ h(\alpha v, w) = \mathbb{T}(\alpha h(v, w)) \in \mathbb{Z} \). Thus \( \alpha v \in (\hat{L})^\sharp \) and \( (\hat{L})^\sharp \subseteq D^{-1}\hat{L}^\sharp \).

For the other inclusion, we are trying to show that \( D(\hat{L})^\sharp \subseteq \hat{L}^\sharp \). For any \( \beta \in \mathcal{O}, v \in (\hat{L})^\sharp \) and \( w \in L \), since \( \mathbb{T}(\beta h(v, w)) = \mathbb{T}(h(v, \beta w)) = b(v, \beta w) \in \mathbb{Z} \), we have \( h(v, w) \in D^{-1} \). Then for any \( \gamma \in D, h(\gamma v, w) = \gamma h(v, w) \in \mathcal{O} \). Thus \( \gamma v \in L^\sharp \) and \( (\hat{L})^\sharp \subseteq D^{-1}\hat{L}^\sharp \). \( \square \)

Now suppose that \( L \) is a positive definite integral unimodular Hermitian lattice of rank \( n \). Let \( d_E \) be the discriminant of \( E \) over \( \mathbb{Q} \). The volume of \( \hat{L} \) is given by:

1. When \( \ell \equiv 1, 2 \pmod{4}, d_E = -4\ell \) and \( \hat{v}\hat{L} = vL^2(d_E/4)^n = \ell^n\mathcal{O} \);
2. When \( \ell \equiv 3 \pmod{4}, d_E = -\ell \) and \( \hat{v}\hat{L} = vL^2(d_E)^n = \ell^n\mathcal{O} \).

Since \( \hat{L} \) is positive definite integral, we can conclude that \( d\hat{L} = \ell^n \).

**Lemma 4.4.** Let \( L \) be a unimodular Hermitian lattice. Then
\[ ((\hat{L})^\sharp)^\ell \cong \hat{L}, \]
where \( ((\hat{L})^\sharp)^\ell \) denotes the lattice \( \hat{L}^\sharp \) with the scaled bilinear form \( b^\ell(v, w) = \ell b(v, w) \).

**Proof.** First we determine the different \( D^{-1} \) of \( E \) over \( \mathbb{Q} \). Note that if we view \( \mathcal{O} \) as a quadratic \( \mathbb{Z} \)-lattice on the quadratic space \( E \), with the bilinear map \( b(\alpha, \beta) = Tr(\alpha\beta) \) for any \( \alpha, \beta \in E \), then \( D^{-1} \) is actually the dual lattice \( \mathcal{O}^\sharp \) of \( \mathcal{O} \).

When \( \ell \equiv 1, 2 \pmod{4}, \mathcal{O} = \mathbb{Z} + \mathbb{Z}\sqrt{-\ell} \). Then \( \frac{1}{2}, \frac{1}{2\sqrt{-\ell}} \) is the dual basis of \( 1, \sqrt{-\ell} \) and
\[ D^{-1} = \mathcal{O}^\sharp = \mathbb{Z}\frac{1}{2} + \mathbb{Z}\frac{1}{2\sqrt{-\ell}}. \]

When \( \ell \equiv 3 \pmod{4}, \mathcal{O} = \mathbb{Z} + \mathbb{Z}^{1+\sqrt{-\ell}}/2 \). Then \( \frac{1}{2} - \frac{1}{2\sqrt{-\ell}}, \frac{1}{\sqrt{-\ell}} \) is the dual basis of \( 1, \frac{1+\sqrt{-\ell}}{2} \) and
\[ D^{-1} = \mathcal{O}^\sharp = \mathbb{Z}\left(\frac{1}{2} - \frac{1}{2\sqrt{-\ell}}\right) + \mathbb{Z}\frac{1}{\sqrt{-\ell}}. \]
Applying Lemma 4.3, we have \((\hat{L})\sharp = 1/\sqrt{-\ell\hat{L}} = 1/\sqrt{-\ell\hat{L}}\) since \(L\) is unimodular. Thus our statement is proved. \(\square\)

Let \(p\) be a rational prime. If \(p\) does not divide \(\ell\), then \(\hat{L}_p\) is unimodular. Now suppose that \(p\) divides \(\ell\). Let \(\hat{L}_p = L_1 \perp \cdots \perp L_t\) be a Jordan splitting of \(\hat{L}_p\), where \(L_i\) is \(\ell^{a_i}\)-modular for \(1 \leq i \leq t\). Then
\[
\left(\left(\hat{L}_p\right)^\ell\right)_p = \left(\left(\hat{L}_p\right)^\sharp\right)_p = \left(\left(L_1^\sharp\right)^\ell \perp \cdots \perp \left(L_t^\sharp\right)^\ell\right),
\]
and \(\left(L_i^\sharp\right)^\ell\) is \(\ell^{1-a_i}\)-modular for \(1 \leq i \leq t\). Since the Jordan splittings of isometric quadratic lattices are of the same type, we have
\[
1 - a_t = a_1 = \ldots = a_1 = a_t,
\]
which implies that \(t = 2\), \(a_1 = 0\), and \(a_2 = 1\). Therefore
\[
\hat{L}_p = L_1 \perp L_2,
\]
where \(L_1\) is unimodular and \(L_2\) is \(\ell\)-modular.

In this section, we use Theorem 3.1 and Theorem 4.1 in [28] to compute the local densities \(\alpha_q(t, \hat{L})\), where \(L\) is a Hermitian lattice in the genus of \(I_m\). For any unexplained notations, the readers can refer to [28].

**Lemma 4.5.** Let \(m \geq 3\), \(L\) be a Hermitian lattice in the genus of \(I_m\), and \(t\) be a positive integer in \(\mathbb{Z}\). Then
\[
\prod_{q: \text{prime}} \alpha_q(t, \hat{L}) \geq \frac{1}{2\ell\zeta(2)}.
\]

**Proof.** Since \(L\) is unimodular, \(d\hat{L} = \ell^m\) and \((\hat{L}_p)\sharp \equiv \hat{L}\). Throughout this proof, \(S_q = (s_{ij})\) is a half-integral matrix over \(\mathbb{Z}_q\), meaning that \(s_{ii}\) and \(2s_{ij}(i \neq j)\) are in \(\mathbb{Z}_q\), but \(q^{-1}S_q\) does not satisfy this condition. We write the Gram matrix of \(\hat{L}_q\) in the form of \(S_q^l = q^lS_q\), where \(0 \leq l \leq 1\), and suppose that \(t = t_0q^a\) with \(t_0 \in \mathbb{Z}_q^\times\) and \(a \in \mathbb{Z}\).
4.2. LOCAL DENSITY

Case 1. First, let us consider the non-dyadic case \( q \neq 2 \). By Theorem 3.1 in [28], we have that

\[
\alpha_q(t, \hat{L}) = \alpha(1, t, S_q)
\]

\[
= 1 + R_1(1, t, S_q)
\]

\[
\geq 1 - |R_1(1, t, S_q)|
\]

\[
\geq 1 - \left[ (1 - q^{-1}) \sum_{0 < k \leq a \atop \ell(k,1) \text{even}} |v_kq^{d(k)}| + |v_{a+1}q^{d(a+1)}f_1(t)| \right]
\]

\[
\geq 1 - \left[ (1 - q^{-1}) \sum_{0 < k \leq a \atop \ell(k,1) \text{even}} q^{d(k)} + q^{d(a+1)-1/2} \right].
\]

(1) \( q \nmid \ell \). In this case, \( \hat{L}_q \) is unimodular and \( q \) is odd, so

\[
S_q \cong \langle 1 \rangle \perp \cdots \perp \langle 1 \rangle \perp \langle \ell^m \rangle,
\]

and

\[
d(k \geq 1) = k + \frac{1}{2} \sum_{l_i < k} (l_i - k)
\]

\[
= k + \frac{1}{2} \cdot 2m \cdot (-k)
\]

\[
= (1 - m)k
\]

\[
\leq -2k
\]

\[
\leq -2.
\]

When \( a = 0 \), we have

\[
\alpha_q(t, \hat{L}) \geq 1 - q^{d(1)-1/2} \geq 1 - q^{-2};
\]

when \( a \geq 1 \), we have
\[ \alpha_q(t, \hat{L}) \geq 1 - \left[ (1 - q^{-1}) \sum_{k \geq 1} q^{d(k)} + q^{d(2)-1/2} \right] \]
\[ \geq 1 - [(1 - q^{-1})(q^{-2} + q^{-4} + q^{-6} + \cdots) + q^{-4}] \]
\[ \geq 1 - [(1 - q^{-1})q^{-2}(1 + q^{-2} + q^{-4} + \cdots) + q^{-4}] \]
\[ \geq 1 - [(1 - q^{-1})q^{-2}(1 + q^{-1}) + q^{-4}] \]
\[ = 1 - q^{-2}. \]

(2) \( \ell = q^{\ell'}, \ell' \in \mathbb{Z}_q^\times \). In this case,
\[ S_q \cong \langle 1 \rangle \underbrace{\langle \varepsilon \rangle \perp \langle \ell \rangle \perp \cdots \perp \langle \ell \varepsilon \rangle}_{l_i=0, \# = m} \]
\[ \underbrace{\langle \varepsilon \rangle \perp \langle \ell \rangle \perp \cdots \perp \langle \ell \varepsilon \rangle}_{l_i=1, \# = m}, \]
where \( \varepsilon \in \mathbb{Z}_q^\times \) and
\[ d(1) = 1 + \frac{1}{2} \cdot m \cdot (0 - 1) \]
\[ \leq 1 - \frac{m}{2} \]
\[ \leq -\frac{1}{2}, \]
\[ d(k \geq 2) = k + \frac{1}{2} \sum_{l_i<k} (l_i - k) \]
\[ = k + \frac{1}{2} \cdot m \cdot (-k) + \frac{1}{2} \cdot m \cdot (1 - k) \]
\[ = k + \frac{1}{2} m (1 - 2k) \]
\[ = \frac{3}{2} - 2k \]
\[ \leq -\frac{5}{2}. \]
When $a = 0$, we have

$$\alpha_q(t, \hat{L}) \geq 1 - q^{d(1)/2} \geq 1 - q^{-1} \geq (1 - q^{-2})/q;$$

when $a \geq 1$, we have

$$\alpha_q(t, \hat{L}) \geq 1 - \left[ (1 - q^{-1}) \sum_{k \geq 1} q^{d(k)} + q^{d(2)}/2 \right]$$

$$\geq 1 - [(1 - q^{-1})(q^{-1/2} + q^{-5/2} + q^{-9/2} + \cdots) + q^{-3}]$$

$$\geq 1 - [(1 - q^{-1})q^{-1/2}(1 + q^{-1}) + q^{-3}]$$

$$\geq 1 - q^{-1/2} \geq (1 - q^{-2})/q.$$

**Case 2.** Now, let us consider the dyadic case $q = 2$. Write $t = 2^l t'$. By Theorem 4.1 in [28], we have that

$$\alpha_q(t, \hat{L}) = \alpha(1, 2^l t', S_q^l)$$

$$\geq 1 + l - 2^l |R_1(1, t', S_q)|$$

$$\geq 1 + l - \sum_{\ell \mid (k - 1), \ell \text{ odd}} 2^l \left| \delta(k)p(k) \left( \frac{2}{\ell(k)} \right) 2^{d(k) - 3/2} \right|$$

$$- \sum_{\ell \mid (k - 1), \ell \text{ even}} 2^l \left| \delta(k)p(k) \left( \frac{2}{\ell(k)} \right) 2^{d(k) - 1} \psi \left( \frac{k}{2} \right) \text{char}(4\mathbb{Z}_2)(\mu) \right|$$

$$\geq 1 + l - \sum_{\ell \mid (k - 1), \ell \text{ odd}} 2^l \left| \delta(k)2^{d(k) - 3/2} \right| - \sum_{\ell \mid (k - 1), \ell \text{ even}} 2^l \left| \delta(k)2^{d(k) - 1} \right|.$$

(1) $2 \nmid \ell$. $\hat{L}_2$ is a unimodular quadratic lattice.
When $\ell \equiv 1 \pmod{4}$, $n\widehat{L}_2 = n(I_m)_2 = \mathbb{Z}_2$,

$$S_2 \cong \langle 1 \rangle \perp \cdots \perp \langle 1 \rangle \perp \langle \ell \rangle \perp \cdots \perp \langle \ell \rangle,$$

and

$$l(k, 1, 1) = \begin{cases} 2m, & \text{if } k \geq 2 \text{ even;} \\ 0, & \text{otherwise}, \end{cases}$$

$$\delta(k) = \begin{cases} 0, & \text{if } k = 1; \\ 1, & \text{if } k \geq 2, \end{cases}$$

$$d(k \geq 2) = k + \frac{1}{2} \sum_{l_h < k-1} (l_h - k + 1)$$

$$= k + \frac{1}{2} \cdot 2m \cdot (-k + 1)$$

$$\leq 3 - 2k$$

$$\leq -1.$$ 

Therefore

$$\alpha_2(t, \widehat{L}) = \alpha(1, 1, S_2) \geq 1 - \sum_{k \geq 2} 2^{d(k)-1}$$

$$\geq 1 - 2^{-1}(2^{-1} + 2^{-3} + 2^{-5} + \cdots)$$

$$\geq 1 - 2^{-1}$$

$$\geq (1 - 2^{-2})/2.$$
When $\ell \equiv 3 \pmod{4}$, $n\hat{L}_2 = n(I_m)_2 = 2\mathbb{Z}_2$,

$$S_2^1 = 2S_2 \cong 2 \left( \begin{array}{cccc} 0 & \frac{1}{2} & & \\ \frac{1}{2} & 0 & & \\ & & \ddots & \vdots \\ & & & 0 \end{array} \right)_{m_i=0, \# = m} \left( 0, \frac{1}{2} \right) \perp \left( \frac{1}{2}, 0 \right)$$

or

$$\cong 2 \left( \begin{array}{cccc} 0 & \frac{1}{2} & & \\ \frac{1}{2} & 0 & & \\ & & \ddots & \vdots \\ & & & 0 \end{array} \right)_{m_i=0, \# = m-1} \left( 0, \frac{1}{2} \right) \perp \left( \frac{1}{2}, 1 \right)_{n_j=0, \# = 1}$$

and

$$d(k \geq 1) = k + \sum_{m_i < k} (m_i - k) + \sum_{n_i < k} (n_i - k)$$

$$= k - mk$$

$$\leq -2k$$

$$\leq -2.$$

Hence if we write $t = 2t'$,

$$\alpha_2(t, \hat{L}) = \alpha_2(2t', \hat{L})$$

$$= \alpha(1, 2t', S_2^1)$$

$$\geq 2 - 2 \sum_{k \geq 1} 2^{d(k)-1}$$

$$\geq 2 \left( 1 - 2^{-2}(2^{-1} + 2^{-3} + 2^{-5} + \cdots) \right)$$

$$\geq 1 - 2^{-2}.$$
(2) $\ell = 2\ell', \ell' \in \mathbb{Z}_2^\times$. In this case $\ell \equiv 2 \pmod{4}$, $n\widehat{L}_2 = n(I_m)_2 = \mathbb{Z}$. Hence

$$S_2 \cong \{1\} \perp \cdots \perp \{1\} \perp \langle \ell \rangle \perp \cdots \perp \langle \ell \rangle,$$

and

$$\delta(k) = \begin{cases} 
0, & \text{if } k = 1, 2; \\
1, & \text{if } k \geq 3,
\end{cases}$$

$$d(k \geq 3) = k + \frac{1}{2} \sum_{l_h < k-1} (l_h - k + 1)$$

$$= k + \frac{1}{2} \cdot m \cdot (1 - k) + \frac{1}{2} \cdot m \cdot (2 - k)$$

$$\leq k + \frac{3}{2} (3 - 2k)$$

$$= \frac{9}{2} - 2k$$

$$\leq -\frac{3}{2}.$$ 

Therefore

$$\alpha_2(t, \widehat{L}) = \alpha_2(1, t, S_2)$$

$$\geq 1 - \sum_{k \geq 3} 2^{d(k)-1}$$

$$\geq 1 - (2^{-5/2} + 2^{-9/2} + 2^{-13/2} + \cdots)$$

$$\geq 1 - (2^{-2} (2^{-1/2} + 2^{-5/2} + 2^{-9/2} + \cdots))$$

$$\geq 1 - 2^{-2}.$$ 

Combining the above results together, we prove that

$$\prod_{q \text{ prime}} \alpha_q(t, \widehat{L}) \geq \frac{1}{2^\ell} \prod_{q \text{ prime}} (1 - q^{-2}) = \frac{1}{2^\ell \zeta(2)},$$

$\square$
4.3. The smallest universal number

Definition 4.6. Let $K$ be a positive definite integral Hermitian lattice. Let $c(K)$ be the smallest positive integer $k$ such that $i \rightarrow K$ for all (even, if $K$ is even) integers $i \geq k$. The smallest universal number is defined to be

$$c(m) := \max\{c(K) : K \in \text{gen}(I_m)\}.$$ 

Definition 4.7. Let $M$ be a positive definite integral quadratic lattice. Let $\tilde{c}(M)$ be the smallest positive integer $k$ such that $j \rightarrow M$ for all (even, if $M$ is even) integers $j \geq k$, and define

$$\tilde{c}(m) := \max\left\{\tilde{c}(\tilde{K}) : \tilde{K} \text{ is a Hermitian lattice in } \text{gen}(I_m)\right\}.$$ 

Lemma 4.8. (Siegel, [26, Lemma 1]) Let $\rho$ be a primitive root of unity of degree $s \geq 1$, $a$ and $b$ be two integers and $\delta = (2a, s)$ be the greatest common divisor of $2a$ and $s$. Then

$$\left|\sum_{h=1}^{s} \rho^{ah^2+bh}\right|^2 \leq \delta s,$$

and the equality holds when $\delta = 1$.

Lemma 4.9. Let $\rho$ be a primitive root of unity of degree $s \geq 1$, $a, b, c$ be integers with $c < a$, and $\delta = (2c, s)$ be the greatest common divisor of $2c$ and $s$. Then

$$\left|\sum_{h_1=1}^{s} \sum_{h_2=1}^{s} \rho^{(ah_1^2+bh_1h_2)h_1v_1+h_2v_2}\right| \leq \delta^{\frac{1}{2}}s^{\frac{3}{2}}.$$

Proof. By Lemma 4.8,

$$\left|\sum_{h_1=1}^{s} \sum_{h_2=1}^{s} \rho^{(ah_1^2+bh_1h_2+ch_2^2)h_1v_1+h_2v_2}\right| \leq \sum_{h_1=1}^{s} \left|\rho^{ah_1^2+h_1v_1}\right| \left|\sum_{h_2=1}^{s} \rho^{ch_2^2+(bh_1+v_2)h_2}\right| \leq \delta^{\frac{1}{2}}s^{\frac{3}{2}}.$$
Lemma 4.10. Let $K$ be a positive definite integral quadratic lattice of rank $n$, and $\mu(K) := \mu$ be the smallest positive integer that is represented by $K$. Let $r(t, K)$ be the number of vectors $v \in K$ such that $Q(v) = t$. Then for a positive integer $t \geq \mu$, we have

$$r(t, K) \leq (2\sqrt{t/\mu} + 1)^n - (2\sqrt{t/\mu} - 1)^n.$$  

Proof. See [13, Lemma 2.1]. \qed

Note that the representation numbers $r(t, K)$ are the Fourier coefficients of the theta function

$$\Theta(z, Q) = \sum_{m \in \mathbb{Z}^n} e(Q(m)z) = \sum_{t=0}^{\infty} r(t, K)e(tz),$$

where $e(z) = e^{2\pi iz}$. Then

$$r(t, K) = \int_0^1 \Theta(z, Q)e(-tz)dx.$$

The following theorem provides us an upper bound of $c(m)$, which is important in deriving our upper bound for $g_E(n)$. Our proof follows Iwaniec [6, Chapter 11], where he uses the circle method to estimate the representation number of an integer by a quadratic form of rank $\geq 4$.

Theorem 4.11. For $m \geq 3$,

$$c(m) \leq \begin{cases}  
(\ell m)^{20}, & \text{if } \ell \equiv 1, 2 \pmod{4}; \\
\frac{1}{2}(\ell m)^{20}, & \text{if } \ell \equiv 3 \pmod{4}.
\end{cases}$$

Proof. Let $L$ be a Hermitian lattice in the genus of $I_m$. Then $L$ is unimodular, and the corresponding quadratic lattice $\hat{L}$ is in the genus of $\hat{I}_m$ by Lemma 2.38. Since

$$c(m) = \begin{cases} 
\tilde{c}(m), & \text{if } \ell \equiv 1, 2 \pmod{4}; \\
\frac{1}{2}\tilde{c}(m), & \text{if } \ell \equiv 3 \pmod{4},
\end{cases}$$

in this proof, we will find an upper bound of $\tilde{c}(m)$ instead.

Let $C \geq 1$ be any real number and $M_\hat{L}$ be the Gram matrix of $\hat{L}$. We define the adjoint quadratic form of $Q$ by

$$Q^* := \frac{1}{2}A^{-1}[x].$$
where \( A = 2M_L \) and \( A[x] := x^tAx \). Define

\[
(4.1) \quad T(c, t; x) = |A|^{-1/2} c^{-2m} \left( \frac{i}{z} \right)^m \sum_{m \in \mathbb{Z}^{2m}} T_m(c, t; x) e \left( -\frac{Q^*(m)}{c^2 z} \right),
\]

where \( c \) is a positive integer less than or equal to \( C \) and

\[
(4.2) \quad T_m(c, t; x) = \sum_{\substack{c < d \leq c+\mathcal{C} \mod{c} = 1, cd < 1}} e \left( \frac{td}{c} \right) \sum_{h \mod c} e \left( -\frac{d}{c} (Q(h) + h'm) \right).
\]

Then

\[
(4.3) \quad r(t, \hat{L}) = 2\text{Re} \sum_{c \leq C} \int_{0}^{1/c} T(c, t; x) e(-tz) dx.
\]

Here, \( z = x + iy \in \mathbb{C} \) with \( y > 0 \) to be chosen later, and \( d \) is the multiplicative inverse of \( d \mod{c} \). If \( 0 < x < \frac{1}{c(c+C)} \), then \( T_m(c, t; x) \) is independent of \( x \). In that case, we simply denote it by \( T_m(c, t) \). Now we divide (4.3) into the following five parts:

\[
\begin{align*}
& r(t, \hat{L}) = |A|^{-1/2} \sum_{c=1}^{\infty} c^{-2m} T_0(c, t) \int_{-\infty}^{\infty} \left( \frac{i}{z} \right)^m e(-tz) dx \cdots (r_1) \\
& - |A|^{-1/2} \sum_{c = [C]+1}^{\infty} c^{-2m} T_0(c, t) \int_{-\infty}^{\infty} \left( \frac{i}{z} \right)^m e(-tz) dx \cdots (r_2) \\
& + 2\text{Re} \sum_{c=1}^{[C]} |A|^{-1/2} c^{-2m} \int_{1/c(c+C)}^{1/c} T_0(c, t; x) \left( \frac{i}{z} \right)^m e(-tz) dx \cdots (r_3) \\
& + 2\text{Re} \sum_{c=1}^{[C]} |A|^{-1/2} c^{-2m} \int_{0}^{1/c} \left( \frac{i}{z} \right)^m \times \\
& \sum_{m \in \mathbb{Z}^{2m}\setminus\{0\}} T_m(c, t; x) e \left( -\frac{Q^*(m)}{c^2 z} \right) e(-tz) dx \cdots (r_4) \\
& - 2\text{Re} \sum_{c=1}^{[C]} |A|^{-1/2} c^{-2m} T_0(c, t) \int_{1/c(c+C)}^{\infty} \left( \frac{i}{z} \right)^m e(-tz) dx \cdots (r_5).
\end{align*}
\]
4.3. THE SMALLEST UNIVERSAL NUMBER

Let

\[ G_{c,d}(Q, m) := \sum_{h \pmod{c}} e \left( -\frac{d}{c} (Q(h) + h'm) \right) \]

be the Gauss sum factor in (4.2). Now we want to find an expression of \( Q(h) \pmod{c} \).

Let \( h = (h_1, \ldots, h_{2m}) \) and \( m = (a_1, \ldots, a_{2m}) \).

**Case 1:** \( \ell \equiv 1, 2 \pmod{4} \).

In this case, the corresponding quadratic lattice \( \hat{I}_m \) of \( I_m \) is

\[ \hat{I}_m = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m + \mathbb{Z}(\sqrt{-\ell}v_1) + \cdots + \mathbb{Z}(\sqrt{-\ell}v_m) \]

\[ \cong \langle 1 \rangle \perp \cdots \perp \langle 1 \rangle \perp \langle \ell \rangle \perp \cdots \perp \langle \ell \rangle. \]

Therefore

\[ Q(h) \equiv h_1^2 + \cdots + h_m^2 + \ell h_{m+1}^2 + \cdots + \ell h_{2m}^2 \pmod{c}. \]

Then by Lemma 4.8, we obtain an upper bound

\[ |G_{c,d}(Q, m)| \leq (2c)^m (c^3)^{m/2} \leq (2c^2)^m. \]

**Case 2:** \( \ell \equiv 3 \pmod{4} \).

In this case, the corresponding quadratic lattice \( \hat{I}_m \) of \( I_m \) is

\[ \hat{I}_m = \mathbb{Z}v_1 + \mathbb{Z} \left( \frac{1 + \sqrt{-\ell}}{2} v_1 \right) + \cdots + \mathbb{Z}v_m + \mathbb{Z} \left( \frac{1 + \sqrt{-\ell}}{2} v_m \right) \]

\[ \cong \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+\ell}{2} \end{pmatrix} \perp \cdots \perp \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+\ell}{2} \end{pmatrix}. \]

So we may assume that

\[ Q(h) \equiv \sum_{k=1}^{m} \left( 2h_{2k-1}^2 + 2h_{2k-1}h_{2k} + \left( \frac{1+\ell}{2} \right) h_{2k}^2 \right) \pmod{c}. \]
Using Lemma 4.9, we have that

\[ |G_{c,d}(Q, m)| = \prod_{i=1}^{m} \left| \sum_{h_{2i-1}, h_{2i}} e \left( -\frac{d}{c} (2h_{2i-1}^2 + 2h_{2i-1}h_{2i} + \left( \frac{1+\ell}{2} \right) h_{2i}^2 + a_{2i-1}h_{2i-1} + a_{2i}h_{2i}) \right) \right| \]

\[ \leq \left( 2c^2 \right)^m. \]

Thus we obtain

(4.5) \[ |G_{c,d}(Q, m)| \leq \left( 2c^2 \right)^m. \]

This and (4.2) imply

(4.6) \[ |T_m(c, t; x)| \leq 2^m c^{\frac{3}{2}m + 1} \text{ for all } m, x \text{ and } t. \]

Now we take \( C = \sqrt{t} \) and \( y = 1/t \). Then

\[ \int_{-\infty}^{\infty} \left( \frac{i}{z} \right)^m e(-tz)dx = (2\pi)^m \Gamma(m)^{-1} t^{m-1}, \]

and

\[ \sum_{c=1}^{\infty} c^{-2m} T_0(c, t) = \prod_{q \text{ prime}} \alpha_q(t, \hat{L}), \]

where \( \alpha_q(t, \hat{L}) \) is the local density at \( q \). Therefore

\[ r_1 = \ell^{-\frac{m}{2}} \pi^m \Gamma(m)^{-1} t^{m-1} \prod_{q \text{ prime}} \alpha_q(t, \hat{L}) \]

\[ \geq \frac{1}{2} \ell^{-\frac{m}{2} - 1} \pi^m \Gamma(m)^{-1} t^{m-1} \zeta^{-1}(2). \]
By applying (4.6), it is easy to derive the following upper bounds for the absolute values of the other $r_i$’s:

$$|r_2| = \left| |A|^{-1/2} \sum_{c=-|C|+1}^{\infty} e^{-2mT_0(c, t)} \int_{-\infty}^{\infty} \left( \frac{i}{z} \right)^m e(-tz)dx \right|$$

$$\leq \frac{2 \frac{1}{2}m - 2 \pi^m t \pi m}{\ell^2 \Gamma(m)},$$

$$|r_3| = \left| 2 \mathop{Re} \sum_{c=1}^{[C]} |A|^{-1/2} e^{-2m} \int_{1/\ell(c+|C|)}^{1/\ell(c+C)} T_0(c, t; x) \left( \frac{i}{z} \right)^m e(-tz)dx \right|$$

$$\leq \frac{2^{m+1} \ell^{2} \pi \pi m}{\ell^2 (m - 1)(m + 2)},$$

$$|r_5| = \left| 2 \mathop{Re} \sum_{c=1}^{[C]} |A|^{-1/2} e^{-2mT_0(c, t)} \int_{1/\ell(c+C)}^{\infty} \left( \frac{i}{z} \right)^m e(-tz)dx \right|$$

$$\leq \frac{2^{m+1} \ell^{2} \pi \pi m}{\ell^2 (m - 1)(m + 2)}.$$

Since $\widehat{\mathbb{L}}^\ell \cong \mathbb{L}$, the number of elements in $\widehat{\mathbb{L}}^\ell$ which represents the integer $k$ is the same as the number of elements in $\mathbb{L}$ which represents the integer $\ell k$. Therefore,

$$\left| \sum_{\mathbf{m} \in \mathbb{Z}^{2m} \setminus \{0\}} e\left( \frac{-Q'(\mathbf{m})}{c^2 z} \right) \right| \leq \sum_{\mathbf{m} \in \mathbb{Z}^{2m} \setminus \{0\}} \left| e\left( \frac{-Q'(\mathbf{m})}{c^2 z} \right) \right|$$

$$= \sum_{\mathbf{m} \in \mathbb{Z}^{2m} \setminus \{0\}} e\left( \frac{-\pi y}{2c^2(x^2 + y^2)}Q^{-1}[\mathbf{m}] \right)$$

$$= \sum_{k=1}^{\infty} r(k, \hat{\mathbb{L}}^\ell) e\left( \frac{-\pi yk}{2c^2(x^2 + y^2)} \right)$$

$$= \sum_{k=1}^{\infty} r(\ell k, \hat{\mathbb{L}}) e\left( \frac{-\pi yk}{2c^2(x^2 + y^2)} \right).$$
Let $\beta = \frac{xy}{2x^2 + y^2}$. We may assume that $r(\ell k, \hat{L}) \leq (8\ell k)^m$. Therefore
\[
\sum_{k=1}^{\infty} r(\ell k, \hat{L}) e^{-\beta k} \leq (8\ell)^m \int_0^{\infty} x^m e^{-\beta x} dx \leq \frac{(8\ell)^m \Gamma(m+1)}{\beta^{m+1}}.
\]
This implies
\[
|r_4| \leq 2 \sum_{c=1}^{|C|} |A|^{-1/2} c^{-2m} \left| \int_0^{1/c^2} \left( \frac{i}{z} \right)^m \sum_{m \in \mathbb{Z}^{2m} \setminus \{0\}} T_m(c, t; x) e\left( -\frac{Q^* (m)}{c^2 z} \right) e(-tz) dz \right|
\]
\[
\leq \frac{2^{5m+6} \ell^m \Gamma(m+1)e^{2\pi}}{\pi^{m+1}(m+3)(m+2)} t^{\frac{3}{4} m}.
\]
Therefore,
\[
r(t, \hat{L}) \geq \left( \frac{2^m}{\ell^{m+1} \Gamma(m)} \right) t^{m-1} - \left( \frac{2^{m+2} \pi^m}{\ell^m \Gamma(m)} \right) t^{\frac{3}{4} m} - 2 \left( \frac{2^{m+1} \pi^{2m}}{\ell^m (m-1)(m+2)} \right) t^{\frac{3}{4} m}
\]
\[
- \left( \frac{2^{5m+6} \ell^m \Gamma(m+1)e^{2\pi}}{\pi^{m+1}(m+3)(m+2)} \right) t^{\frac{3}{4} m}.
\]
Consequently, if $t \geq (\ell m)^{20}$, then $r(t, \hat{L}) > 0$. □

4.4. Main theorem

Let $q$ be a rational prime and $\mathcal{Q}$ be a prime ideal in $\mathcal{O}$ which is above $q$. By abuse of notations, in this section we will regard individual lattices in $\mathfrak{M}(L, \mathcal{Q})$ as representatives of their isometry classes, and simply say that all the Hermitian lattices in the isometry class of $M$ are $\mathcal{Q}$-neighbors of $N$ if $M$ is a $\mathcal{Q}$-neighbor of $N$.

**Definition 4.12.** For two Hermitian lattices $M, N \in \mathfrak{M}(L, \mathcal{Q})$, define the distance between $M$ and $N$ to be the minimum number of edges between $M$ and $N$, denoted as $d(M, N)$.

Suppose that $q$ remains inert in $E$. Then $\mathcal{Q} = q\mathcal{O}$ is the unique prime ideal in $\mathcal{O}$ which is above $q$. In this situation, $M$ is a $\mathcal{Q}$-neighbor of $N$ if and only if $N$ is a $\mathcal{Q}$-neighbor of $M$, so that we do not need to worry about the direction of the edge. We can also see that there exists some $\phi \in \mathfrak{U}(V)$ such that $\phi(\mathcal{Q}^{d(M, N)} M) \subseteq N$. 
From now on, we assume that $p$ is the smallest prime which is inert in $E = \mathbb{Q}(\sqrt{-\ell})$, and $\mathfrak{P} = p\mathcal{O}$ is the prime in $\mathcal{O}$ lying above $p$. Let $K$ be a Hermitian lattice in the genus of $I_m$, we want to use the theory of neighbors of Hermitian lattices to find a positive integer $l$ such that $\mathfrak{P}^lK$ is represented by some $I_s$, where $s$ is a positive integer.

**Lemma 4.13.** Let $m \leq 2$, $K$ be a Hermitian lattice in the genus of $I_m$. Then

$$\mathfrak{P}^{h_3}K \rightarrow I_3,$$

where $h_3$ is the class number of $I_3$.

**Proof.** By Proposition 2.19, we may assume that $K \subseteq M \in \text{gen}^0(I_3)$. Since

$$\text{gen}^0(I_3) \subseteq \mathfrak{N}(I_3, \mathfrak{P}) \subseteq \text{gen}(I_3),$$

$M$ is in the neighborhood of $I_3$ and $d(M, I_3) \leq h_3$. Hence $\mathfrak{P}^{h_3}K \subseteq \mathfrak{P}^{h_3}M \rightarrow I_3$. \[\square\]

Using [5, Main Theorem 5.1], we can find an upper bound for $h_3$:

$$h_3 \leq |d_E|B_{3,\chi}/144 + |d_E|^3,$$

where $\chi$ is the Dirichlet character associated to $E$, $B_{3,\chi}$ is the third Bernoulli number twisted by $\chi$, and $d_E$ is the discriminant of $E$.

**Lemma 4.14.** Let $m \geq 3$, and $K$ be a Hermitian lattice in the genus of $I_m$. Suppose that 2 is unramified. Then

$$\mathfrak{P}^{\tau_E(m)}K \rightarrow I_{m+1},$$

where

$$\tau_E(m) = \sum_{i=3}^{m} \lceil 10 \log_p (i\ell) \rceil + \ell B_{3,\chi}/144 + \ell^3.$$

**Proof.** Since $K \in \text{gen}(I_m)$, by the result of Theorem 4.11, a positive integer is represented by $K$ if it is greater than or equal to $(m\ell)^{20}$. Now take $t = 2\lceil 10 \log_p m\ell \rceil$. Then there is some $v \in K$, such that $p^t = h(v)$. Suppose that $a_v$ is the coefficient ideal of $v$ in $K$, and $-s = \text{ord}_{\mathfrak{P}}a_v$. Then $p^{-s}v \in K$ and $h(p^{-s}v) = N(p^{-s})h(v) = p^t - 2s$. Thus we may assume that $\text{ord}_{\mathfrak{P}}a_v = 0$. 

We would like to construct a Hermitian lattice $K_1$ in the neighborhood $\mathfrak{N}(K, \mathfrak{P})$ of $K$ such that $1 \to K_1$. If $t = 0$, then we are done. Otherwise we may assume that $h(v) = p^t \in \mathfrak{P}$. Since $v \in K \setminus \mathfrak{P}K$, by Lemma 3.4, the Hermitian lattice

$$K' := \mathfrak{P}^{-1}v + \{w \in K \mid h(v, w) \in \mathfrak{P}\}$$

is a $\mathfrak{P}$-neighbor of $K$, and $K'$ represents $p^{t-2}$. By repeating this procedure if necessary, we may conclude that there exists a Hermitian lattice $K_1 \cong \langle 1 \rangle \perp K_{12}$ in the neighborhood $\mathfrak{N}(K, \mathfrak{P})$, and $d(K, K_1) \leq t/2$. Therefore $\mathfrak{P}^{d(K,K_1)}K \to K_1$.

When 2 is unramified, there is only one genus of unimodular lattices on the same Hermitian space. Thus we may assume that $K_{12} \in \text{gen}(I_{m-1})$. Applying the same procedure as before in a repeated manner, we obtain a Hermitian lattice

$$K_s \cong I_{m-2} \perp K_{s2} \in \mathfrak{N}(K, \mathfrak{P}),$$

where $K_{s2} \in \text{gen}(I_2)$ and

$$d(K, K_s) \leq \sum_{i=3}^{m} \lceil 10 \log_p(i\ell) \rceil.$$

It follows that $\mathfrak{P}^{d(K,K_s)}K \to K_s$. Since $\mathfrak{P}^{h_3}K_{s2} \to I_3$ by Lemma 4.13, therefore

$$\mathfrak{P}^{h_3}K_s \cong \mathfrak{P}^{h_3}(I_{m-2} \perp K_{s2}) \to I_{m+1}.$$  
Hence $\mathfrak{P}^{d(K,K_s)+h_3}K \to I_{m+1}$. Note that in this case $|d_E| = \ell$. Therefore, if we let

$$\tau_E(m) = \sum_{i=3}^{m} \lceil 10 \log_p(i\ell) \rceil + \ell B_3 \chi/144 + 64\ell^3,$$

we have $\mathfrak{P}^{\tau_E(m)}K \to I_{m+1}$. \hfill \qed

**Lemma 4.15.** Let $m \geq 3$, and $K$ be a Hermitian lattice in the genus of $I_m$. Suppose that 2 is ramified and $\Re$ is the prime in $\mathcal{O}$ lying above 2. Then

$$\mathfrak{P}^{\tau_E(m)}\Re^{m-3}K \to I_{m+1},$$

where

$$\tau_E(m) = \sum_{i=3}^{m} \lceil 10 \log_p(i\ell) \rceil + \ell B_3 \chi/36 + 64\ell^3.$$
Proof. We can apply a procedure similar to the one for Lemma 4.14. But the problem here is that when 2 is ramified in \( E \), \( K_{12} \) may be an even unimodular lattice which is not contained in the genus of \( I_{m-1} \). In this case, it is enough to show that we can construct a \( \mathfrak{R} \)-neighbor \( K_{13} \) of \( K_{12} \) such that \( K_{13} \in \text{gen}(I_{m-1}) \). Assume that \( K_{12} \) is even unimodular. Then \( n(K_{12}) = 2\mathcal{O} \) and there is some \( z \in K_{12} \) with \( h(z) = 2\varepsilon, 2 \nmid \varepsilon \). Since \( z \) is an admissible vector with respect to \( \mathfrak{R} \), we can construct a \( \mathfrak{R} \)-neighbor

\[
K_{13} = \mathfrak{R}^{-1}z + \{ w \in K_{12} \mid h(z, w) \in \mathfrak{R} \},
\]

which is an odd unimodular lattice, and thus \( K_{13} \in \text{gen}(I_{m-1}) \). We also have that

\[
\mathfrak{P}^{10\log_p(m\ell)}\mathfrak{R} \to \mathfrak{K} \to 1 \perp K_{13}.
\]

Since 2 is ramified, \( |d_E| = 4\ell \) in this case, and

\[
\tau_E(m) = \sum_{i=3}^{m} \left[10\log_p(i\ell)\right] + \ell B_{3,\chi}/36 + 64\ell^3.
\]

Define

\[
\delta(n) := \begin{cases} 
  n - 3, & \text{if } n \geq 3 \text{ and } 2 \text{ is ramified;} \\
  0, & \text{otherwise.}
\end{cases}
\]

In the following corollary, we describe a sufficient condition under which a positive definite integral Hermitian lattice is represented by some sum of norms.

Corollary 4.16. Let \( L \) be a positive definite integral Hermitian lattice of rank \( n \), such that \( \mathfrak{a}L \subseteq 2\delta(n+1)p^2\tau_E(n+1)\mathcal{O} \). Then \( L \to I_{n+2} \).

Proof. Note that \( \mathfrak{P}^{-\tau_E(n+1)}\mathfrak{R}^{-\delta(n+1)}L \) is positive definite integral. By Proposition 2.19, there exists some \( M \in \text{gen}^0(I_{n+1}) \) such that \( \mathfrak{P}^{-\tau_E(n+1)}\mathfrak{R}^{-\delta(n+1)}L \to M \).

By Lemma 4.14 and Lemma 4.15, \( \mathfrak{P}^{\tau_E(n+1)}\mathfrak{R}^{\delta(n+1)}M \to I_{n+2} \), therefore

\[
L \to \mathfrak{P}^{\tau_E(n+1)}\mathfrak{R}^{\delta(n+1)}M \to I_{n+2}.
\]
Let $L$ be a Hermitian lattice of rank $n$ which is a sublattice of $I_g$ for some positive integer $g$. Since $L = \mathcal{O}v_1 + \cdots + \mathcal{O}v_{n-1} + \mathfrak{A}v_n$ with $\mathfrak{A} = \beta \mathcal{O} + \gamma \mathcal{O} \supseteq \mathcal{O}$, we can write

$$L = \mathcal{O}v_1 + \cdots + \mathcal{O}v_{n-1} + \mathcal{O}\beta v_n + \mathcal{O}\gamma v_n \subseteq I_g,$$

where $v_i = (a_{i1}, \ldots, a_{ig})$ for $1 \leq i \leq n$.

For $1 \leq j \leq g$, let $u_j = (a_{1j}, \ldots, a_{n-1,j}, \beta a_{nj}, \gamma a_{nj})^t$, where $A^t$ is the transpose of a matrix or a vector $A$. Since these $u_j$’s also determine $L$ uniquely, we also denote $L$ by $S_n(u_1, \ldots, u_g)$. Note that for positive integers $s_1, \ldots, s_t$,

$$S_n(u_1, \ldots, u_1, \ldots, u_t, \ldots, u_t)$$

is a sublattice of $I_{s_1+\ldots+s_t}$ and represented by a Hermitian lattice $\langle s_1 \rangle \perp \cdots \perp \langle s_t \rangle$ of rank $t$.

**Definition 4.17.** Let $c \geq 2$ be an integer. Define

$$\lambda_E(n, c) := \min\{g \mid L \to I_g \perp \langle c, \ldots, c \rangle \text{ for all } L \in \mathcal{S}_E(n)\}.$$

Let $M$ and $N$ be Hermitian lattices. For a sublattice $L$ of $M \perp N$, we denote by $L(M)$ and $L(N)$ the orthogonal projections of $L$ in $M$ and $N$, respectively.

**Definition 4.18.** Let $L$ be a Hermitian lattice in $\mathcal{S}_E(n)$. We say that $L$ is $c$-terminal if $\sigma(L)(\langle c, \ldots, c \rangle) = 0$ for any representation $\sigma : L \to I_g \perp \langle c, \ldots, c \rangle$. The set of all $c$-terminal lattices of rank $n$ is denoted by $\mathcal{T}_E(n, c)$, which is a subset of $\mathcal{S}_E(n)$.

**Lemma 4.19.** For all $L \in \mathcal{S}_E(n)$, either $L \to \langle c, \ldots, c \rangle$ or there exists an $L' \in \mathcal{T}_E(m, c)$ where $m \leq n$ and a representation $\phi : L \to I_g \perp \langle c, \ldots, c \rangle$ such that

$$\phi(L)(I_g) = L'.$$

**Proof.** If there is some representation $\varphi : L \to I_g \perp \langle c, \ldots, c \rangle$ such that $\varphi(L) \subseteq \langle c, \ldots, c \rangle$, then it is clear that $L \to \langle c, \ldots, c \rangle$. Otherwise, we may assume that for any $\varphi : L \to I_g \perp \langle c, \ldots, c \rangle$, $\varphi(L)(I_g) \neq 0$. 

4.4. MAIN THEOREM

Let \( \mu_i(L) \) be the \( i \)-th successive minimum of \( L \). We will apply an induction on

\[
m(L) := \prod_{i=1}^{n} \mu_i(L).
\]

When \( m(L) = 1 \), we can find \( O \)-linearly independent vectors \( w_1, \ldots, w_n \in L \) such that \( h(w_i) = \mu_i(L) = 1 \) for \( 1 \leq i \leq n \). Then \( L \supseteq \mathcal{O}w_1 + \cdots + \mathcal{O}w_n \cong I_n \). Since \( \mathcal{O} \supseteq vL \supseteq vI_n = \mathcal{O} \), therefore \( vL = vI_n \), and hence \( L = \mathcal{O}w_1 + \cdots + \mathcal{O}w_n \cong I_n \), and thus \( L \) is itself a \( c \)-terminal lattice.

Suppose that \( \varphi : L \to I_g \perp \langle c, \ldots, c \rangle \) and \( \varphi(L)\langle (c, \ldots, c) \rangle \neq 0 \), then \( m(\varphi(L)(I_g)) < m(L) \). Hence by induction hypothesis, there exists \( \varphi' : \varphi(L)(I_g) \to I_h \perp \langle c, \ldots, c \rangle \), such that \( \varphi'(\varphi(L)(I_g))(I_h) \) is a \( c \)-terminal lattice. Take \( \phi = \varphi' \circ \varphi \), and the lemma follows immediately. \( \square \)

**Lemma 4.20.** Let \( c \geq 2 \) be an integer. For any \( n \geq 1 \),

\[
\lambda_E(n, c) = \min \{ g \mid L \to I_g, \text{ for all } L \in \mathcal{T}_E(n, c) \}.
\]

**Proof.** Let \( \lambda'_E(n, c) = \min \{ g \mid L \to I_g, \text{ for all } L \in \mathcal{T}_E(n, c) \} \). Since \( \mathcal{T}_E(n, c) \) is a subset of \( \mathcal{G}_E(n) \), \( \lambda'_E(n, c) \leq \lambda_E(n, c) \). Conversely, by the above lemma, we have that \( \lambda_E(n, c) \leq \lambda'_E(n, c) \). \( \square \)

The following lemma provide us an upper bound for \( \lambda_E(n, c) \). This bound will be used recursively in Theorem 4.23 to obtain an upper bound for the \( g \)-invariants.

**Lemma 4.21.** Let \( n \geq 1, c \geq 2 \) be integers. Then

\[
\lambda_E(n, c) \leq \frac{3}{2}(c - 1)f^{n+1},
\]

where \( f = (c + 5)/2 \) when \( c \) is odd, and \( f = (c + 4)/2 \) when \( c \) is even.

**Proof.** For \( L \in \mathcal{T}_E(n, c) \), let \( L = S_n(u_1, \ldots, u_g) \) and \( u_j \neq 0 \) for all \( 1 \leq j \leq g \). We may assume that \( g \) is the smallest positive integer for which \( I_g \) represents \( L \). Divide the set \( T = \{ u_1, \ldots, u_g \} \) into \( t \) different equivalence classes \( T_1, \ldots, T_t \): \( u_i, u_j \) are in the same class if and only if \( u_i = u_j \). Note that the cardinality of each subset \( T_k \) is less than \( c \), since \( L \notin \mathcal{T}_E(n, c) \) otherwise. Thus \( g \leq (c - 1)t \).
4.4. MAIN THEOREM

Let $w_i$ be a representative of class $T_i$, and set $\tilde{T} = \{w_1, ..., w_t\}$. Suppose that $t(t-1) \geq 2 \times f^2(n+1)$ where $f = (c+5)/2$ when $c$ is odd, and $f = (c+4)/2$ when $c$ is even. Then, by the Pigeon Hole Principle, either (i) there exist two distinct indices $i, j$ such that $w_i \equiv w_j \pmod{f}$ or (ii) there exist four distinct indices $i, j, k, l$ such that

$$w_i + w_j \equiv w_k + w_l \pmod{f}.$$ 

For case (i), note that

$$S_n(w_i, w_j) \cong S_n\left(\frac{w_i - w_j}{f}, ..., \frac{w_i - w_j}{f}, \frac{w_i + (f-1)w_j}{f}, \frac{-(f-1)w_i - w_j}{f}\right).$$

This contradicts the fact that $L \in \Sigma_E(n, c)$.

Let us consider case (ii). If $w_i + w_j = w_k + w_l$, then $S_n(w_i, w_j, w_k, w_l) \rightarrow I_3$ and $L \rightarrow I_{g-1}$ which is impossible. So, $w_i + w_j \neq w_k + w_l$. One easily show that

$$S_n(w_i, w_j, w_k, w_l) \cong S_n\left(\frac{w_i + w_j - w_k - w_l}{f}\right).$$

This again contradicts to the fact that $L \in \Sigma_E(n, c)$. \hfill \Box

Remark 4.22. Let $L$ be a Hermitian lattice of rank $n$. Suppose that $L \rightarrow \langle a, ..., a \rangle$, where $a$ is a positive integer. Then $L \rightarrow \langle a \rangle \perp \langle ac, ..., ac \rangle$, where $g \leq \lambda_E(n, c)$, and the notation $\langle a \rangle_g$ denotes the orthogonal sum of $g$ copies of $\langle a \rangle$.

Theorem 4.23. When $n \geq 1$, we have

$$g_E(n) \leq \delta(n+1)\lambda_E(n, 2) + 3\tau_E(n+1)\lambda_E(n, p) + n + 6.$$ 

Proof. Assume that $L \rightarrow I_g$ with $g > \lambda_E(n, 2)$. Then by Definition 4.17, there exist $\lambda_0$ and $g_1$ such that

$$L \rightarrow I_{\lambda_0} \perp \langle 2 \rangle_{g_1},$$

where $\lambda_0 \leq \lambda_E(n, 2)$. If $g_1 > \lambda_E(n, 2)$, then by the above remark, there exist $\lambda_1, g_2$ such that

$$L \rightarrow I_{\lambda_0} \perp \langle 2 \rangle_{\lambda_1} \perp \langle 4 \rangle_{g_2},$$
where \( \lambda_1 \leq \lambda_E(n, 2) \). Repeating this process, if applicable, we obtain a representation

\[
\sigma : L \rightarrow I_{\lambda_0} \perp (2)_{\lambda_1} \perp \cdots \perp (2^{s-1})_{\lambda_{s-1}} \perp (2^s)_{g_s},
\]

where \( s = \delta(n+1) \) and \( \lambda_j \leq \lambda_E(n, 2) \) for all \( 0 \leq j \leq s - 1 \).

Applying the same process to the orthogonal projection of \( \sigma(L) \) in the last component with respect to \( p \), the smallest inert prime in \( E \), we obtain a representation

\[
\sigma(L)((2^s)_{g_s}) \rightarrow (2^s)_{\lambda_s} \perp \cdots \perp (2^s p^{t-1})_{\lambda_{s+t-1}} \perp (2^s p^t)_{g_{s+t}},
\]

where \( t = 2\tau_E(n+1) \) and \( \lambda_j \leq \lambda_E(n, p) \) for all \( s \leq j \leq s + t - 1 \).

Therefore, we obtain a representation

\[
\tau : L \rightarrow I_{\lambda_0} \perp \cdots \perp (2^{s-1})_{\lambda_{s-1}} \perp (2^s)_{\lambda_s} \perp \cdots \perp (2^s p^{t-1})_{\lambda_{s+t-1}} \perp (2^s p^t)_{g_{s+t}}.
\]

Note that \( (2)_k \rightarrow I_{k+1} \) and \( (c)_k \rightarrow I_{2(k+1)} \) for any positive integer \( c \). Therefore,

\[
I_{\lambda_0} \perp \cdots \perp (2^{s-1})_{\lambda_{s-1}} \rightarrow I_{\delta(n+1)\lambda_E(n,2)+1},
\]

\[
(2^s)_{\lambda_s} \perp \cdots \perp (2^s p^{t-1})_{\lambda_{s+t-1}} \rightarrow I_{3\tau_E(n+1)\lambda_E(n,p)+3},
\]

and

\[
\tau(L)((2^s p^t)_{g_{s+t}}) \rightarrow I_{n+2}.
\]

Combining these results together, we have

\[
g_E(n) \leq \delta(n+1)\lambda_E(n, 2) + 3\tau_E(n+1)\lambda_E(n, p) + n + 6.
\]

\[\square\]

**Theorem 4.24.** When \( n \geq 1 \), we have that

\[
g_E(n) \leq \frac{3^{n+2}}{2} \delta(n+1) + \frac{9(p-1)(p+5)n+1}{2^{n+2}} \left[ \sum_{i=3}^{n+1} [10 \log_p(i\ell)] + G(\ell) \right] + n + 6,
\]

where

\[
G(\ell) = \begin{cases} \\
\ell B_{3,\chi}/36 + 64\ell^3, & \text{if } 2 \text{ is ramified}; \\
\ell B_{3,\chi}/144 + \ell^3, & \text{otherwise}.
\end{cases}
\]

**Proof.** This theorem follows immediately by plugging in the upper bounds for \( \lambda_E(n, 2) \) and \( \lambda_E(n, p) \), as well as the value of \( \tau_E(n+1) \). \[\square\]
REM 4.25. Suppose that 2 is inert. Since \((2)_k \to I_{k+1}\), the bound in Theorem 4.24 can be improved to

\[
g_E(n) \leq 3^{n+2} \left[ \sum_{i=3}^{n+1} \left\lceil 10 \log_2(i!) \right\rceil + G(\ell) \right] + n + 3.
\]

REM 4.26. It is well known that \(B_{3,\chi} = O(\ell^3)\) and \(p \ll \ell^{1/2}\), i.e., \(p \leq C\ell^{1/2}\) for some constant \(C\). Therefore

\[
g_E(n) = O(C^n + 2\ell^{n/2} + 5n \log(n\ell)).
\]
Bibliography